UNA
CURSO DE PÓS-GRADUAÇÃO EM GESTÃO DE PROJETOS

Projeto de Implantação de Segurança da Informação

Lydia Alvarenga de Figueiredo

Belo Horizonte 2º semestre/2009

Orientador: Marcus Augusto Silva – Centro Universitário UNA

Melhores práticas, políticas e normas para implantação de segurança da informação no DER/MG

Lydia Alvarenga de Figueiredo – Centro Universitário UNA
Orientador: Marcus Augusto Silva – Centro Universitário UNA
Data: 2º semestre/2009

RESUMO

Este artigo tem como objetivo mostrar como as melhores práticas em gestão de Projetos, políticas e normas de segurança podem minimizar impactos, riscos e auxiliar para se alcançar melhores resultados na implantação de um projeto de segurança nas organizações. Atualmente, a Segurança da Informação é uma ferramenta essencial para alcance do sucesso nos negócios de toda organização. Gerir ativos, informações, recursos e usuários, de forma confiável e íntegra, estruturada e sustentável é o grande desafio dos profissionais dessa área. Independente do tamanho da empresa há uma grande preocupação e uma maior atenção para a questão da segurança das informações e tecnologia da informação e comunicação. A segurança visa também aumentar a produtividade dos usuários através de um ambiente mais organizado, com maior controle sobre os recursos de informática e finalmente, viabilizar aplicações críticas das empresas. Implementar um projeto de segurança em uma organização, apesar de necessário é uma tarefa árdua e difícil e para isto é preciso contar com o apoio da alta gerência, com um comitê de segurança bem estruturado e com a colaboração de todos envolvidos neste projeto, isto é um item essencial para se alcançar os objetivos esperados. Agregar conhecimento e melhores práticas em gestão de projetos e pessoas, baseadas em metodologias normas e políticas de segurança, podem também contribuir para o sucesso de um projeto de segurança da informação em uma organização.

Palavras Chaves – Tecnologia da Informação e Comunicação, integração, normas, políticas de segurança.

ABSTRACT

This article as a objective show how best practices for managing the projects to minimize impacts of the deployment in organizations using the best practices for managing projects to minimize risk and achieve better results. Today, Information Security is an essential tool to achieve success in the business of an entire organization. Manage assets, information, resources and users, so reliable and full, structured and sustainable is the great challenge for professionals in the area. Regardless of company size is a major concern and greater attention to the issue of security of information and TIC. The more each day the process has changed and organizations have been concerned to have a security policy to ensure your information. Security is also intended to increase the productivity of users through a more organized, more control over the resources of the computer and finally, enable critical applications businesses. Great is the need to ensure the assets of IT (Information Technology), but also great are the difficulties of implementing projects in security organizations because it reflects in controls, restrictions on access, investment and for this there must be change of culture and membership and involvement users and managers to process safety. This article aims to show

how the best practices of project management and people, based on methods of management in projects and policies can contribute to a good project on IT security and minimize risks and impacts in this deployment.

Keys Works – Information Technology, integration, methods, policies de security

INTRODUÇÃO

No mundo de hoje, as informações se tornam a cada dia mais complexas e com o decorrer do tempo e da evolução tecnológica altamente insegura, sem confiabilidade, vulneráveis e com grande risco de acesso.

Com o surgimento das redes de computadores o comércio eletrônico e a necessidade da transparência das informações nos serviços públicos, houve uma maior atenção para a questão da segurança das informações, tecnologia e comunicação. De início, esta preocupação era ainda muito pequena, porém, com o passar do tempo este processo tem mudado e as organizações e pessoas tem se preocupado em assegurar suas informações tanto organizacional como pessoal. (Security officer 2006) A segurança da informação, torna-se cada vez mais necessária levando empresas, executivos e inclusive pessoas físicas a obterem conhecimentos de no mínimo conceitos básicos de segurança de TIC (tecnologia, informação e comunicação). Esta proteção é desejada por uma razão simples, evitar e minimizar prejuízos. O problema de segurança da informação afeta vários pontos da organização e alguns problemas mais visíveis são priorizados, como furtos de computadores, como vírus que geram perda de produtividade, porém o fato atualmente é que os incidentes têm ocorrido com maior freqüência, e com isto a grande preocupação das organizações em proteger seus ativos.

O propósito deste artigo é mostrar a melhor maneira de alinhar processos, políticas e normas, usando as melhores praticas de projetos para se conseguir fazer um projeto que vise à implantação de segurança de TIC com sucesso no DER/MG. Também visa mostrar a melhor maneira de implantar políticas e normas de seguranças da informação, leis e requisitos legais.

Este artigo deverá dar a visão da melhor maneira de integrar a alta gerência a participar do projeto de segurança de TIC, como comunicar, informar o usuário e motivá-lo a ser parceiro da implementação da segurança da informação no DER/MG, com foco na importância deste projeto de segurança para o órgão e sua integração com as estratégias da empresa. Mostrar como, o bom gerente de TI (tecnologia da informação) deve estar alinhado com as necessidades e com todo o projeto, buscando usar as melhores práticas de projeto para conseguir sucesso. Medir o grau da necessidade dos usuários (satakeholders) em relação a proteção das informações e dos sistemas e das tecnologias a serem usadas para conseguir os resultados esperados, bem como, a equipe de gerentes de TIC, deve estar alinhada e comprometida com as práticas de gestão. Como as melhores práticas podem auxiliar na questão da resistência coletiva que existe dentro das organizações para com as medidas de segurança da informação.

