ROSÂNGELA MOREIRA GONÇALVES

RECOMENDAÇÕES DE BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO EM GESTÃO DE PROJETOS DE TI COM O MODELO PMBOK

Monografia apresentada à Escola Politécnica da Universidade de São Paulo para a conclusão do curso de MBA em Tecnologia da Informação.

Orientador: Professor Marco Túlio Carvalho de Andrade

São Paulo/SP
2007

Dedicatória

Dedico este trabalho ao meu pai, que no
fim da vida, me ensinou que não podemos
desistir jamais e que sempre há motivos para lutar.

Nelson Moreira dos Santos

Agradecimentos

Agradeço ao meu marido Marcos Augusto Sanfelice Gonçalves e minha filha Laís Moreira Sanfelice Gonçalves pelo amor, compreensão, companheirismo e paciência.

Agradeço ao meu amigo Augusto Quadros Paes de Barros, que me apoiou e incentivou para a realização de grandes conquistas.

Agradeço ao meu orientador, professor Marco Túlio Carvalho de Andrade pela aceitação, dedicação e apoio, por ser meu amigo nos momentos difíceis que a vida nos proporcionou neste ano que passamos juntos.

"Não é preciso ter olhos abertos para ver o sol, nem é preciso ter ouvidos afiados para ouvir o trovão. Para ser vitorioso você precisa ver o que não está visível."

Sun Tzu

FICHA CATALOGRÁFICA

Gonçalves, Rosângela Moreira

Recomendações de Boas Práticas de Segurança da Informação em Gestão de Projetos de TI com o Modelo PMBOK / R.M. Gonçalves. -- São Paulo, 2007.
51 p.

Monografia (MBA em Tecnologia da Informação) – Escola Politécnica da Universidade de São Paulo. Programa de Educação Continuada em Engenharia.

1. Gerenciamento de projeto 2. Segurança da Informação. Universidade de São Paulo. Escola Politécnica. Programa de Educação Continuada em Engenharia.

1825335

RESUMO

Este trabalho elabora e apresenta algumas recomendações de segurança para o ambiente de TI, com foco principal no ciclo de vida de um projeto. Para alcançar esse objetivo, parte-se de conceitos básicos de boas práticas, normas e legislações vinculadas ao tema. Com isto consegue-se apresentar a importância da ocorrência de mudanças culturais na empresa e a conscientização dos profissionais envolvidos em projetos.

O trabalho destaca que todas as fases do projeto possuem aspectos de segurança a serem analisados, porém, nem todas as áreas de conhecimento, contidas nessas fases são relacionadas a aspectos de segurança.

No entanto, para implementar a segurança da informação faz-se necessário um conjunto de controles adequados com o objetivo de garantir que as expectativas do negócio e a segurança da organização sejam atendidas.

As recomendações de controles de Segurança da informação aqui citadas, podem ser associadas aos processos de contratação de pessoas, fornecedores, processos de comunicação, políticas de segurança, classificação de informação e análise de riscos. Permitindo de forma geral, identificar os principais processos e as conseqüências para um risco ignorado.

Palavras-chave: Recomendações de segurança, Ciclo de vida do projeto, Áreas de Conhecimento.

ABSTRACT

This work brings some information on security recommendations for the IT environment with main focus on a project life cycle. To reach this objective, we worked based on best practices, policies and legislation related to this matter. This allows us to state the importance of the occurrence of cultural changes in a company and the awareness of the professionals involved in projects.

This work emphasizes that all phases of a project have security aspects to be analyzed, however, not all areas of knowledge contained in these phases are related to security aspects.

On the other hand, to make information security effective, it's necessary to put in place a set of controls customized in order to ensure that business expectations and the security of the organization are being addressed.

The information security controls mentioned in this work can be associated to the employees and suppliers hiring process, communication processes, security policies, information classification and risk analysis, in order to make possible to identify the main processes and the consequences for ignored risks.

Key words: Security recommendations, Project Life Cycle and Areas of Knowledge.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGI.br	Comitê Gestor da Internet no Brasil
IEC	International Eletrotechnical Comission
IIL	International Institute for Learning
ISO	International Organization for Standardization
LAN	Local Area Network
PDCA	Plan-Do-Check-Act
PIB	Produto Interno Bruto
PIN	Personal Identification Number
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
SGSI	Sistema de Gerenciamento de Segurança da Informação
TI	Tecnologia da Informação
TR	Technical Report
VPN	Virtual Private Network
WAN	World Area Network
WEB	World Wide Web

SUMÁRIO

1. INTRODUÇAO

Um dos objetivos da gerência de projetos é manter o menor nível possível de riscos durante o ciclo de vida do projeto. O risco de um projeto terminar mal sucedido, ou até, não ser concluído, aumenta de acordo com a falta de definição em todas as fases do projeto.

Um ponto de vista alternativo diz que gerenciamento de projetos é a disciplina de definir e alcançar objetivos ao mesmo tempo em que se aperfeiçoa o uso de recursos (tempo, dinheiro, pessoas, espaço, etc). [© 2004/2005 Instituto Aprender Mais].

Como pode ser observado na figura 1.1, os executivos demonstram uma constante preocupação com a Gestão de seus Projetos e isso pode ser comprovado através de pesquisas realizadas por empresas especializadas.

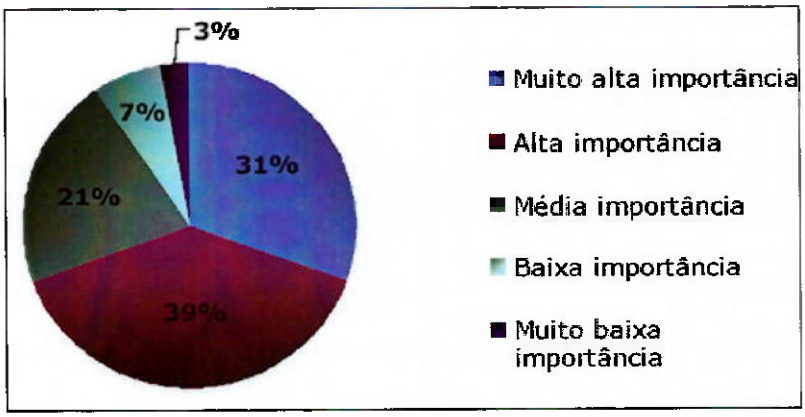

Figura 1.1: Grau de Importância que a Alta Administração dá ao Gerenciamento de Projetos
Estudo de Benchmarking em Gestão de Projetos, PMI-RJ, 2003
International Institute for Learning IIL - Brasil

Durante um projeto é importante gerenciar algumas ameaças que podem comprometer o sucesso do resultado final, além de gerar risco de imagem e perda financeira para a organização, como por exemplo, os itens citados na figura 1.2.

Figura 1.2: Problemas que geraram perda financeira

10ª Pesquisa Nacional de Segurança da Informação – Módulo Security Solutions, 2007.

Com o mercado atual, complexo e competitivo, vários cuidados são exigidos, e é possível identificar através deste trabalho que uma das principais preocupações das organizações deve ser a segurança da informação, e é por isso que independente do segmento de atuação e do tamanho da organização, esse investimento pode ser justificável.

1.1. Motivação

Segundo o CERT.br, a disponibilidade de recursos e a divulgação ampla e rápida de formas de fraude e intrusão, aliadas ao valor da informação presente nos sistemas, têm despertado o interesse de usuários mal intencionados e colocado em pauta a Segurança da Informação das empresas.

Como pode ser observado na figura 1.3, o número de notificações de incidentes de segurança tem aumentado muito ao longo dos últimos anos.

Figura 1.3 – Total de Incidentes de Segurança reportados ao CERT.br, 2007

Fonte: Cert.br

As informações contidas nesse gráfico poderiam ser mais exatas se as empresas não apresentassem tanta resistência em reportar seus incidentes, pois algumas consideram que esta exposição pode comprometer sua imagem no mercado.

