FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE
NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO

ALUNO: MAX RICARDO BORGES RIBEIRO
maxricardobr@gmail.com

TCC

SEGURANÇA DA INFORMAÇÃO: FUNDAMENTOS, NORMAS E CONFORMIDADE

Aracaju, 31 de Julho de 2011

SEGURANÇA DA INFORMAÇÃO: FUNDAMENTOS, NORMAS E CONFORMIDADE

RIBEIRO, Max Ricardo Borges
maxricardobr@gmail.com

RESUMO

Vivemos na era do conhecimento, época em que o bem mais precioso que uma empresa possui são as informações que trafegam em suas dependências e as pessoas que custodiam esses valores. A preocupação com a confidencialidade, a integridade e a disponibilidade dessas informações vem tomando um caráter mais agudo e, desta forma, se fez necessária a criação de padrões que venham disciplinar e direcionar as corporações nas melhores práticas para protegê-las. A ISO/IEC 27000 dá início a uma família de normas que versam sobre segurança da informação e será estudo desse trabalho. No tema, como um dos atores principais na excelência das práticas de segurança da informação, estudaremos ainda normas relacionadas a conformidade e legalidade de alguns ramos de negócio que incrementaram significativamente os sistemas gerenciados no tema.

PALAVRAS CHAVE: Segurança da Informação, Gestão de Riscos, Padrões ISO, ISO 27000.

ABSTRACT

We live in the knowledge era, a time when the most valuable asset a company owns is the information that travels on its premises and people who watch those values. The concern for confidentiality, integrity and availability of this information has been taking a more acute and thus became necessary to create patterns that will guide and discipline the corporations on best practices to protect them. ISO / IEC 27000 launchs a family of standards that deal with information security and will be studying this work. On the topic, as one of the main actors in the excellence of safety practices, we will study further related standards compliance and legality of certain lines of business that significantly increased the information security managed system.

KEYWORDS: Information Security, Risk Management, ISO Standards , ISO 27000.

1. INTRODUÇÃO

O objetivo desse estudo é aprofundar conhecimentos através de uma pesquisa qualitativa e bibliográfica a respeito dos padrões e normativas para implementação das melhores práticas de segurança da informação em um ambiente corporativo. Neste contexto explicaremos também alguns conceitos sobre conformidade através de exemplos de normativas aplicadas em setores específicos.

Quando falamos em segurança da informação estamos necessariamente falando sobre qualquer assunto que impacte positivamente ou negativamente nas atividades da organização, ou seja, falamos sobre confiança que a empresa passa para seus clientes, fornecedores, colaboradores e gerentes.

Não é pertinente oferecer qualquer negócio ou serviço sem que o mesmo denote um nível aceitável de confiança no mercado. Para garantir a eficácia desse processo se faz necessário que a organização adote certos princípios que controlem, protejam e disponibilizem as informações quando necessário e a quem de direito.

Para atestar esses procedimentos algumas organizações se utilizam de certificações. Nesse contexto, quando se publica que determinado processo da empresa possui uma certificação de segurança mundialmente aceita, espera-se que a comunidade visualize aquela organização como confiável oferecendo assim vantagem competitiva no mercado.

Existem alguns negócios que necessitam de algo além de uma certificação - a conformidade. Os perigos da universalização da informação através da internet fez com que algumas áreas precisassem de um cuidado especial, geralmente as áreas que envolvem fluxo de capital. Como exemplo temos os bancos e entidades financeiras que

precisam estar em confomidade com normas do banco central. Tais normas descrevem um conjunto de práticas necessárias para as entidades operarem dentro de seu escopo, podendo impedir o funcionamento do serviço enquando a conformidade não for alcançada.

Veremos nesse trabalho uma descrição inicial dos fundamentos da segurança da informação(SI), um conjunto de normas que versam diretamente sobre o assunto, ou demais normas que tratam orientações de forma universal mas que podem ter conceitos adotados a nossas nessidades.

A principal entidade que padroniza melhores práticas a nível mundial é a ISO(International Organization for Standardization) em conjunto com a IEC(*International Electrotechnical Commission),* e, no âmbito nacional temos a ABNT(Associação Brasileira de Normas Técnicas) que se utiliza das NBRs para normatizar diversos assuntos, dentre eles a segurança da informação.

2. FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO

Um aspecto importante da Segurança da Informação é preservar a confidencialidade, integridade e disponibilidade das informações de uma organização. A perda de um ou mais desses atributos pode ameaçar a confiança na empresa e até mesmo a existência de qualquer organização.

Confidencialidade é a garantia de que a informação é compartilhada apenas entre as pessoas ou organizações autorizadas. Quebras de sigilo podem ocorrer quando os dados não são tratados de forma adequada. Essa divulgação pode ocorrer de boca em boca, através de impressão, cópia, e-mails, criação de documentos e outros dados, etc. A classificação das informações deve determinar o nível de confidencialidade e, conseqüentemente, as garantias e controles adequados.

A integridade assegura que a informação é autêntica e completa. Garante que as informações podem ser invocadas para ser suficientemente precisas para a sua finalidade.

A Disponibilidade garante que os sistemas responsáveis pela entrega, armazenamento e processamento de informação são acessíveis quando necessário, por aqueles que necessitam dessas informações. Um exemplo simples é quando uma loja de comércio eletrônico fica fora do ar, ou seja, indisponível. Isso impacta diretamente nos negócios e reduz a confiança nos mesmos.

Um Sistema de Gestão de Segurança da Informação(SGSI) deve ser implantado de forma coesa e proporcionar algumas funcionalidades de auxílio para o profissional de segurança. Uma delas é a análise de impacto de negócio. Nesse contexto, a empresa começa a visualizar qual é a importância de cada processo para a atividade fim da empresa, ou seja, quanto a empresa perde se aquele processo é interrompido.

Para minimizar tais ocorrências, qualquer SGSI deve necessariamente documentar e implementar planos de continuidade de negócios, que serão ativados sempre que ocorrer um incidente de segurança que indisponibilize um serviço.

3. NORMAS

As normas destacadas a seguir encontram relacionamento direto com a doutrina “Segurança da Informação” assim entidade ISO criou uma família de padrões(Família ISO 27000) que se relacionam entre si e nos ambientam em vários escopos relacionados ao tema.

A finalidade de uma corporação adotar tais padrões é criar um sistema de gerenciamento de segurança da informação (ISO 27001) que servirá como núcleo central para acoplamento das demais normas.

Devemos pensar em Sistema Gerenciado de Segurança da Informação(SGSI) como um ambiente controlado, ou seja, como um conjunto de políticas que regem o ambiente e as respectivas medições e análises dos riscos envolvidos.

Como todos os sistemas de gestão, um SGSI deve se manter efetivo e eficiente ao longo do tempo, para isso, portanto, a norma ISO/IEC 27001 incorpora a metodologia PDCA(Plan-Do-Check-Act) que consiste em “Plan”, planejar; “Do”, fazer ou agir; “Check”, checar ou verificar; e “Action”, no sentido de corrigir ou agir de forma corretiva. Desta forma o ciclo de vida da norma demonstra um caráter cíclico em seu sistema de gestão, sempre partindo do princípio de que nada é tão bom que não possa ser melhorado.

Vale ressaltar que, apesar da família ISO 27000 buscar disciplinar diversos escopos no âmbito da segurança da informação, alguns outros padrões podem ser adotados/adaptados na formação de um SGSI, como veremos mais a frente nas normas complementares.

3.1. Família ISO/IEC 27000

ISO / IEC 27000 é parte de uma família crescente e se revela como um padrão internacional intitulado: Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerenciamento de Segurança da Informação – Visão geral e vocabulário.

A intenção dessa norma é nos fornecer os objetivos, orientações e definições aplicáveis ao padrão.

A família ISO 27000 possui duas componentes que se configuraram como normas de requerimento, sendo elas a ISO 27001 que define os requerimentos genéricos para a definição de um sistema gerenciado de segurança da informação, e a 27006 que define um escopo de requerimentos para certificar uma organização em ISO 27001.

