FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE - FANESE

NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO – NPGE

CURSO DE PÓS-GRADUAÇÃO "LATO SENSU"

MBA EM GERÊNCIA DE PROJETOS

NBR ISO/IEC 27002:2005 CONCEITOS E GESTÃO DE RISCO EM TI

ANDRÉ LUIZ VIEIRA DE JESUS SILVEIRA

Aracaju

2014

ANDRÉ LUIZ VIEIRA DE JESUS SILVEIRA

NBR ISO/IEC 27002:2005 CONCEITOS E GESTÃO DE RISCO EM TI

Trabalho de Conclusão de Curso apresentado ao Núcleo de Pós-graduação e Extensão da Faculdade de Administração e Negócios de Sergipe como exigência para obtenção do título de MBA em Gerência de Projetos, sob orientação do Esp. Adriano Lima.

Orientação: Adriano Lima.

ARACAJU

2014

NBR ISO/IEC 27002:2005 CONCEITOS E GESTÃO DE RISCO EM TI

André Luiz Vieira de Jesus **SILVEIRA**[1]
andreinfrati@gmail.com
Orientação: Adriano **LIMA**[2]**.**

RESUMO

Esta pesquisa científica apresenta um estudo sobre Técnicas de Segurança da Informação e Gestão de Risco em TI, baseado na normal NBR ISSO/IEC 27002:2005, Código de prática para a gestão da segurança da informação, onde fala sobre a informação, objetivos do negócio e requisitos de qualidade. A norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos proveem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação. Os objetivos de controle e os controles da norma tem como finalidade ser implementados para atender aos requisitos identificados por meio da análise/avaliação de riscos. Com a norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança, e para ajudar a criar confiança nas atividades interorganizacionais.

PALAVRAS CHAVE

Tecnologia da Informação, Segurança, Risco.

ABSTRACT

This research presents a scientific study on Technical Information Security and Risk Management in IT, based on standard NBR ISO / IEC 27002:2005, Code of practice for information security management, where he talks about information, business objectives and quality requirements. The standard establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization. The goals set general guidelines reactions come on generally accepted goals for the management of information security. The control objectives and controls of the standard is intended to be implemented to meet the requirements identified by the analysis / risk assessment. With the standard can serve as a practical guide to develop procedures for information security in the organization and efficient security management practices, and to help build confidence in inter-organizational activities.

---

[1] Graduado em Gestão de Tecnologia da Informação, Pós-graduando em Gestão de Tecnologia da Informação e MBA em Gerência de Projetos, possuo algumas certificações como ITIL, Cobit, ISO 20000 e MCP em Windows Server 2003.

[2] Gerente de Projetos, Graduado em Ciências da Computação, Especialista em Segurança da Informação, Certificado PMP, E-mail: ssa.adriano@gmail.com.

KEYWORDS

Information Technology, Security.

1 INTRODUÇÃO

Segundo a norma NBR ISO/IEC 27002:2005, A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.

A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Segurança da informação é a proteção de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negocio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

A segurança da informação é 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 que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão de negócio.

Segundo a norma NBR ISO/IEC 27002:2005, A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação pode ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o

atendimento aos requisitos legais e a imagem da organização junto ao mercado.

As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, hackers e ataques de denial of servisse estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

A segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infraestruturas criticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como o governo eletrônico (e-gov) ou o comércio (e-business), e evitar ou reduzir os riscos relevantes. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída reduz a eficácia da implementação de um controle de acesso centralizado.

Muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser alcançada por meios técnicos e limitada e deve ser apoiada por uma gestão e por procedimentos apropriados. A identificação de controles a serem implantados requer um planejamento cuidadoso e uma atenção aos detalhes. A gestão da segurança da informação requer pelo menos a participação de todos os funcionários da organização. Pode ser que seja necessária também a participação de acionistas, fornecedores, terceiras partes, clientes ou outras partes externas. Uma consultoria externa especializada pode ser também necessária.

Segundo George Westerman , 2008. “O termo Risco é utilizado para designar o resultado objetivo da combinação entre a probabilidade de ocorrência de um determinado evento, aleatório, futuro e que independa da vontade humana, e o impacto resultante caso ele ocorra. É também uma a probabilidade de ocorrência de um determinado evento que gere prejuízo econômico.”

Podemos dizer que as empresas assumem riscos ao colocar produtos ou serviços novos no mercado. Um risco pode ser classificado como uma oportunidade e/ou uma ameaça. Uma empresa corre o risco de ganhar muito dinheiro com o novo produto/serviço (oportunidade) ou corre o risco de ter um grande prejuízo (ameaça). Grande parte dos riscos fogem do controle das empresas, portanto, a única opção é ter planos para caso os riscos se tornem verdade. A importância de se analisar os riscos cresce a cada dia.