Os meios de comunicação atuais expõem as organizações a um número crescente dos mais variados tipos de ameaças. As mudanças ocorrem dinamicamente em diversos aspectos, como culturais, tecnológicos, políticos, econômicos, sociais. Segundo [Vieira, 2002], é comum associarmos essas mudanças ao resultado de projetos.

Como conseqüência, o gerenciamento de projetos torna-se um grande desafio. [Kerzner 2001].

Tendo em vista as informações acima apresentadas, somando-se com a experiência prática da autora, a mesma motivou-se a pesquisar e sugerir recomendações de boas práticas de segurança da informação que se apliquem a projetos de TI, procurando com isso contribuir para o desenvolvimento seguro.

1.2. Escopo

As recomendações geradas consideram aspectos de confidencialidade, integridade e disponibilidade como sendo os pilares essenciais para as boas práticas da segurança da informação, com foco nos níveis estratégicos e táticos. Vale ressaltar que controles operacionais de segurança da informação não é o foco deste trabalho.

Este trabalho apresenta recomendações de segurança para algumas áreas de conhecimento, porém, em algumas áreas podem não ser apresentadas permitindo assim, a continuidade deste trabalho.

1.3. Objetivos

Este trabalho tem como objetivo elaborar a recomendação de boas práticas de segurança da informação com base em análises de diretrizes e princípios gerais da Norma [NBR ISO/IEC 17799:2001] e associada aos grupos de processos de Gestão de Projetos baseados no modelo PMBOK. Este objetivo principal não exclui pesquisas em outras normas relacionadas ao assunto.

A ótica deste trabalho deve ser a do Gerente de Projetos, a fim de apoiar esse profissional a identificar as necessidades sobre segurança da informação que por ventura podem ocorrer durante o projeto.

1.4. Metodologia utilizada

Para a elaboração deste trabalho, realizaram-se pesquisas bibliográficas com a coleta de dados em livros, normas, padrões, artigos e utilização de meio eletrônico (Internet).

Para consolidar os principais conceitos envolvidos no tema abordado alguns profissionais foram entrevistados informalmente.

As normas ISO/IEC 17799, ISO/IEC 27001 e ISO/IEC 15408, que exercem influência sobre os aspectos de segurança nos projetos de TI foram consultadas para direcionar e embasar a pesquisa, outras normas foram consultadas para fins comparativos ou padronização de nomenclaturas. O PMBOK foi utilizado como guia para nortear o ciclo de vida do projeto.

1.5. Estrutura do trabalho

Este trabalho está organizado de acordo com a estrutura que se apresenta a seguir:

O segundo capítulo apresenta uma revisão bibliográfica dos conceitos de Segurança da Informação, enfocando a sua importância e benefício da sua aplicação dentro das empresas. São apresentados temas, principalmente, sobre a Norma [NBR ISO/IEC 17799:2001], conceitos e controles de segurança da informação. Também demonstra os conceitos de Gestão de Projetos, enfocando a sua importância e benefício da sua aplicação dentro das empresas. São apresentadas, além dos conceitos básicos, informações sobre processos de gestão, estrutura de gerenciamento, norma de gerenciamento e áreas de conhecimento em gerenciamento de projetos.

O terceiro capítulo aborda as recomendações de Segurança associadas à Gestão de Projetos, apresenta medidas para que os projetos sejam conduzidos seguramente, destaca aspectos que enfatizam as boas práticas de segurança da informação,

O quarto capítulo apresenta as considerações finais das análises realizadas.

Adicionalmente destacam-se as referências bibliográficas utilizadas como alicerce para construção desta pesquisa. Foram apresentadas referências aos meios físicos e eletrônicos que suportaram as pesquisas realizadas.

Posteriormente a citação de uma bibliografia adicional que contribuiu para o alicerce de conhecimento.

Finalmente aparecem o glossário e os anexos do trabalho.

2. REVISÃO BIBLIOGRÁFICA

Neste capítulo destacam-se alguns conceitos básicos sobre Segurança da Informação com o objetivo de contextualizar os assuntos citados nos outros capítulos que se seguem.

2.1. ASPECTOS DA SEGURANÇA DA INFORMAÇÃO

2.1.1 Norma [NBR ISO/IEC 17799:2001]

A Norma sugere recomendações de segurança da informação que podem ser utilizadas por profissionais envolvidos no gerenciamento dos processos de segurança da informação e também aqueles que precisam identificar pontos de vulnerabilidades em seus projetos.

O objetivo principal desta norma é estabelecer uma estrutura básica para o desenvolvimento de normas de segurança organizacional e das práticas de gestão da segurança, proporcionando confiança nos relacionamentos entre as organizações e seus relacionados.

A Norma está estruturada em cláusulas gerais, através da seguinte ordem lógica:

1. Política de segurança da informação;
2. Segurança organizacional;
3. Classificação e controle dos ativos de informação;
4. Segurança em pessoas;
5. Segurança física e ambiental;
6. Gerenciamento das operações e comunicações;
7. Controle de acesso;
8. Desenvolvimento de sistemas e manutenção;
9. Gestão da continuidade do negócio;
10. Conformidade.

Os controles e objetivos de controle são itens que se aplicam a cada cláusula. Convém declarar que nem todas essas cláusulas serão abordadas neste trabalho e suas aplicações podem ser encontradas em uma ou mais áreas de conhecimento da gestão de projetos.

Conforme mostrado na figura 2.1, pode-se observar que as organizações consideradas na pesquisa, apontam o uso da Norma para nortear sobre legislações, normas e regulamentações de segurança.

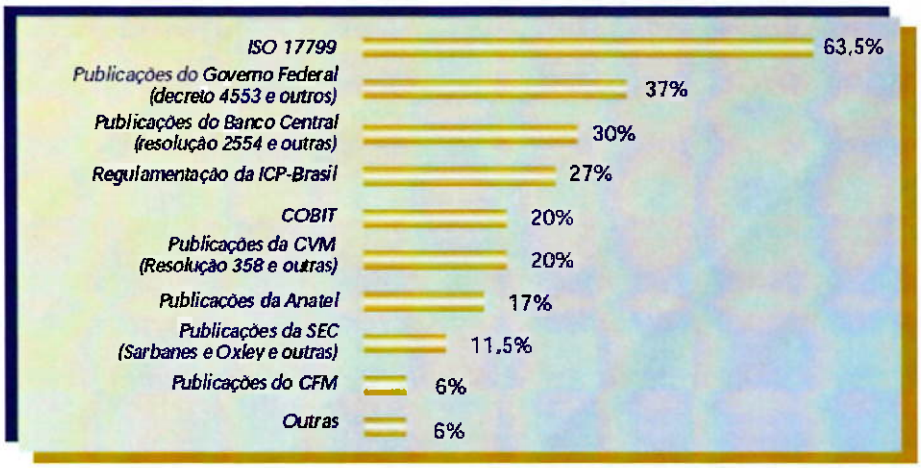

Figura 2.1: Pesquisa sobre Adequação a Legislações / Normas e Regulamentações
9ª Pesquisa Nacional de Segurança da Informação – Módulo Security Solutions, 2003

O total de citações é maior que 100% devido à questão aceitar múltiplas respostas.

2.1.2 Conceitos de Segurança da Informação

Segundo a Norma [NBR ISO/IEC 17799:2001], a informação é um ativo que tem valor para a organização e por isso precisa ser devidamente resguardada.

Independente da forma como a informação é representada ou armazenada, é recomendado que sejam estabelecidos processos para garantir que ela esteja protegida adequadamente. Essa recomendação pode contribuir para o sucesso de um projeto.