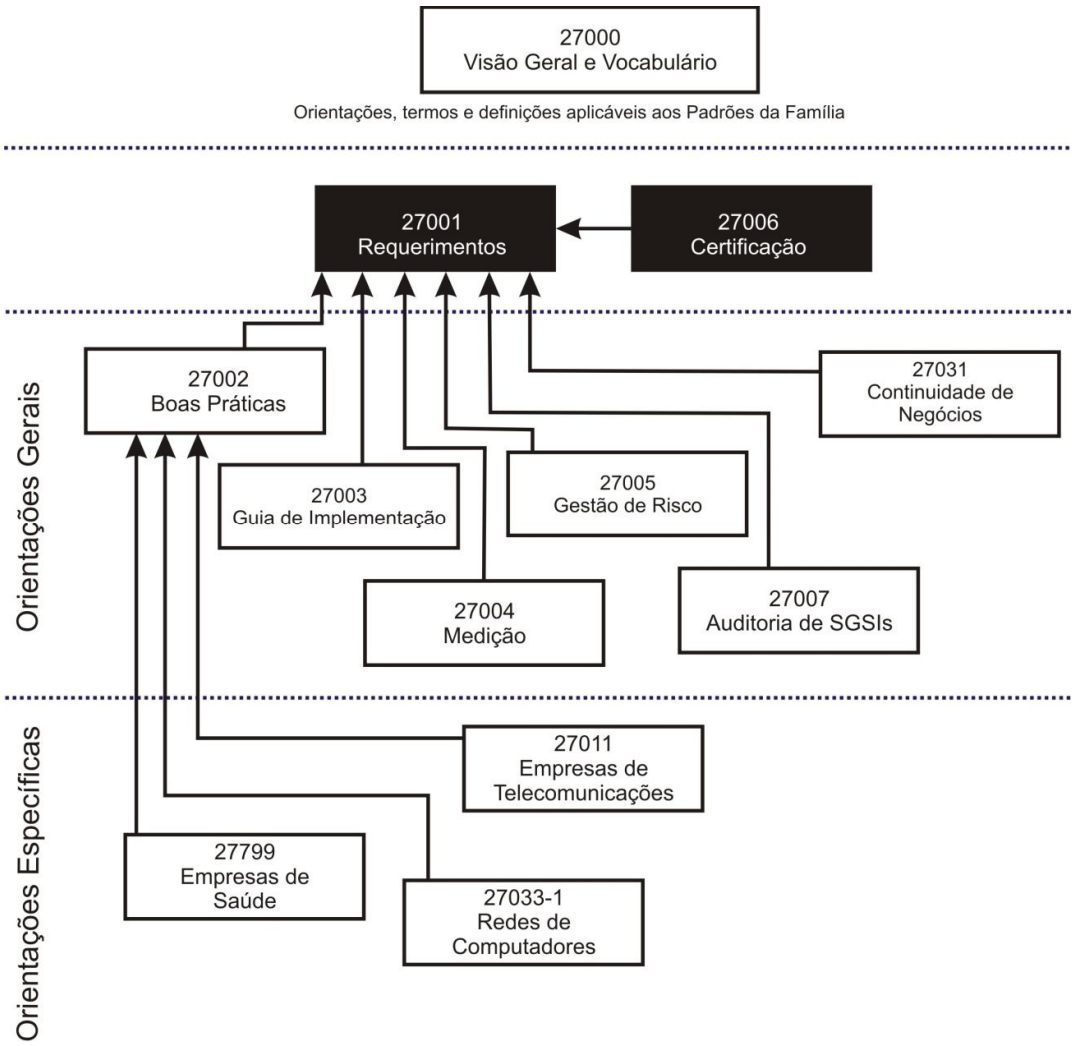
Em seguida temos normas orientativas genéricas que tratam vários campos da segurança da informação, tais como auditoria, gestão de riscos, continuidade de negócios e melhores práticas em segurança.

Existem ainda normas orientativas específicas para determinados ramos de atuação. Em caráter de exemplo podemos citar normas para indústria de saúde, normas para empresas de telecomunicações e para redes de computadores.

Vale ressaltar que as listas não são taxativas e existem várias normas desta família que se encontram em fase de desenvolvimento.

O seguinte gráfico promove uma visão de relacionamento entre algumas das normas da família ISO/IEC 27000:

GRÁFICO 01
PANORAMA DE RELACIONAMENTO DA FAMÍLIA ISO 27000



3.1.1. ISO 27001

Seu nome completo é "*ISO / IEC 27001:2005 - Tecnologia da informação - Técnicas de segurança - sistemas de gestão de segurança da informação – requisitos*" mas é popularmente conhecida somente como "ISO 27001".

