UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

SABRINA VITÓRIO OLIVEIRA SENCIOLES

PROPOSTA DE CRITÉRIOS PARA AVALIAÇÃO DA SEGURANÇA DA INFORMAÇÃO

MONOGRAFIA

CURITIBA
2011

SABRINA VITÓRIO OLIVEIRA SENCIOLES

PROPOSTA DE CRITÉRIOS PARA AVALIAÇÃO DA SEGURANÇA DA INFORMAÇÃO DE UMA ORGANIZAÇÃO

Monografia apresentada como requisito parcial à obtenção do título de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Augusto Foronda

CURITIBA
2011

Dedico este trabalho à minha família, pelo apoio nesta e em todas as outras fases da minha vida.

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela oportunidade de aprender sempre, a cada dia.

Agradeço a meus pais, pela oportunidade que me deram de estudar.

A meu marido, por as vezes não concordar, mas sempre me apoiar nas minhas “loucuras”.

Ao Prof. Dr. Augusto Foronda, por conduzir e lapidar os conceitos aqui apresentados.

RESUMO

SENCIOLES, Sabrina Vitório O. **Proposta de critérios para avaliação da segurança da informação de uma organização**. 2011. 56 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná, Curitiba, 2011.

O projeto de pesquisa tem como tema central a segurança da informação. A elaboração de uma proposta para avaliação de aspectos físicos, lógicos e culturais de uma organização de menor porte em relação a segurança da Informação é o seu principal objetivo. A pesquisa é predominantemente bibliográfica. Entre os resultados esperados, destaca-se um conjunto de critérios para apoio a avaliação de qualquer empresa em relação a sua aderência a norma ABNT NBR ISO/IEC 27002:2005.

Palavras-chave: Segurança da informação. ABNT NBR ISO/IEC 27002:2005. Política de Segurança da informação.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

PDCA	- Planejamento, Execução, Controle e Ação
RH	- Recursos Humanos
SGSI	- Sistema de gestão de segurança da informação
TI	- Tecnologia da Informação
VPN	- *Virtual Private Network*

LISTA DE SIGLAS

ABNT	- Associação Brasileira de Normas e Técnicas
CERT.BR	- Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil
CNPq	- Conselho Nacional de Desenvolvimento Científico e Tecnológico
IEC	- *International Electrotechnical Commission*
ISO	- *International Organization for Standardization*
UTFPR	- Universidade Tecnológica Federal do Paraná

SUMÁRIO

1 INTRODUÇÃO

Este capítulo de introdução apresentará tema, problema e premissas, objetivos, justificativa e procedimentos metodológicos.

1.1 APRESENTAÇÃO

Durante as primeiras décadas de sua existência, os computadores eram sistemas centralizados que necessitavam de pessoas altamente especializadas para que pudessem gerar algum tipo de informação útil.

As redes de computadores surgiram da necessidade de compartilhar dados e recursos de *hardware*. Ao longo do tempo, elas foram crescendo e sendo usadas nos mais diversos lugares da vida moderna, tais como, banco de dados centralizados ou comércio *on line*.

No início, a troca de informações livres e a qualquer momento foi a grande preocupação dos engenheiros e responsáveis pelas redes de computadores. Este cenário se modificou com o surgimento da Internet e sua popularização, uma vez que qualquer pessoa de qualquer lugar pode ter acesso não autorizado a determinada informação que foi colocada na rede de maneira incorreta.

> Cerca de um terço das pequenas e médias empresas brasileiras está vulnerável aos perigos da internet. Pesquisa da Symantec, empresa especializada em segurança de sistemas, apurou que 30% dessas empresas não possuem sequer um antivírus para proteção de seus computadores (BURGHI, 2009).

Ao longo do tempo, observa-se que a informação passou a ser um dos ativos mais importantes das empresas e manter esta informação longe dos olhos alheios tem sido uma das grandes preocupações dos administradores de rede.

Diante deste novo momento, como definir se uma informação foi ou não transmitida de forma segura? Como garantir que acessos externos ou internos não autorizados não tenham acontecido? O que vem a ser segurança da informação?

Alguns autores chegaram a conclusão das seguintes questões, quando se fala em comunicação segura (KUROSE, 2010; COMER, 2007):

- **Confidencialidade**: somente as pessoas envolvidas na comunicação devem ter acesso ao conteúdo da mensagem transmitida.
- **Autenticação**: as pessoas envolvidas na comunicação devem garantir suas identidades.
- **Integridade**: o conteúdo recebido deve ser o mesmo conteúdo transmitido, verificando-se se a comunicação ocorreu com sucesso e se nenhuma modificação intencional foi feita na mensagem.
- **Disponibilidade**: a informação deve estar disponível sempre que for necessária ao usuário.
- **Controle de acesso**: todo e qualquer acesso deve ser registrado, para que possa ser auditado.

"Na prática, a segurança na rede envolve não apenas proteção, mas também detecção de falhas em comunicações seguras e ataques à infraestrutura e reação a esses ataques." (KUROSE, 2010).

O fato é que segurança da informação não é uma tecnologia pronta que pode ser adquirida e implantada.

