SEGURANÇA DA INFORMAÇÃO

Prof. Luis Gonzaga de Paulo

TEMA 1 – CARACTERÍSTICAS DA SEGURANÇA DA INFORMAÇÃO

O que é segurança da informação? O conceito de segurança em si já comporta vários significados. No idioma inglês, por exemplo, isso é diferenciado: o termo *security* refere-se à proteção contra ameaças intencionais, enquanto que seu sinônimo *reliability* indica a confiabilidade, a tolerância às falhas. Já o termo *safety* designa a proteção ao ambiente e aos seres vivos, incluindo-se aí a proteção à saúde e à vida. A segurança da informação é a parte da ciência da informação que tem por objetivo proteger os dados, as informações e o conhecimentos de modo a preservar o valor destes para os processos, produtos e serviços das pessoas e organizações.

A norma ABNT NBR ISO/IEC 27002:2013 define informação como sendo um ativo – isto é, bem, patrimônio – da organização, de grande importância e valor, e que por isso necessita de proteção adequada. Para isto deve-se considerar a informação em suas diversas formas e nos diversos meios utilizados para obter, armazenar, transportar e modificar a informação:

> O valor da informação vai além das palavras escritas, números e imagens: conhecimentos, conceito, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações que, como os outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos. (ABNT, 2013b)

Fontes (2011) caracteriza a informação como um bem, um ativo de suma importância para os negócios, a saber:

> A informação, independentemente de seu formato, é um ativo importante da organização. Por isso os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos. A informação tem valor para organização. Sem informação a organização não realiza seu negócio. (Fontes, 2011)

A informação é um item de valor, reconhecido na atualidade como um ativo para as organizações. Em função disso, as informações podem ser classificadas e, de acordo com a sua criticidade, devem ser protegidas contra incidentes que resultem na sua destruição ou indisponibilidade – temporária ou permanente –, na alteração indevida ou desfiguração, ou mesmo na divulgação não autorizada. A norma ABNT NBR 16167 trata dessa questão ao apresentar as “diretrizes básicas para a classificação, rotulação e tratamento da informação de acordo com sua sensibilidade e criticidade para a Organização, visando os níveis adequados de

proteção” (ABNT, 2013a), ou seja, ela provê uma base para o planejamento e a tomada de decisão quanto aos procedimentos de Segurança da Informação.

Em nossos dias há uma ênfase na segurança da informação que geralmente está vinculada a informações pertencentes ao domínio da TIC (a informação *eletrônica* ou *digital*), o principal meio de informação da nossa era e o mais vulnerável, e que, portanto, precisa ser protegido das inúmeras ameaças às quais está exposta. Porém a segurança da informação pode ser afetada por diversos outros fatores, como os ambientais e comportamentais, incluindo-se neste último as ações dos usuários de sistemas – deliberadas ou não – e de criminosos.

Embora grande parte da informação de valor esteja sob o domínio da tecnologia, há um valioso conjunto que extrapola esse domínio, o qual também deve ser abrangido pelas medidas de segurança: informações registradas em papel à mão e impressos em geral (escritos ou imagens) compõem esse universo de ativos valoráveis. Dessa forma, a segurança da informação deve-se aplicar a todos os aspectos da proteção de informações e dados, com o intuito de tratar as três características básicas da informação no que se refere à segurança, a saber: a *confidencialidade*, a *integridade* e a *disponibilidade*.

Figura 1 – As características principais da segurança da informação

Alguns autores acrescentam a esses três objetivos o princípio da legalidade, ou seja, a garantia de que a informação foi produzida em conformidade com a lei ou ainda o uso legítimo, isto é, a garantia de que os recursos de informação são usados para propósitos benéficos (Beal, 2008). Entretanto podemos situar melhor a legalidade e legitimidade no domínio dos objetivos organizacionais, como decorrência das propriedades da segurança da informação, como o próprio autor acentua (Beal, 2008):

> Por exemplo, o objetivo de legalidade decorre da necessidade de a organização zelar para que as informações por ela ofertadas – em especial aquelas entregues a terceiros por determinação legal – sejam fidedignas e produzidas de acordo com as normas vigentes. Esse objetivo gera, no campo da Segurança da Informação, exigências no tocante à confidencialidade, integridade e disponibilidade de dados e informações (tais como requisitos de proteção do sigilo de informações pessoais, da consistência dos demonstrativos financeiros divulgados, da disponibilidade de serviços de informação e comunicação contratados por clientes).

