POLITÍCA DE SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS

Fabio Eder Cardoso [1]
Paulo Cesar de Oliveira [2]

Faculdade de Tecnologia de Ourinhos - FATEC

1. INTRODUÇÃO

A informação é o elemento básico para que a evolução aconteça e o desenvolvimento humano se realize de forma completa (COURY, 2001). Para Campos, (2007, p. 21) “A informação é elemento essencial para todos os processos de negócio da organização, sendo, portanto, um bem ou ativo de grande valor”. Logo pode se dizer que a informação se tornou o ativo mais valioso das organizações, podendo ser alvo de uma série de ameaças com a finalidade de explorar as vulnerabilidades e causar prejuízos consideráveis. Portanto, faz necessário a implementação de políticas de se segurança da informação que busque reduzir as chances de fraude ou perda de informações.

A Política de Segurança da Informação (PSI) é um documento que deve conter um conjunto de normas, métodos e procedimentos, os quais devem ser comunicado a todos os funcionários, bem como analisado e revisado criticamente, em intervalos

---

[1] Professor da Faculdade de Tecnologia de Ourinhos (FATEC). Av. Vitalina Marcusso 1400 – Campus Universitário – Cep: 19910-206 – Ourinhos/SP, E-mail: fabioeder.professor@gmail.com

[2] Aluno do curso de Analise de Sistemas e Tecnologia da Informação – Faculdade de Tecnologia de Ourinhos (FATEC) e-mail: paulo_gape@yahoo.com.br

regulares ou quando mudanças se fizerem necessárias. É o SGSI que vai garantir a viabilidade e o uso dos ativos somente por pessoas autorizadas e que realmente necessitam delas para realizar suas funções dentro da empresa. (FONTES, 2006)

Para se elaborar uma Política de Segurança da Informação, deve se levar em consideração a NBR ISO/ 27001:2005, que é uma norma de códigos de práticas para a gestão de segurança da informação, onde podem ser encontradas as melhores práticas para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.

2. A INFORMAÇÃO E A SUA SEGURANÇA

2.1 A INFORMAÇÃO

Segundo a ISO/IEC 27002:2005(2005), a informação é um conjunto de dados que representa um ponto de vista, um dado processado é o que gera uma informação. Um dado não tem valor antes de ser processado, a partir do seu processamento, ele passa a ser considerado uma informação, que pode gerar conhecimento. Portanto pode-se entender que informação é o conhecimento produzido como resultado do processamento de dados.

Ainda, segundo a ISO/IEC 27002:2005, a informação é um ativo que como qualquer outro ativo é importante, é essencial para os negócios de uma organização, e deve ser adequadamente protegida. A informação é encarada, atualmente, como um dos recursos mais importantes de uma organização, contribuindo decisivamente para a uma maior ou menor competitividade. De fato, com o aumento da concorrência de mercado, tornou-se vital melhorar a capacidade de decisão em todos os níveis.

“A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas” (ISO/IEC 27002:2005, 2005, p. x). Seja qual for a forma em que é apresentada ou meio pelo qual é

compartilhada ou armazenada, é importante no mundo dos negócios, cada vez mais competitivo. Como resultado deste significante aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.

2.2 SEGURANÇA DA INFORMAÇÃO

Para a ABNT NBR ISO/IEC 17799:2005 (2005, p.ix), “segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”. Entende-se melhor essa necessidade de uma segurança da informação analisando um banco de dados de uma agência bancária, onde as informações são em grandes quantidades e muito sigilosas. Pois ali, estão armazenados dados pessoais e também da conta bancária dos clientes. Devido a necessidade de extremo sigilo da informação, exige-se uma segurança eficaz.

> “Em primeiro lugar, muitas vezes é difícil obter o apoio da própria alta administração da organização para realizar os investimentos necessários em segurança da informação. Os custos elevados das soluções contribuem para esse cenário, mas o desconhecimento da importância do tema é provavelmente ainda o maior problema”. (CAMPOS, 2007, p.29)

A informação é um ativo que deve ser protegido e cuidado por meio de regras e procedimentos das políticas de segurança, do mesmo modo que protegemos nossos recursos financeiros e patrimoniais. Segundo Campos (2077, p. 17), “um sistema de segurança da informação baseia-se em três princípios básicos: confidencialidade, integridade e disponibilidade.”