A Norma [NBR ISO/IEC 17799:2001] define que a segurança da informação é caracterizada pela preservação de três aspectos principais:

a) **confidencialidade**: é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;

b) **integridade**: é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

c) **disponibilidade**: é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

A Norma [NBR ISO/IEC 17799:2001] demonstra que a implementação de controles como políticas, procedimentos, boas práticas, estruturas organizacionais e funções de software contribuem para alcançar a segurança da informação. Uma vez estabelecidos estes controles é possível garantir que os objetivos de segurança específicos da organização sejam atendidos.

2.1.3 Controles de Segurança da Informação

Segundo a Norma [NBR ISO/IEC 17799:2001], a identificação de quais controles convém que sejam implantados requer planejamento cuidadoso. Toda recomendação de segurança tende a ter o custo reduzido se incorporada na fase de planejamento do projeto.

É essencial que uma organização identifique os seus requisitos de segurança, seja para mitigá-los ou gerenciá-los. Existem três fontes principais para viabilizar o processo de identificação destes requisitos:

- A primeira fonte é derivada da avaliação de risco dos ativos da organização. Através da avaliação de risco são identificadas as ameaças aos ativos, as vulnerabilidades e sua probabilidade de ocorrência são avaliadas, bem como o impacto potencial é estimado;
- A segunda fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm que atender;
- A terceira fonte é o conjunto particular de princípios, objetivos e requisitos para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

Segundo a Norma [NBR ISO/IEC 17799:2001], é necessário realizar análises críticas periódicas dos riscos de segurança e dos controles implementados para:

- Considerar as mudanças nos requisitos de negócio e suas prioridades;
- Considerar novas ameaças e vulnerabilidades;
- Confirmar que os controles permanecem eficientes e adequados.

Identificados os requisitos de segurança, é recomendado que as ações mitigantes sejam colocadas em prática para assegurar que os riscos sejam reduzidos a um nível aceitável. Em alguns casos, o custo para implementação destas ações não é justificável e mitigar o risco se torna inviável. Neste caso, é recomendado que a alta direção formalize e documente o risco assumido.

Segundo a Norma [NBR ISO/IEC 17799:2001], os controles considerados essenciais para uma organização, sob o ponto de vista legal, incluem:

1. Proteção de dados e privacidade de informações pessoais;
2. Proteção de registros organizacionais;
3. Direitos de propriedade intelectual.

Segundo a Norma [NBR ISO/IEC 17799:2001], os controles considerados como melhores práticas para a segurança da informação incluem:

- Documento da política de segurança da informação;
- Atribuição de responsabilidades para a segurança da informação;
- Conscientização, educação e treinamento em segurança da informação;
- Processamento correto nas aplicações;
- Gestão de vulnerabilidades técnicas;
- Gestão da continuidade do negócio;
- Gestão de incidentes de segurança da informação e melhorias.

2.2 GESTÃO DE PROJETOS

2.2.1 Projeto

Uma das características de um projeto é ter um início e fim definidos, portanto, é considerado como um evento temporário. O encerramento de um projeto se dá quando os objetivos são alcançados ou quando não há mais necessidade do mesmo [PMBOK 2004]. Projeto é entendido como algo que não foi realizado anteriormente e seu resultado final é diferente de qualquer outro.

Um projeto para ser executado precisa ser gerenciado. Segundo Koontz e O'Donnel [1980], gerenciar é orquestrar diversas atividades desenvolvidas por pessoas distintas para que os objetivos sejam alcançados.

Segundo o PMBOK 2004, os projetos são normalmente autorizados como um resultado de uma ou mais das seguintes considerações estratégicas:

- Uma demanda de mercado;
- Uma necessidade organizacional;
- Uma solicitação de um cliente;
- Um avanço tecnológico;
- Um requisito legal.

O gerenciamento do projeto pode ser facilitado quando segmentado em fases consideradas como ciclo de vida [Dinsmore e Cavalieri 2003].

2.2.2 Gerenciamento de Projeto

As áreas de conhecimento de gerenciamento, citadas no PMBOK 2004 são:

- Gerenciamento de Integração do Projeto;
    - Desenvolvimento do plano do projeto;
    - Execução do plano do projeto;
    - Controle integrado de mudanças.
- Gerenciamento de Escopo do Projeto;
    - Iniciação;
    - Planejamento do escopo;
    - Detalhamento do escopo;

- Verificação do escopo;
- Controle de mudanças do escopo.

- Gerenciamento do Tempo do Projeto;
  - Definição das atividades;
  - Seqüenciamento das atividades;
  - Estimativa da duração das atividades;
  - Desenvolvimento do cronograma;
  - Controle do cronograma.
- Gerenciamento do Custo do Projeto;
  - Planejamento dos recursos;
  - Estimativa dos custos;
  - Orçamento dos custos;
  - Controle dos custos.
- Gerenciamento da Qualidade do Projeto;
  - Planejamento da qualidade;
  - Garantia da qualidade;
  - Controle da qualidade.
- Gerenciamento de Recursos Humanos do Projeto;
  - Planejamento organizacional;
  - Montagem da equipe;
  - Desenvolvimento da equipe.
- Gerenciamento de Comunicação do Projeto;
  - Planejamento das comunicações;
  - Distribuição das informações;
  - Relato de desempenho;
  - Encerramento administrativo.
- Gerenciamento do Risco do Projeto;
  - Planejamento da Gerência de Risco;
  - Identificação dos riscos;
  - Análise qualitativa de riscos;
  - Análise quantitativa de riscos;
  - Desenvolvimento das respostas aos riscos;
  - Controle e monitoração de riscos.

- Gerenciamento de Contratação/Aquisições do Projeto.
  - Planejamento das aquisições;
  - Preparação das aquisições;
  - Obtenção de propostas;
  - Seleção de fornecedores;
  - Administração dos contratos;
  - Encerramento do contrato.

Por ser um esforço integrado, a não execução de processos identificados como necessários de uma área pode trazer conseqüências e comprometer o projeto. Os projetos podem ser divididos em fases ou etapas para oferecer maior facilidade no gerenciamento.

2.2.3 PMBOK

É um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos que inclui práticas tradicionais amplamente aplicadas e práticas inovadoras, por isso, está em constante evolução.

O Guia PMBOK® fornece e promove um vocabulário comum para se discutir, escrever e aplicar o gerenciamento de projetos por todos os profissionais da área. Destina-se a projetos individuais e aos processos de gerenciamento de projetos reconhecidos como boas práticas [PMBOK 2004].

O guia PMBOK terceira edição possui 44 processos distribuídos em nove áreas de conhecimentos.

2.2.4 Grupo de processos de gerenciamento de projetos

Existem cinco grupos de processos que promovem o acompanhamento de um projeto, são eles:

- Iniciação;
- Planejamento;
- Execução;
- Controle;
- Finalização.

Estes grupos são compostos por um ou mais processos [PMBOK 2004].

A figura 2.2 apresenta a interação entre os processos que podem se repetir ao longo do projeto.

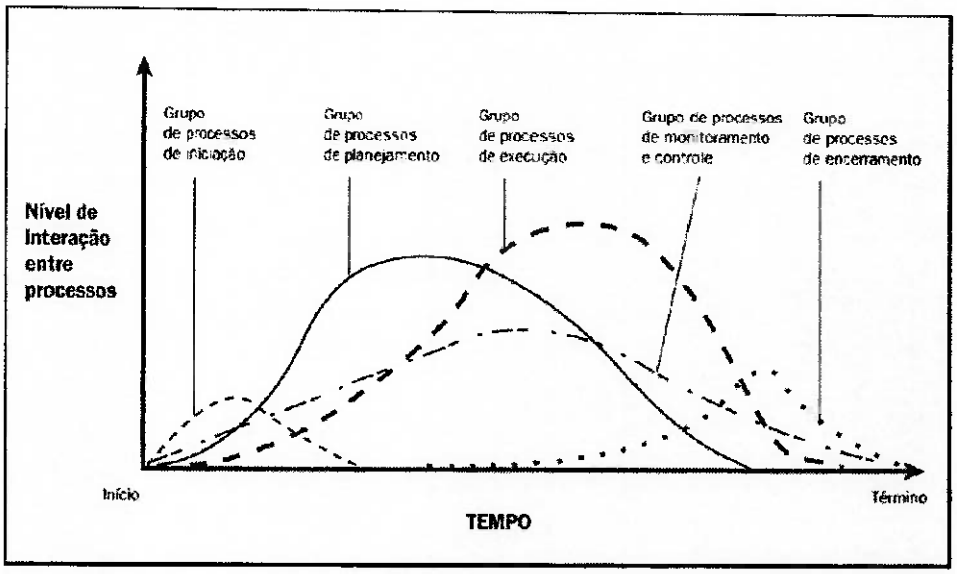

Figura 2.2 Integração de grupos de processos em um projeto [PMBOK 2004]

2.2.5 Ciclo de Vida do Projeto

O ciclo de vida do projeto tem como principal função definir o início e o fim de um projeto.