Em seu trabalho, Avizienis et al. (2004) abordam a segurança da informação sob a ótica da **dependabilidade**, isto é, a capacidade de um *software* em fornecer um serviço que pode justificadamente ser confiável, ou a habilidade de evitar, de forma aceitável pelo usuário, falhas no provimento dos serviços, seja em frequência ou em severidade. Para esses autores, a segurança é entendida como um conjunto das seguintes características:

- **Confidencialidade**, ou ausência de divulgação não autorizada da informação;
- **Integridade**, ou ausência de alterações indevidas;
- **Disponibilidade** dos serviços corretos para os usuários autorizados;
- **Confiabilidade**, isto é, a continuidade na execução correta dos serviços;
- **Segurança** do usuário, ou seja, a ausência de consequências catastróficas para o usuário e para o ambiente;
- **Manutenibilidade**, quer seja, a capacidade de submeter-se a modificações e reparos;

Nesse mesmo estudo (Avizienis et al, 2004) ressalta-se que a segurança da informação tem por objetivo garantir essas características, evitando os incidentes de segurança, ou seja, eventos que atentem contra qualquer uma delas, inviabilizando o uso adequado da informação. Estes **incidentes** – ou **ataques** – são eventos provocados por incompetência, descuido, mau uso ou uso de má-fé que, explorando a existência de falhas, situações não previstas ou

fraquezas do projeto ou em decorrência delas (as vulnerabilidades) provocam o uso impróprio do sistema ou das informações tratadas por ele. O autor observa que, para reduzir ou mitigar essa possibilidade, são adotadas as defesas ou contramedidas de segurança, que são procedimentos, técnicas e ferramentas cujo objetivo é reduzir o risco dos incidentes, seja pela diminuição da probabilidade de um ataque por meio da eliminação das vulnerabilidades, seja pela adoção de defesas ou contramedidas que possam reduzir a perda em potencial representada por um possível ataque, já que o risco é o produto da probabilidade do ataque pela perda em potencial que este pode causar.

De acordo com Ribeiro (2002), a segurança da informação é algo tão esperado pelos usuários quanto o desempenho ou o uso otimizado dos recursos computacionais, mesmo que não faça parte das especificações iniciais do sistema. O usuário de qualquer sistema espera que esse seja intrinsecamente seguro a despeito de ter solicitado ou não com essa característica. Caso não receba o que espera, certamente não ficará satisfeito. Para esse autor (Ribeiro, 2002), a segurança da informação contempla também:

- A necessidade de **autenticação**, que garante ao usuário ou ao sistema que seu interlocutor é realmente quem diz ser;
- O **não repúdio**, que é a capacidade de comprovar quem executou determinada ação;
- A **legalidade**, que trata da conformidade do uso da informação com os dispositivos normativos, regulatórios e legais;
- A **privacidade**, que tem o propósito de restringir, além do acesso indevido, a vinculação de um usuário a uma atividade executada;
- A **auditabilidade**, cujo objetivo é o rastreamento e a reconstituição de toda a movimentação e das alterações da informação em função do tempo.

Para garantir o objetivo organizacional do uso legítimo da informação, os requisitos de **confidencialidade**, **integridade** e **disponibilidade** podem ser atribuídos de forma diferentes aos diversos tipos de informação, em função do papel que estas desempenham nos processos organizacionais.