A ISO 27001 especifica formalmente um sistema de gestão que visa trazer segurança da informação sob o controle de gestão explícita. Ser uma especificação formal significa que a mesma possui regras mandatórias sobre o assunto explanado. As empresas que afirmam ter adotado a norma ISO / IEC 27001 e requerem a certificação devem ser formalmente auditadas em conformidade com o conteúdo da referida norma.

A ISO 27001 requer:

- Analisar sistematicamente os riscos de segurança da organização da informação, tendo em conta as ameaças, vulnerabilidades e impactos;
- Formular e implementar um conjunto coerente e abrangente de controles de segurança da informação e/ou outras formas de tratamento de risco (tal como a prevenção de risco ou de transferência de risco) para enfrentar os que são considerados inaceitáveis;
- Adotar um processo de gestão global para assegurar que os controles de segurança da informação continuam a atender a segurança da organização necessidades de informação em uma base contínua.

3.1.2. ISO 27002

ISO / IEC 27002 fornece as melhores práticas recomendações sobre a gestão da segurança da informação para uso por parte dos responsáveis por iniciar, implementar ou manter Sistema de Gestão de Segurança da Informação (SGSI).

Esta norma se alinha com a sua irmã ISO/IEC 27001 na medida em que relaciona um enumerado de controles e discrimina de forma menos abstrata os caminhos para a implementação das boas práticas.

3.1.3. ISO 27003

Intitulada como *"Diretrizes para Implantação de um Sistema de Gestão da Segurança da Informação"e* segundo a própria ISO/IEC 27003, "O propósito desta norma é fornecer diretrizes práticas para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), na organização, de acordo com a ABNT NBR ISO/IEC 27001:2005

3.1.4. ISO 27004

Seu nome completo é "*tecnologia da informação - Técnicas de segurança - Gestão da informação de segurança – Medição"*.

Tem como fundamento o auxílio para a Governança da Segurança da informação atribuindo padrões de medição e métricas. Elenca alguns pontos chaves que devem ser medidos para avaliar se a corporação está atingindo suas metas.

O objetivo da ISO / IEC 27004 é ajudar as organizações a medir, gerar relatórios e, consequentemente, melhorar a eficácia dos seus SGSIs.

O padrão inclui as seguintes seções principais:

- Informações gerais sobre métricas de segurança;
- Responsabilidades de gestão;
- Medidas e desenvolvimento de medição;
- operação de medição;
- Análise de dados e medição de resultados de relatórios;

- Segurança da Informação Programa de Medição, avaliação e melhoria.

3.1.5. ISO 27005

Seu título completo é "*ISO / IEC 27005:2008 Tecnologia da informação - Técnicas de segurança - Informações de gestão de riscos de segurança"*.

O objetivo da ISO 27005 é fornecer diretrizes para a gestão de risco de segurança. Ela suporta os conceitos gerais especificados na ISO/IEC 27001 e é projetada para auxiliar a implementação satisfatória da segurança da informação baseada em uma abordagem de gestão de risco.

A gestão de riscos é uma das principais atividades relacionadas com a segurança da informação. É aqui que será definido o que será protegido e que nível de proteção cada ativo demanda. São demonstrados nesse processo qual o valor de cada ativo para a continuidade do negócio da empresa e quais controles esses ativos necessitam.

3.1.6. ISO 27006

Chama-se *"Requisitos para auditorias externas em um Sistema de Gerenciamento de Segurança da Informação"*. Especifica como o processo de auditoria externa de um sistema de gerenciamento de segurança da informação deve ocorrer. A intenção dessa norma é fornecer parâmetros certificação de processos de organizações na ISO 27001.

3.1.7. ISO 27031

A ISO 27031 foi publicada pela BSI no primeiro semestre de 2011 e se intitula "*A tecnologia da informação - - Técnicas de Segurança - Orientações para a preparação da TI para a Continuidade dos Negócios"*. Esta norma fornece a orientação detalhada sobre como as empresas podem aumentar a resiliência da sua infraestrutura de

TI, alinhando seus objetivos no contexto da GCN corporativa, norteada pelos objetivos estratégicos da organização e seu apetite ao risco.