Ao se falar em segurança da informação, deve-se levar em consideração estes três princípios básicos, pois toda ação que venha a comprometer qualquer uma

desses princípios, seja confidencialidade, integridade ou disponibilidade, estará atentando contra a sua segurança.

Confidencialidade

A confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso (NBR ISO/IEC 27002:2005). Caso a informação seja acessada por uma pessoa não autorizada, intencionalmente ou não, ocorre a quebra da confidencialidade. A quebra desse sigilo pode acarretar danos inestimáveis para a empresa ou até mesmo para uma pessoa física. Um exemplo simples seria o furto do número e da senha do cartão de crédito, ou até mesmo, dados da conta bancária de uma pessoa.

Integridade

A integridade é a garantia da exatidão e completeza da informação e dos métodos de processamento (NBR ISO/IEC 27002:2005). “Garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente”. (DANTAS, 2011, p11). Quando a informação é alterada, falsificada ou furtada, ocorre à quebra da integridade. A integridade é garantida quando se mantém a informação no seu formato original.

Disponibilidade

A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (NBR ISO/IEC 27002:2005). Quando a informação está indisponível para o acesso, ou seja, quando os servidores estão inoperantes por conta de ataques e invasões, considera-se um incidente de segurança da informação por quebra de disponibilidade. Mesmo as

interrupções involuntárias do sistema, ou seja, não intencionais, configuram quebra de disponibilidade.

2.2.1 SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

A norma ISO 27001 estabelece diretrizes e princípios gerais para se iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Essa norma possui uma seção introdutória sobre o processo de avaliação e tratamento de riscos e está dividida em onze seções específicas, que são: política de segurança da informação; organização da segurança da informação; gestão de ativos; segurança em recursos humanos; segurança física e do ambiente; gestão das operações e comunicações; controle de acesso; aquisição, desenvolvimento e manutenção de sistemas de informação; gestão de incidentes de segurança da informação; gestão da continuidade do negócio, e conformidade. Essas seções totalizam trinta e nove categorias principais de segurança, e cada categoria contém um objetivo de controle e um ou mais controles que podem ser aplicados, bem como algumas diretrizes e informações adicionais para a sua implementação. Para Fontes e Araujo (2008), o sistema de gestão de segurança da informação é o resultado da sua aplicação planejada, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para a segurança da informação.

2.2.2 CLASSIFICANDO AS INFORMAÇÕES

Segundo Fontes (2008), a principal razão em classificar as informações, é de que elas não possuem o mesmo grau de confidencialidade, ou então as pessoas podem ter interpretações diferentes sobre o nível de confidencialidade da informação. Para um simples operário de uma empresa um relatório contendo o seu balanço anual pode não significar nada, já para o pessoal do financeiro e a alta direção é uma

informação de suma importância, e que deve ser bem guardada. Para poder classificar uma informação, é importante saber quais as conseqüências que ela trará para a organização caso seja divulgada, alterada ou eliminada sem autorização. Somente através da interação com as pessoas diretamente responsáveis pela informação da empresa será possível estabelecer estas conseqüências e criar graus apropriados de classificação.

> Antes de se iniciar o processo de classificação, é necessário conhecer o processo de negócio da organização, compreender as atividades realizadas e, a partir disso, iniciar as respectivas classificações. As informações podem ser classificadas em informações públicas, quando não necessita de sigilo algum; informações internas, quando o acesso externo as informações deve, ser negado; e informações confidencias, as informações devem ser confidencias dentro da empresa e protegida contra tentativas de acesso externo. (Freitas e Araujo, 2008)

2.2.3 ATIVOS

A definição clássica é que o ativo compreende ao conjunto de bens e direitos de uma entidade. Entretanto, atualmente, um conceito mais amplo tem sido adotado para se referir ao ativo como tudo aquilo que possui valor para a empresa. (DANTAS, 2011, p.21). A informação ocupa um papel de destaque no ambiente das organizações empresariais, e também adquire um potencial de valorização para as empresas e para as pessoas, passando a ser considerado o seu principal ativo.