Foram usadas neste artigo as metodologias: de pesquisa exploratória, sendo a observação informal, comportamento e fatos de interesse para o problema em estudo. Metodologia documental realizada em documentos conservados no interior do DER/MG como: normas e portarias e a Metodologia bibliográfica com base em material publicado revista, livros etc.. As metodologias serão aplicadas ao DER/MG, onde há necessidade de implantar uma política de segurança interna do órgão e a política do Estado de Minas Gerais como estipula a Resolução Conjunta Nº016, de 17 de junho de 2008. Foi verificado através de entrevista com os usuários a falta de informação e de conscientização sobre segurança da

informação, o que torna-se um grande problema para a implantar um projeto de segurança no órgão. Foi observado também o pouco envolvimento da alta administração no processo de implantação de uma política de segurança, além da dificuldade de se criar um comitê de segurança, fazendo com que os gerentes de segurança tenham um enorme problema de resistência para implantar uma política que vise segurança. Também foi verificada a ausência da cultura em gestão de projeto no órgão que é outro problema a se enfrentar. Pouca comunicação, entre as equipe e os usuários envolvidos no processo, faz com que as informações não fluam de maneira segura e com clareza, trazendo a falta de comprometimento dos envolvidos no projeto dificultando ainda mais a implantação de um projeto de segurança.

O impacto da falta de um projeto que visa segurança da informação para o DER/MG, faz com que os usuários destas informações, sintam inseguros quanto à confiabilidade, vulnerabilidade e integridade das informações que trafegam na rede do DER/MG, o que, afeta não só aos usuários internos, mas também aos externos e ao Governo como o responsável pelas informações.

A solução que se busca para o DER/MG, é implantar um projeto de segurança no DER/MG contando com as melhores práticas de projeto, com o guia de melhores práticas de projetos PMBOK (Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos), políticas e normas para se alcançar o sucesso.

1. REFERENCIAL TEÓRICO

1.1 Seguranças da Informação

Informação representa a inteligência competitiva dos negócios, é um ativo crítico que deve ser cuidado porque equivale a desempenho de toda a empresa. Toda a segurança da informação deve ter objetivos alinhados com os objetivos estratégicos da empresa, pois este alinhamento permite sustentar riscos e implementar as políticas de segurança. (Security Officer, 2006).

Dentro de uma organização, a segurança costuma se aplicar a tudo aquilo que possui valor e, conseqüentemente demanda de proteção, são os ativos da organização. (Security Officer, 2006) São vários os ativos de uma empresa como os Ativos tangíveis - informações impressas ou digitais, impressoras móveis de escritório, sistemas; os Ativos intangíveis - imagens de uma empresa, confiabilidade de um órgão, marca de um produto; os Ativos Lógicos - Dados armazenados, sistema de ERP, rede; Ativos Físicos - Estação de trabalho, servidores, etc. e os Ativos Humanos, Empregados prestadores de serviços; Atualmente a informação é um dos ATIVO mais valioso que uma empresa pode ter. (COBIT 4.1) As proteções são as medidas para fornecer segurança a estes ativos.

A segurança da informação é importante para os negócios, tanto do setor público como do setor privado para proteger as infra-estruturas críticas. Em ambos os setores, a função da segurança da informação, é viabilizar os negócios como governo eletrônico (e-gov), ou o comercio eletrônico (e-business), assegurar a transparência da informação e evitar ou reduzir os riscos relevantes. Os princípios básicos e os objetivos da política de segurança da informação são a Integridade da informação que é a condição na qual a informação ou os recursos da informação, são protegidos contra modificações não autorizadas, envolve proteger as informações contra alterações em seu estado original; a confidencialidade da informação significa garantir que apenas as pessoas que devem ter conhecimento a seu respeito poderão

acessá-las; a disponibilidade que se relaciona diretamente a possibilidade de acesso, por parte daqueles que a necessitam para o desempenho de suas atividades; e a legalidade da informação que é um estado legal da informação, em conformidade com os preceitos da legislação em vigor. Preocupações com esta segurança da informação visam reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer estes princípios básicos. (Security Officer, 2006)

Segurança da informação como diz a norma ABNT NBR ISSO/IEC 17799:2005 –

"é a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco do negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio".

A segurança da informação deve ser obtida a partir da implementação de um conjunto de controles adequados incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados onde necessário para garantir os objetivos do negócio e de segurança da organização. (Vieira, 2005)

1.2 Normas /Políticas de Segurança da Informação

Normas são padrões definidos, para assegurar a segurança das informações e de praticas efetivas de segurança da informação. (ISSO/IEC 27001:2005)

Políticas e Normas devem ser seguidas, como quebra de resistência na implantação de um projeto de segurança da informação e tecnologia em uma empresa. Apesar da maioria do corpo executivo das empresas estarem conscientes da necessidade da criação e cumprimento de uma Política de Segurança da Informação, faz-se necessário um esforço grande para que as Unidades de Segurança possam lançar mão dos recursos necessários para esta criação e manutenção.

