FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE

SERGIPE - FANESE

NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO – NPGE

MBA GESTÃO EM REDES E SEGURANÇA DA INFORMAÇÃO

ALEXANDRE LIMA DE FARIAS

ADOÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO COMO DIFERENCIAL ESTRATÉGICO EM PEQUENAS E MÉDIAS EMPRESAS

ARACAJU
2015

RESUMO

Este artigo visa justificar a adoção de Políticas de Segurança da Informação no ambiente corporativo de Pequenas e Médias Empresas buscando gerar um Diferencial Estratégico sobre os concorrentes no mercado independente do ramo de negócio de uma empresa, possibilitando que a mesma possua normas definidas que gerem segurança a suas informações e possua ainda um Plano de Continuidade de Negócios e Recuperação de Desastres.

Palavras chave: Políticas de Segurança da Informação; Diferencial Estratégico; Plano de Continuidade de Negócios; Recuperação de Desastres; Pequenas e Médias Empresas.

INTRODUÇÃO

De forma genérica, um dos únicos itens que não é mensurável dentro de uma organização é a informação. Tal produto é tão valioso no mercado que um pequeno vazamento ou perda pode causar prejuízos irreparáveis nas organizações e quiçá até mesmo a destruição de uma empresa.

Para que uma informação tenha valor a mesma deverá preservar os seguintes requisitos: integridade, disponibilidade e confidencialidade. A Segurança da Informação preza ainda pela autenticidade.

Segurança da Informação não se basta apenas em aplicativos ou sistemas implantados dentro de uma empresa que gerem restrições ou proteções contra acesso. São políticas criadas e gerenciadas que visam mitigar os riscos de roubo ou vazamento, bem como garantir que no momento necessário ela esteja disponível a quem for de direito.

Diversos processos são responsáveis por garantir tais aspectos na informação, mas não vale apenas proteger a mesma sem pensar que um infortúnio possa ocorrer e tais valores se perderem se existem ferramentas e processos que gerem maneiras de se recuperar tais informações.

Sendo assim, para que se pense em Políticas de Segurança da Informação (PSI) é necessário vislumbrar simultaneamente um Plano de Continuidade de Negócios (PCN) e processos de Recuperação de Desastres (PRD).

Mas como proteger algo que não se sabe o valor e de que maneira essa proteção pode gerar um diferencial estratégico?

Algumas *frameworks* internacionais demonstram através de melhores práticas que a gestão de Políticas de Segurança da Informação geram valor comercial aos seus produtos e negócios, como *CobiT* e a ISO/IEC 27000.

Fernandes e Abreu (2012) afirmam que a adoção de frameworks como CobiT geram benefícios como a redução da exposição a riscos, assim como a melhoria da imagem da empresa perante seus clientes, através do aumento do grau de confiabilidade e a ISO/IEC 27000 a prevenção de perdas financeiras.

Mas investir em diversas políticas e sistemas pode gerar um diferencial estratégico perante seus concorrentes no momento que ameaças são lançadas na rede mundial diariamente e todos estão vulneráveis a esses riscos. A partir do momento que uma empresa possui normas e políticas descritas e gerenciadas que visam reduzir esses riscos, visivelmente, já esta a frente de seus concorrentes que não a possuem.

O gerenciamento de tais processos gera também para seus clientes e fornecedores a imagem de uma organização séria e comprometida com seus bens, sendo a informação um dos seus maiores ativos.

Como exemplos de PSI podemos citar dentre os âmbitos da mesma:

- Segurança Física – Uso de equipamentos de vigilância, monitoramento através de circuito interno de TV, alarmes, cercas e etc.;
- Segurança Lógica – Utilização sistemas de gerenciamento de usuários e acessos, bloqueio de uso de internet e aplicações;
- Segurança em Pessoas – Proteção por vigias, segurança armada; fator humano;
- Segurança em Processos – Processos de acesso a empresa, processo de cadastro de visitantes, treinamento de colaboradores.