2.2.4 AMEAÇA

Segundo Campos (2007), a ameaça pode ser considerada um agente externo ao ativo de informação, pois se aproveita de suas vulnerabilidades para quebrar a os princípios básicos da informação, a confidencialidade, integridade ou disponibilidade. Atualmente, o mundo dos negócios apresenta-se bastante competitivo, onde as empresas devem estar sempre atentas para as ameaças aos negócios corporativos, que, se concretizadas poderão causar grandes perdas, e conseqüentemente encerrar suas atividades para sempre.

As ameaças podem ser, naturais: são aquelas que se originam de fenômenos da natureza; involuntárias: são as que resultam de ações desprovidas de intenção para causar algum dano e intencionais: são aquelas deliberadas, que objetivam causar danos, tais como hackers. (DANTAS, 2011)

2.2.5 VULNERABILIDADE

A NBR ISO/IEC 27002:2005 define a vulnerabilidade como uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Segundo Campos (2007), vulnerabilidade são as fraquezas presentes nos ativos, que podem ser exploradas, seja ela intencionalmente ou não, resultando assim na quebra de um ou mais princípios da segurança da informação. Ao ter sido identificado as vulnerabilidades ou os pontos fracos, será possível dimensionar os ricos aos quais o ambiente esta exposto e assim definir medidas de segurança apropriada para sua correção.

> "As vulnerabilidades podem advir de vários aspectos: instalações físicas desprotegida contra incêndios, inundações, e desastres naturais; material inadequado empregado nas construções; ausência de política de segurança para RH; funcionários sem treinamento e insatisfatório nos locais de trabalho; ausência de procedimento de controle de acesso e utilização de equipamentos por pessoal contratado; equipamento obsoletos, sem manutenção e sem restrições para sua utilização; software sem patch de atualização e sem licença de funcionamento, etc". (DANTAS, 2001, p.25-26)

2.2.6 RISCO

Com relação a segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas. É medido pela possibilidade de um evento vir a acontecer e produzir perdas. (DANTAS, 2001). Para evitar possíveis perdas de informações, que dependendo do seu grau de sigilo, poderá levar a empresa à falência, é necessária a elaboração de uma gestão de risco, onde os riscos são

determinados e classificados, sendo depois especificado um conjunto equilibrado de medidas de segurança que permitirá reduzir ou eliminar os riscos a que a Empresa se encontra sujeita. A norma NBR ISO 27002(2005) nos oferece uma métrica, em que o risco pode ser calculado pela seguinte formula:

RISCO = (Ameaça) x (Vulnerabilidade) x (Valor do Risco)

> É cada vez mais importante para uma organização, mesmo em sua fase inicial, formalizar um documento com a sua análise de risco, o que provê alta administração um indicador sobre o futuro da própria empresa, em que serão relacionados os ativos que serão protegidos com investimentos adequados ao seu valor ao seu risco (LAUREANO, 2005).

2.2.7 BAKUP

A ISO/IEC 27002 (2005) recomenda que backup dos sistemas seja armazenado em outro local, o mais longe possível do ambiente atual, como em outro prédio. Um dos maiores erros cometidos em questão de segurança de backup, foi o atentado de 11 de setembro, onde foram derrubadas as torres gêmeas nos EUA, onde empresas localizadas na torre A tinham backups na torre B, e empresas da torre B tinham backup na torre A, depois da queda das duas torres, varias empresas simplesmente sumiram, deixando de existir, um erro que poderia ser controlado caso o backup estivesse localizado em outro lado da cidade. “É evidente que o procedimento de backup é um dos recursos mais efetivos para assegurar a continuidade das operações em caso de paralisação na ocorrência de um sinistro”. (FFREITAS E ARAUJO, 2008, p. 133)

2.*2.* 8 SEGURANÇA FÍSICA

O objetivo é prevenir o acesso físico não autorizado. Convém que sejam utilizados perímetros de segurança para proteger as áreas que contenham informações e instalações de processamento da informação, segundo a ISO/IEC 27002:2005(2005). Pode-se obter proteção física criando uma ou mais barreiras físicas ao redor das instalações e dos recursos de processamento da informação, tais como, leitores

biométricos, portas de acesso com cartões magnéticos, portões elétricos, colocando vigias em local de acesso restrito. Controlar o acesso de quem entra e sai das instalações é um aspecto importante na segurança física. Não basta ter um guarda na entrada identificando os visitantes. É fundamental ter a certeza, por exemplo, de que os visitantes não levem materiais ou equipamentos da empresa.