3.1.8. ISO 27037

Essa ISO encontra-se em desenvolvimento e oferecerá um guia para identificação, coleta , aquisição e preservação de evidencia em mídias digitais. Será de grande auxílio na perícia forense e servirá como linha base para auditores validarem provas e evidências definidas em argüição forense.

3.2. Normas Complementares

As normas descritas nesse tópico não fazem parte da família criada especificamente para a segurança da informação, mas por ter conceitos relacionados e por terem importância para o tema, merecem ser explanadas nesse trabalho.

3.2.1. ISO 31000

A ISO 31000 destina-se a ser uma família de normas relativas à gestão de risco em aspecto amplo, não se limitando a tecnologia da informação. Foi codificada pela Organização Internacional de Normalizaçã e seu objetivo é estabelecer princípios e diretrizes genéricas sobre a gestão de risco. A ISO 31000 visa proporcionar um paradigma universalmente reconhecido por profissionais e empresas que empregam processos de gestão de risco para substituir a miríade de normas existentes, metodologias e paradigmas que diferem entre as indústrias, temas e regiões.

Atualmente, a família ISO 31000 inclui:

- ISO 31000: Princípios e Orientações sobre a aplicação
- IEC 31010: Gestão de Risco - Técnicas de Avaliação de Risco
- ISO / IEC 73: Gestão de riscos - Vocabulário

3.2.2. ISO 19011

A ISO 19011:2002 versa sobre diretrizes para auditorias de sistemas de gestão da qualidade e/ ou ambiental.

Essa norma é utilizada para fundamentar critérios de decisão entre análises de riscos qualitativas e quantitativas.

3.2.3. ISO 18044

A norma estabelece critérios que definem o que é incidente de segurança e fornece gestão sobre eles.

3.2.4. ISO 15408

A ISO/IEC 15408 (2005a, 2005b, 2005c) versa sobre o desenvolvimento seguro de software e envolve segurança tanto do ambiente de desenvolvimento quanto da aplicação desenvolvida. As necessidades de segurança devem ser tratadas em todo o ciclo de vida, passando pela gerência de requisitos de segurança, especificação funcional, projeto de alto nível, projeto de baixo nível, até a implementação final do sistema em seu ambiente de produção.

3.2.5. NBR 15999-1

A norma NBR 15999-1 serve como um guia para orientar as empresas na preparação de um plano alternativo em caso de algum incidente, com a adoção de melhores práticas em Gestão de Continuidades de Negócios e orientação de planos de respostas a incidentes, fornecendo uma base para propiciar o entendimento, desenvolvimento e implementação de um documento de GCN em uma organização, independente do seu tamanho e setor.

3.2.6. ISO 38500

Versa sobre governança de tecnologia da informação e provê uma orientação para as organizações a utilizarem de maneira eficaz, eficiente e aceitável.

4. CONFORMIDADE E LEGALIDADE

Conformidade é um conceito muito amplo se definirmos a idéia de adequação com um conceito preestabelecido, porém, no âmbito da segurança da informação podemos definir como qualquer normativa imposta que venha a alterar significativa o escopo ou política de segurança de uma organização.

Podemos definir de forma simples que conformidade é a necessidade que a empresa tem de se adequar com alguma normativa quem um órgão regulador/controlador instituiu em determinado momento. Muitas vezes para que a empresa exista é necessário que haja conformidade de suas práticas de segurança com o regulamento vigente.

Serão tratados exemplos clássicos onde a conformidade ajudou no desenvolvimento dos padrões de segurança em vários segmentos de mercado.

4.1. Sarbanes-Oxley(SOX)

A Lei Sarbanes-Oxley é uma lei estadunidense, assinada em 30 de julho de 2002 pelo senador Paul Sarbanes (Democrata de Maryland) e pelo deputado Michael Oxley (Republicano de Ohio).

A lei Sarbanes-Oxley, apelidada de Sarbox ou ainda de SOX, visa garantir a criação de mecanismos de auditoria e segurança confiáveis nas empresas, incluindo

ainda regras para a criação de comitês encarregados de supervisionar suas atividades e operações, de modo a mitigar riscos aos negócios, evitar a ocorrência de fraudes ou assegurar que haja meios de identificá-las quando ocorrem, garantindo a transparência na gestão das empresas.