A política de segurança da informação é a formalização explícita de quais ações serão realizadas em um sentido único de garantir a segurança e disponibilidade das informações, esta política é de extrema importância, uma vez que, descreve as regras necessárias para o uso seguro das informações e é por meio delas que a estratégia de SI é montada e passada para todas as áreas envolvidas.(Security Officer, 2006)

Hoje nos órgãos públicos, além das próprias políticas de segurança (políticas internas) ainda seguimos as políticas que a lei exige**, s**e a legislação exige um controle, a sua implementação não está aberta a questionamento.

1.3 Necessidades da Política da Segurança da Informação

Políticas de segurança da Informação devem atender algumas necessidades básicas para ser útil no processo de segurança da informação como: Identificar os objetivos da empresa em relação a segurança da informação, identificar os ativos mais relevantes ao alcance destes objetivos, definir as preocupações que podem causar danos aos ativos, definir o escopo. Deve-se definir de maneira clara, contra o que é necessário proteger, bem como as necessidades das pessoas em relação ao ativo a ser protegido, de forma a buscar a proteção das situações nas quais, os prejuízos são causados por conta de danos diretos aos ativos, ou

por situações prejudiciais inesperadas; Atribuir responsabilidade – é fundamental, no sentido de definir e explicar aos diversos colaboradores quais as suas responsabilidades. Essas responsabilidades devem ser trabalhadas dentro da organização, de forma a catequizá-los de seus papeis, no que se diz a respeito a SI (sistema de informação), criando o que se chama de cultura de segurança. (Security Officer, 2006)

Políticas de Segurança da Informação demonstram também o comprometimento da alta direção das organizações com a segurança, ponto fundamental para que a política possa ser implementada e gerida com eficácia e assim contar com um maior número de colaboradores. Elas devem resumir os princípios e objetivos importantes de SI que devem estar presente no dia a dia das atividades. A existência de política significa que a organização esta alinhada aos objetivos do negócio.

A necessidade da política surge também na perspectiva da conformidade legal. O desenvolvimento das políticas é ponto fundamental em uma série de normas e regulamentações além de incentivado por normas internacionais de melhores práticas. (Security Officer, 2006)

São fatores críticos de sucesso de uma política de segurança da informação em uma empresa: os objetivos e atividades que reflitam a sustentabilidade do negócio e uma boa estrutura para implementar, manter, monitorar a busca constante de melhoria da segurança da informação, que seja consistente com a cultura organizacional. O comprometimento e o apoio de todos os níveis gerenciais com um bom entendimento dos requisitos da segurança da informação. A análise/avaliação de riscos e da gestão de riscos com uma eficiente divulgação da segurança da informação a ser aplicada em todos os níveis da organização, buscando alcançar a conscientização. Contar com uma boa divulgação de normas, políticas de segurança da informação para todos os usuários. A busca de recursos financeiros no estabelecimento, com um eficiente processo de gestão de incidentes de segurança da Informação. Avaliar o desempenho da gestão de segurança da informação com a obtenção de sugestões para melhorias.

À medida que as políticas de segurança são desenvolvidas controles são criados como um de seus principais propósitos, controles tem ganho inquestionável em relação ao seu custo de adoção, por isto, são recomendados a adoção das políticas por toda a organização, pois tornam-se um controle padrão de segurança.(Vargas, 2005)

2 A EQUIPE DE GERENTES DE SEGURANÇA

Para evitar problemas de conformidade, a equipe de gerentes de TIC, deve estar alinhada e comprometida com as práticas de gestão para buscar sucesso no projeto. Devem ser rigorosos na execução e não podem ser tolerantes a falhas no procedimento. O profissional gerente do projeto de implantação de segurança na organização deve ter capacidade de persuasão e liderança, para conseguir resultados em termos de cooperação e, além disso, deve ter o apoio da alta administração da organização onde atua, isto é imprescindível para uma boa implementação das políticas de segurança. .O profissional de segurança com sua postura pode influenciar na resistência que ele enfrentará durante a implementação de políticas e controles.

O gerente de segurança deve ter algumas habilidades para exercer o papel de gestor de projeto precisa de habilidades de administração geral, tais como: Liderança, comunicação, negociação, solução de problemas, influência na organização. (VIEIRA, 2007)

O profissional de segurança deve possuir sensibilidade para perceber o quanto é delicada e incômoda a mera existência de um departamento de segurança, devem observar o quanto o contexto é capaz de mudar o comportamento das pessoas que nele atuam. A realidade é que é difícil implementar medidas de segurança e deve-se ter estratégias para implementá-las com sucesso. Deve-se perceber que a equipe de segurança não pode assumir a responsabilidade pela proteção que deve ser compartilhada por todos, mas é a ela que cabe indicar os melhores controles, conscientizar os usuários a respeito do uso desta segurança, administrá-los e monitorá-los, além de verificar se todos na organização estão colaborando com as medidas. (Securuty Officer, 2006)

3 O APOIO DA ALTA ADMINISTRAÇÃO E O COMITÊ DE SEGURANÇA DA INFORMAÇÃO

É muito importante o envolvimento e apoio da alta administração da organização nas medidas de segurança a serem tomadas, o ideal é que haja um grupo de pessoas na alta administração apoiando as iniciativas. Recomendação contida na NBR ISO/IEC 27002 (antiga 17799). As responsabilidades principais deste grupo são exigir compromisso dos colaboradores e prover recursos adequados. (Vieira, 2007)

As atividades de um colegiado de profissionais para tratarem o tema Segurança da Informação objetivam, principalmente, prover o apoio necessário aos negócios da organização. Portanto, por maior que seja a capacidade profissional e a experiência das equipes de segurança da informação, a participação de outros setores ou áreas de negócio, é indispensável para o sucesso das atividades.