Todos estes exemplos servem para diferenciar uma empresa que se preocupa com suas informações, bem como com seus clientes e isso a difere no mercado.

Se tomarmos por exemplo duas pequenas lojas comerciais e observarmos o tratamento da segurança onde uma investe em câmeras de monitoramento, alarmes de roubo e protocolos de compra; e a outra loja nada o faz, com certeza a primeira será mais valorizada pelos clientes tanto pela qualidade dos serviços prestados, como também pela confiança que é repassada pela empresa.

DIFERENCIAL ESTRATÉGICO

> *"Administrar bem um negócio é administrar seu futuro; e administrar seu futuro é administrar informações." (Marion Harper Jr)*

A palavra estratégia tem por significado "a arte do general". Em épocas remotas significava a arte e ciência de conduzir forças militares para derrotar o inimigo ou minimizar os resultados da derrota.

Oliveira (2011, p.181) explica que no âmbito corporativo a estratégia está correlacionada à arte de utilizar adequadamente os recursos tendo em vista a minimização dos problemas internos e maximização das oportunidades que estão no ambiente empresarial, o qual não são controláveis.

Sendo assim, toda empresa que planeja crescer no mercado, ou até mesmo sobreviver deve planejar suas metas e objetivos e para isso, deve sempre procurar conhecer todos os riscos e procurar sempre mitiga-los. O uso de PSI visa auxiliar portanto esse planejamento reduzindo ainda mais os riscos sobre a informação, seja ela de qualquer forma: digital, documental ou até mesmo pessoal.

Uma corporação que se preocupa em administrar seu negócio possui um planejamento estratégico, mesmo que este não esteja definido ou documentado, mas a diretoria da empresa deve sempre pensar no futuro dos seus negócios.

A prática mostra que o Planejamento Estratégico visa gerar formas de atuação inovadoras e diferenciadas bem como conhecer os riscos inerentes aos negócios, objetivo esse que a adoção de PSI também possuem. A frase de Julian Huxley retrata de maneira simples e singela tal afirmação: "Quem define um problema, já o resolveu pela metade" (Oliveira, 2011, p. 143).

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

A informação é o elemento que permitiu a evolução do homem, bem como a descoberta de várias ferramentas e objetos que auxiliaram ainda mais no aprimoramento da sociedade. Essas evoluções só foram possíveis porque essas informações foram compartilhadas. Sem esse compartilhamento as descobertas teriam fim, não evoluiriam.

Todas as organizações só existem por conta das informações. Não existe negócio ou corporação sem uso de informações. Fontes (2012, p. 01) explica que a informação possibilita que a organização tenha mais chances no mercado competitivo, pois ter a informação correta e disponível no momento certo, pode ser uma vantagem competitiva. Esse elemento é um fator estrutural para o sucesso e continuidade da organização.

Por outro lado, a ausência da mesma atrapalha ou até mesmo não permite a tomada de decisão, bem como gera a possibilidade de perdas irreparáveis para vida da empresa.

Para que as PSI sejam aplicadas elas precisam ser divulgadas. Para tal processo se faz necessário realizar um levantamento prévio de toda estrutura de TI, bem como processos de negócio da organização para que essas políticas sejam alinhadas com os objetivos da empresa.

Esse documento não é um documento único e sim um conglomerado de políticas que abordam diversas áreas específicas, como área de informática, uso de e-mails, formas de autenticação na rede, direitos e deveres dos usuários sobre os ativos de TI, políticas de navegação na Web, entre outras informações.

Se faz necessário ainda que o linguajar utilizado seja de fácil compreensão por todos que serão afetados e não exclusivamente profissionais da área de TI ou afins.

Algumas questões devem ser levantadas no momento em que a decisão de Adoção de Políticas de Segurança da Informação seja autorizada pelo corpo diretor da organização, onde as principais são:

- Quais informações devem ser protegidas?
- Quantos usuários serão afetados por essas políticas?
- Qual orçamento disponível?
- Quem são os responsáveis pelo gerenciamento dessas Políticas?