Qualquer empresa que negocie ações na bolsa de Nova Iorque deve necessariamente estar em conformidade com a SOX. Entre as empresas nacionais podemos citar: Petrobras, GOL Linhas Aéreas, Sabesp, TAM Linhas Aéreas, Brasil Telecom, Ultrapar (Ultragaz), Companhia Brasileira de Distribuição (Grupo Pão de Açúcar), Banco Itaú e a Telemig Celular.

4.2. PCI

O PCI Security Standards Council é um fórum aberto global para contínuo desenvolvimento, aprimoramento, armazenamento, disseminação e implementação de padrões de segurança para a proteção de dados de contas.

A missão do PCI Security Standards Council é aprimorar a segurança de dados de contas de pagamento, promovendo a educação e a conscientização sobre os Padrões de Segurança PCI. A organização foi fundada pelo American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa, Inc.

Para que uma entidade financeira adote alguma das bandeiras ou efetue convênios com empresas regulamentadas, esta deve estar em conformidade com as regras estabelecidas pelo PCI.

4.3. Banco Central

Através de cartas circulares, o Banco Central disciplina diversas atividades dos demais bancos e alguma entidades financeiras no aspecto de segurança dos processos.

No âmbito nacional ele se mostra como bom exemplo de exigência de conformidade na medida que suas exigências não se limitam no escopo da contabilidade, auditoria e financeiro. Adentra também áreas de tecnologia da informação, engenharia, segurança física e operacional, dentre outras.

4.4. Ordenamento Jurídico

Em vários países é comum que o legislador se preocupe com a área de segurança da informação e baixe normas no âmbito do direito digital. No Brasil, apesar do esfoço de aprovar o projeto de lei 89/2003 de autoria do senador Eduardo Azeredo e que versa sobre crimes digitais e internet, ainda não tivemos sucesso na conversão da mesma em norma jurídica efetiva.

Ainda assim, juristas se utilizam do código civil e código penal para cobrir crimes na internet sempre que a norma se mostra de forma genérica. Quando a norma for taxativa, é comum a utilização de analogia. Desta forma, sem norma atualizada, especifica e disciplinadora, os tribunais vem conseguindo solucionar as lides.

4.5. Convenção de Budapeste

Em 01 de julho de 2004 entrou em vigor a convenção de Budapeste que tratou especificamente sobre crimes digitais.

Para se tornar signatário, é necessário que o país ratifique o acordo e possua no seu ordenamento jurídicio norma versando sobre crimes digitais. Assim, é apresentada a intenção para o Comitê de Ministros do Conselho Europeu que defere ou não o pedido.

Uma parte da convenção é contemplada pelo ordenamento jurídico atual, porém, para o Brasil se tornar signatário, necessariamente terá que aprovar lei sobre os crimes tipificados no âmbito do Direito Eletrônico.

5. REFERÊNCIAS PARA CERTIFICAÇÃO

Inicialmente vale a pena considerar que o caminho para a certificação de um processo de determinada empresa deve ser considerado como um projeto. Com escopo, objetivos e prazos bem definidos.

O processo de certificação consiste de duas fases. Na primeira são reunidos documentos que serão descritos a seguir e estes serão apresentados para a entidade certificadora em caráter não necessariamente presencial. Esses documentos comprovarão que a empresa se encontra no direcionamento correto para implementação das boas pratícas em segurança da informação. Caso haja alguma irregularidade nessa apresentação, serão apontados os problemas e as correções deverão ser feitas em um intervalo de tempo apontado. Na segunda fase, a certificadora fará uma auditoria dos processos e documentos que implantaram o sistema de gestão de segurança da informação dentro das dependências da solicitante. É uma abordagem muito mais aprofundada para determinar se a empresa está ou não habilitada para condição de certificada.

A seguir serão apresentados os principais passos para a certificação de acordo com o ciclo PDCA.