> A segurança é um processo. Pode-se aplicar o processo seguidamente à rede e à empresa que a mantém e, dessa maneira, melhorar a segurança dos sistemas. Se não iniciar ou interromper a aplicação do processo, sua segurança será cada vez pior, à medida que surgem novas ameaças e técnicas (WADLOW, 2000).

Para garantir que todas estas questões sejam atendidas de forma satisfatória, as empresas tem modificado, ao longo do tempo, sua forma de trabalhar e utilizar as redes de computadores, mas as dificuldades são imensas, uma vez que a facilidade de uso e a segurança caminham sempre em sentidos opostos.

Inserida neste contexto introdutório, esta pesquisa aborda os temas referentes à adequação das melhores práticas de segurança da informação em

redes de computadores utilizando a ABNT NBR ISO/IEC 27002:2005 como ponto de referência para as questões de segurança da informação de organizações de menor porte, que não possuem uma equipe específica para esta atividade.

Vive-se hoje o grande desafio de acessar a informação de qualquer lugar a qualquer momento. Para isto, mecanismos de autenticação e controle de acesso são necessários para garantir o sigilo da comunicação e a sua veracidade. As organizações ainda não conseguiram lidar muito bem com estas novas questões.

A segurança da informação é um processo e como tal, deve ser elaborado e aperfeiçoado para se adequar sempre as novas realidades. Diante destas preocupações, **como avaliar a aderência de uma empresa as normas da ABNT NBR ISO/IEC 27002:2005?**

Este estudo, dentro deste escopo, vai tratar de uma proposta de verificação de como uma empresa pode melhorar a segurança de sua informação com base na norma ABNT NBR ISO/IEC 27002:2005.

A ideia é questionar o que deve ser verificado e o que deve ser melhorado dentro de uma empresa para que os dados fiquem disponíveis mas, ao mesmo tempo, seguros.

Diante do que foi apresentado, cabe ressaltar que a pesquisa não tem por objetivo resultar em uma proposta plena para suportar as particularidades de cada empresa, dado a diversos fatores como a cultura de cada organização e o quanto a informação é valiosa para a mesma.

Procura-se com este trabalho, suprir o mercado e o mundo acadêmico com um estudo que apresente uma análise para verificar a aderência das empresas a norma de segurança da informação.

Este projeto é constituído por uma estrutura formada por 4 partes, distribuídas em capítulos específicos, porém complementares e integrados. Na introdução, capítulo 1, são apresentados o tema da pesquisa e seus delineamentos, seguidos pela apresentação do problema, dos objetivos, das justificativas, dos procedimentos metodológicos, do embasamento teórico e da estrutura da dissertação, aqui descrita.

No capítulo 2 se concentra a fundamentação teórica da pesquisa, a base de definição das categorias de análise.

No capítulo 3 se encontra a elaboração do questionário para verificar qual o nível de aderência de uma empresa a norma ABNT NBR ISO/IEC 27002:2005.

As considerações finais e as proposições para trabalhos futuros são apresentadas no capítulo 4. Após este, constam os elementos pós-textuais habituais, como as referências, os apêndices e os anexos.

1.2 OBJETIVOS

1.1.1 OBJETIVO GERAL

O objetivo central deste trabalho é sugerir mecanismos que permitam verificar o quanto uma empresa está aderente as normas da ABNT NBR ISO/IEC 27002:2005.

1.1.2 OBJETIVOS ESPECÍFICOS

Para alcançar ao objetivo geral proposto, a seguir são apresentados os objetivos específicos:

a) Mapear conceitos e aplicações da norma ABNT NBR ISO/IEC 27002:2005;
b) Descrever os fundamentos teóricos que caracterizam a segurança da informação;
c) Desenvolver um questionário que permita verificar o nível de aderência de uma empresa a norma ABNT NBR ISO/IEC 27002:2005.

1.3 JUSTIFICATIVA

A informação é um ativo de suma importância para a organização, porque ela representa o ativo mais competitivo em um mundo em que as tecnologias estão acessíveis a todos.

“As medidas de segurança de rede são necessárias para proteger os dados durante sua transmissão e para garantir que as transmissões de dados sejam autênticas”. (STALLINGS, 2005, p. 380)

“Políticas de segurança são complexas porque envolvem comportamento humano tanto quanto computador e facilidades de rede [...]” (COMER, 2007). Criar uma política de segurança é um desafio constante para as empresas. É a política que vai dizer o que pode ou não pode ser feito na empresa usando a tecnologia da informação. Ao mesmo tempo, a organização precisa criar mecanismos que possam limitar acessos não autorizados e adquirir tecnologias que permitam que a comunicação seja auditada de forma confiável.

Com este trabalho, por meio de levantamento bibliográfico e sistematização dos conhecimentos, pretende-se contribuir para que uma empresas de menor porte consiga verificar o quanto ela está aderente a ABNT NBR ISO/IEC 27002:2005 ou quais itens devem ser implementados primeiro para que ela possa se resguardar de ataques externos.