Um dos acontecimentos mais conhecidos relacionados à mitigação de riscos é o “Acordo de Basiléia I” de 1988 na cidade de Basiléia na Suíça. O acordo de Basiléia tem o objetivo de fixar índices, criando uma padronização financeira mundial, tendo como objetivo diminuir o risco operacional, e consequentemente o risco das instituições financeiras “quebrarem”. Um exemplo do acordo é que os bancos só podem emprestar 12 vezes o valor de seu capital e reservas. Em 2004 o acordo ganhou sua segunda versão, o Basiléia II, trazendo melhorias nas regras estabelecidas. Existem uma série de outras regras, entre elas regras que impactam diretamente a área de TI.

Alguns pontos que o Acordo Basiléia II impacta em TI são: capacidade de armazenamento de dados, integridade das transações, segurança, contingência, planejamento da capacidade, integridade na emissão de relatórios entre outros.

A Gestão de Riscos de TI precisa estar no dia-a-dia dos CIOs através de: processos que precisam ser implementados para mitigação de riscos, ajustes na estrutura organizacional para acomodar estes novos processos, definição de indicadores “de riscos”, incluir a análise de riscos no Plano Diretor de TI ou Plano de Tecnologia da Informação, fazendo com que este assunto seja recorrente dentro da TI.

A primeira norma mundial (similar a ISO) referente Gestão de Riscos é a AS/NZS 34, elaborada em 1999. As etapas da gestão dos riscos são divididas em 2 fases: Identificação e avaliação.

Fase 1) Identificação

Estabelecimento do contexto: Relacionada ao escopo da avaliação que será realizada. Dentro de qual cenário o risco será analisado. Exemplo: E se uma enchente ocorrer em Blumenau?

Identificação de Riscos: É identificar o que pode dar errado dentro do escopo definido. O que uma enchendo afetaria na nossa organização para clientes e colaboradores?

Análise dos Riscos: Quais as consequências do risco caso ocorra. Dentro da análise dos riscos, temos 2 sub-atividades:

Análise qualitativa dos riscos: Identificar o impacto que certo risco poderá trazer para a organização e qual a probabilidade dela ocorrer.

Análise quantitativa: Estimar em valores $$ o quanto este risco poderá custar para a organização.

Fase 2) Avaliação

Plano de Resposta aos Riscos: Diante de um risco pode-se tomar 4 tipos de ação.

Evitar: Tomar uma ação para evitar totalmente um risco. Por exemplo, proibir o acesso a internet dentro da organização. Isto evita que vírus sejam copiados da internet.

Transferir: Pode-se transferir o risco para um terceiro. Exemplo: passar a administração de um servidor para um terceiro, e colocar em contrato penalidades caso o acordo estabelecido não seja cumprido.

Mitigar: Tomar ações para minimizar riscos. Exemplo: Limitar o uso da internet para alguns sites confiáveis somente.

Aceitar: Existem alguns riscos que são tão caros de serem “combatidos” que vale mais á pena aceitar o risco e ter um “plano B” para caso o mesmo ocorra. Exemplo: Guardar backup fora da empresa caso algum sinistro ocorra. Isso é geralmente utilizado pois o custo de se ter uma estrutura de TI de continuidade a parte não justifica (que é a realidade da maioria das organizações). Guarda-se somente um backup fora da empresa para restaurar o ambiente caso o sinistro ocorra.

Monitorar e controlar os Riscos: Acompanhar o dia-a-dia, fazendo o monitoramento dos riscos atuais e identificando novos riscos. Esta etapa também tem o objetivo de verificar se as políticas e procedimentos quanto a

gestão dos riscos estão sendo seguidas. Também os indicadores referentes riscos são acompanhados nesta etapa.
Bem, a gestão de riscos é um processo importante e contínuo, e deve fazer parte da estratégia das organizações, já que como sabemos, os riscos de TI, não são de responsabilidade somente de TI, mas sim de toda a organização, principalmente dos tomadores de decisão.

2 COMO ESTABELECER REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

Segundo a norma NBR ISO/IEC 27002:2005, É essencial que uma organização identifique os seus requisitos de segurança da informação. Existem três fontes principais de requisitos de segurança da informação.