TEMA 2 – SEGURANÇA NO CICLO DA VIDA DE INFORMAÇÃO

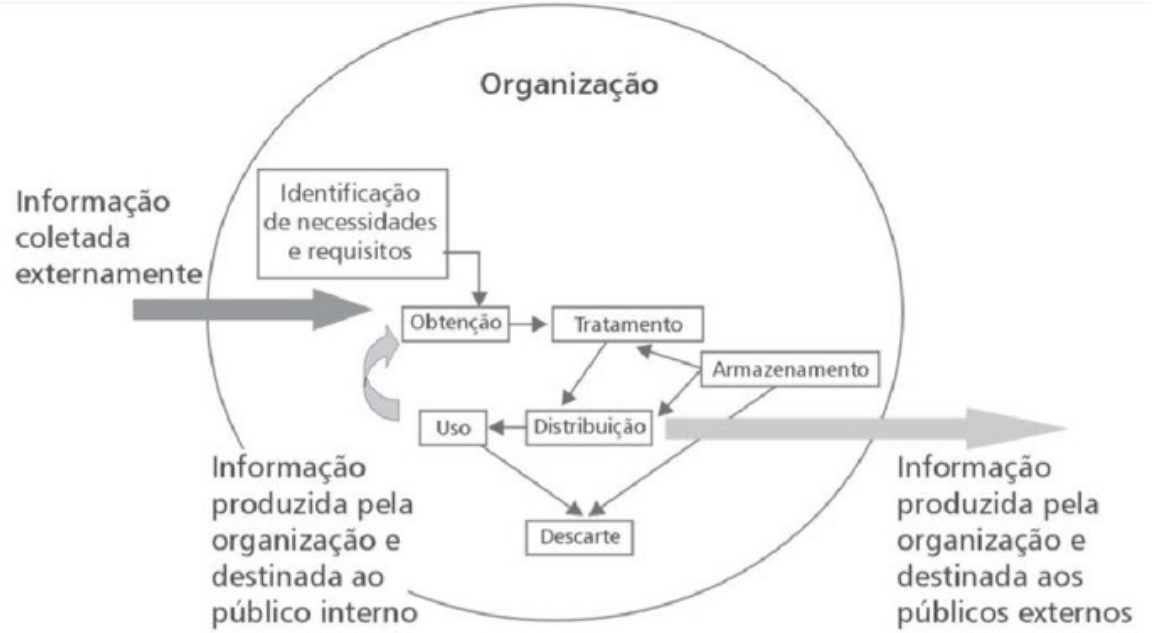
Os objetivos da segurança da informação se aplicam a praticamente todos os tipos de informação e seus processos, porém esses objetivos diferenciam-se

em importância e forma nas diversas etapas do ciclo de vida da informação. Para Beal (2008), essa variação ocorre em função do tipo de informação e ao longo do tempo:

> Uma declaração formal da direção da organização destinada à imprensa em geral deverá desencadear ações de proteção de sua integridade (em especial, a autenticidade, para evitar, por exemplo, que alguém, fazendo-se passar por diretor, encaminhe ao setor de divulgação um comunicado prejudicial à organização e este venha a ser divulgado sem a devida conferência da fonte) e da integridade do conteúdo (para impedir que um comunicado legitimo seja indevidamente alterado antes de sua liberação para terceiros). Nesse caso, a preocupação com a confidencialidade poderá existir de forma temporária até a distribuição do comunicado, assim como provavelmente a questão da disponibilidade também será rapidamente superada, a menos que se identifique uma necessidade de consulta interna à informação após esta ter sido publicada. Do ponto de vista da segurança, a principal preocupação será a preservação da integridade da mensagem. Tratando-se de um documento destinado ao público em geral, a questão da autenticidade do receptor seria desprezível, e as preocupações com a autenticidade do emissor e com a irretratabilidade da comunicação fariam mais sentido do lado do receptor da mensagem, interessado em garantir que a organização não tenha depois como recusar seu papel de emissor do comunicado.

A informação submete-se, então, a um ciclo, isto é, a um processo que se origina na sua produção ou obtenção e encerra-se no descarte, como mostrado na Figura 2 a seguir. A atividade de identificação de necessidades e requisitos inicia o processo, na etapa que trata da obtenção da informação, passando pelo tratamento, depois pela distribuição e/ou armazenamento, para então ser utilizada - a etapa de maior importância nos processos decisórios e operacionais da organização. A distribuição ou comunicação pode levar as informações produzidas pela organização ao público externo.

Figura 2 – Ciclo de vida da informação nas organizações



Fonte: Beal, 2008.

As informações estratégicas da organização (sobre estratégia de negócios, por exemplo) estão sujeitas a um controle mais rígido da confidencialidade. Esse controle é intenso na fase de elaboração das estratégias, porém demanda menos controle a partir do momento em que essa informação passa a ser de conhecimento público – do ambiente externo e da concorrência.

2.1 Etapas do ciclo de vida da informação

Durante a sua existência e seu período útil (o seu ciclo de vida), a informação é submetida a diversos processos, seja dentro da organização ou em qualquer ambiente onde se faz presente ou necessária. Esses processos estão divididos e identificados pelas etapas do ciclo de vida da informação, as quais analisaremos na sequência.