1.4 PROCEDIMENTOS METODOLÓGICOS

Observando os critérios para classificação de pesquisas propostos por Gil (2010), quanto à área de conhecimento, a pesquisa tem como especialidade a área de tecnologia e gestão, segundo referência do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) para este critério. Quanto a sua finalidade e utilização dos benefícios, a pesquisa é aplicada. Já quanto aos objetivos gerais e propostos, é descritiva. E por fim, quanto ao método empregado, a pesquisa é predominantemente bibliográfica (GIL, 2010).

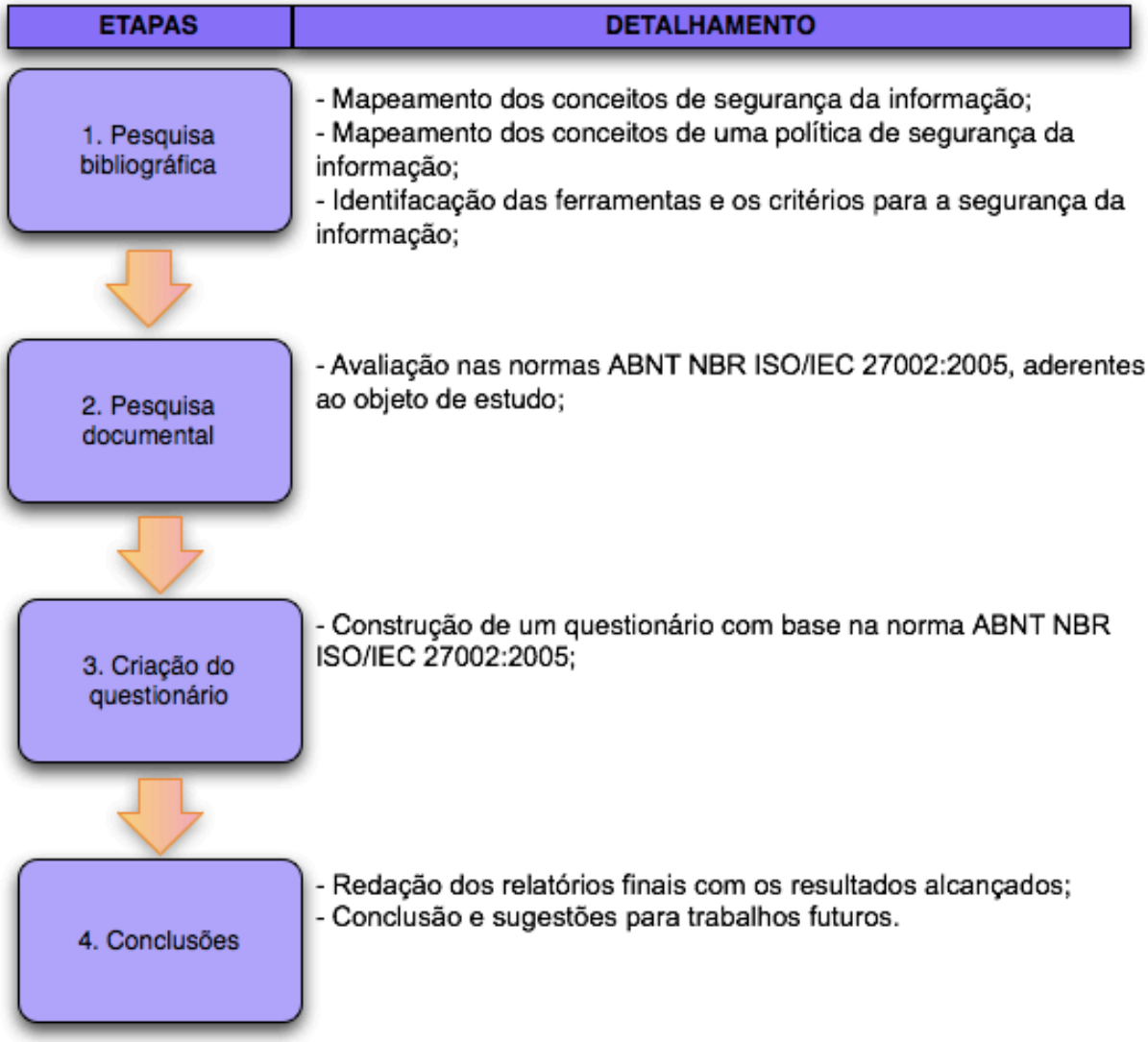


Figura 1: Diagrama das etapas da pesquisa
Fonte: Autoria própria

2 REFERENCIAIS TEÓRICOS

Este capítulo de referencial teórico apresentará o contexto em que a pesquisa se encontra inserida.

2.1 SOCIEDADE DA INFORMAÇÃO

“Na chamada Era do Conhecimento, o saber, nas suas diversas formas, constitui o principal ativo estratégico da empresa. A sua administração torna-se um processo crítico no novo contexto competitivo”. (CAVALCANTI, 2011, p. 249). Deste conhecimento depende a sua competitividade, frente a crescente disponibilização de tecnologias no mercado.

Assim, “Os dados, a informação e o conhecimento [...] são o que capacita os membros da organização a resolver problemas, satisfazer as solicitações dos clientes ou responder a mudanças no mercado.” (BUKOWITZ; WILLIAMS, 2002, p. 49). Desta forma, proteger esta informação é crucial para que este permaneça confiável e sigilosa.