1. Uma fonte é obtida a partir da análise/avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negocio da organização. Por meio da análise/avaliação de riscos, são identificadas as ameaças aos ativos e as vulnerabilidades destes, realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.
2. Uma outra fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural.
3. A terceira fonte é um conjunto particular de princípios, objetivos e os requisitos do negócio para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

3 ANALISANDO/AVALIANDO OS RISCOS DE SEGURANÇA DA INFORMAÇÃO

Segundo a norma NBR ISO/IEC 27002:2005, Os requisitos de segurança da informação são identificados por meio de uma análise/avaliação sistemática dos riscos de segurança da informação. Os gastos com os controles precisam

ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança da informação.

Os resultados da análise/avaliação de riscos ajudarão a direcionar e a determinar as ações gerenciais apropriadas e as prioridades para o gerenciamento dos riscos da segurança da informação, e para a implementação dos controles selecionados para a proteção contra estes riscos.

Convém que a análise/avaliação de riscos seja periodicamente para contemplar quaisquer mudanças que possam influenciar os resultados desta análise/avaliação.

4 EVOLUÇÃO EM 05 PASSOS

Segundo Hon Tran, os cinco passos listados a seguir podem auxiliar as organizações na avaliação de seus níveis de riscos de TI, no desenvolvimento de programas de remediação e finalmente, construir efetivos e contínuos programas de Gerenciamento de Riscos de TI.

4.1 Desenvolver a consciência dos riscos de TI

A mitigação dos riscos de TI começa com um levantamento completo, incluindo:
- estabelecimento do escopo do programa (Até que ponto a identificação dos riscos de TI é apropriada?)

- construção de um perfil de riscos para a organização baseado em suas prioridades totais

- identificação das áreas de risco da TI

Essa avaliação deve considerar também os requerimentos, capacidades e vulnerabilidades atuais da organização. Por último, esta etapa envolve a identificação e classificação de suas ameaças, vulnerabilidades e fraquezas com consequente associação de prioridades a estas de acordo com o risco.

4.2 Quantificar os impactos aos negócios

A quantificação dos impactos aos negócios é normalmente o passo mais difícil - e o mais importante. Até que estes impactos sejam quantificados, positiva ou negativamente, a gestão da TI deve ser capaz de priorizá-los juntamente a seus pares e obter os recursos necessários à suas mitigações.

A quantificação do impacto aos negócios pode ser estabelecida de duas formas:
1) Através da priorização dos riscos baseado em seus potenciais de impacto aos negócios de acordo com o perfil de riscos da organização e a facilidade ou dificuldade de suas mitigações, medidas em tempo, recursos funcionais e investimentos.
2) Através da construção de argumentos de negócios detalhados somente para aqueles riscos identificados como de alto impacto.

4.3 Desenvolvimento de soluções

Neste ponto, a organização conhece o escopo e os componentes do programa de gerenciamento de riscos de TI, seu status atual e a priorização de cada área dos riscos de TI.

O próximo passo é desenvolver um conjunto de soluções de remediação, considerando os elementos clássicos: pessoas, processos e tecnologias. Cada um com seus respectivos requerimentos, especificações, objetivos e funções.

Esta fase também inclui uma detalhada análise de custos para manter os custos e benefícios das iniciativas propostas alinhados aos objetivos organizacionais.

4.4 Alinhar a TI ao valor dos negócios; implementar as soluções

A fase de implementação determina se as iniciativas voltadas à mitigação dos riscos estão satisfatoriamente implementadas considerando as pessoas, processos e tecnologias envolvidos e também considerando os objetivos de todos os interessados dentro da organização. Esta fase também requer avaliações e melhorias constantes no sentido de obter a mais eficiente

mitigação considerando as diferentes prioridades associadas aos riscos. Com um sistema de métricas coerente e com capacidades de gerenciamento de performance, as organizações conseguem alcançar a etapa de obtenção da dados base, ajustes de performance e avaliação da efetividade do programa ante o cenário original.

4.5 Construção e gerenciamento unificado de capacidades

Uma vez iniciada a implementação da primeira onda de soluções de risco de TI, as organizações podem instituir a elaboração de programas visando à melhoria contínua da governança de seus programas de gerenciamento de riscos de TI.

Adaptando seus esforços, suas experiências e a evolução de sua maturidade, as organizações podem evitar ou superar os desafios mais comuns da fase de implementação, como projetos reativos e ausência de progressos quantificáveis.

Embora não exista uma fórmula mágica para o gerenciamento de riscos de TI, estes processos podem auxiliar as organizações a gerenciar seus recursos efetivamente na busca por melhorias reais e duradouras ao gerenciamento de riscos, com frequente redução da complexidade e dos custos da infraestrutura de TI.