2.1.1 Identificação das necessidades e dos requisitos

Como mostrado na Figura 2, nessa etapa inicia-se o fluxo de informação. Nela são realizadas as atividades que analisam os processos e atividades e consultam todos os interessados para obter um cenário amplo e detalhado das informações disponíveis e das que são necessárias: formato, fonte, quantidade, periodicidade, área do conhecimento e etc. O objetivo é identificar as informações

e os critérios para a obtenção dessas informações, bem como as necessidades de informação para a organização e para as pessoas envolvidas – os requisitos, como são denominados na especificação de sistemas e de processos.

2.1.2 Obtenção

Uma vez estabelecidos os requisitos e identificadas as necessidades de informação para os processos organizacionais, é necessário estabelecer a sua forma de obtenção ou de produção. Além dos métodos, técnicas e ferramentas apropriadas, é necessário abordar os aspectos externos ao ambiente da organização: a sociedade, o governo, o meio ambiente, a cadeia de relacionamentos dos negócios etc. Critérios de legalidade e legitimidade associados às práticas de *compliance* e governança são imprescindíveis nessa fase.

2.1.3 Tratamento

Para a maioria dos processos de negócios e atividades humanas é necessária uma adequação da informação, seja a organização, adaptação de forma e estrutura, tradução, classificação, análise, síntese, apresentação e reprodução. Desse modo, a informação torna-se mais acessível, organizada e, principalmente, mais fácil de armazenar, transportar, localizar e recuperar. No decorrer dessas adequações, deve haver um cuidado especial com a integridade, já que diversas modificações e transformações podem comprometer a fidedignidade da informação. Também é necessário que o método de transformação – o algoritmo – seja claro, preciso e reproduzível.

2.1.4 Distribuição

Trata-se de levar as informações a quem – pessoa ou processo – necessita delas. Nesse processo, destaca-se a necessidade de meios para a comunicação efetiva, que possibilitem a distribuição rápida e confiável. Esses meios são responsáveis por manter a qualidade da comunicação, o que é indispensável para a acuracidade dos processos e a tomada de decisões cujo resultado será proveitoso. É importante ressaltar que meios de comunicação distintos podem requerer distintas transformações da informação para possibilitar seu transporte.

2.1.5 Uso

A etapa mais importante do ciclo de vida da informação é o seu uso. Nesse momento, a informação comprova sua eficácia, produzindo os resultados esperados e possibilitando o andamento dos processos. Para seu uso, a informação deve ser íntegra e estar disponível, portanto essas são as características da segurança da informação mais proeminentes dessa etapa.

2.1.6 Armazenamento

Refere-se à preservação e à conservação da informação pelo tempo que for necessário, e ainda a classificação, a organização e a rotulação para que possa ser recuperada e manuseada com facilidade e adequadamente. Os critérios de integridade e disponibilidade também são os mais importantes nessa etapa e representam desafios exponenciais à medida que o volume de informações cresce e a variedade dos meios de armazenamento aumenta. O fator tempo é um elemento de alto risco nessa etapa, pois é notório que o volume de informações cresce com o tempo, bem como o tempo e as evoluções tecnológicas podem comprometer a integridade e a disponibilidade das informações.

2.1.7 Descarte

Ao término do ciclo de vida da informação, quando esta perde totalmente seu valor por tornar-se ultrapassada ou por já ter cumprido seu papel nos processos dos quais tomou parte, a informação deve ser descartada. Esse descarte é imprescindível para preservar a velocidade e a efetividade dos processos de armazenagem, transporte e uso, bem como reduzir o custo dessas etapas, porém é imprescindível que seja feito com estrita observância à legislação, às normas, às regras, às políticas operacionais e às demais exigências, incluindo-se aí os aspectos de preservação de patrimônio histórico e cultural. Nessa etapa é necessária especial atenção às características de confidencialidade e disponibilidade.

TEMA 3 – SEGURANÇA DA INFORMAÇÃO SUPORTADA POR TIC

Na atualidade, a imensa maioria das informações significativas para as pessoas e para as organizações estão sob o domínio da tecnologia da informação

e da comunicação – as TICs. Como já vimos, as organizações e as pessoas dependem (e muito) da informação para realizarem seus negócios e alcançarem seus objetivos. Vivemos na sociedade da informação, do conhecimento e, como expressa Kolbe Jr. (2017),

> Como o próprio nome indica, o *saber* é o valor central dessa sociedade. Nela as indústrias de *software*, a robótica, a computação, entre outras áreas do conhecimento humano, toma as tecnologias da informação e da comunicação (TICs) como linguagem dominante.