- Qual risco tal Adoção trará para os negócios da organização?
- Quais as vantagens na implantação de tais Políticas?
- O que ocorrerá caso haja uma falha?

Certas questões mais especificas serão levantadas de acordo com os processos de negócio de cada organização.

Vale ainda ressaltar que esse processo não é único e possui data de vencimento. Na verdade o mesmo é um processo continuo, pois o risco é alterado diariamente, bem como as vulnerabilidades de cada organização tendem a crescer a medida em que seus processos se alterem ou seu corpo de colaboradores seja alterado.

Sendo assim, tais Políticas devem ser sempre acompanhadas e atualizadas, bem como os indivíduos e processos por ela afetados.

ANÁLISE DE RISCO E PLANEJAMENTO

Para uma PSI seja bem elaborada, se faz necessário planejar quais investimentos são necessários e como os mesmos serão implantados na organização, bem como suas reais necessidades de acordo com os negócios da empresa. Sendo assim, o primeiro passo para se criar uma PSI condizente com as demandas da organização é realizar uma análise de risco e seus respectivos impactos sobre a saúde da empresa.

Não se pode realizar esse levantamento sem se conhecer os processos de negócio que a organização possui, bem como suas devidas criticidades e, por vezes, realizar investimentos desnecessários sobre ativos com menor impacto nos negócios. Sendo assim, é correto afirmar que quanto menor a organização, menor será o investimento realizado para suas Políticas de Segurança da Informação e estas Políticas deverão ser diferentes para cada ramo de negócio do mercado, obrigando assim a devida analise sobre a empresa.

Um dos conceitos mais simples e de maior retorno sobre a Segurança da Informação da empresa é a utilização de Backups. Existem formas diversas de se utilizar tal ferramenta, desde uso de equipamentos de alto custo até um simples dispositivo removível, como um Pen Drive. A escolha e forma de utilização deverá sempre ser feita de acordo com o porte da empresa e da

criticidade de tais ativos. Pode-se dizer até que uma empresa que possui um sistema de backup ativo e corretamente aplicado já possui um grande diferencial sobre seus concorrentes, por ser um simples processo que por vezes não é tratado como essencial, mas que pode gerar um enorme impacto sobre os negócios de qualquer que seja a organização para sua sobrevivência e continuidade.

Realizar um Backup semanalmente com certeza diferencia a organização das demais, mas se o mesmo não possui documentação, não passa de uma cópia sem a sua devida referência. Uma política de Backup necessita de informações mais completas, como origem, destino, data, tipo, criticidade e validade. Essas informações são valiosas no momento de sua utilização, principalmente em um segundo ponto que as Políticas de Segurança da Informação geram diferencial: Recuperação de Desastres.

Existe uma grande diferença quando se fala de Plano de Recuperação de Desastres (PRD) e Plano de Continuidade de Negócios (PCN), onde o PRD trata exclusivamente de restaurar os processos da empresa, mesmo que com desempenho reduzido, mas que não permita a completa paralização dos seus processos e o PCN visa ter o máximo de controle sobre os riscos inerentes que poderão ocorrer na organização, visando identificar e preservar os serviços essenciais após um desastre ocorrido.

Por estes motivos podemos dizer que o PRD deve ser elaborado em conjunto com o PCN garantindo assim uma maior segurança a organização. Filadoro (2014) explica que os objetivos do PRD e PCN são sempre a restauração e identificação de prioridades que devem sempre ser dimensionadas ainda na fase do planejamento e análise de riscos.

Em posse de um Backup, seja ele de qualquer tipo, o PRD deverá conter informações sobre como, quem e de que maneira o Backup deverá ser restaurado, bem como outras informações mais detalhadas sobre os processos de negócios particulares de cada organização.

A documentação destes processos gera um valor sobre a empresa quando, em caso de necessidade, ela precisa utilizar estas ferramentas para restaurar rapidamente suas informações e seus negócios, diferenciando assim sua imagem corporativa perante seus concorrentes.