“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.” (ABNT, 2005, p. X)

2.2 INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

De acordo com o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), o total de incidentes de segurança da informação no Brasil, aumentou no período de 1999 a 2006, diminuiu no ano de 2010 e voltou a crescer consideravelmente no ano de 2011 de acordo com a figura 2. Cabe ressaltar

que este número é somente dos incidentes reportados, não levando em conta as empresas que não informaram sobre os incidentes, por não quererem ou por não terem conhecimento que sofreram um ataque de segurança da informação.

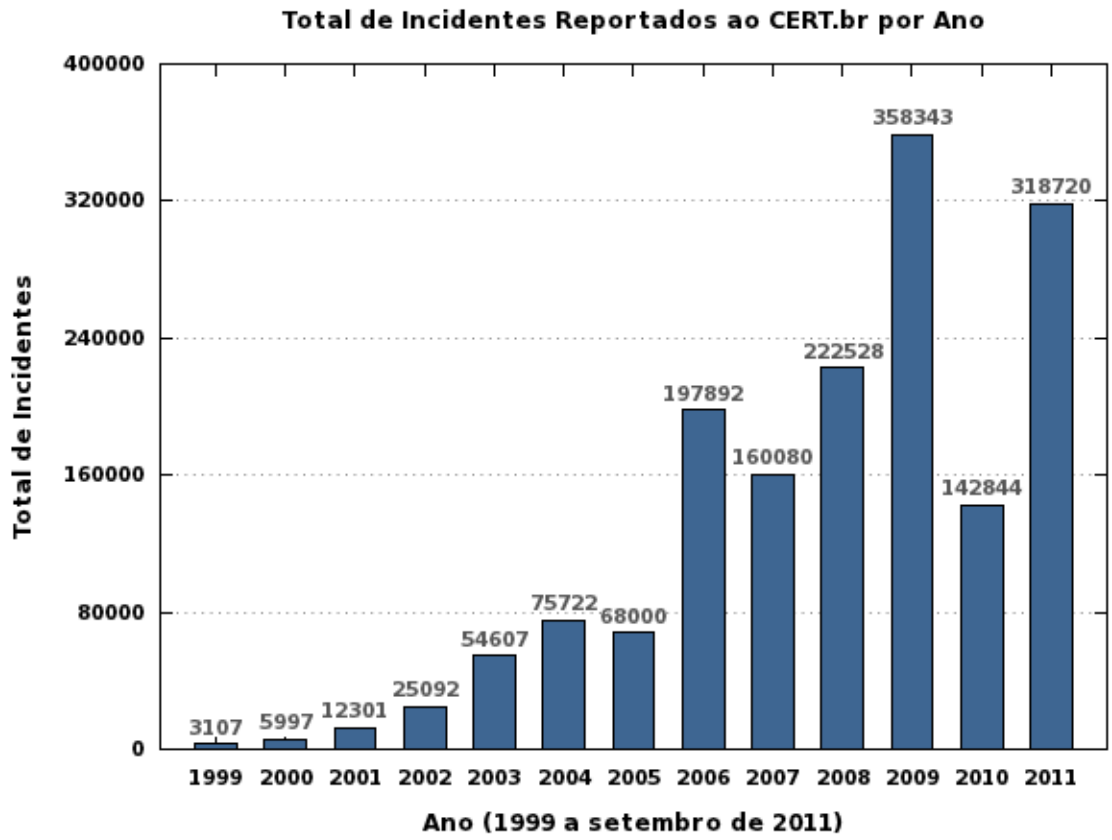


Figura 2: Incidentes Reportados de 1999 a setembro de 2011
Fonte: http://www.cert.br/stats/incidentes

"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." (ABNT, 2005, p. X) Na figura 3 é possível verificar os tipos de ataques que se sobressaíram entre janeiro e setembro de 2011.