Os grupos de processos são alimentados pelas realizações dos grupos antecessores que podem ser alterados ao longo do projeto, necessitando assim de uma integração e atualização contínua.

Os processos interagem-se e relacionam-se ligados por suas entradas e saídas. Cada processo possui 3 itens:

- Entradas - são documentos ou itens documentáveis que influenciarão o processo;
- Ferramentas e técnicas - são mecanismos aplicados às entradas para criar as saídas;
- Saídas - são documentos ou itens documentáveis resultantes do processo.

3. RECOMENDAÇÕES DE SEGURANÇA DA INFORMAÇÃO EM GESTÃO DE PROJETOS DE TI

Neste capítulo são apresentadas as recomendações de segurança associadas às áreas de conhecimento da gestão de projetos de TI baseadas no ciclo de vida do projeto.

3.1 Proposição das recomendações de segurança

A segurança da informação deve ser apoiada por uma gestão e por procedimentos apropriados, pois os recursos técnicos são limitados.

As recomendações aqui citadas propiciam que os projetos de TI sejam planejados e desenvolvidos com segurança o que muito provavelmente fornecerá um resultado final mais completo.

3.2 Abordagem de Processos para a Gestão de Segurança da Informação

É aplicado um modelo para estruturar todos os processos de um Sistema de Gestão de Segurança (SGSI), conhecido como "Plan-Do-Check-Act" (PDCA).

1. Plan – Planejar
2. Do – Executar
3. Check – Monitorar e Controlar
4. Act – Manter e Melhorar

A aplicação dos processos de gerenciamento de projetos a um projeto é interativa e muitos processos são repetidos e revisados ao longo da execução do projeto. Os grupos de processos de gerenciamento de projetos têm uma similaridade com a técnica PDCA, pois consiste em várias interações no qual são modificados alguns requisitos e objetivos ao longo do projeto.

3.3 O Gerenciamento Seguro de Projetos de TI

3.3.1 Iniciação

Está contemplado apenas pelo processo da área de conhecimento da Integração do Gerenciamento do Projeto (P.4), e este processo está subdividido em outros dois subprocessos que são:

1. Desenvolver o Termo de Abertura do Projeto (P.4.1);
2. Desenvolver a Declaração do Escopo Preliminar do Projeto (P.4.2).

Aspectos de Segurança Recomendados

Nesta fase do projeto, é importante que seja definido um responsável pela informação.

Recomenda-se que os responsáveis da informação sejam profissionais com alçada superior ou pessoas por eles delegadas, pessoas que sustentam as aplicações de negócios, como tais, são os responsáveis para gerir os riscos associados às informações sob seu controle.

Além disto, eles são responsáveis por gerir os privilégios de acesso, sempre seguindo a lei do menor privilégio, especificar os acessos permitidos e quais as condições necessárias.

Para a segurança da informação, convém dizer que as informações podem ser de diversos tipos, mas para este trabalho serão observadas apenas duas: as transmitidas ou armazenadas. Cada uma exige considerações exclusivas de proteção das informações.

- **Informação transmitida**

  A informação é "transmitida" quando vai de uma pessoa ou entidade para outra. Exemplos de informação transmitida incluem:

  - Informações colocadas em sites da Internet/intranet;
  - Mensagens transmitidas através de redes;
  - E-mail;
  - Correspondência escrita;
  - Correio de voz;
  - Conversa telefônica;

- Reuniões de negócios;
- Apresentações;
- Transmissão de fax/telex;
- Quadros de avisos e quadros brancos.

- **Informação armazenada**

  A informação é "armazenada" quando for mantida para referência em futura ação. Exemplos de informação armazenada incluem:

  - Fitas, discos, bancos de dados, filmes ou microficha;
  - Discos rígidos de computador;
  - Impressas ou escritas;
  - Web sites;
  - LAN/WAN's compartilhados (arquivos de rede e armazenagem).

A necessidade da classificação da informação

Recomenda-se que para a informação escrita, falada ou eletrônica deve existir uma classificação e isto deve ser revelado de acordo com sua exigência de confidencialidade e/ou privacidade. A classificação da informação deve ser revista periodicamente por seu responsável para determinar se a reclassificação é necessária devido à mudança de circunstâncias. Vale lembrar que diferentes organizações utilizam diferentes tipos de classificação, a classificação abaixo foi adotada como sugestão para as colocações que se seguem.

- CONFIDENCIAL;
- PROPRIETÁRIA;
- PÚBLICA.

Investir tempo para ter certeza de que a classificação está correta é muito melhor do que ter que lidar com as conseqüências de falhas nos processos de manuseio, guarda e descarte de informações.

- **Informação Confidencial**

Informação de conhecimento restrito, condicionado à necessidade da função de quem a acessa. A revelação não autorizada da informação confidencial pode causar dano significativo, forte impacto legal, regulador, financeiro ou de percepção pública negativa a empresa, seus clientes, parceiros de negócios ou funcionários.

Recomenda-se ser identificada utilizando a palavra "Confidencial" em destaque na página, tela, formulário ou qualquer outra forma de meios de apresentação. Para identificar mídias que sejam muito pequenas para rotulagem física, a marcação pode ser colocada em um recipiente de armazenagem e a mídia deve ser marcada para associá-la com o recipiente marcado.

- **Informação Proprietária**

Informação restrita à distribuição interna. Sua revelação não autorizada não afetaria significativamente a empresa, seus clientes, parceiros de negócios ou funcionários. Pode ser compartilhada fora da empresa se houver uma necessidade legítima de negócios e com a aprovação da administração. Um contrato de confidencialidade deve ser celebrado quando compartilhada com entidades externas (empresas contratadas).

Recomenda-se ser identificada utilizando a palavra "Proprietária" em destaque na página, tela, formulário ou meios físicos, tanto para documentos eletrônicos quanto não eletrônicos. A correspondência interna, inclusive correio eletrônico, é considerada exclusiva a menos que esteja identificada de outra forma.

- **Informação Pública**

Informação "obtida de" ou "destinada a" revelação pública através de fontes públicas. É de natureza geralmente informativa e é freqüentemente dirigida a clientes ou ao público em geral. Nenhuma identificação é necessária.

- **Transmissão de Informação Confidencial**

  Geral: as informações confidenciais e proprietárias são compartilhadas com terceiros sob acordo contratual de sigilo (Ver Anexo-1) e com a aprovação adequada da administração.

  Informação eletrônica: autenticar positivamente o destinatário antes da transmissão, usando mais que uma senha para informação confidencial e no mínimo uma senha para informação proprietária. Deve-se utilizar criptografia na transmissão da informação confidencial, podendo ser utilizada também para informação proprietária quando apropriado e viável para transmissão em redes públicas, e é recomendada para outros canais de entrega.

  Informação não eletrônica: use embalagem lacrada com dispositivo que evidencie violação para ocultar o conteúdo da comunicação.