SEGURANÇA DA INFORMAÇÃO EM PEQUENAS E MÉDIAS EMPRESAS

Desenvolver PSI em Pequenas e Médias Empresas (PMEs) onde, provavelmente o investimento será baixo não precisa ser uma tarefa tão árdua. Pequenas soluções geram um diferencial estratégico sobre os concorrentes no mercado e podem ser facilmente implantadas a baixo custo.

Empresas com esse porte geralmente não possuem estrutura tecnológica com redundância e por vezes utilizam serviços terceirizados/alugados. Estes por si só devem ofertar certa segurança e estabilidade, p.e. hospedagem de e-mail e site da corporação.

Contudo podemos definir de acordo com os investimentos reduzidos das PMEs que as políticas abaixo podem ser implantadas gradativamente, possibilitando assim uma maior segurança das informações com baixos custos de investimento, sendo elas:

1. Definição de um responsável pela Segurança da Informação: delegar a um responsável ou a um grupo a tarefa de supervisionar a aplicação das Políticas e Normas da Segurança da Informação, bem como realizar a manutenção de tais Políticas;
2. Classificação das informações: garantir que os princípios básicos da Informação (disponibilidade, integridade e confiabilidade) sejam mantidos, devendo o responsável garantir que as informações sejam classificadas como públicas, restritas e disponibilizadas a quem for de direito sempre que necessário;
3. Políticas de uso dos equipamentos de TI: normas definidas com direitos e deveres dos usuários da empresa em documento disponível a todos colaboradores que atuam na empresa utilizando estes ativos;
4. Políticas de uso de equipamentos móveis: normas de uso dos ativos da empresa como notebooks, tablets, smartphones;
5. Políticas de Backup: documento descrevendo como o backup dos sistemas e ativos da empresa é realizado, informando a maneira como o mesmo é feito, bem como data, horário da execução e validade de tais arquivos;
6. Utilização de e-mail corporativo: e-mail com domínio da empresa onde há a possibilidade de monitoramento, backup e adoção de uma assinatura padrão trazem a empresa uma visão mais madura e organizada da estrutura de TI;

7. Políticas de uso da Internet: documento disponível a todos colaboradores que utilizam a rede mundial, definindo direitos e deveres do mesmo para com os ativos, possibilitando ainda monitorar seu uso;
8. Redes Sociais: regras que definem a permissão do uso e acesso a Redes Sociais através da rede da empresa;
9. PCN: documentação informando os riscos inerentes as operações de negócio da empresa e formas de continuidade em caso de desastre mesmo que com menor desempenho, sendo esta informação também documentada e com suas devidas mensurações;
10. PRD: formas de recuperação em caso de interrupção das operações normais, bem como prazos necessários para restauração dos processos de negócio;
11. Controle de acesso: maneira como os colaboradores, fornecedores e clientes deverão ter acesso a empresa e seus devidos serviços;
12. Wi-Fi para visitantes: o cliente sentirá uma maior segurança ao visitar a empresa e verificar que a mesma possui uma internet disponível somente para os visitantes, assim como uma maior segurança aos ativos de TI da empresa.

Estas são algumas políticas genéricas que podem ser aplicadas em diversos ramos de negócio, devendo sempre avaliar sua criticidade sobre as informações da empresa, bem como a imagem que a mesma irá repassar a seus clientes e fornecedores. Diversas das políticas citadas não necessitam devidamente de investimento tecnológico, sendo apenas processos definidos e documentados que deverão ser constantemente avaliados de acordo com o planejamento estratégico da organização. Vale ressaltar que todas estas informações devem ser disponibilizadas, em sua grande maioria, a todos seus colaboradores.

A Adoção de Políticas de Segurança da Informação deverá tanto trazer benefícios sobre a imagem da Organização como, principalmente, gerar valor sobre as informações da empresa, reduzindo assim o risco de vazamento ou perda e possibilitando a tomada de decisão de maneira mais rápida, confiável e no momento correto, benefícios estes que por si só auxiliam a direção da organização a crescer de maneira mais sólida no mercado assim como ter um diferencial estratégico sobre seus concorrentes.