5 SELEÇÃO DE CONTROLES

Segundo a norma NBR ISO/IEC 27002:2005, Uma vez que os requisitos de segurança da informação e os riscos tenham sido identificados e as decisões para o tratamento dos riscos tenham sido tomadas, convém que controles apropriados sejam selecionados e implementados para assegurar que os riscos sejam reduzidos a um nível aceitável. Os controles podem ser selecionados a partir desta Norma ou de um outro conjunto de controles ou novos controles podem ser desenvolvidos para atender às necessidades específicas, conforme apropriado. A seleção de controles de segurança da informação depende das decisões da organização, baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado

à organização, e convém que também esteja sujeito a todas as legislações e regulamentações nacionais e internacionais, relevantes.

Alguns dos controles nesta Norma podem ser considerados como princípios básicos para a gestão da segurança da informação e podem ser aplicados na maioria das organizações. Estes controles são explicados em mais detalhes no item “Ponto de partida para a segurança da informação”.

6 PONTO DE PARTIDA PARA A SEGURANÇA DA INFORMAÇÃO

Segundo a norma NBR ISO/IEC 27002:2005, Certo número de controles pode ser considerado um bom ponto de partida para a implementação da segurança da informação normalmente usada.

Os controles considerados essenciais para uma organização, sob o ponto de vista legal, incluem, dependendo da legislação aplicável:

a) Proteção de dados e privacidade de informações pessoais;
b) Proteção de registros organizacionais;
c) Direitos de propriedade intelectual.

Os controles considerados práticas para a segurança da informação incluem:

a) Documento da politica de segurança da informação;
b) Atribuição de responsabilidades para a segurança da informação;
c) Conscientização, educação e treinamento em segurança da informação;
d) Processamento correto nas aplicações;
e) Gestão de vulnerabilidades técnicas;
f) Gestão da continuidade do negócio;
g) Gestão de incidentes de segurança da informação e melhorias.

Esses controles se aplicam para a maioria das organizações e na maioria dos ambientes.

Convém observar que, embora todos os controles sejam importantes e devem ser considerados, a relevância de qualquer controle deve ser determinada segundo os riscos específicos a que uma organização está exposta. Por isto,

embora o enfoque acima seja considerado um bom ponto de partida, ele não substitui a seleção de controles, baseado na análise/avaliação de riscos.

7 FATORES CRÍTICOS DE SUCESSO

Conforme a norma NBR ISO/IEC 27002:2005, A experiência tem mostrado que os seguintes fatores são geralmente críticos para o sucesso da implementação da segurança da informação dentro de uma organização:

a) Politica de segurança da informação, objetivos e atividades, que reflitam os objetivos do negocio;
b) Uma abordagem e uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional;
c) Comprometimento e apoio visível de todos os níveis gerenciais;
d) Um bom entendimento dos requisitos de segurança da informação, da análise/avaliação de riscos e da gestão de risco;
e) Divulgação eficiente da segurança da informação para todos os gerentes, funcionários e outras partes envolvidas para se alcançar a conscientização;
f) Distribuição de diretrizes e normas sobre a politica de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas;
g) Provisão de recursos financeiros para as atividades da gestão de segurança da informação;
h) Provisão de conscientização, treinamento e educação adequados;
i) Estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação;
j) Implementação de um sistema de medição, que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria.

8 ANALISANDO/AVALIANDO OS RISCOS DE SEGURANÇA DA INFORMAÇÃO

Segundo a norma NBR ISO/IEC 27002:2005, Convém que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios para aceitação dos riscos e dos objetivos relevantes para a organização. Convém que os resultados orientem e determinem as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação, e para a implementação dos controles selecionados, de maneira a proteger contra estes riscos. O processo de avaliar os riscos e selecionar os controles pode precisar ser realizado várias vezes, de forma a cobrir diferentes partes da organização ou de sistemas de informação específicos.

Convém que a análise/avaliação de riscos inclua um enfoque sistemático de estimar a magnitude do risco (análise de riscos) e o processo comparar os riscos estimados contra os critérios de risco para determinar a significância do risco (avaliação do risco).

Convém que as análises/avaliações de riscos também sejam realizadas periodicamente, para contemplar as mudanças nos requisitos de segurança da informação e na situação de risco, ou seja, nos ativos, ameaças, vulnerabilidades, impactos, avaliação do risco e quando uma mudança significativa ocorrer. Essas análises/avaliações de riscos devem ser realizadas de forma metódica, capaz de gerar resultados comparáveis e reproduzíveis.