- **Armazenagem e retenção de informação Confidencial**

  Informação eletrônica: autenticar positivamente as pessoas solicitando acesso pelo uso de senhas ou autenticação forte, tais como cartões inteligentes ou certificados. A modificação é restrita ao proprietário da informação ou outras partes autorizadas pelo proprietário. Criptografia deve ser usada para informação confidencial e é recomendada para proteção da privacidade. Deve ser feito um backup da informação para facilitar sua recuperação.

  Informação não-eletrônica: Informações confidenciais não devem ser deixadas sem atenção e devem ser guardadas em local com fechadura e chave.

- **Destruição da Informação Confidencial**

  Informação eletrônica: Apague os arquivos dos meios de armazenagem usando ferramentas específicas para garantir que as informações não sejam recuperáveis, mesmo que sejam utilizadas as melhores ferramentas para recuperação de dados.

  Informação não-eletrônica: Os documentos não devem ser descartados em cestos de lixo regular. A destruição dos documentos,

através de um processo especial de descarte, elimina a possibilidade de descartar por engano documentos sensíveis no lixo normal.

Pode haver razões comerciais ou legais para reter ou destruir documentos. Nestas situações, a administração e o departamento jurídico devem ser contatados para determinar se há alguma exigência específica em relação à destruição ou retenção de documentos. Quando necessário, os documentos devem ser colocados diretamente nos cestos de coleta trancados ou devem ser apropriadamente fragmentados.

3.3.2 Planejamento

Pode-se considerar que seja o grupo de processos mais abrangente do ciclo de vida, baseado no modelo do PMBOK, estão contidos nesse grupo de processos, todas as áreas de conhecimento.

1. No Processo de Integração de Gerenciamento de Projetos (P.4), é destacado o processo de Desenvolver o Plano de Gerenciamento do Projeto (P.4.3);
2. No processo de Gerenciamento do Escopo do Projeto (P.5), estão contidos o Planejamento do Escopo (P.5.1), Definição do Escopo (P.5.2) e a Criação da EAP (P.5.3);
3. No processo de Gerenciamento do Tempo do Projeto (P.6), destacam-se os processos de Definição da Atividade (P.6.1), o Seqüenciamento da Atividade (P.6.2), a Estimativa de Recursos da Atividade (P.6.3), a Estimativa de Duração das Atividades (P.6.4) e o Desenvolvimento do Cronograma (P.6.5);
4. No processo de Gerenciamento de Custos do Projeto (P.7), nessa fase, é necessário contemplar a Estimativa de Custos (P.7.1) e a Orçamentação (P.7.2);
5. No processo de Gerenciamento da Qualidade do Projeto (P.8) é desenvolvido o Planejamento da Qualidade (P.8.1);
6. No processo de Gerenciamento de Recursos Humanos do Projeto (P.9), está incluso o Planejamento de Recursos Humanos (P.9.1);

7. No processo de Gerenciamento das Comunicações do Projeto (P.10) é realizado o Planejamento das Comunicações (P.10.1);
8. No Gerenciamento de Riscos do Projeto (P.11), considera-se o Planejamento do Gerenciamento de Riscos (P.11.1), a Identificação de Riscos (P.11.2), a Análise Qualitativa de Riscos (P.11.3), a Análise Quantitativa de Riscos (P.11.4) e o Planejamento de Respostas a Riscos (P.11.5);
9. No Gerenciamento de Aquisições do Projeto (P.12), devemos Planejar Compras e Aquisições (P.12.1) e Planejar Contratações (P.12.2).

Aspectos de Segurança Recomendados

Nessa fase do projeto, dependendo da classificação designada, convém que as preocupações com a confidencialidade das informações geradas passem a ter uma atenção especial. Por exemplo, se o assunto envolvido no projeto é um lançamento de um novo produto ou uma estratégia de marketing, essa informação, estará classificada como confidencial durante o ciclo de vida do projeto, mesmo que posteriormente ela seja reclassificada como pública e seus controles passem a ser mais flexíveis.

Nessa etapa, convém que as políticas de segurança envolvidas estejam devidamente identificadas e que todos os participantes do projeto tenham consciência do impacto do não cumprimento das mesmas.

As políticas de segurança podem ser denominadas de diversas formas, nesse trabalho adota-se como denominação as Diretrizes, Normas e Procedimentos, e sugere-se o direcionamento de cada uma delas para públicos distintos e atuações em diferentes níveis hierárquicos.

- Diretrizes estão no nível estratégico de decisão da empresa;
- Normas estão no nível tático;
- Procedimentos são considerados no nível operacional.

Na definição do escopo do projeto recomendam-se alguns controles que impactam a segurança dos projetos de TI, como por exemplo:

- Controles Operacionais;

  - Acesso a dados de funcionários, clientes e fornecedores;
  - Interfaces necessárias com sistemas existentes;
  - Configuração das tecnologias de segurança envolvidas;
  - Necessidade de VPN's.
- Segurança Física;
- Segurança em Ambientes Computacionais.

Esses controles podem demandar a contratação de empresas especializadas e com isso impactar vários processos desta fase. Esses controles são identificados através de uma avaliação de riscos sobre o escopo do projeto, a fim de mensurar as ameaças envolvidas e as vulnerabilidades que este projeto está exposto.

A gestão de riscos é parte de processos mais ampla de gestão das organizações. A gestão de riscos depende do contexto no qual é utilizada. Destacam-se a seguir algumas normas e padrões para a Gestão de Riscos: Seguem algumas definições segundo o ABNT ISO/IEC Guia 73:2005:

- **Risco** é a combinação da probabilidade de um evento e de suas conseqüências.
- **Probabilidade** é o grau de possibilidade de que um evento ocorra;
- **Evento** é a ocorrência de um conjunto específico de circunstâncias.
- **Conseqüência** é o resultado de um evento.

O Guia 73:2005 da ABNT ISO/IEC especifica que a gestão de riscos de segurança pode ser dividida em quatro fases:

1. Análise/Avaliação de riscos;
2. Tratamento do risco;
3. Aceitação do risco;
4. Comunicação do risco.

A AS/NZS 4360 é uma Norma Australiana / Neozelandesa para gerenciamento de riscos. É uma norma genérica que fornece orientações para gerenciamento de riscos de qualquer natureza. Sua principal característica é avaliar,

considerando-se tanto os riscos com resultados positivos (ganhos potenciais), quanto os riscos com resultados negativos (perdas potenciais), fornecendo uma visão única do gerenciamento de riscos.

As principais etapas do processo de gestão de riscos, segundo a AS/NZS 4360 são:

1. Comunicação e consulta;
2. Estabelecimento dos contextos;
3. Identificação do risco;
4. Análise de riscos;
5. Avaliação de riscos;
6. Tratamento de riscos;
7. Monitoramento e análise crítica.

A figura abaixo apresenta o percentual de empresas que realizam análise de riscos na área de TI e a freqüência que ela ocorre.

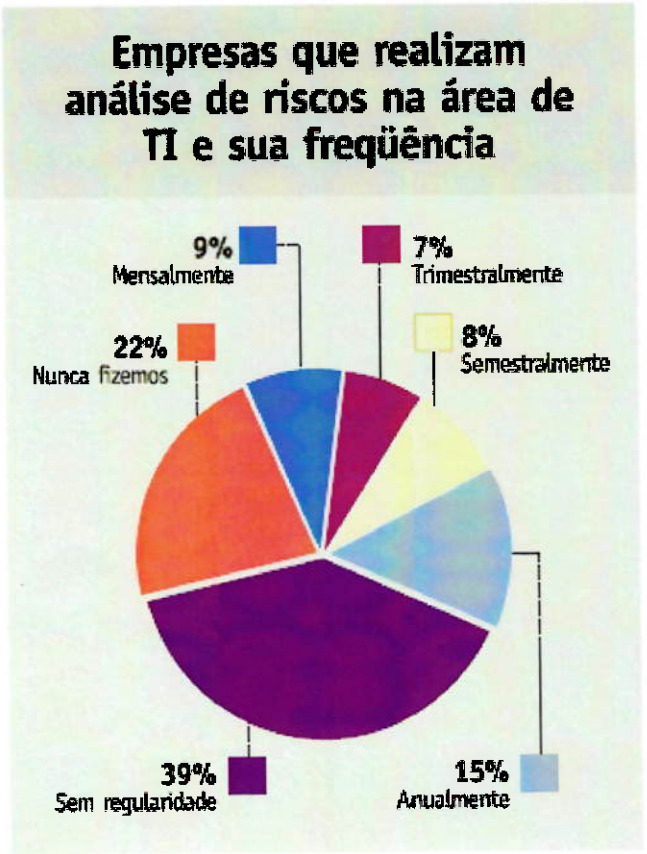

Figura 3.1: Empresas que realizam análise de riscos na área de TI e sua freqüência
10ª Pesquisa Nacional de Segurança da Informação – Módulo Security Solutions, 2007.