CONCLUSÃO

O desenvolvimento de um PSI passa por várias fases de criação, desde a "compra" da ideia pela direção das organizações, como por vários processos de desenvolvimento, onde vários setores serão consultados, desde Recursos Humanos à TI, porque todos os processos de negócio envolvidos serão analisados e criticados de acordo com o risco que trazem a empresa. Sendo assim, várias PMEs acabam não implementando um PSI por ser um processo complexo e que necessita de maturidade da organização.

De maneira macro, podemos definir que PSI é um complexo de normas adotadas pelas organizações que objetivam ter um crescimento no mercado mais seguro e de maneira precavida que auxiliado por diversas ferramentas como PRD e PCN conseguem se diferenciar dos concorrentes.

Uma organização que possui um PSI trabalha de maneira mais segura perante seus concorrentes, visto que diversos fatores que hoje dependem exclusivamente de TI estão assegurados ou ao menos controlados. Não existe risco zero, mas quanto maior o conhecimento e o devido tratamento para mitigar ou aproximar deste valor, mais estável e seguro esta empresa no mercado. Portanto, quanto maior o alcance do PSI sobre os processos da empresa maior será a quantidade de investimento necessário.

PMEs por vezes não investem em TI como deveriam para alavancar seus negócios ou melhorar a qualidade de seus produtos ou serviços. Estudos mostram que 48% das empresas brasileiras já perderam algum tipo de dado confidencial ou proprietário nos últimos anos. Um relatório apresentado pela Symantec (www.symantec.com.br) no primeiro semestre de 2010 mostra que empresas da América Latina perderam mais de U$ 500 mil por decorrência de ataques virtuais e que 50% dessas empresas não se veem como alvos de ataques cibernéticos apesar de 50% das empresas terem conhecimento das ameaças à segurança de seus negócios.

Em 2013 a Symantec realizou uma nova pesquisa com Pequenas e Médias Empresas (PMEs) no planeta e dividiu a pesquisa de acordo com o nível de confiança da organização em relação a TI. As empresas que mais confiam e buscam definir suas estratégias juntamente com o setor de TI (empresas top-tier segundo o relatório) tendem a crescer mais:

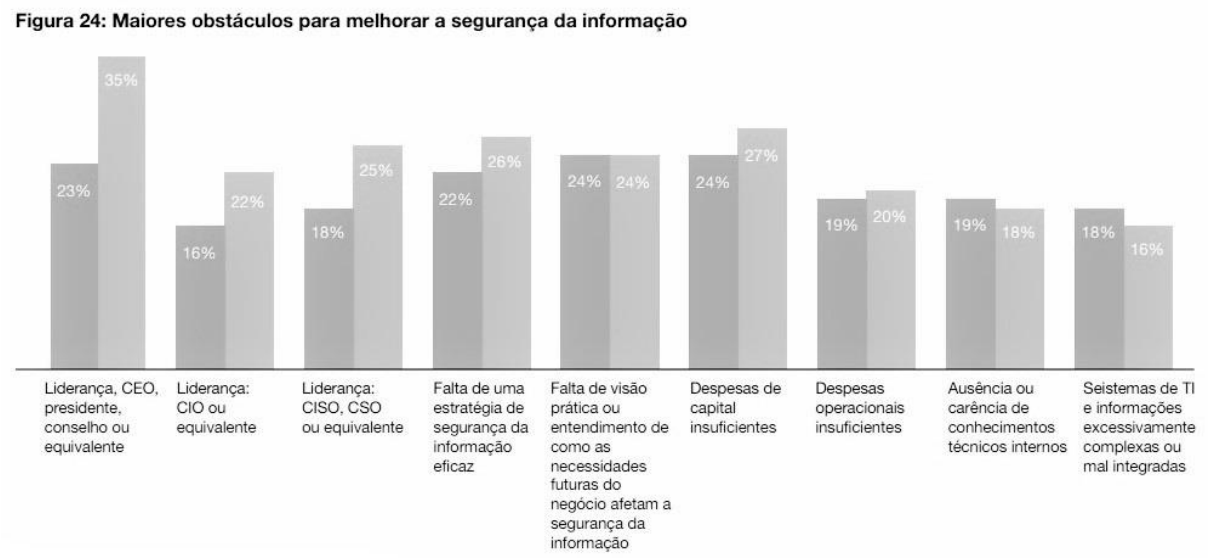
> *"81% das empresas top-tier relataram que o uso da informática para promover avanços estratégicos nos negócios foi eficaz no aumento da participação de mercado, que é um importante objetivo de negócios"*. (Pesquisa Symantec 2013)