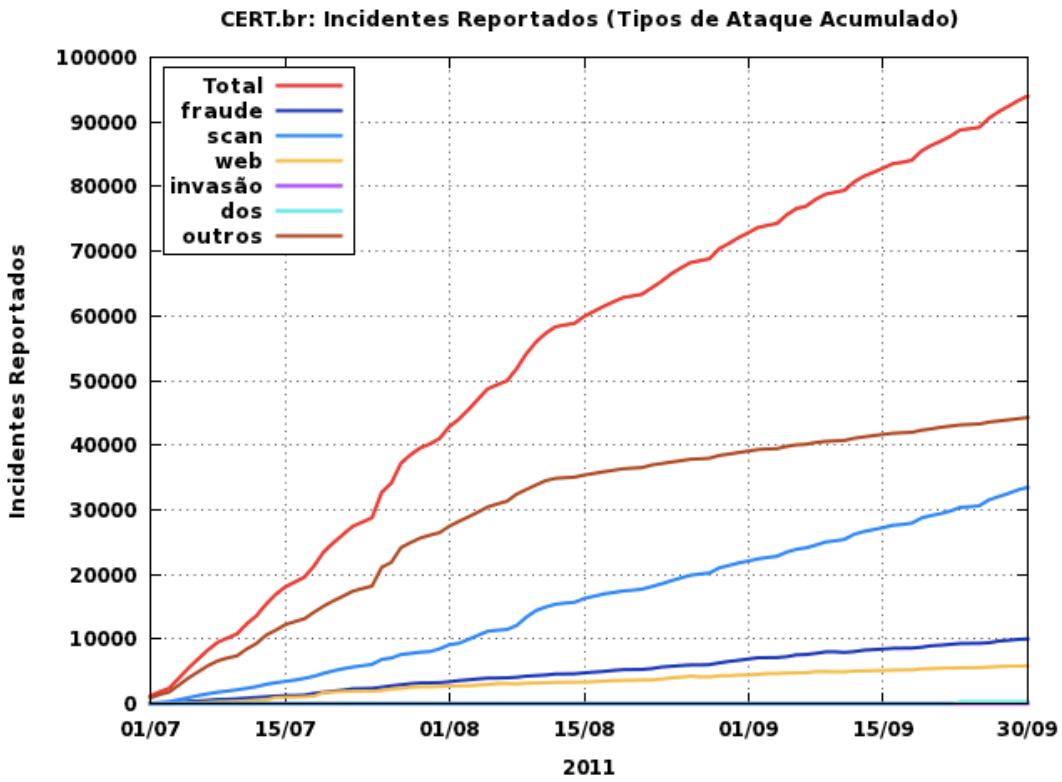


Figura 3: Tipos de incidentes de segurança da informação reportados pelo CERT
Fonte: http://www.cert.br/stats/incidentes/2011-jul-sep/tipos-ataque-acumulado.html

2.3 SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)

De acordo com a ABNT, “Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.” (ABNT, 2005, p. X)

“[...] a gestão da segurança da informação é um mecanismo cada vez mais presente no atual processo de governança corporativa das organizações.” (ALEXANDRIA, 2009, p. 14) O que se percebe é que a organização está começando a ver a importância de sua informação e principalmente, que seu valor intangível deve ser mantido sobre um processo de segurança em que todos (partes internas e partes externas da organização) participem e saibam de suas responsabilidades.

Com base nesta definição, “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.” (ABNT, 2005, p. X)

“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.” (ABNT, 2005, p. X)

“A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão da Segurança da Informação (SGSI) documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta.” (ABNT, 2006) Conforme a figura 4, o Planejamento, Execução, Controle e Ação (PDCA) é um modelo que irá criar, manter e aperfeiçoar o SGSI.

Modelo PDCA aplicado aos processos do SGSI

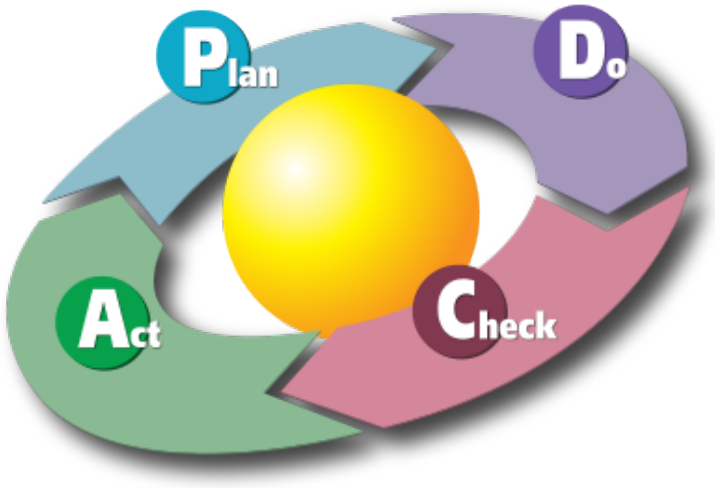


Figura 4: PDCA aplicado aos processos do SGSI
Fonte: ABNT (2006)

Plan* - *Planejar **- *Estabelecer o SGSI***	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
***Do* - Fazer** **- Implementar e operar o SGSI**	Implementar e operar a política, controles, processos e procedimentos do SGSI.
***Check* - Checar** **- Monitorar e analisar criticamente o SGSI**	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
***Act* - Agir** **- Manter e melhorar o SGSI**	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Tabela 1: Ciclo do PDCA
Fonte: ABNT (2006)

De acordo com a (ABNT, 2005, p. X) a segurança da informação requer a participação de todos os funcionários da empresa, além dos acionistas, fornecedores, terceiros, e clientes e as vezes, uma consultoria externa.