Dessa constatação depreende-se uma segunda: as organizações e as pessoas dependem da acuracidade das informações fornecidas pelos sistemas ou pelas tecnologias para a consecução de seus objetivos e a realização de suas atividades. Face a essa dependência, também depositam sua confiança na tecnologia e nos sistemas que lhes fornecem as informações: se essa confiança for quebrada, podemos considerar que se tornam inviáveis e inúteis tanto os sistemas quanto a tecnologia que os suporta.

Disso decorre a própria definição de tecnologia da informação: "é o conjunto de atividades e soluções envolvendo *hardware*, *software*, banco de dados e redes que atuam para facilitar o acesso, análise e gerenciamento de informações. Simplificando, a TI foi criada para auxiliar o ser humano a lidar com informações" (Silva, 2015).

A informação suportada pela TIC é majoritariamente digital e trafega nos meios e na infraestrutura de comunicação, sendo armazenada e processada por computadores e dispositivos eletrônicos – geralmente manipulada pelo conjunto *software* + *hardware*. Nesse ambiente, a preocupação com a segurança da informação é crescente – do mesmo modo que essa modalidade da informação cresce de forma exponencial. Essa preocupação decorre, entre muitos outros, dos seguintes fatores:

I. **Dependência da tecnologia da informação e das comunicações –** Serviços de qualidade, adequados e prestados no tempo certo são a chave para a sobrevivência da maioria das organizações. Os computadores e os sistemas de comunicação possibilitam que as organizações sejam capazes de fornecer serviços, processar faturas, contatar fornecedores e clientes ou efetuar pagamentos de forma efetiva e ágil. Porém esses recursos também respondem por informações e dados sigilosos, os quais, tornados públicos, podem resultar em prejuízos ou mesmo no fracasso da

organização.

II. **Vulnerabilidade da infraestrutura tecnológica** – *Hardware* e *software* exigem um ambiente controlado, pois podem ser danificados por desastres naturais (fogo, inundação ou terremotos), falhas nos controles (temperatura, umidade, energia elétrica) ou componentes, acidentes ou sabotagens. Os equipamentos de TIC portáteis são também passíveis de extravio, perda, furto ou roubo, pois apresentam facilidade de transporte e podem ser facilmente vendidos.

III. **Alto volume e grande valor da informação armazenada** – As informações suportadas pela TIC compõem-se geralmente de vastas quantidades de dados corporativos e de expressivo valor, o que as torna um alvo muito atraente para criminosos (*hackers*, espiões, crime organizado) e até mesmo de colaboradores dispostos a abusar de seus privilégios em troca de dinheiro ou vantagens indevidas, às vezes oferecidas por concorrentes ou até mesmo parceiros de negócio.

IV. **Pouca atenção dada à segurança da informação nos estágios iniciais do desenvolvimento de *software* –** A maioria dos *softwares*, sejam eles desenvolvidos internamente ou adquiridos de terceiros, não são projetados com base na segurança da informação. É comum que características de segurança (por exemplo, relacionadas à definição de níveis de permissão de acesso a funcionalidades, segregação de atividades no sistema etc.) sejam adicionadas nas etapas finais de desenvolvimento, quando sua eficácia já pode ter sido prejudicada por decisões de projeto tomadas sem levar em conta os requisitos de segurança.

V. **Rápido avanço da tecnologia e obsolescência tecnológica** – Por tratar-se de ramos do conhecimento bastante recente, as TIC sofrem um vertiginoso processo evolutivo, que é recorrente e recursivo: cada novo avanço tecnológico gera novas oportunidades de negócio, que geram novas demandas, as quais geram novos avanços. *Smartphones* e *tablets*, internet das coisas (IoT – *Internet of Things*), realidade virtual (VR – *Virtual Reality*), realidade aumentada (AR - *Augmented Reality*), realidade mista, *Cloud Computing*, *Big Data*, automação (robótica, domótica), VANT (veículos aéreos não tripulados ou *drones*), redes virtuais e Impressão em 3D são exemplos reais desses avanços. Ao mesmo tempo, o avanço

tecnológico causa a superação de tecnologias – às vezes até mesmo das mais recentes – os *smartphones* e *tablets*, por exemplo, superaram rapidamente os PDAs (*Personal Digital Assistants*), *handhelds* e *palmtops*. Porém as tecnologias superadas continuam em uso, pois muitas vezes o custo de substituição é elevado, seja em função do volume ou em função da especialização. Em se tratando de *software*, a questão é ainda mais abrangente e complexa. Estima-se que, no Brasil, quase metade das empresas não atualiza seus *softwares* com a frequência necessária. E cabe notar que parte desses *softwares* são justamente destinados à proteção da informação, como antivirus e *firewalls*, por exemplo!

