Politicas de Segurança da Informação

Rodrigo Pionti[1], Daniel Paulo Ferreira[2]

Faculdade de Tecnologia de Ourinhos – FATEC

INTRODUÇÃO

Com o avanço da tecnologia de modo acelerado, o uso da internet tem se tornado imprescindível nas nossas atividades diárias, sendo esse um dos recursos mais utilizados para troca de informações tanto empresariais quanto pessoais. Devido a essa exposição cresce também a preocupação com a segurança da informação.

A política de segurança da informação nada mais é que um conjunto de praticas e controles adequados, formada por diretrizes, normas e procedimentos, com objetivo de minimizar os riscos com perdas e violações de qualquer bem. Se aplicada de forma correta ajudam a proteger as informações que são consideradas como um ativo importante dentro da organização.

INFORMAÇÃO

Informação é um conjunto que dados que processados ganham significado que tornam possível sua compreensão e interpretação. As informações constituem um dos objetos de grande valor para as empresas.

A ISO/IEC 13335-1/2004 caracteriza como ativo qualquer coisa que tenha valor para a organização. É considerado como ativo de informação todo bem da empresa que se relaciona com informação e que tenha valor para a organização, pode ser um componente humano, tecnológico, físico ou lógico que realize processos de negócio dentro da empresa.

---

[1] Graduado em Análise de Sistemas e Tecnologia da Informação com habilitação em Tecnólogo em Segurança da Informação. rpionti@hotmail.com

[2] Professor da Faculdade de Tecnologia de Ourinhos (FATEC), Avenida Vitalina Marcusso,1400 Campus Universitário CEP 19910-260 Ourinho/ SP . Tel/fax: (14) 3324-3986, E-mail : dir.fatecourinhos@centropaulasouza.sp.gov.br

Atualmente a informação é de valor altamente significativo e pode representar grande poder para quem a possui, seja pessoa, seja a empresa. A informação apresenta-se como recurso estratégico sob a ótica da vantagem competitiva. Possui valor, pois está presente em todas as atividades que envolvem pessoas, processos, sistemas, recursos financeiros, tecnologias e etc.

Classificação da informação

Cada informação tem um diferente grau de importância, por esse motivo é necessário classificá-las. Essa classificação norteia-se mediante ao impacto que causaria a sua perda, alteração ou uso sem permissão. Ferreira afirma que ”quanto mais estratégica e decisiva para a manutenção ou sucesso da organização maior será sua importância”. (FERREIRA, 2008, p. 78)

Classificações excessivas podem causar confusões e dificultar o processo, elas devem ser claras, de fácil entendimento e descritas para diferenciação entre si. Normalmente três níveis podem ser suficientes para uma boa classificação. Entre os níveis mais utilizados na classificação de informação estão: informação pública, informação interna e informação confidencial.

- Informações públicas: são aquelas de menor importância, não necessitam de sigilo, por isso é desnecessário investimentos para torná-las seguras. Exemplo: teste de sistema e serviços, folders.
- Informações internas: são as que devem ser mantidas fora do alcance de acesso externo, mas que, se for acessada de forma indevida não causarão grande impacto. Exemplo: agenda telefônica.
- Informações confidenciais devem ser protegidas de acesso externo, pois se utilizadas por pessoas não autorizadas poderão levar a organização a ter prejuízos financeiros ou perda de competitividade. Exemplo: salários, dados de clientes, senhas.

Segurança da Informação

Devido à importância de cada informação devemos mantê-las seguras, porem muitas vezes sua importância só é percebida quando ela é destruída, perdida ou até roubada.

Os princípios da segurança da informação abrangem basicamente os seguintes aspectos: confidencialidade, integridade e disponibilidade (CID), toda ação que possa comprometer um desses princípios pode ser tratada como atentado a sua segurança.

Confidencialidade: É a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso. Para PEIXOTO (2006, p.38) “A tramitação das informações deve contar com a segurança de que eles cheguem sem que se dissipem para outros meios ou lugares onde não deveriam passar”.

Integridade: É a preservação da exatidão da informação e dos métodos de processamento. Segundo Lyra (2008, p.3) “A informação deve estar correta, ser verdadeira e não estar corrompida”.

Disponibilidade: É a Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

As informações estão sujeitas a ameaças e riscos devido suas vulnerabilidades.

Ameaça é o que provoca um risco dano o u perca. A ABNT ISSO/IEC 27002,2005 define risco como combinação da probabilidade de um evento e de suas consequências.

Moreira (2001) aponta a vulnerabilidade como sendo o ponto onde qualquer sistema é suscetível a um ataque, condição causada muitas vezes pela ausência ou ineficiência das medidas de proteção utilizadas de salvaguardar os bens da empresa.

Portanto a função básica da segurança da informação é minimizar os riscos até que esses estejam em níveis aceitáveis.

Adachi (2004) que estudou a gestão da segurança em Internet Banking estudou os aspectos envolvidos na segurança da informação agrupando-os em três camadas: física, lógica e humana. Portanto torna-se essencial que haja segurança em cada uma das três camadas.

A segurança física tem como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses

recursos, pode ser abordada sob duas formas: Segurança de acesso - trata das medidas de proteção contra o acesso físico não autorizado; e Segurança ambiental trata da prevenção de danos por causas naturais.