Para que a avaliação do risco de segurança da informação seja realizada é recomendada a utilização de uma metodologia de análise de riscos para possibilitar o cálculo do índice de risco. Essa metodologia deve atender as necessidades da organização e estar em conformidade com as normas internacionais de gestão de riscos e segurança da informação.

A figura 3.2 destaca o percentual de empresas que possuem metodologia para a análise de riscos.

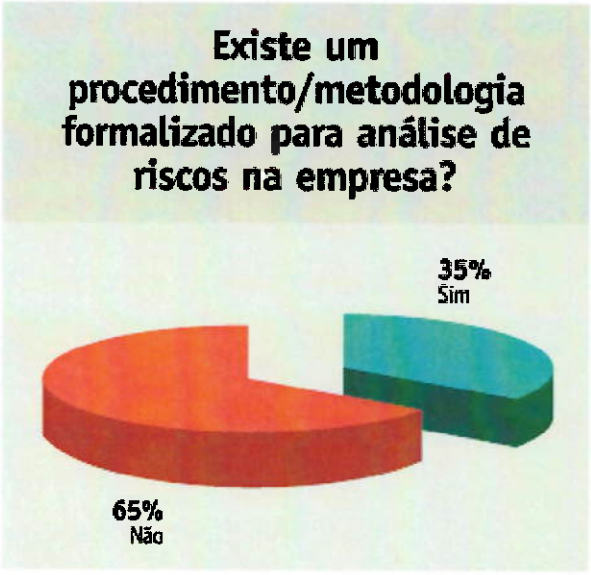

Figura 3.2: Empresas que possuem procedimento/metodologia formalizado para análise de riscos

10ª Pesquisa Nacional de Segurança da Informação – Módulo Security Solutions, 2007.

A análise de riscos visa identificar as vulnerabilidades nos elementos tecnológicos, processuais, físicos e comportamentais da organização.
Vale ressaltar que as vulnerabilidades identificadas na análise de riscos devem ser pontuadas com relação à probabilidade de ocorrência e relevância para o negócio.

No gerenciamento de aquisições do projeto, é recomendado que a área responsável pelo processo estabeleça mecanismos para analisar se os

fornecedores atendem os requisitos mínimos de segurança da empresa. Recomenda-se elaborar uma análise formal deste fornecedor.
É recomendado que todos os fornecedores homologados pela empresa que tenham contrato vigente tenham completado o processo de avaliação de segurança de seus processos, pessoas e ambiente tecnológico.

A idéia principal é que quando o projeto entrar nos processos de execução, toda avaliação de riscos esteja realizada, pois as recomendações de controles interferem diretamente na execução do projeto.

3.3.3 Execução

Nessa fase estão envolvidos os processos relacionados abaixo:

1. Gerenciamento de Integração do Projeto (P.4), com o objetivo de Orientar e Gerenciar a Execução do Projeto (P.4.4);
2. Gerenciamento da Qualidade do Projeto (P.8) para Realizar a Garantia da Qualidade (P.8.2);
3. Gerenciamento de Recursos Humanos do Projeto (P.9) para Contratar ou Mobilizar a Equipe do Projeto (P.9.2) e Desenvolver a Equipe do Projeto (P.9.3);
4. Gerenciamento das Comunicações do Projeto (P.10) a fim de viabilizar a Distribuição das Informações (P.10.2);
5. Gerenciamento de Aquisições do Projeto (P.12) com o intuito de Solicitar Respostas de Fornecedores (P.12.3) e Selecionar Fornecedores (P.12.4).

Aspectos de Segurança Recomendados

Segundo a [NBR ISO/IEC 17799:2001], para a o gerenciamento de recursos humanos vale ressaltar a importância da existência de controles para reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações.
Recomenda-se que todos os funcionários e prestadores de serviço envolvidos em projetos confidenciais assinem um acordo de sigilo. Um modelo deste acordo pode ser visto no Anexo-1.

A contratação de um profissional para atuar em atividades com informações sensíveis requer uma análise mais apurada.

Alguns aspectos de segurança a serem considerados na seleção do candidato:

1. Verificação da exatidão das informações apresentadas pelo candidato;
2. Confirmação das qualificações acadêmicas e profissionais;
3. Verificação da idoneidade de crédito, essa verificação pode ter uma periodicidade pré-estabelecida;
4. Antecedentes criminais.

Após a contratação, através de treinamentos, a pessoa deve ser conscientizada das ameaças e das preocupações de segurança da informação relevantes para o projeto, isso minimizará a ocorrência de incidentes.

No gerenciamento das comunicações, o meio mais utilizado nas empresas é o correio eletrônico, e este está sujeito a algumas vulnerabilidades, por isso, a [NBR ISO/IEC 17799:2001] recomenda que exista uma política de uso do correio eletrônico, incluindo:

1. Como proteger anexos de correio eletrônico;
2. Orientações de quando não se deve utilizar o correio eletrônico;
3. Informar sobre o correto uso do correio eletrônico para não comprometer a organização;
4. Utilização de criptografia para proteger informações sensíveis enviadas por esse meio.

As comunicações de um projeto precisam estar protegidas contra a divulgação indevida. As pessoas privilegiadas com informação sensível devem se precaver para evitar a sua divulgação através de conversas em locais inadequados ou para pessoas não autorizadas, evitando assim que o projeto seja comprometido estrategicamente pelo vazamento de informações privilegiadas. Esse tipo de informação não deve ser objeto de recados e deve ser transmitida apenas a pessoas previamente autorizadas.

No gerenciamento de aquisições do projeto, a avaliação de fornecedores permite analisar os procedimentos de segurança adotados pelo fornecedor que

estará envolvido na geração, processamento ou guarda das informações do projeto.

O envolvimento de um fornecedor no projeto pode gerar um aumento do grau de exposição, por isso, recomenda-se que os riscos deste fornecedor sejam identificados e os controles adequados sejam acordados e incluídos no acordo de serviço.

O Anexo-2 sugere um modelo inicial para avaliação de aspectos de segurança em ambientes de fornecedores.

Após o processo de análise dos aspectos de segurança do fornecedor ser concluído, deve ser elaborado um relatório com resumo executivo e recomendações de controles de segurança para que o gestor do projeto tenha ciência das vulnerabilidades que este fornecedor está exposto. Conseqüentemente, os riscos que ele pode trazer para o projeto ou até mesmo para a empresa.