5.1. Planejamento

Para estabelecer um sistema de gestão, a empresa deve seguir os seguintes passos:

- Definir o escopo do processo a ser certificado e seus limites
- Definir políticas voltadas ao SGSI.
- Definir a abordagem de avaliação de risco que será adotada

- Identificar os Riscos
- Analisar e avaliar os riscos
- Identificar e avaliar as opções de tratamento dos riscos
- Definir controles e seus objetivos para tratamento do risco
- Obter aprovação da gerência sobre a proposta de riscos residuais
- Preparar uma declaração de aplicabilidade

5.1.1. Produtos gerados nesta fase

- Política de segurança da informação
- Escopo
- Relatório de análise de riscos
- Declaração de aplicabilidade – Esta tem grande importância no processo pois demonstra um panorama geral do processo, informando os objstivos de controle, os controles aplicados, os responsáveis, os documentos associados e as ultimas revisões.

Aqui terminam os passos necessários para propor a auditoria de fase um.

5.2. Execução

Implementação e operação de um sistema de gestão de segurança da informação. Seguem os passos que descrevem essa fase.

- Planejar e implementar um plano de tratamento de riscos
- Implementar os controles selecionados na fase de planejamento
- Definir métricas de efetividade

- Implementar programa de treinamento e conscientização em segurança da informação
- Gerenciar as operações e os recursos do SGSI
- Implementar ações para detecção e resposta a incidentes de segurança da informação

5.2.1. Produtos desta fase

- Plano de Tratamento de Risco
- Documentação de controles e respectivos objetivos
- Definições de métricas
- Plano de treinamento e conscientização dos colaboradores
- Documentação de resposta a incidentes

5.3. Checar

Monitorar e revisar o sistema de gestão de segurança da informação. a seguir os passos são apresentados.

- Executar procedimentos para revisão e monitoramento dos controles
- Proceder revisões regulares sobre a efetividade do SGSI
- Medir a eficácia dos controles
- Revisar em períodos definidos as avaliações de riscos
- Conduzir auditorias internas ao SGSI
- Atualizar planos de segurança
- Registrar ações e eventos sobre segurança da informação

5.3.1. Produtos desta fase

- Revisão de avaliação de riscos
- Revisão de controles
- Revisão de eficácia
- Documentação de auditoria interna
- Documentação de ações e eventos
- Planos de Segurança atualizados

5.4. Agir

Essa fase tem como internção manter e melhorar o sistema de gestão de segurança da informação.

- Implementar as melhorias identificadas na fase anterior
- Tomar medidas corretivas e preventivas apropriadas
- Comunicar as melhorias a todas as partes interessadas
- Assegurar que as melhorias alcançarão seus objetivos

5.4.1. Produtos desta fase

- Plano de implementação de melhoria
- Plano de ações corretivas
- Plano de ações preventivas
- Plano de comunicação
- Plano de revisão de melhorias implementadas

5.5. Passos para Certificação

Passo 1: A efetiva decisão da empresa em obter a certificação ISO 27001.

Passo 2: A gerência se compromete, atribui responsabilidades e aloca recursos.

Passo 3: Definição de uma política de segurança da informação.

Passo 4: Definição do escopo do sistema de gestão de segurança da informação.

Passo 5: Executar uma análise de riscos para o escopo definido.

Passo 6: Definir como vão ser gerenciados os riscos encontrados.

Passo 7: Definir objetivos de controles e controles que serão implementados

Passo 8: Preparar uma Declaração de Aplicabilidade.

Passo 9: Implementar os controles.

Passo 10: Identificar a entidade certificadora

Passo 11: Apresentar à certificadora:

- Declaração da empresa – descrição da empresa(quem somos nós);
- Declaração de escopo do sistema de gestão de segurança da informação;
- Declaração de aplicabilidade.

Passo 12: Auditoria fase I – Revisão de documentação pela certificadora.

Passo 13: Resolução de problemas encontrados na primeira auditoria.

Passo 14: Auditoria fase II – Auditoria completa in loco para determinar se:

- O SGSI está implementado e operante;
- O SGSI está sendo revisado e monitorado;
- O SGSI está sendo mantido e melhorado.

Passo 15: Recomendação para certificação, recomendação para certificação condicional ou Rejeição.

6. O VALOR DA CERTIFICAÇÃO ISO 27001 NO AMBIENTE CORPORATIVO

Em pesquisa em cases de empresas que adquiriram a certificação ISO 27001, são encontrados alguns benefícios que justificam o esforço empreendido para implementar o sistema de gestão.