Frente a esses desafios e vários outros, a segurança da informação suportada pela TIC é fundamental, e ao mesmo tempo complexa. Muitas vezes devido a essa complexidade, as organizações relegam esse aspecto da segurança da informação a um plano inferior, ou buscam tratá-la do ponto de vista tecnológico apenas: o uso de antivírus e *firewalls* é uma prática constante, entendida como satisfatória e suficiente para prover a segurança da informação no ambiente tecnológico. A excessiva confiança na tecnologia acaba por expor fragilidades, e é notório que qualquer iniciativa de sucesso na segurança da informação deve ser suportada – e apoiar – a conhecida tríade dos negócios: *pessoas, processos* e *tecnologia*, como mostrado na Figura 3.

Figura 3 – A tríade pessoas-processos-tecnologia e a segurança da informação

Fonte: Africa Studio/Shutterstock.

TEMA 4 – SEGURANÇA DA INFORMAÇÃO NÃO SUPORTADA POR TIC

Embora a ênfase dos cuidados com a segurança da informação nos dias atuais seja voltada para aquelas sob o domínio da tecnologia, as ameaças à segurança da informação estão presentes em outros domínios. Aspectos de infraestrutura física como controle de acesso (Figura 4) e monitoramento, fornecimento de energia, prevenção contra incêndios e alagamentos, descargas elétricas, terremotos, acidentes de trânsito, invasões, depredações, atentados terroristas, sabotagens e muitas outras devem fazer parte do planejamento para a garantia (também) da segurança. É por isso que Beal (2008) acentua que "existem muitas razões para se proteger também a informação não armazenada em computadores", entre as quais:

- A organização geralmente necessita e dispõe de dados, informações e conhecimentos valiosos que não fazem uso da TIC devido à sua idade ou volume, falta de interesse do detentor da informação em registrá-la, ou por estar temporariamente disponível, ou registrada apenas em documentos impressos, manuscritos, microfilmes, fitas de áudio ou vídeo ou outro tipo de mídia obsoleta.
- Alguns documentos têm sua validade vinculada ao seu suporte físico em papel, precisando serem protegidos fisicamente mesmo quando existem cópias eletrônicas deles. Um exemplo disso são os documentos históricos.
- Mesmo as informações armazenadas em computadores podem ser impressas e ter sua confidencialidade comprometida pela falta de manuseio adequado dessas versões em papel.

Figura 4 – O controle de acesso físico: um dos principais controles de segurança

Fonte: Hotsum/Shutterstock.

Em decorrência disso, os processos de segurança da informação devem abranger tanto as informações suportadas pela TIC quanto as que são armazenadas em meios não digitais ou eletrônicos, visando garantir uma proteção holística adequada a todos os dados e informações de valor para o negócio da organização. “Ter uma noção clara de quais informações valiosas permanecem fora do domínio das TICs permite aos responsáveis pela preservação desses ativos planejar e implementar as medidas necessárias para sua proteção” (Beal, 2008).

4.1 Proteção dos ativos informacionais

Além da proteção da informação em si, é necessário também manter os ativos que suportam a informação protegidos contra roubo, furto, alteração, perda, defeitos, depredação e outros problemas que afetam a segurança da informação. Portanto o planejamento da segurança da informação das organizações deve contemplar medidas de proteção compostas de uma vasta diversidade de iniciativas, desde os cuidados com os processos e meios de comunicação até a segurança de pessoas e instalações, passando pelos ativos da TIC e meios de registro e armazenamento em geral.