O Comitê de Segurança da Informação tem a função de alinhar as estratégias de Segurança da Informação aos objetivos da organização. Nele, são analisados os resultados parciais e finais das ações de segurança para medir seus efeitos, compará-los com as metas e realizar ajustes. A estruturação do Comitê de Segurança da Informação de acordo com as melhores práticas de mercado, e de acordo com a norma NBR ISO/IEC 27001:2006, NBR ISO/IEC 27002:2005, foca: Na identificação dos principais processos e gestores de negócio; No mapeamento das necessidades de segurança de cada área ou setor; na análise da estrutura hierárquica de decisões; Na identificação de necessidades recorrentes de Segurança da Informação.

O comitê de Segurança deve conter representantes das diversas áreas funcionais, que suportarão ações e decisões relativas à segurança da informação da empresa. Este comitê, que cria e aprova um conjunto de diretrizes básicas que formarão o primeiro documento de uma Política de Segurança da Informação, é ele que deve definir o escopo da segurança da informação e as responsabilidades das pessoas envolvidas. A publicação dessas diretrizes é uma manifestação clara de apoio às iniciativas de segurança da informação na empresa. Todas as normas e procedimentos que serão posteriormente definidos, buscarão respaldo nas diretrizes (políticas internas) formadas pelos gestores. Dessa forma as diretrizes e políticas se tornam uma espécie de documento formal que dá poderes ao gerente de segurança da informação para definir e implementar as medidas necessárias.(Vieira, 2007)

4 CONSCIENTIZAÇÕES DO USUÁRIO PARA MINIMIZAR OS IMPACTOS

O elemento mais vulnerável de qualquer sistema de informação, é o ser humano. São parte integrante e o elo fraco de qualquer sistema de segurança. Será necessário muito trabalho para a conscientização, treinamento e educação dos colaboradores a respeito da segurança da informação. (Security Officer, 2006)

É muito importante nas organizações públicas, a comunicação em relação às políticas de seguranças das informações e de TI (tecnologia da informação), que estão sendo implantadas e contar com o apoio dos usuários para minimizar os impactos da implantação destas políticas. Na implementação das políticas de segurança, os usuários não devem sentir restringidos a certas informações ou até mesmos de certas configurações de seus equipamentos, e sim contribuir dando seu apoio para a maior segurança destas informações.A melhor maneira de acontecer esta parceria é este usuário estar sempre informado/comunicado das medidas que serão tomadas em relação a segurança. A implantação das políticas de segurança deve mudar a cultura do órgão de como lidar com a informação e tem de contar com o respaldo da alta administração e do comitê de segurança, que estará ligado ao grupo de gerenciamento de segurança apoiando as medidas.

É importante ter uma estratégia de marketing ajudando a conseguir os objetivos de implantação da segurança pretendida e mais ainda, motivar o usuário a sentir-se parte do projeto de segurança, que irá melhorar a qualidade do trabalho de todos e de própria informação. Outro passo importante e muitas vezes ignorado que ira ajudar a conscientizar os usuários sobre a importância da SI (segurança da informação) é recorrer à área de Recursos Humanos, esta equipe tem experiência de como lidar com pessoas e pode ajudar em várias tarefas como, a criação de material de apoio, organização de palestras, motivação do usuário, etc. Escolher as mídias que serão utilizadas para implantar as idéias e desenvolvê-las é também de suma importância nesta conscientização. Combinar diversas mídias sobre o assunto costuma também ser a melhor e mais eficaz idéia. Esta comunicação deve ser simples e concisa. Explicar porque a organização precisa da colaboração dos funcionários, quais são os prejuízos atuais e quais os cenários futuros, caso nada seja feito em relação à segurança da informação. A Segurança da Informação não é muito diferente da segurança que as pessoas estão acostumadas a vivenciar em seu dia-a-dia. Usar estratégias diferentes para usuários de diferentes níveis hierárquicos é uma ótima idéia. (Vieira, 2007)

A campanha de conscientização deve ter algumas tarefas preliminares básicas como: o desenvolvimento de uma Política de Segurança da Informação interna, nem que ela seja pequena e superficial. A organização tem que ter bem claro quais os pontos a serem abordados, quais os mais importantes, mais urgentes, os que trazem maiores prejuízos, etc. O apoio da alta direção, também é fator crucial neste e em todos os outros assuntos ligados a SI (segurança da Informação). Deve avaliar também o conhecimento que a organização tem sobre o assunto e avaliar a necessidade de se contratar uma empresa especializada. Fazer uma campanha com palestrantes experientes e trazer conhecimentos importante sobre o assunto é de grande valia para aumentar o conhecimento dos envolvidos no processo. Se for possível, é bom avaliar e considerar pelo menos um treinamento no assunto para os membros da equipe interna que trabalharão no projeto.

Ter procedimentos bem definidos para permitir que os usuários relatem os incidentes de segurança é de grande valia. Isso traz a sensação de que sua iniciativa é realmente importante e que sua ajuda é útil. Isto é excelente para o processo de conscientização em si, é uma oportunidade de dar um passo adiante e passar de uma realidade de usuários

conscientizados para uma de usuários participativos, uma vez que, eles são hoje um alvo em potencial para intrusos, devemos vê-los como soldados e usá-los, sempre que possível.