Desta forma, SOLMS & SOLMS (2004 apud ALEXANDRIA, 2009) apresenta 10 importantes aspectos, que eles chamam de "Os 10 pecados mortais da segurança da informação", os quais costumeiramente conduzem ao fracasso a implementação de um plano de segurança da informação:

1. não perceber que segurança da informação é uma responsabilidade de governança corporativa;
2. não perceber que segurança da informação é uma questão de negócio e não uma questão técnica;
3. não perceber que a governança de segurança da informação é uma disciplina multidimensional (complexa), e que não existe uma solução pronta e/ou milagrosa que vá resolver o problema;
4. não perceber que um plano de segurança da informação deve está baseado na identificação de riscos;
5. não perceber (e utilizar) a importância das melhores práticas internacionais para a gestão da segurança da informação;
6. não perceber que a política corporativa de segurança da informação é absolutamente essencial;
7. não perceber que o cumprimento das normas e o monitoramento das mesmas são absolutamente essenciais em segurança da informação;
8. não perceber que uma estrutura organizacional adequada de governança da segurança da informação é absolutamente essencial;
9. não perceber a importância da conscientização dos usuários em segurança da informação; e
10. não disponibilizar aos gestores da segurança da informação infraestrutura, ferramentas e mecanismos de suporte adequados para o desempenho de suas responsabilidades.

2.4 SEGURANÇA DA INFORMAÇÃO

A política de segurança da informação “[...] não especifica como obter proteção, mas declara claramente e de forma não ambígua os item que devem ser protegidos.” (COMER, 2007, p. 547)

“Uma política de segurança não pode ser definida a menos que uma organização entenda o valor de suas informações.” (COMER, 2007, p. 548) O apoio da direção é determinante neste momento, a política não deve ser um projeto da TI, mas de toda a organização para que todos possam entender a gravidade da segurança de suas informações.

Além disso, “[...] a comunicação é um fator crítico de sucesso para a correta disseminação das políticas corporativas, já que esta provoca alterações no status quo de praticamente todos os colaboradores.” (FERREIRA; ARAÚJO, 2008, p. XXXII)

> Os riscos 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. (ABNT, 27002, p. XI)

Uma vez que os riscos tenham sido identificados, a organização precisa selecionar os controles apropriados para reduzir os riscos a um nível aceitável (ABNT, 2005, p. XI).

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 política 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. (ABNT, 2005, p. XII)

Fatores críticos para o sucesso da implementação da segurança da informação dentro de uma organização:

a) política de segurança da informação, objetivos e atividades, que reflitam os objetivos do negócio;
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 política 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 de melhoria. (ABNT, 2005, p. XIII)

2.5 CONTROLES DA ABNT NBR ISO/IEC 27002: 2005

2.5.1 Política de segurança

Objetivo: “Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e

regulamentações pertinentes.” (ABNT, 2005)

A política de segurança da informação deve ser um documento relevante e compreensível, aprovado pela direção (demonstrando o seu apoio) e acessível para todos os funcionários, fornecedores e terceiros. Nesta política deve ter definições dos termos relevantes (no intuito de equalizar a informação), deve informar os objetivos da política, suas normas, controles e consequências no caso de violação. (ABNT, 2005)

2.5.2 Organizando a segurança da informação

2.5.2.1 Organização interna

Objetivo: “Gerenciar a segurança da informação.” (ABNT, 2005)

A segurança da informação deve ser de responsabilidade do comitê gestor de segurança da informação (integrantes de várias áreas da organização). O comitê deve cuidar da atribuição das responsabilidades dentro da empresa, pois, muitos ativos podem estar sobre a responsabilidade da TI, mas a TI não tem como conhecer o seu verdadeiro valor. Neste sentido, deve-se verificar quem é o dono de cada ativo (informações de banco de dados, planilhas que se encontram no servidor de arquivos) e delegar a sua responsabilidade e o seu proprietário. (ABNT, 2005)

2.5.2.2 Partes externas

“Objetivo: Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas.” (ABNT, 2005)

Deve-se identificar todos os possíveis riscos relacionados com partes externas. No caso de fornecedores, verificar os tipos de acesso físico e lógico que estão autorizados. No caso de clientes, verificar a proteção dos ativos e declarar que todo acesso que não seja explicitamente autorizado, é proibido. No caso de terceiros, construir acordos legais que tenham sempre em questão a política de segurança da informação e declarar explicitamente o que irá ocorrer no caso de não comprimento de algum item do acordo. (ABNT, 2005)

2.5.3 Gestão de ativos

2.5.3.1 Responsabilidade pelos ativos

Objetivo: “Alcançar e manter a proteção dos ativos da organização.” (ABNT, 2005)

A organização deve criar e manter um inventário de todos os ativos físicos e lógicos importantes para a mesma. Para que isto aconteça, deve-se determinar um proprietário do ativo, pois este irá cuidar da criação, desenvolvimento, manutenção e uso deste ativo. Após este processo, deve-se criar as regras para o acesso dos ativos, sempre associado a necessidade da utilização pelo usuário. (ABNT, 2005)

2.5.3.2 Classificação da informação

Objetivo: “Assegurar que a informação receba um nível adequado de proteção.” (ABNT, 2005)

A informação deve ser classificada ou reclassificada de acordo com o seu grau de importância e sensibilidade. A classificação “pública, interna e confidencial” se aplica na maioria das organizações e pode ser usada no início do processo, para facilitar a implementação da classificação. De acordo com a classificação estabelecida, os ativos devem possuir rótulos, para que não ocorra erros de vazamento de informação. (ABNT, 2005)