A segurança lógica aplica-se em casos onde um usuário ou processo da rede tenta obter acesso a um objeto que pode ser um arquivo ou outro recurso de rede (estação de trabalho, impressora, etc.) sendo assim um conjunto de medida e procedimentos, adotados com objetivo de proteger os dados, programas e sistemas contra tentativas de acessos não autorizados, feitas por usuários ou outros programas.

Todos colaboradores da empresa fazem parte do fator humano, principalmente os que têm acesso direto aos recursos de T.I. trata-se do fator mais difícil de se gerenciar e avaliar riscos. A dificuldade encontrada em gerenciar o fator humano está relacionada às características individualizadas de cada pessoa, pois cada uma delas lida de forma diferente com intrusos maliciosos ou ingênuos, alguns são mais instruídos e outros não, e responde diferentemente a engenharia social.

Ferreira afirma que:

> A grande maioria dos incidentes tem a intervenção humana, seja de forma acidental ou não. A segurança está relacionada a pessoas e processos antes da tecnologia. Consequentemente nada valerão os milhões investidos em recursos de tecnologia da informação se o fator humano for deixado em segundo plano. Quanto mais bem preparados os funcionários de uma organização, mais segura ela será. (FERREIRA;FERNANDO,2008,p.121)

Políticas de Segurança da Informação

A política de segurança define normas, procedimentos, ferramentas e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação para garantir o controle e a segurança da informação na empresa. É formalmente o documento que dita quais são as regras aplicadas dentro da empresa para uso de recursos tecnológicos e descarte de informações.

A política de segurança define o que é e o que não é permitido em termos de segurança durante a operação de qualquer sistema ou material que contenha informações empresariais, com base na aplicação de regras que delimitam o acesso às informações. Assim, a base da política de segurança é a definição do comportamento esperado das pessoas que interagem com um sistema.

Á grosso modo pode-se afirmar que com a implantação de uma política de segurança da informação é a significativa a redução da probabilidade de ocorrência de quebra da confidencialidade, da integridade e da disponibilidade da informação, tal como a redução de danos causados por eventuais ocorrências.

> A politica, preferencialmente deve ser criada antes da ocorrência de problemas com a segurança, ou depois, para evitar reincidências. Ela é uma ferramenta tanto para prevenir problemas legais como para documentar a aderência ao processo de controle de qualidade. (FERREIRA;FERNANDO, 2008, p.36)

As políticas de bem elaboradas, possuem certa semelhança entre si, mesmo as mais rígidas ou mais brandas, isso porque todas exploram os mesmos aspectos.

Características e Benefícios

Para seu efetivo funcionamento a politica ela deve ter certas peculiaridades como: ser verdadeira, ser valida para todos, ser simples, contar com o comprometimento dos gestores da empresa. De nada adiantaria implantar uma politica que não fosse coerente com as ações executadas pela empresa, pois isso impossibilitaria seu cumprimento.

Ferreira afirma que á curto prazo pode-se notar a prevenção de acessos não autorizados, danos ou interferências no andamento do negócio, além de já se conseguir maior segurança nos processos do negócio, em médio prazo surge a padronização dos procedimentos, a adaptação já de forma segura de novos processos e a qualificação e quantificação de respostas a incidentes; e a

longo prazo obtém-se o retorno do investimento, por meio da diminuição de problemas relacionados a incidentes de segurança da informação, e a empresa consegue firmar-se como uma empresa associada a segurança da informação.

Considerações Finais

Nem sempre se pode ter o controle sobre as ameaças que geralmente origina-se de um agente externo, portanto é essencial a diminuição das vulnerabilidades existentes para que se diminua o risco.

Existem diversas medidas de segurança que podem ser adotadas pelas empresas com o intuito de proteger suas informações, por isso as politicas de segurança da informação são tão importantes, elas que nortearão os colaboradores a como agir baseados nos procedimentos pré-estabelecidos na politica.

Referências

ADACHI, Tomi. **Gestão de Segurança em Internet Banking -** São Paulo: FGV, 2004. 121p. Mestrado. Fundação Getúlio Vargas - Administração. Orientador: Eduardo Henrique Diniz

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002. **Tecnologia da informação** - técnicas de segurança - código de pratica para gestão da informação. Rio de Janeiro, 2005.

FERREIRA,F.N.F; ARAÚJO,M.T. **Politicas de Segurança da Informação – Guia prático para elaboração e Implementação**.2 ed. Rio de Janeiro: Ciência Moderna, 2008.

FONTES, E.L.G. **Praticando a Segurança da Informação**. Rio de Janeiro: Brasport, 2008.

JÚNIOR, Byron L.M. e tal. **Proteja o maior bem da sua empresa, a informação com: política de segurança da informação.** disponível em : <.http://www.fatec.edu.br/html/fatecam/images/stories/dspti_ii/asti_ii_material_apoio_4_seguranca_informacao_politicas.pdf>. Acesso em 26 abr 2013

LYRA, Maurício R. **Segurança e Auditoria em Segurança da Informação**. Rio de Janeiro: Ciência Moderna,2008.

PEIXOTO, Mauro C.P. **Engenharia Social e Segurança da Informação**. Rio de Janeiro: Brasport, 2006.

PINHEIRO,J.M.S. **Auditoria e análise de segurança da informação: segurança física e lógica.** Disponível em http://www.projetoderedes.com.br/aulas/ugb_auditoria_e_analise/ugb_apoio_auditoria_e_analise_de_seguranca_aula_02.pdf> Acesso em 18 mar 2013.