5 PARTES INTERESSADAS NO PROJETO

As partes interessadas (stakeholders) no projeto são pessoas e organizações ativamente envolvidas ou cujos interesses podem ser afetados como resultado da execução ou do término do projeto. Eles podem também exercer influência sobre os objetivos e resultados do projeto. A equipe de gerenciamento de projetos precisa identificar as partes interessadas, determinar suas necessidades e expectativas e, na medida do possível, gerenciar sua influência em relação aos requisitos para garantir um projeto bem-sucedido. (PMBOK, 2004)

As partes interessadas são os indivíduos ou grupos que tem o interesse no desempenho e sucesso de uma organização, eles possuem diversos níveis de responsabilidade e de autoridade quando participam de um projeto e eles podem mudar durante o ciclo de vida do projeto. A responsabilidade e autoridade variam desde pequenas contribuições até o patrocínio total do projeto, que inclui o fornecimento de apoio financeiro e político. As partes interessadas, não podem ignorar a sua responsabilidade, porque isto trás prejuízos ao projeto. Os gerentes de projetos que ignoram as partes interessadas, também podem esperar impacto negativo nos resultados do projeto. Devem identificar as partes interessadas no projeto que apesar de ser um trabalho difícil é importante para o sucesso do projeto. As partes interessadas influenciam positivamente ou negativamente em um projeto. Partes interessadas positivas são as que normalmente se beneficiariam de um resultado bem-sucedido do projeto, enquanto partes interessadas negativas são as que enxergam resultados negativos a partir do sucesso do projeto. (PMBOK, 2004)

Os envolvidos no projeto devem ser identificados tão logo quanto possível e analisadas quanto ao nível de influencia e de interesse que ele terá no projeto. O foco nestes *stakeholders* é pensando nos efeitos que eles podem trazer ao projeto, fazer com que eles sintam parte do processo e que colaborem para que o projeto seja implantado com todo o sucesso. Outro fator importante para o sucesso da SI é identificar as necessidades das partes interessadas e determinar uma maneira adequada para atender estas necessidades. O levantamento das necessidades destes *stakeholders*, normalmente é feito na parte inicial do projeto, mas devem ser sempre examinadas e revisadas durante todo o projeto para que dentro do escopo sejam atendidas.

6 GESTÃO DE RISCO

É praticamente impossível tratar de segurança da informação sem deparar com conceitos de Gestão do Risco ou Análise de Risco. Ambos os conceitos encontram-se intimamente relacionados com o processo de Gestão da Segurança da Informação, ligada a riscos como: vulnerabilidade, confidencialidade, integridade e outros que afetam os ativos da empresa.. Os riscos sempre estarão associados a estes eventos. Em segurança eles são nomeados de incidentes, os riscos podem ser positivos ou negativos, mas analisados perante a segurança da informação, suas conseqüências serão negativas. O processo de Gestão de risco,

provavelmente é um dos componentes mais importantes da SI, é por meio deste processo que os riscos são identificados e tratados. (Security officer, 2006)

O termo Análise de Risco, inserido no contexto da segurança da informação, pode ser entendido como o processo que identifica e avaliam os riscos de segurança a que os recursos críticos de negócio das organizações se encontram sujeitos, possibilitando a definição dos meios através dos quais estes podem ser protegidos.

A realização de uma análise de risco compreende diversas etapas ou passos: Identificar dos ativos considerados críticos para a atividade e sobrevivência da organização, Identificar as vulnerabilidades, bem como a sua probabilidade de ocorrência e impacto esperado. Determinar as perdas e danos (tangíveis e intangíveis) associados aos impactos resultantes da concretização de uma ou mais ameaças, sobre o ativo.

Para tratar riscos de segurança de TIC é necessário que a organização defina os critérios para que os riscos possam ou não ser aceitos. Um nível de risco pode não ser aceito quando o custo de proteção contra um determinado risco não vale a pena.

É indispensável monitorar o nível de risco a que os ativos, e o negócio da organização, se encontram expostos, de forma a garantir a eficiência e a eficácia da gestão desse risco, processo que compreende, tanto a análise, como o tratamento dos riscos identificados.

O desempenho do negócio está atrelado diretamente à gestão de riscos e, cada vez mais, as empresas passam a perceber a importância do papel da segurança da informação nesse processo. (PMBOK, 2004)

As atitudes em relação aos riscos devem ser comunicadas sempre que possível. Uma abordagem consistente do risco que atenda aos requisitos da organização deve ser desenvolvida para cada projeto, e a comunicação do risco e o seu tratamento deve ser aberto e transparente.

7 AS METODOLOGIAS E MELHORES PRÁTICAS DE GERENCIAMENTO DE PROJETOS

De acordo com o PMBOK (2004)

> O gerenciamento de projetos é a aplicação de conhecimento, habilidades, ferramentas e técnicas às atividades do projeto a fim de atender seus requisitos. O gerenciamento de projetos é realizado através da aplicação e integração dos seguintes processos de gerenciamento de projetos: iniciação, planejamento, execução, monitoramento, controle e encerramento e das nove áreas de conhecimento de gerenciamento de projetos.