6.1. Benefícios diretos

- Maior confiabilidade e segurança nos sistema da empresa.
- Maior disponibilidade do sistema com a redução das vulnerabilidades.
- Visitas e auditorias de re-certificação garatem o negócio sempre atualizado com as melhores práticas em segurança da informação.
- Aumento de lucros devido ao aumento da disponibilidade dos serviços, à aplicação correta dos recursos e à percepção dos clientes em relação ao negócio da empresa. A certificação demonstra que a empresa pode ser confiável de modo a garantir aos clientes que seus dados estão seguros. Assim, esta cria um melhor posicionamento competitivo no mercado. O cliente aceita pagar um pouco mais devido à confiança que tem no serviço.
- Cumprimento da legislação - Implementar ISO27001 obriga as empresas a manter a conformidade com a legislação e as normas pertinentes ao negócio.

6.2. Benefícios indiretos

- Os gerentes têm mais controle sobre a organização e informação de melhor de qualidade. O esforço de gestão é, portanto, reduzido.
- Melhoria nas relações humanas através de políticas claras, procedimentos e orientações melhor definidas.
- Aumento do profissionalismo na empresa, pois os colaboradores entendem que a segurança é parte importante para o crescimento dos negócios.

CONSIDERAÇÕES FINAIS

Cabe analisar esse trabalho como um repositório de definições, conceitos, normas e orientações no que se reporta à segurança da informação em seu caráter corporativo. A adoção de alguns padrões apresentados são não só contributivos para a segurança corporativa, como também são estratégicos na medida que, em alguns ramos de atividades, um incidente de segurança pode gerar danos financeiros significativos e até acabar com o negócio.

As normas apresentadas aqui não se isolam em seus conceitos, e sim, partem de um critério de completude entre as mesmas sobre um tema muito mais amplo que trata de risco operacional, segurança da informação ou continuidade de negócios.

A família ISO 27000 é apresentada como um rol de normas criado para tratar dos assuntos elencados acima, e tem como sua principal norma, norteadora de todas as demais a ISO 27001 que traz requisitos para a definição de um sistema gerenciado de segurança da informação. Todas as demais normas da família, de forma direta ou indireta, se referem a conceitos definidos pela ISO 27001.

Vale ressaltar que a lista apresentada não é taxativa, existem diversas outras normas dessa família, algumas em versão “draft”(ainda não estão em sua versão final para publicação) e outras prestes a serem lançadas.

A conformidade vem balizar a segurança da informação com um aspecto de obrigatoriedade. Temos nela um grande suporte para incremento de qualidade dos serviços oferecidos com maior nível de risco possível. Isso faz com que a confiança que o público tem nos serviços prestados por determinado ramo aumente.

Por fim, defino que segurança não trata de outra coisa, senão de confiança. A confiança que o usuário tem de utilizar serviços bancários pela internet depende da

imagem que a empresa tem em relação ao tratamento de suas informações. Se o usuário compra ou não em um e-commerce é devido a confiança de que aquele site cumpre padrões de segurança que estejam de acordo com seus anseios.

Devido a isso, devemos lembrar que a segurança da informação não deve ser considerada um freio ao negócio, como algo que venha burocratizar os serviços prestados. E sim como um panorama estratégico que pode posicionar uma empresa positivamente ou negativamente no mercado.

REFERÊNCIAS

BEAL, Adriana. Gestão Estratégica da Informação. 1ª edição.144 páginas. SãoPaulo: Editora Atlas, 2004.

RAMOS, Anderson. Security Officer – 1º guia oficial para formação de gestores em segurança da informação. 1ª edição. 460 páginas. Rio Grande do Sul: Editora Zouk, 2006.

SÊMOLA, Marcos. Gestão da Segurança da Informação: Uma Visão Executiva. 1ª edição. 160 páginas. São Paulo: Editora Campus, 2003.

http://www.degrandison.ie/ - Acessado em 01/05/2011.

http://www.iso27001security.com/ - Acessado em 03/05/2011.

http://www.iso27000.com.br – Acessado em 28/05/2011.

http://pt.wikipedia.org/wiki/ISO_27001 - Acessado em 12/05/2011

http://www.*iso*.org – *Acessado em 12/05/2011*