Convém que a análise/avaliação de riscos de segurança da informação tenha um escopo claramente definido para ser eficaz e inclua os relacionamentos com análises/avaliações de riscos em outras áreas, se necessário.

9 TRATANDO OS RISCOS DE SEGURANÇA DA INFORMAÇÃO

Segundo a norma NBR ISO/IEC 27002:2005, Convém que, antes de considerar o tratamento de um risco, a organização defina os critérios para determinar se os riscos podem ser ou não aceitos. Riscos podem ser aceitos se, por exemplo, for avaliado que o risco é baixo ou que o custo do tratamento não é

economicamente viável para a organização. Convém que tais decisões sejam registradas.

Para cada um dos riscos identificados, seguindo a análise/avaliação de riscos, uma decisão sobre o tratamento do risco precisa ser tomada. Possíveis opções para o tratamento do risco incluem:

a) Aplicar controles apropriados para reduzir os riscos;
b) Conhecer e objetivamente aceitar os riscos, sabendo que eles atendem claramente à politica da organização e aos critérios para a aceitação de risco;
c) Evitar riscos, não permitindo ações que poderiam causar a ocorrência de riscos;
d) Transferir os riscos associados para outras partes, por exemplo, seguradora ou fornecedores.

Convém que, para aqueles riscos onde a decisão de tratamento do risco seja a de aplicar os controles apropriados, esses controles sejam selecionados e implementados para atender aos requisitos identificados pela análise/avaliação de riscos. Convém que os controles assegurem que os riscos sejam reduzidos a um nível aceitável, levando-se em conta:

a) Os requisitos e restrições de legislação e regulamentações nacionais e internacionais;
b) Os objetivos organizacionais;
c) Os requisitos e restrições operacionais;
d) Custo de implementação e a operação em relação aos riscos que estão sendo reduzidos e que permanecem proporcionais às restrições e requisitos da organização;
e) A necessidade de balancear o investimento na implementação e operação de controles contra a probabilidade de danos que resultem em falhas de segurança da informação.

Os controles podem ser selecionados através da norma da ABNT NBR ISSO/IEC 17799:2005 ou de outros conjuntos de controles, ou novos controles

podem ser considerados para atender às necessidades específicas da organização. É importante reconhecer que alguns controles podem não ser aplicáveis a todos os sistemas de informação ou ambientes, e podem não ser praticáveis para todas as organizações.

Convém que os controles de segurança da informação sejam considerados na especificação dos requisitos e nos estágios iniciais dos projetos e sistemas. Caso isso não seja realizado, pode acarretar custos adicionais e soluções menos afetivas, ou mesmo, no pior caso, incapacidade de se alcançar a segurança necessária.

Convém que seja lembrado que nenhum conjunto de controles pode conseguir a segurança completa, e que uma ação gerencial adicional deve ser implementada para monitorar, avaliar e melhorar a eficiência e eficácia dos controles de segurança da informação, para apoiar as metas da organização.

10 O QUE É A ORGANIZAÇÃO ISO.

Conforme informação passada pela autora Márcia Regina Guerra, membro da Tiexames, A ISO – International Organization for Standardization – é a maior organização para desenvolvimento e publicação de normas. Ela faz o relacionamento entre os órgãos nacionais de normatização de diferentes países. É uma organização não governamental, que forma uma ponte entre os setores público e privado. Sediada em Genebra, na Suiça, foi fundada em 1946. Mais de 160 países integram esta importante organização internacional, especializada em padronização e cujos membros são entidades normativas de âmbito nacional. O Brasil é representado pela Associação Brasileira de Normas Técnicas – ABNT. O propósito da ISO é desenvolver e promover normas que possam ser utilizadas igualmente por todos os países do mundo. A sigla ISO foi originada da palavra isonomia.

REFERÊNCIAS BIBLIOGRÁFICAS

Acesso ao site http://www.iso.org em 17/05/2014.

Acesso ao site http://tiexames.com.br em 18/05/2014.

Acesso ao site http://www.comexito.com.br em 24/05/2014.

Acesso ao site http://www.virtue.com.br/blog/?p=28 em 07/06/2014.

ABNT NBR ISO/IEC 27002:2005 - Primeira edição 31.08.2005.

GUERRA, Márcia Regina, 2010. Fundamentos da Segurança da Informação com base na ISO/IEC 27002.

The Basics of Information Security - A Practical Handbook.

Information Security Foundation based on ISO/IEC 27002 edition April 2009.

Westerman, George, 2008. Risco de TI, O

Hunter, Richard, 2008. Risco de TI, O