3.3.4 Monitoramento e Controle

Nesses processos estão envolvidos os processos de:

1. Gerenciamento da Integração do Projeto (P.4) com o objetivo de Monitorar e Controlar o Trabalho do Projeto (P.4.5) e realizar o Controle Integrado de Mudanças (P.4.6);
2. Gerenciamento do Escopo do Projeto (P.5) é envolvido na Verificação do Escopo (P.5.4) e no Controle do Escopo (P.5.5);
3. Gerenciamento do Tempo do Projeto (P.6) é responsável pelo Controle do Cronograma (P.6.6);
4. Gerenciamento de Custos do Projeto (P.7) realiza o Controle dos Custos (P.7.3);
5. Gerenciamento da Qualidade do Projeto (P.8) é incumbido de Realizar o Controle da Qualidade (P.8.3);
6. Gerenciamento de Recursos Humanos do Projeto (P.9) tem como objetivo nessa fase, Gerenciar a Equipe do Projeto (P.9.4);
7. Gerenciamento das Comunicações do Projeto (P.10) desenvolve o Relatório de Desempenho (P.10.3) e é responsável também por Gerenciar as Partes Interessadas (P.10.4);

8. Gerenciamento de Riscos do Projeto (P.11) faz o Monitoramento e Controle de Riscos (P.11.6);
9. Gerenciamento de Aquisições do Projeto (P.12) realiza a Administração de Contrato (P.12.5).

Aspectos de Segurança Recomendados

É recomendada a monitoração sobre os recursos de processamento de informação. Essa monitoração tem como objetivo averiguar se as atividades são executadas por pessoas devidamente autorizadas e apurar se existe algum desvio de comportamento que pode indiciar a ocorrência de atos ilícitos.
Este procedimento permite averiguar se os controles adotados estão adequadamente implementados.

A Norma [NBR ISO/IEC 17799:2001] enfatiza que os desvios de comportamento de funcionários e terceiros podem levar a fraudes, roubos e erros que podem comprometer a segurança do projeto.
Todos os incidentes de segurança devem ser monitorados e reportados tempestivamente através de meios apropriados. Um procedimento de resposta a incidentes deve apoiar a tomada de decisão sobre a ação a ser tomada ao se receber a notificação.

Quando necessária alguma ação disciplinar ou averiguação de fatos, o monitoramento das trocas de e-mails pode ser utilizado como evidência. Recomenda-se que as empresas que realizam a monitoração de suas comunicações, através do correio eletrônico ou outro meio, notifiquem os envolvidos previamente do procedimento. Essa notificação pode ocorrer através do código de ética da empresa ou através de um simples memorando ou e-mail.

3.3.5 Encerramento

Neste grupo de processos, apenas dois Gerenciamentos são envolvidos:

1. Gerenciamento da Integração do Projeto (P.4) responsável por Encerrar o Projeto (P.4.7);
2. Gerenciamento de Aquisições do Projeto (P.12) que faz o Encerramento do Contrato.

Aspectos de Segurança Recomendados

Recomenda-se a revisão de todos os acessos concedidos durante o processo de desenvolvimento do projeto para que, nenhum envolvido permaneça com os acessos que nessa fase podem ser considerados como desnecessários, atenção especial deve ser dedicada aos fornecedores que possuem acessos remotos.

A documentação gerada durante o ciclo de vida do projeto deve ser reclassificada e armazenada no repositório conforme sua nova classificação de confidencialidade.

4 CONSIDERAÇÕES FINAIS

4.1 Quanto ao cumprimento dos objetivos

A proposta deste trabalho foi baseada na geração de recomendações de segurança da informação que pudessem apoiar os gerentes de projetos, direcionando aspectos de segurança que podem fazer a diferença no resultado final.

Com esse trabalho, o gerente de projetos identifica as principais necessidades a serem avaliadas para que a condução do projeto possa ser realizada com mais efetividade e segurança. Esta proposta foi alcançada através das recomendações de boas práticas citadas em todas as fases do ciclo de vida do projeto.

4.2 Quanto ao desenvolvimento e dificuldades encontradas

Inicialmente a idéia do trabalho foi desenvolver recomendações baseadas nas nove áreas de conhecimento do PMBOK, porém, durante o desenvolvimento houve grande dificuldade em associar as recomendações, pois nas normas de segurança analisadas, são existem controles associados formalmente e sua aplicabilidade nem sempre é evidente.

Por este motivo, o trabalho foi replanejado para que as recomendações fossem associadas ao ciclo de vida do projeto, possibilitando uma abrangência geral das recomendações. É importante citar que a associação foi baseada principalmente na experiência de necessidades de trabalhos realizados nessa área.

4.3 Conclusões

Embora não exista associação formal entre os processos de segurança da informação e os processos de gestão de projetos, pode-se identificar que na prática eles estão relacionados e podem interferir no resultado final do projeto. Essa interferência pode ser identificada no comprometimento dos custos, prazos e na confiabilidade do produto ou serviço gerado pelo projeto.

Este trabalho possui recomendações de segurança aplicadas à gestão de projetos que auxiliam na identificação dos riscos envolvidos em cada processo do ciclo de vida do projeto.

Incidentes de segurança podem comprometer um projeto e permitir que o mercado conheça as estratégias de negócios da organização, podendo gerar como conseqüências: prejuízos financeiros, comprometimento da imagem da organização e perda de competitividade.

O uso do guia PMBOK visa melhores resultados, aplicação de lições aprendidas em outros projetos e compartilhamento de técnicas e habilidades para atingir as expectativas dos stakeholders.

Podemos dizer que a vantagem competitiva se fortalece com a associação dos aspectos de segurança aos projetos de TI, promovendo a confiabilidade dos processos e apoiando a tomada de decisão, permitindo que as ações sejam preventivas e não reativas.

Proteger as informações contra ameaças e vulnerabilidades, minimizar riscos, garantir a continuidade dos negócios e maximizar o retorno sobre os investimentos é a expectativa das organizações e prover projetos seguros é o meio adequado para que essa necessidade seja atendida.

4.4 Trabalhos futuros

Esse trabalho explora recomendações de segurança nos níveis estratégico e tático para todas as fases do ciclo de vida do projeto, porém, algumas áreas de conhecimento não foram abordadas neste contexto. Por esse motivo, é possível sugerir sua continuidade visando dois focos diferentes:

- Pesquisa de recomendações de Segurança no nível operacional;
- Pesquisa de recomendações de segurança em áreas específicas de conhecimento do PMBOK.

REFERÊNCIAS BIBLIOGRÁFICAS

[ABNT NBR ISO/IEC Guia 73:2005] Gestão de Riscos – Vocabulário – Recomendações para uso em normas, 2005, ABNT – Associação Brasileira de Normas Técnicas.

[ABNT NBR ISO/IEC 15408-1:1999 (E)] Information Technology – Security Techniques – Evaluation Criteria for IT Security - 1999, ABNT – Associação Brasileira de Normas Técnicas.

[ABNT NBR ISO/IEC 17799:2001] Tecnologia da Informação, Código de prática para a gestão da segurança da informação, 2003, ABNT – Associação Brasileira de Normas Técnicas.

[ABNT NBR ISO/IEC 27001:2006] Tecnologia da Informação, Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos, 2006, ABNT – Associação Brasileira de Normas Técnicas.

[Dinsmore e Cavalieri 2003] Dinsmore, C. e Cavalieri, A.; (2003). Como se Tornar um Profissional em Gerenciamento de Projetos: Livro-Base de "Preparação para Certificação PMP - Project Management Professional". Rio de Janeiro. QualityMark.

[Kerzner 2001] Kerzner, H.; (2001). Project Management – A Systems Approach to Planning, Scheduling, and Controlling, New York NY, John Willey & Sons.

[Koontz e O'Donnel 1980] Koontz, H. e O'Donnel,C; (1980). Os Princípios de Administração: Uma Análise das Funções Administrativas. São Paulo, Pioneira.

[PMBOK 2004] PMI Standard Comitee, "Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos (Guia PMBOK®), 2004, Project Management Institute, Global Stantdard, Terceira Edição.