A pesquisa ainda relatou que 31% dos ataques realizados a empresas miram as PMEs pois os criminosos estão voltando seus ataques para empresas com segurança mais fraca.

Sendo assim é válido afirmar que as PMEs devem iniciar o processo de Adoção de Políticas de Segurança da Informação com o objetivo de assegurar o crescimento e continuidade de seus negócios, como afirma a Symantec quando finaliza seu relatório afirmando que a necessidade da tecnologia nos negócios das empresas não irá desaparecer e que investir e adotar processos que visam contribuir ativamente no fortalecimento dos seus negócios pode ser mais barato e vantajoso do que aguardar o risco do incidente.

Uma pesquisa realizada pela PwC (www.pwc.com.br) demonstra que um dos maiores obstáculos para melhorar a Segurança da Informação nas empresas está relacionado a liderança da organização, como mostra o gráfico abaixo:

Figura 24: Maiores obstáculos para melhorar a segurança da informação



Fato é que uma empresa atualmente não vive sem uso de tecnologia e precisa de suas informações para tomar decisões estratégicas ou obter vantagem competitiva sobre seus concorrentes. Novas ameaças e formas de ataque são lançados diariamente no mundo digital e a corporação que compreende estes riscos e os trata já está um passo à frente de seus concorrentes. Quão cedo a organização adote Políticas de Segurança da Informação menor será o impacto e consequentemente o risco levando assim as empresas que ainda não a possuem como as PMEs a crescerem e conquistarem um mercado ainda maior com os benefícios da tecnologia.

REFERENCIAS

FONTES, EDISON. Políticas e Normas para a Segurança da Informação. Rio de Janeiro, Brasport, 2012.

MOREIRA, NILTON S. Segurança Mínima - uma visão corporativa da segurança de informações. Rio de Janeiro, Axcel Books, 2001.

OLIVEIRA, DJALMA DE PINHO REBOUÇAS DE. Planejamento Estratégico – Conceitos, Metodologia e Práticas. São Paulo, Editora Atlas S.A., 2011.

BRAGA, José Luis. Riscos e a disponibilidade de informação. Disponível em http://www.tiespecialistas.com.br/2013/07/riscos-e-a-disponibilidade-de-informacao/ Acesso 13/mar/2015

CABRAL, João Francisco P. A concepção de ciência de Karl Popper. Disponível em http://www.brasilescola.com/filosofia/a-concepcao-ciencia-karl-popper.htm Acesso 12/fev/2015.

DODT, Cláudio. Gestão de Continuidade de Negócios x Plano de Recuperação de Desastres: entenda a diferença. Disponível em http://www.profissionaisti.com.br/2014/05/gestao-de-continuidade-de-negocios-x-plano-de-recuperacao-de-desastres-entenda-a-diferenca/ Acesso 19/fev/2015

FILADORO, Adriano. Alinhar o plano de recuperação de desastres com o de continuidade nos negócios é mais inteligente. Disponível em http://www.tiespecialistas.com.br/2014/09/alinhar-o-plano-de-recuperacao-de-desastres-com-o-de-continuidade-nos-negocios-e-mais-inteligente/ Acesso 20/fev/2015

FILADORO, Adriano. Recuperação de desastres: questão que ainda intriga muitas empresas e exige medidas urgentes. Disponível em http://www.tiespecialistas.com.br/2013/12/recuperacao-de-desastres-questao-que-ainda-intriga-muitas-empresas-e-exige-medidas-urgentes/ Acesso 10/mar/2015

IETEC - Instituto de Educação Tecnológica. Gerenciamento estratégico de segurança da informação. Disponível em http://www.techoje.com.br/site/techoje/categoria/detalhe_artigo/261 Acesso 09/mar/2015.