Os mecanismos de monitoramento, controle e defesa precisam ser definidos com base no tipo de informação a ser protegida, seu valor e os riscos aos quais pode estar submetida. Outro critério de suma importância para essa definição é a vulnerabilidade, isto é, o grau de exposição da informação aos riscos. Também é essencial que o planejamento da segurança da informação na organização considere uma visão sistêmica das suas necessidades de segurança, dos ativos que necessitam de proteção e das ameaças às quais a informação e os ativos a ela estão relacionados. Essa visão sistêmica e a avaliação dos riscos busca estabelecer um conjunto de práticas que seja economicamente viável e operacionalmente prático, cuja implementação resulte em um modo efetivo de reduzir ou eliminar os principais riscos.

4.2 A gestão de riscos na segurança da informação

A gestão de riscos é a área do conhecimento humano apropriada para promover a adequada proteção, não somente à informação, mas também a todo o negócio da organização. A gestão de riscos em si é um processo organizacional

de suma importância e, no que tange à segurança da informação, é indispensável. Há uma frase de uso corrente por parte dos profissionais da área que diz: “Não se pode proteger o que não se controla, e não se pode controlar o que não se conhece”.

Figura 5 – O processo de gestão de riscos

Fonte: Trueffelpix/Shutterstock.

A gestão de riscos promove a identificação das informações críticas, dos ativos de TIC vinculados a estas, e das vulnerabilidades e riscos aos quais estão submetidos ambos. Na próxima aula apresentaremos os conceitos de análise de riscos em segurança da informação e os benefícios de se ter uma gestão de riscos adequada.

TEMA 5 – SEGURANÇA DA TIC NA OPERAÇÃO DOS NEGÓCIOS

Na atualidade entendemos a segurança da informação como sendo a segurança da TIC. Isso ocorre devido ao intenso uso da tecnologia e da vasta gama de informações que utilizamos no cotidiano e que são providas por meio do uso dessas mesmas tecnologias, porém já vimos que não são somente essas informações tecnológicas que são utilizadas pelas pessoas que compõem o mundo dos negócios, e que é necessário expandir o tratamento de segurança a todos os aspectos que envolvem as informações.

Entretanto, ao tratarmos do assunto *segurança da informação* no âmbito da tecnologia, vamos diretamente para aquilo que envolve *hardware* e *software*: inevitavelmente vinculamos a segurança a mecanismos de tecnologia e aos termos afeitos a ela, por exemplo, *backups, firewalls*, criptografia, antivírus,

antispam, *antispyware*, *antiphishing* e assim por diante. Evidentemente esses termos não estão no senso comum por acaso: representam, sim, uma boa parcela do arsenal de proteção da informação digital e eletrônica. O *firewall*, por exemplo (Figura 4) é um importante elemento que se interpõe à comunicação da rede interna da organização com a Internet, provendo a proteção da primeira: "Os *firewalls* e os sistemas de detecção de invasão são colocados na rede para monitorar e controlar o tráfego de informação de uma rede a outra" (Turban, Volonino, 2013).

Figura 6 – O *firewall* protege a rede interna da organização

Fonte: Borodatch/Shutterstock.

Reforçando o que já dissemos anteriormente, essa segurança tecnológica é imprescindível, porém não deve ser adotada de forma isolada, pois isso certamente não será suficiente. Segundo a análise de Turban e Volonino (2013), proteger dados e operações de negócio envolve as seguintes questões:

a. Tornar dados e documentos disponíveis e acessíveis 24 horas por dia, 7 dias da semana e, ao mesmo tempo, controlar e restringir o acesso a esses.
b. Implementar e fiscalizar procedimentos e políticas de uso aceitável para os dados, *hardware*, *software* e redes pertencentes à empresa.
c. Promover a segurança e o compartilhamento legal de informações entre pessoal autorizado e parceiros.
d. Garantir o cumprimento de leis e regulamentações governamentais.
e. Prevenir ataques, mantendo as defesas contra a invasão da rede em funcionamento.
f. Detectar, diagnosticar e reagir a incidentes e ataques em tempo real.
g. Manter controles internos para prevenir a manipulação de dados e registros.

h. Recuperar-se rapidamente de desastres de negócios e de interrupções.