> "Apesar de todos os cuidados em se definir os perímetros de segurança, essa ação não produzira resultados positivos se os colaboradores não estiverem sintonizados com a cultura de segurança da informação. Essa cultura deve estar pulverizada em toda a organização e especialmente consolidada dentro das áreas críticas de segurança. A informação pertinente ao trabalho dentro dessas áreas deve estar restrita a própria área e somente durante a execução das atividades em que ela se torna necessária. Essas atividades sempre deverão ser realizadas sob supervisão para garantir a segurança. Quando houver atividade, essas áreas devem permanecer fechadas de forma validável, como, por exemplo, através do uso de lacres de segurança, e supervisionadas regularmente (Campos, 2077, p.169)".

A NBR ISO/IEC 27002 (2005) recomenda que seja feito um projeto para a implementação de áreas de segurança com salas fechadas e com vários ambientes seguros de ameaças como fogo, vazamento de água, poeira, fumaça, vibrações, desastres naturais, e manifestações. Os locais escolhidos para a instalação dos equipamentos devem estar em boas condições de uso, com boas instalações elétricas, saídas de emergência, alarme contra incêndio, devem conter extintores de incêndios, entre outros aspectos que devem ser levados em consideração.

2.3 POLITÍCAS DE SEGURANÇA DA INFORMAÇÃO

Para Dantas (2001), pode-se definir a política de segurança como um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades sobre o que deve ser feito par alcançar um padrão desejável de proteção para as informações. Ela é basicamente um manual de procedimentos que descreve como os recursos de TI da empresa devem ser protegidos e utilizados e é o

pilar da eficácia da segurança da informação. Sem regras pré-estabelecidas, ela torna-se inconsistentes e vulnerabilidades podem surgir. A política tende a estabelecer regras e normas de conduta com o objetivo de diminuir a probabilidade da ocorrência de incidentes que provoquem, por, exemplo a indisponibilidade do serviço, furto ou até mesmo a perda de informações. As políticas de segurança geralmente são construídas a partir das necessidades do negócio e eventualmente aperfeiçoadas pele experiência do gestor.

O intervalo médio utilizado para a revisão da política é de seis meses ou um ano, porem deve ser realizada uma revisão sempre que forem identificados fatos novos, não previstos na versão atual que possam ter impacto na segurança das informações da organização. (FREITAS e ARAUJO, 2008).

Segundo a NBR ISSO/IEC27002(2005), é recomendado que a política de segurança da informação seja revisada periodicamente e de forma planejada ou quando ocorrerem mudanças significativas, para assegurar a sua continua pertinência, adequação e eficácia.

"Atualmente, a PSI é adotada em grande parte das organizações em todo o mundo, inclusive no Brasil. Mesmo aquelas empresas que ainda não tem uma política efetiva, reconhecem a necessidade de elaborar e implementar uma". (CAMPOS, 2007, P. 131). A política de segurança da informação deve estabelecer como será efetuado o acesso as informações de todas as formas possíveis, seja ela internamente ou externamente, e quais os tipos de mídias poderão transportar e ter acesso a esta informação. A política deve especificar os mecanismos através dos quais estes requisitos podem ser alocados.