Atender os requisitos do projeto envolve o balanceamento das seguintes demandas: Escopo, tempo, custo, risco qualidade do projeto, satisfação dos interessados com suas diversas expectativas e necessidades, onde necessidades são os requisitos identificados e as expectativas são os requisitos não identificados. (Vieira, 2007)

O controle e monitoramento é um ponto essencial no gerenciamento de projetos, sem controle não é possível atender os requisitos do cliente.(Vieira, 2007)

7.1 As nove áreas do conhecimento auxiliando a minimizar o impacto na implantação de projeto de tecnologia da informação de segurança

De acordo com o PMBOK 2004 o gerenciamento de projetos ocorre nas nove áreas de conhecimento de gerenciamento e influenciam diretamente no sucesso do projeto, estas nove áreas do conhecimento podem ser utilizadas parcialmente ou totalmente, podendo ser adaptadas as necessidades de um projeto de implantação de segurança. As quatro áreas centrais incluem o escopo o tempo, os custos e a qualidade. As áreas facilitadoras são os recursos humanos, comunicação aquisição e risco e estas áreas são consideradas facilitadoras porque são maneira de se alcançar os objetivos. A integração garante que todas as áreas se integrem como um todo e garante que as necessidades dos interessados sejam atendidas. As nove áreas do conhecimento são de grande valia para se ter um projeto de segurança implantado com sucesso e elas são usadas a medida da necessidade do projeto. (Vieira, 2007)

7.1.1 A Gerência de integração de projetos

> A área de conhecimento em gerenciamento integração do projeto inclui os processos e as atividades necessárias para identificar, definir, combinar, unificar e coordenar os diversos processos e atividades de gerenciamento de projetos dentro dos grupos de processos de gerenciamento de projetos. (PMBOK, 2004)

Este gerenciamento tem como objetivo que todos os elementos do projeto estejam coordenados e integrados, através do ciclo de vida do projeto. A gestão de integração de projeto tem como base a unificação, consolidação, articulação e ações integradoras que são imprescindíveis para atender com sucesso às necessidades do cliente e de todas as partes interessadas e para gerenciar as expectativas do projeto. Integrar todos os elementos do projeto tem como o objetivo garantir que os elementos dentro do projeto estejam devidamente integrados e coordenados. Em um projeto de tecnologia da informação e comunicação este tipo de gerenciamento é mais complicado, pois a tecnologia está sempre em transição e sempre se espera encontrar mudança em todo o ciclo do projeto. É preciso muita habilidade do gerente do projeto para lidar com estas incertezas, ele deve ser além habilidoso para lidar com os problemas. Para se ter uma boa integração gerencial é preciso que o gerente tenha comprometimento com a organização e que a alta administração repasse poderes, responsabilidades e atribuições a estes gerentes. (Vieira, 2007) Também é de suma importância, que esta integração sempre esteja alinhada com os objetivos estratégicos dos negócios da empresa. Na gestão de integração do projeto, devem-se concentrar recursos e esforços para se antecipar problemas, antes que eles se tornem críticos visando o bem de todo o projeto. Integrar também requer esforços para se resolver conflitos na busca de alternativas para atender as necessidades, sem com isto desviar dos objetivos propostos. O gerenciamento de projetos é um empreendimento integrador. A integração do gerenciamento de projetos exige que cada processo do projeto e do produto seja adequadamente associado e conectado a outros processos para facilitar a sua coordenação. (PMBOK, 2004)

7.1.2 Gerência de escopo do projeto

O escopo refere-se a todo trabalho envolvido na criação do produto do projeto e dos processos utilizados para criá-lo. O escopo de um projeto consiste basicamente em definir a justificativa do projeto. (Securuty officer, 2006) Em um projeto de implantação de segurança o escopo do projeto tem de estar alinhado com as estratégias da empresa, tem de estar com o

escopo bem definido para evitar erros futuros e futuras decisões do projeto.. Os requisitos dos envolvidos devem ser muito bem entendidos e verificados. A definição do escopo é o mais importante aspectos do gerenciamento de um projeto.(Vieira, 2007). Toda mudança de escopo em um projeto gera impacto, e não é fácil mudar nem implementar novas funcionalidades em um projeto, por isto deve-se gastar muito tempo definindo o escopo, principalmente em um projeto que visa segurança da informação onde a empresa será afetada como um todo. Para um projeto de segurança da informação, tecnologia e comunicação, deve-se ter um escopo muito bem definido, desde a descrição do produto e dos requisitos dos usuários e deve ser definido com a participação e consentimento formal de todos os envolvidos no projeto.

7.1.3 Gerência de tempo

São os processos necessários para que o projeto termine no prazo previsto. Muito dos projetos de tecnologia da informação não tem sucesso por problemas na definição do tempo do projeto. Em um projeto que se pretende implantar segurança da informação, este tempo deve ser bem definido, porque existem portarias, decretos, legislações e políticas a serem cumpridas em um prazo muitas vezes curto. Outro problema para os projetos de tecnologia da informação é que o ciclo de vida de um produto de tecnologia da informação é curto e ele pode ficar obsoleto em poucos meses.

7.1.4 Gerência de custo

O gerenciamento de custos do projeto inclui os processos envolvidos em planejamento, estimativa, orçamento e controle de custos, de modo que seja possível terminar o projeto dentro do orçamento aprovado. (PMBOK, 2004)

Em um projeto que envolve tecnologia da informação o custo é um fator crítico, o custo e o escopo estão fortemente relacionados, e devem depender de um bom entendimento de requisitos do usuário para poder ser estimado. Erros de estimativas podem ser evitados se forem usados os processos de gerenciamento de custo no projeto de tecnologia da informação e comunicação como: Orçamento – fazer orçamentos para estimar custos (para estabelecer uma linha de base dos custos.