Então “as políticas, os procedimentos, o treinamento e os planos de recuperação de desastres empresariais, juntamente com a tecnologia, desempenham um papel fundamental na segurança em TI” (Turban; Volonino, 2013). Ou seja, a segurança das tecnologias da informação e das comunicações implica processos de prevenção e de proteção das informações que vão além dos equipamentos, das redes de comunicação e das operações de comércio eletrônico tradicionais para garantir sua confidencialidade, integridade, disponibilidade e seu uso autorizado. De acordo com Turban e Volonino (2013), até por volta de 2002, a segurança da informação “era considerada apenas uma questão técnica atribuída às áreas ligadas diretamente à TI. Incidentes eram resolvidos caso a caso, por meio de reparos; não havia uma abordagem de prevenção para se proteger das ameaças”. Isso era muito ligado ao custo dessa atividade, pois a segurança da informação era classificada como um custo e não como um investimento que traz retornos, com benefício para as atividades administrativas.

Essa visão depreciativa mostrou-se perigosa e inadequada para fornecer a segurança adequada aos níveis necessários às organizações. A partir daí, com a intensificação do uso comercial da internet e a expansão dos negócios entre organizações, pessoas e nações por intermédio da TIC, houve um vertiginoso crescimento do comércio eletrônico e foi necessário repensar o modelo de segurança então vigente. Novas legislações regulamentações e normas foram estabelecidas, e a segurança da TIC passou a ser tratada como um componente dos negócios, vista de modo indissociável dos objetivos da organização. É nesse período também que observamos o surgimento do termo *malware*, que é uma contração, na língua inglesa, de *malicious software* (*software* malicioso). É uma referência genérica aos vírus, *worms*, cavalos de Troia, *spyware* e todos os outros tipos de código e de programas que interrompem o sistema, são destrutivos e indesejados. Representam ameaças que vão desde emprego de componentes de alta tecnologia para obter acesso à rede de uma empresa e ao seu banco de dados até estratégias para capturar informações pessoais como senhas de cartão de crédito ou de contas bancárias. Mas as ameaças vão além das ações meramente tecnológicas e incluem ações mais corriqueiras do crime, como roubar equipamentos portáteis e qualquer outro recurso acessível que permita a obtenção de informações de valor.

Em geral, medidas de segurança em TI têm focado em proteger a empresa de *malwares* e de agentes que estão fora da organização. Os maiores riscos em segurança da informação, na maioria das vezes, envolvem ações internas (intencionais ou não) ou algum erro do processo de gestão, já que cuidados bastante simples, como controlar o acesso físico aos bancos de dados e redes, ainda não é algo trivial para algumas organizações. As empresas sofrem perdas tremendas com fraudes cometidas por seus funcionários. É um problema geral que afeta todas as empresas, independentemente de seu tamanho, localização ou setor" (Turban; Volonino, 2013).

A segurança em TI está tão integrada aos objetivos de negócio que não pode ser tratada como uma função isolada. As falhas causam impacto direto no desempenho dos negócios, nos clientes, nos parceiros e nos demais envolvidos e podem levar a multas, ações legais e quedas acentuadas de valor de mercado, conforme os investidores reagem às crises.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR 16167** – Diretrizes para a classificação, rotulação e tratamento da informação. Coletânea de normas técnicas de segurança da informação. Rio de Janeiro: ABNT, 2013a.

_____. **ABNT NBR ISO/IEC 27002:2013** – Tecnologia da informação – Técnicas de segurança – Código de práticas para controles de segurança da informação. Coletânea de normas técnicas de segurança da informação. Rio de Janeiro: ABNT, 2013b.

AVIZIENIS, A. et al. Basic concepts and taxonomy of dependable and secure computing. **IEEE Transactions on Dependable and Secure Computing** v..1 n. 1, 2004.

BEAL, A. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2008.

FONTES, E. **Segurança da informação**. 1. ed. São Paulo: Saraiva, 2001.

KIM, D. **Fundamentos de segurança de sistemas de informação**. 1. ed. Rio de Janeiro: LTC, 2014.

KOLBE Jr. A. **Sistemas de segurança da informação na era do conhecimento**. Curitiba: InterSaberes, 2017.

RIBEIRO, R. A**. Segurança no desenvolvimento de *software***. Rio de Janeiro: Campus, 2002.

SILVA, A. O que é TI (Tecnologia da Informação)? **Adam Silva**, Santo André, 19 mar. 2015. Disponível em http://www.adamsilva.com.br/tecnologia/o-que-e-ti/#ixzz4yzh7smju. Acesso em: 12 set. 2018.

TURBAN, E.; VOLONINO, L. **Tecnologia da informação para gestão**: em busca de um melhor desempenho estratégico e operacional. 8. ed. São Paulo: Bookman, 2013.