2.3.1 ELABORANDO A POLÍTICA

Para Ferreira e Araujo (2008), deve-se formar um comitê de segurança da informação, constituído por profissionais de diversos departamentos, como informática, jurídico, engenharia, infra-estrutura, recursos humanos e outro que for necessário. O

comitê será responsável por divulgar e estabelecer os procedimentos de segurança, se reunindo periodicamente, ou a qualquer momento conforme requerido pelas circunstancias, com o objetivo de manter a se segurança em todas as áreas da organização. “Convêm que a política de segurança da informação tenha um gestor que tenha responsabilidade de gestão aprovada para desenvolvimento, análise crítica e avaliação da política de segurança da informação”.(ISSO/IEC 27002:2005, 2005. P. 9)

2.3.2 IMPLEMENTANDO A POLÍTICA DE SEGURANÇA

Para que a cultura da empresa seja mudada em relação à segurança da informação, é fundamental que os funcionários estejam preparados para a mudança, por meio de avisos, palestras de conscientização, elaboração de guias rápidos de consulta e treinamento direcionado. (FREITAS E ARAUJO, 2008, P. 47). A política deve ser escrita de forma clara, não gerando qualquer dúvida entre os usuários. Todos os funcionários da organização, incluindo aqueles que são terciários e prestadores de serviço, deverão receber um treinamento adequado para que se adéqüem as mudanças. De acordo com a NBR ISSO IEC 27002 (2005) os usuários devem estar clientes das ameaças e das vulnerabilidades de segurança da informação e estejam equipados para apoiar a política de segurança da informação da organização durante a execução normal do trabalho.

A política de segurança deve contar com o apoio e comprometimento da alta direção da organização, pois é fundamental para que a política de Segurança seja efetiva, sem a presença deste apoio, iniciar qualquer ação neste sentido é algo inviável

3. CONSIDERAÇÃOES FINAIS

No cenário atual, em que as empresas dependem cada vez mais da tecnologia e da informação, é vital garantir a segurança adequada deste ativo, considerado estratégico em sua missão de prestar serviços de qualidade. A solução mais adequada

é o estabelecimento de um conjunto de normas e regras que regulem a utilização dos sistemas das empresas, assim como o acesso a redes sociais e e-mails pessoais. As empresas necessitam aliar essa política de segurança da informação ao contrato de trabalho dos colaboradores. Todo processo de segurança começa no recrutamento. Também é importante lembrar que os trabalhadores devem estar cientes do monitoramento das informações.

Com base nos princípios da Política de Segurança da Informação, foi possível avaliar o segmento dos paradigmas básicos em sua composição: a integridade, como sendo condição na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas, a confidencialidade, visando a propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização prévia do seu dono e a disponibilidade, característica essa que se relaciona diretamente a possibilidade de acesso por parte daqueles que a necessitam para o desempenho de suas atividades a qualquer hora.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISSO/IEC 27002:2005 tecnologia da informação - técnicas de segurança - código de pratica para gestão da informação. Rio de janeiro: 2005, Disponível em: http://search.4shared.com/postDownload/M0vePGU6/ISO-IEC_27002-2005.html>, Acessado em 02 de novembro de 20012

CAMPOS, A. SISTEMAS DE SEGURANÇA DA INFORMAÇÃO. 2 ed. Florianopolis: Visual Books, 2007.

COURY, RICARDO. Informação é poder. Disponível em <HTTP//www.timester.om.br/entrevista/artigos/main_artigo.asp?Codigo=424>>, Acessado em 28 de outubro de 2012

DANTAS, M. SEGURANÇA DA INFORMAÇÃO: UMA ABORDAGEM FOCADA EM GESTÃO DE RISCOS. 1 ed. Olinda: Livro rápido, 2011

FONTES, E. PRATICANDO A SEGURANÇA DA IONFORMAÇÃO. Rio de Janeiro: Brasport, 2008

FREITAS,F;ARAUJO, M. POLITICAS DE SEGURANÇA DA INFORMAÇÃO: Guia pratico para elaboração e implementação. 2ed. Rio de Janeiro: Ciência Moderna LTDA, 2008

NETTO, A; SILVEIRA, M. GESTÃO DE SEGURANÇA DA INFORMAÇÃO: FATOS QUE INFLUENCIAM SUA ADOÇÃO EM PEQUENAS E MÉDIAS EMPREAS. Disponível em <http://dialnet.unirioja.es/descarga/articulo/2734365.pdf> Acessado em 07 de Novembro de 2012.