Controle de custos – controle dos fatores que criam as variações de custos e controle das mudanças no orçamento do projeto. Esses processos interagem entre si e também com processos nas outras áreas de conhecimento. Cada processo pode envolver esforço de uma ou mais pessoas ou grupos de pessoas, dependendo das necessidades do projeto.

O gerenciamento de custos do projeto considera as necessidades de informação das partes interessadas no projeto. (PMBOK, 2004)

7.1.5 Gerência de qualidade

Qualidade tem foco na satisfação do cliente e da conformidade deste projeto com a satisfação do cliente. (Vargas -2005) A gerencia da qualidade é o gerenciamento dos processos para que os requisitos dos projetos sejam satisfeitos. A qualidade está intimamente ligada ao sucesso. Muito ainda se tem de melhorar na qualidade de projetos de tecnologia da informação e é muito importante o gerenciamento de qualidade nestes projetos para se alcançar as melhorias.

7.1.6 Gerência de recursos humanos do projeto

De acordo com o PMBOK 2004 - Gerenciamento de recursos humanos é necessário para melhor utilização das pessoas envolvidas no processo. Gerenciar recursos humanos é um grande desafio, pois o sucesso do projeto também depende das atitudes destes profissionais. Lidar com as pessoas não é uma tarefa nada fácil, e o gerente de projetos deve estar sempre atento em atender as necessidades dos recursos humanos da organização, pessoas felizes vão auxiliar e muito no sucesso de implantação de um projeto de segurança da informação ou qualquer outro projeto a ser implantado.

7.1.7 Gerência de comunicações de projetos

Gerenciamento que descreve os processos necessários para assegurar a distribuição e comunicação das informações do projeto.(Vieira, 2007). O processo de Planejamento das comunicações determina as necessidades de informações e comunicações das partes interessadas (PMBOK, 2004). De acordo com Vargas (2005), um efetivo processo de comunicação é necessário para garantir que todas as informações cheguem às pessoas corretas, no tempo certo e de maneira eficaz. A comunicação tem de serem claras e efetivas, as pessoas não tem de concordar para cooperar com uma decisão, mas tem de compreender como e porque ela foi tomada. No planejamento das comunicações do projeto, os interessados devem estar sempre bem informados sobre o projeto se sentindo parte integrante dele. Um principal problema em um projeto é a falta de comunicação entre as equipes e a retenção de informação. Um grande risco são falhas de comunicação no projeto, o usuário deve ser sempre comunicado de qualquer mudança no projeto. Uma das maiores ameaças ao sucesso dos projetos, principalmente para projetos de tecnologia da Informação, refere-se às falhas de comunicação. (Vieira, 2007). Três destas ameaças merecem destaque: o não envolvimento dos usuários em todas as fases e etapas do projeto, a falta de apoio dos altos executivos, o levantamento de requisitos inconsistente. Em um projeto que envolve segurança da informação o usuário deve estar sempre bem informado, para se sentir parte integrante deste projeto não causando assim dificuldades na implantação..

7.1.8 Gerência de Riscos

Análise de riscos basicamente como já falada visa à identificação dos pontos de riscos que a informação está exposta, identificando desta maneira quais os pontos que necessitam de maior empenho em proteção. Os riscos são incertezas que podem impedir o alcance dos objetivos propostos. Conforme Prado, 1998 os riscos são as conseqüências que poderão ocorrer caso o projeto se atrase ou ultrapasse o orçamento estimado ou tenha problemas técnicos. O gerenciamento de riscos possibilita a chance de melhor compreender a natureza do projeto envolvendo a equipe de projeto de modo a identificar e responder as incertezas. Os riscos do projeto geralmente estão associados a custo, tempo e qualidade.(Vargas, 2005).

Em um projeto de segurança da informação deve-se aprimorar a gestão de riscos, automatizarem controles internos e externos associados à identificação de melhorias, essa

gestão de riscos deve estar associada a controle e monitoramento de acessos. Os riscos devem ser sempre analisados e controlados para evitar falhas futuras.

7.1.9 Gerência de Aquisições

É o gerenciamento dos processos necessários para aquisições de mercadorias e serviços (Vargas, 2005). A gerência do projeto deve analisar bem os aspectos envolvidos na aquisição do projeto, deve tomar decisões relevantes baseadas nas necessidades deste projeto e das prioridades da organização. O gerenciamento de aquisições do projeto inclui os processos de gerenciamento de contratos e o de controle de mudanças necessário para administrar os contratos ou pedidos de compra. (PMBOK, 2004)

Os processos de gerenciamento de aquisições do projeto incluem:

O processo Planejar compras e aquisições identifica quais necessidades do projeto podem ser melhor atendidas pela compra ou aquisição de produtos, serviços ou resultados fora da organização do projeto e quais necessidades podem ser realizadas pela equipe durante a execução do projeto (observe quantas vezes citou a palavra projeto numa mesma frase.). Esse processo envolve a consideração de como, o que, quanto, se e quando adquirir. (PMBOK, 2004)

8 CONCLUSÃO

A grande dificuldade de implementar qualquer sistema que vise a mudança cultural, é que o trabalho deve ser contínuo e persistente. Os verdadeiros resultados aparecem somente de médio a longo prazo. É primordial considerar que, uma boa estratégia para se abordar a problemática da segurança da informação, passe por uma visão holística, ou seja, pelo cuidado com todos os pilares fundamentais: Pessoas, Processos e Tecnologia.