2.5.4 Segurança em recursos humanos

2.5.4.1 Antes da contratação

Objetivo: “Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis, e reduzir o risco de furto ou roubo, fraude ou mau uso de recursos.” (ABNT, 2005)

Os papéis e responsabilidades relacionados a segurança da informação devem estar descritos em cada um dos cargos da organização. No momento da seleção, informações passadas pelos candidatos devem ser confirmadas para verificar sua autenticidade. Já no contrato de trabalho, deve existir itens relacionados a responsabilidades na questão da segurança da informação. (ABNT, 2005)

2.5.4.2 Durante a contratação

Objetivo: “Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.” (ABNT, 2005)

A direção deve apoiar a política de segurança da informação. Além disso, processos de conscientização, educação e treinamento periódicos são necessários para que todos se lembrem da responsabilidade de cada um no quesito de segurança da informação. No mais, processos disciplinares devem ser formalizados e aplicados caso ocorra algum incidente de segurança. (ABNT, 2005)

2.5.4.3 Encerramento de atividades

Objetivo: “Assegurar que funcionários, fornecedores e terceiros deixem a organização ou modem de trabalho de forma ordenada.” (ABNT, 2005)

No caso de mudança de cargo/função ou de encerramento de atividades, deve existir uma comunicação interna padrão informando sobre este acontecimento, para que providências sejam tomadas: requisição de devolução de ativos, mudança ou retirada de acessos, criação de novos acessos, de acordo com a necessidade da situação. (ABNT, 2005)

2.5.5 Segurança física e do ambiente

2.5.5.1 Áreas seguras

Objetivo: “Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.” (ABNT, 2005)

Devem existir perímetros de segurança física (portões, paredes, controles de acesso ou recepcionistas) para proteger as áreas da organização. Visitantes devem ser identificados (controle de entradas e saídas). Áreas de acesso público, áreas de entrega e de carregamento devem estar bem definidas. Além disso, deve-se verificar os riscos relacionados a localização da empresa (enchentes, desastres naturais, etc). (ABNT, 2005)

2.5.5.2 Segurança de equipamentos

Objetivo: “Impedir perdas, danos, furto ou roubo, ou comprometimento de

ativos e interrupção das atividades da organização.” (ABNT, 2005)

Os equipamentos devem ser instalados por pessoal especializado e devem ter a devida proteção, quando necessário. Deve-se ficar atento a questões de falta de energia e a criticidade deste acontecimento nos equipamentos. A parte de cabeamento deve estar protegida contra danos e a manutenção dos equipamentos deve fazer parte da rotina para assegurar sua disponibilidade. Quando os equipamentos forem descartados, deve-se atentar para a remoção de dados importantes da organização. (ABNT, 2005)

2.5.6 Gerenciamento das operações e comunicações

2.5.6.1 Procedimentos e responsabilidades operacionais

Objetivo: “Garantir a operação segura e correta dos recursos de processamento da informação.” (ABNT, 2005)

Os procedimentos de operação devem ser documentados e atualizados para refletir a realidade da empresa. Deve existir uma política de gestão de mudança, para que haja um controle das alterações feitas no ambiente de produção. Deve existir uma segregação de funções, para reduzir a alteração indevida do ambiente. Além disso, deve existir uma separação dos recursos de desenvolvimento, teste e produção. (ABNT, 2005)

2.5.6.2 Gerenciamento de serviços terceirizados

Objetivo: “Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados.” (ABNT, 2005)

A organização deve possuir contratos claros com seus terceiros. Ao mesmo tempo, deve verificar constantemente a entrega dos serviços prestados, monitorando e analisando criticamente estas entregas. A política de gestão de mudança deve incluir o controle das alterações realizadas pelos terceiros. (ABNT, 2005)

2.5.6.3 Planejamento e aceitação dos sistemas

Objetivo: “Minimizar o risco de falhas nos sistemas.” (ABNT, 2005)

A organização deve possuir um gerenciamento de capacidade de seus

recursos para que ajustes possam ser feitos de acordo com a implementação de novos sistemas. No caso de aceitação de sistemas, deve existir critérios de aceite para novas versões de sistemas já existentes ou para novos sistemas que serão implementados. (ABNT, 2005)

2.5.6.4 Controle contra códigos maliciosos

Objetivo: “Proteger a integridade do *software* e da informação.” (ABNT, 2005)

Deve-se proibir a instalação de programas não autorizados. Deve-se possuir *softwares* que verifiquem a existência de códigos maliciosos em arquivos e acessos a *web*. (ABNT, 2005)

2.5.6.5 Cópias de seguranças das informações

Objetivo: “Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.” (ABNT, 2005)

Deve-se fazer cópia de segurança das informações relevantes para a empresa. Além disso, testes periódicos destas cópias devem ser feitas, para verificar sua integridade. (ABNT, 2005)

2.5.6.6 Gerenciamento da segurança em redes

Objetivo: “Garantir a proteção das informações em redes e a proteção da infraestrutura de suporte.” (ABNT, 2005)

As redes precisam ser controladas e monitoradas para que acessos indevidos não ocorram. Serviços como autenticação, encriptação e monitoramento devem ser implementados de acordo com a sensibilidade da informação. (ABNT, 2005)