BIBLIOGRAFIA DA INTERNET

2004/2005 Instituto Aprender Mais .- Acessado em 31/05/2007.
http://www.aprendermais.com.br/pos/cdesta_gestaoprojetos.php

9º e 10ª Pesquisa Nacional de Segurança da Informação
Módulo Security Solutions - Acessada em 04/12/2007
www.modulo.com.br

Associação Brasileira de Normas Técnicas - Acessada em 05/06/2007
http://www.abnt.com.br/default.asp?resolucao=1024X768

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - Acessado em 27/11/2007
http://www.cert.br e http://cartilha.cert.br

Comitê Gestor da Internet no Brasil - Acessado em 05/06/2007
http://www.cgi.br/

Estudo de Benchmarking em Gestão de Projetos, PMI-RIO, 2003
International Institute for Learning IIL-Brasil - Acessada em 06/06/2007
http://www.iil.com.br/

PMI 2004 PROJECT MANAGEMENT INSTITUTE – PMI. - Acessado em 31/05/2007.
http://www.pmi.org.

BIBLIOGRAFIA ADICIONAL

[ABNT/NBR 6023:2000] – Elaboração de Referências

[ABNT/NBR 6027:2003] – Informação e Documentação – Sumário - Apresentação

[ABNT/NBR 6034:2004] - Informação e Documentação – Índice – Apresentação

[ABNT/NBR 10520:2002] – Apresentação de Citações em Documentos

[ABNT/NBR 14724:2002] - Apresentação de Trabalhos Acadêmicos

[ABNT/NBR 15287:2006] – Informação e Documentação – Projeto de Pesquisa – Apresentação

Ricardo Albuquerque / Bruno Ribeiro – 2002
Segurança no Desenvolvimento de Software – Como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15408.

Kenneth C. Laudon / Jane P. Laudon – 2004
Sistemas de Informações Gerenciais – Administrando a Empresa Digital. 5ª Edição.

Gilbert Probst / Steffen Raub / Kai Romhardt – 2002
Gestão do Conhecimento – Os elementos construtivos do sucesso.

GLOSSÁRIO

Avaliação de risco

Avaliação das ameaças, impactos e vulnerabilidades da informação e das instalações de processamento da informação e da probabilidade de sua ocorrência.

Correio de Voz

Correio de voz (ou voice mail, vmail ou VMS) é um sistema centralizado de gerenciamento de mensagens telefônicas para um grande número de pessoas. Em sua forma mais simples, ele reproduz o funcionamento de uma secretária eletrônica, utiliza um monofone padrão como interface do utilizador e usa um sistema centralizado, computadorizado, em vez de um dispositivo num telefone individual.

Criptografia

Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

E-mail

E-mail, correio-e, ou correio eletrônico, ou ainda e-mail é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação.

Firewall

Dispositivo constituído pela combinação de *software* e *hardware*, utilizado para dividir e controlar o acesso entre redes de computadores.

Gerenciamento de risco

Processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável.

Hardware

O hardware, material ou ferramental é a parte física do computador, ou seja, é o conjunto de componentes eletrônicos, circuitos integrados e placas, que se comunicam através de barramentos.

Incidente

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

Internet

A Internet é um conglomerado de redes em escala mundial de milhões de computadores interligados pelo Protocolo de Internet que permite o acesso a informações e todo tipo de transferência de dados.

Intranet

Uma intranet é uma rede de computadores privada que assenta sobre a suíte de protocolos da Internet.

Normas Técnicas

Uma norma técnica é um documento, normalmente emitido por um órgão oficialmente reconhecido para tal, que estabelece diretrizes e restrições à elaboração de uma atividade ou produto técnico.

Política de Segurança

A política de segurança atribui direitos e responsabilidades às pessoas que lidam com os recursos computacionais de uma instituição e com as informações neles armazenados. Ela também define as atribuições de cada um em relação à segurança dos recursos com os quais trabalham.

Segurança da Informação

Segurança de Informação está relacionada com métodos de proteção aplicados sobre um conjunto de dados no sentido de preservar o valor que possui para um indivíduo ou uma organização.

Senha

Conjunto de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser.

Software

Software ou programa de computador é uma sequência de instruções a serem seguidas e/ou executadas, na manipulação, redirecionamento ou modificação de um dado/informação ou acontecimento.

TI

Sigla que significa Tecnologia da informação. Aqui é citado como sendo o tipo de projeto a ser desenvolvido. Pode englobar apenas uma análise de viabilidade ou o desenvolvimento e/ou manutenção de um aplicativo ou sistema.

Usuário

Pessoa que opera um microcomputador, que tem acesso á informações da empresa através e que faz parte do escopo deste projeto.

Vulnerabilidade

Falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

ANEXOS

ANEXO 1 – Acordo de Sigilo

Manter sigilo a respeito de todas as informações a que tiver acesso em decorrência deste contrato:

1. Se a **CONTRATADA**, por determinação de autoridade pública ou em decorrência de ordem judicial, tiver que revelar qualquer das informações sigilosas, procederá como segue:

    a) Imediatamente dará notícia à **CONTRATANTE** a respeito da ordem da autoridade pública ou do juiz;

    b) Prestará todas as informações e subsídios que possam ser necessários para que a **CONTRATANTE** possa defender-se contra a divulgação de qualquer informação sigilosa.

2. É vedada a utilização das informações sigilosas para qualquer outro fim que não:

    (a) A execução normal deste contrato previamente assinado;

    (b) A manutenção de registros e arquivos exigidos pela legislação.

Qualquer que seja a causa de dissolução deste contrato, a **CONTRATADA**:

1. Restituirá à **CONTRATANTE**, apagará ou destruirá todos os documentos referentes às informações sigilosas;
2. Continuará obrigada por si, seus empregados, prepostos ou representantes a respeitar o dever de sigilo;
3. O pagamento de indenização não desobriga a **CONTRATADA**, seus empregados, prepostos ou representantes de continuarem cumprindo, no que cabível, o dever de sigilo.

ANEXO 2 - Documento para Avaliação de Segurança no Ambiente de Fornecedores

VISÃO GERAL DO PROJETO

Gerente do Projeto:

Responsável pelos Dados:

Responsável pela Área de Negócios:

Sistema

Nome do Sistema:

Propósito do sistema:

Serviço provido pelo Fornecedor:

Qual a Classificação da Informação:

☐ **Confidencial** ☐ **Proprietária** ☐ **Pública**

INFORMAÇÕES DO FORNECEDOR

Data de Término do Contrato:

Nome do Fornecedor:

Localização do Fornecedor:

Responsável pelo preenchimento:

Telefone para contato:

Função do responsável:

AMBIENTE DO FORNECEDOR

Controles Gerais do Ambiente

1) Existe um analista de segurança na equipe de funcionários?
2) São realizadas analises periódicas das funções dos empregados?
3) São publicados padrões e políticas de segurança?
4) Existe um documento que estabeleça um programa de Controle de Resposta de Incidentes de Informática?

5) Neste documento estão incluídos os procedimentos de notificação e escalonamento para os clientes em caso de um evento de segurança?
6) Existe um documento que estabeleça um Programa de Controle de Mudanças?
7) Os dados de produção são usados nos ambientes de teste?
8) Os ambientes de desenvolvimento, teste e produção são segregados?
9) Recentemente foi realizado algum teste de vulnerabilidade por alguma empresa reconhecida? (ex: avaliação de vulnerabilidade e penetration test)?
   - Em caso afirmativo, o resultado poderia ser compartilhado com o contratante? Neste caso, providenciar uma cópia.
   - Em caso negativo, é de consentimento passar por um teste de vulnerabilidade no ambiente?
10) Qual a freqüência de execução dos testes de vulnerabilidade?
11) Existe um Departamento de Auditoria Interno?
12) Como os dados da contratante serão protegidos pelas equipes da empresa (ex: empregados e contratados) para as pessoas que não devem ter conhecimento destas informações?
13) Existe uma segregação de deveres para empregados com acessos privilegiados?
14) Como são os controles de acesso físico ao(s) data(s) center(s) e salas de computadores?
15) Os empregados são treinados a questionar visitantes que não são acompanhados ao data center?