O DER tem de estar com uma visão global do que é importante ser protegido de seu ativo e o porquê deve-se proteger, além de estar alinhado com as políticas do Estado, buscar uma visão abrangente dos impactos causados pelos problemas de segurança, principalmente do descrédito da organização perante seus usuários externos e internos.

A segurança da informação, busca a proteção dos ativos de informação contra as ameaças, tentando diminuir as ocorrências dos impactos e diminuir os riscos. A forma de alcançar estes objetivos de segurança é descobrindo e tratando as vulnerabilidade da organização, implementando proteções e corrigindo as falhas.

O aumento da exposição das informações, as convergências, os problemas tecnológicos, leis e regulamentações têm aumentado muito os desafios da SI, por isto é necessário visão, metas e hierarquia para conseguir alcançar o almejado em um projeto de segurança no DER/MG.

O gestor de SI para desempenhar suas funções com eficácia deve-se valer de ferramentas já aceitas como gestão de riscos e desenvolvimento de políticas de segurança da informação, metodologias e as melhores praticam de projetos. Deve ter o benefício da padronização trazido pelas políticas e o uso de análise sistemática para tomada de decisões o que traz impessoalidade para iniciativa de segurança. Assim o trabalho é facilitado, pois ficará acima de disputas internas, focando unicamente em dados objetivos, e em tratamento igual para todos.

Seguir regras e definir as políticas para implementar um projeto de segurança da informação, é a melhor maneira de minimizar as oposições, resistências desta implantação. Para implementar segurança em um órgão como o DER/MG, a alta gerencia deve estar informada e apoiando todas as medidas a serem tomadas, deve-se ter o apoio de um comitê de segurança bem estruturado, além de ter de contar com recursos tanto financeiro quanto humanos e a colaboração dos envolvidos. Procurar estar em sintonia com a área de recurso humanos buscando a colaboração destes, na organização do gerenciamento dos trabalhos e trazendo as habilidades e qualificações necessárias ao projeto. Buscar sempre, a ajuda para motivar os usuários a participar do projeto e sentir parte integrante desta implementação, devemos contar com o apoio da área de marketing/comunicação, a fim de divulgar as informações necessárias, isto é sempre estratégico e faz com que os usuários estejam sempre informado das ações a serem tomadas e quais as benfeitorias que estão sendo buscadas.

Conclui-se que em todo projeto de tecnologia da informação é essencial estar alinhado com as estratégias da empresa e também com o plano diretor de informática e no DER/MG ainda com as políticas do Estado. Os projetos de segurança da informação são importantes para empresa, pois afetam diretamente a confiabilidade dos negócios. É de extrema importância usar as melhores práticas de projetos para atingir os objetivos do projeto como, garantir o cumprimento dos requisitos, escopo, prazos, custos, qualidade e uma efetiva utilização dos recursos humanos, é usando estas práticas de projeto já testadas mundialmente com sucesso que iremos alcançar o sucesso esperado no projeto.

Segurança da Informação deve estar alinhado com as melhores práticas de projetos, voltado para o objetivo do negócio da empresa na busca constante do sucesso.

REFERENCIAS BIBLIOGRÁFICAS

ABNT NBR ISSO/IEC 17799:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para gestão da Segurança da Informação, 2005

ABNT NBR ISSO/IEC 27001:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para gestão da Segurança da Informação, 2006

Antônio Mendes da Silva Filho - Protegendo Sistemas e Informações, 2004

Cobit 4.1

Darci Prado – Planejamento e Controle de Projetos vol.2, 2008

http://www.isaca.org/ Acesso em: 6/10/2009

http://internativa.com.br/artigo_seguranca_01.html Acesso em: 6/10/2009

http://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o Acesso em: 16/09/2009

http://aramos.org/2006/07/conscientizacao-de-usuarios-e-seguranca-da-informacao/ Acesso em: 16/09/2009

http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm Acesso em: 6/06/2009

www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao Acesso em: 18/05/2009

www.elojas.com.pt/artigos/analise-e-gestao-do-risco-em-seguranca-da-informacao Acesso em: 16/10/2009

Marconi Fábio Vieira -2007 Gerenciamento de projetos de Tecnologia da Informação

PMBOK 2004

Ricardo Vargas – 2005

Revista Fonte Segurança da Informação nº 7, 2007 - Prodemge

Security Officer Ed. 1 - Modulo Education Center - Guia Oficial para Formação de Gestores em Segurança da Informação – 2006

Harold, Kerzner – 2 ed 2006 Gestão de Projetos as melhores praticas

Portaria BRASIL. Ministério do Trabalho e Emprego. Portaria n.1.029, de 11 de agosto de 2003. Direito do Trabalho, São Paulo, Ano 29, n.112, p.299-304, out./dez. 2003.

LARA, Marilda Lopes Ginez de. Recensão. Ciência da Informação, Brasília, v.32, n.2, maio/ago. 2003. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652003000200014&lng

=PT Acesso em: 16/10/2009