IETSUGU, Matheus do Val. Segurança da Informação no ambiente corporativo. Disponível em http://www.profissionaisti.com.br/2013/09/seguranca-da-informacao-no-ambiente-corporativo/ Acesso 18/fev/2015

MANOEL, Sergio. Como a Segurança da Informação pode criar oportunidades para o seu negócio? Disponível em http://segurancadainformacao.modulo.com.br/como-a-seguranca-da-informacao-pode-criar-oportunidades-para-o-seu-negocio. Acesso 14/fev/2015

MENDES, Bruno. Segurança da Informação em Microempresas – Estudo de caso. Disponível em http://www.profissionaisti.com.br/2013/07/seguranca-da-informacao-em-microempresas-estudo-de-caso/ Acesso 18/fev/2015

MENI, Carlos. Backup e sobrevivência empresarial. Disponível em http://www.administradores.com.br/noticias/tecnologia/backup-e-sobrevivencia-empresarial/52510/ Acesso 14/fev/2015.

MORALES, Ivan. 11 de Setembro e a Segurança da Informação. Disponível em https://securityinformationnews.wordpress.com/2013/09/11/11-de-setembro-e-a-seguranca-da-informacao/ Acesso 15/fev/2015.

NEVES, Frederico. Como anda o seu backup? Disponível em http://www.tiespecialistas.com.br/2013/04/como-anda-o-seu-backup/ Acesso 13/mar/2015

PIONTI, Rodrigo. Política de Segurança da Informação – conceitos, características e benefícios. Disponível em http://www.profissionaisti.com.br/2013/08/politica-de-seguranca-da-informacao-conceitos-caracteristicas-e-beneficios/ Acesso 18/fev/2015

PRICOLA, Lilian. Incidentes de segurança. Disponível em http://www.tiespecialistas.com.br/2013/08/incidentes-de-seguranca/ Acesso 12/mar/2015

PWC. Uma defesa ultrapassada. Disponível em https://www.pwc.com.br/pt_BR/br/publicacoes/servicos/assets/consultoria-negocios/pesq-seg-info-2014.pdf Acesso 13/04/2015

RODRIGUES, Gleidson. COBIT – DS5 – Garantir a segurança dos sistemas. Disponível em http://www.tiespecialistas.com.br/2014/04/cobit-ds5-garantir-seguranca-dos-sistemas/ Acesso 25/fev/2015

SENA, Ezequias. Segurança da Informação: Empresas devem reforçar vigilância. Disponível em http://www.profissionaisti.com.br/2013/07/seguranca-da-informacao-empresas-devem-reforcar-vigilancia/ Acesso 18/fev/2015

SYMANTEC. Pesquisa Global de PMEs 2013. Disponível em http://www.symantec.com/content/pt/br/enterprise/images/smb_survey/Symantec%202013%20SMB%20Survey%20Report%20-%20LAM.pdf Acesso 13/04/2015

TELES, Guilherme. Política de segurança da informação. Disponível em http://www.tiespecialistas.com.br/2014/01/politica-de-seguranca/ Acesso 14/fev/2015.

TEOTÔNIO, Ítalo Diego. Entendendo os Fundamentos da Segurança da Informação. Disponível em http://www.profissionaisti.com.br/2013/10/entendendo-os-fundamentos-da-seguranca-da-informacao/ Acesso 19/fev/2015

WIKIPÉDIA. COBIT. Disponível em http://pt.wikipedia.org/wiki/COBIT Acesso 09/mar/2015.

WIKIPÉDIA. Segurança da informação. Disponível em http://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o Acesso 09/mar/2015.