2.5.6.7 Manuseio de mídias

Objetivo: “Prevenir contra divulgação não autorizada, modificação, remoção ou destruição dos ativos, e interrupções das atividades do negócio.” (ABNT, 2005)

Deve-se verificar a necessidade do uso de mídias removíveis. Caso haja, deve existir um controle do que está sendo transferido para este tipo de mídia. Deve existir uma preocupação no descarte de mídias removíveis, para que este descarte aconteça de forma segura, sem comprometer informações sensíveis da organização. Procedimentos devem ser estabelecidos para que não ocorra usos indevidos. (ABNT, 2005)

2.5.6.8 Troca de informações

Objetivo: “Manter a segurança na troca de informações e *softwares* internamente à organização e com quaisquer entidades externas.” (ABNT, 2005)

A troca de informações deve possuir políticas, procedimentos, controles e monitoramentos para que o compartilhamento da informação ocorra de forma segura. (ABNT, 2005)

2.5.6.9 Serviços de comércio eletrônico

Objetivo: “Garantir a segurança de serviços de comércio eletrônico e sua utilização segura.” (ABNT, 2005)

Se a organização possuir comércio eletrônico, cuidados devem ser implementados para garantir a integridade e disponibilidade dos dados. As transações *on-line* devem possuir controles que verifiquem transmissões incompletas, erros, alterações não autorizadas, duplicação de solicitações. (ABNT, 2005)

2.5.6.10 Monitoramento

Objetivo: “ Detectar atividades não autorizadas de processamento da informação.” (ABNT, 2005)

O monitoramento dos serviços importantes deve existir. *Logs* de atividades e de falhas devem ser armazenados por tempo determinado pela política da segurança da informação de acordo com o seu critério de relevância. Estes *logs* devem possuir informações relevantes que permitam uma auditoria, caso necessário. Os relógios dos equipamentos devem estar sincronizados para que os *logs* sejam um retrato fiel da realidade. (ABNT, 2005)

2.5.7 Controle de acessos

2.5.7.1 Requisitos de negócio para controle de aceso

Objetivo: “Controlar acesso à informação.” (ABNT, 2005)

Deve ter procedimentos estabelecidos para o acesso à informação. Solicitações de criação, mudança ou retirada de acesso devem ser formalizados. (ABNT, 2005)

2.5.7.2 Gerenciamento de acesso do usuário

Objetivo: “Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.” (ABNT, 2005)

Deve-se utilizar uma identificação única por usuário, para facilitar a criação, manutenção, controle de acesso e cancelamento do mesmo. O usuário deve assinar um documento que explique detalhadamente os seus direitos de acesso. O gerenciamento de privilégios deve ser feito rigorosamente e auditado periodicamente. O controle de senhas deve ser formalizado, não permitindo senhas de fácil adivinhação. Além disso, senhas temporárias devem ser únicas e o processo deve solicitar rapidamente a sua troca. A política de mesa limpa e tela limpa devem ser implementadas e divulgadas periodicamente para um processo de conscientização. (ABNT, 2005)

2.5.7.3 Controle de acesso à rede

Objetivo: “Prevenir acesso não autorizado aos serviços de rede.” (ABNT, 2005)

Deve existir políticas de acesso à rede, tanto internamente quanto externamente. No caso de acessos internos, a segregação das redes pode ser um processo simples e eficiente para que dados sensíveis não circulem por toda a organização. No caso de acessos externos, maiores cuidados devem ser tomados e deve-se buscar a implementação de VPNs (*Virtual Private Network*) com criptografias fortes que garantam que os dados não serão acessados por pessoas não autorizadas. (ABNT, 2005)

2.5.7.4 Controle de acesso ao sistema operacional

Objetivo: “Prevenir acesso não autorizado aos sistemas operacionais.” (ABNT, 2005)

Os sistemas operacionais devem possuir um procedimento de entrada (*log-on*), devem registrar tentativas de acesso com sucesso e com falhas, devem obrigar o uso de identificação do usuário e de uma senha, devem ter um limite de tempo de sessão e de horário de conexão. (ABNT, 2005)

2.5.7.5 Controle de acesso à aplicação e à informação

Objetivo: “Prevenir acesso não autorizado à informação contida nos sistemas

de aplicação.” (ABNT, 2005)

Deve existir restrição de acesso à informação de acordo com o perfil de cada usuário. Sistemas sensíveis devem ser isolados e monitorados constantemente. (ABNT, 2005)

2.5.7.6 Computação móvel e trabalho remoto

Objetivo: “Garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.” (ABNT, 2005)

Deve existir políticas e procedimentos que garantam a disponibilidade das informações sem comprometer seu conteúdo e ao mesmo tempo, garantir que os dados não estão sendo acessados por pessoa não autorizada. (ABNT, 2005)

2.5.8 Aquisição, desenvolvimento e manutenção de sistemas de informação

2.5.8.1 Requisitos de segurança de sistemas de informação

Objetivo: “Garantir que segurança é parte integrante de sistemas de informação.” (ABNT, 2005)

Requisitos de segurança da informação devem ser analisados no momento da criação de novos projetos, para que estes já nasçam embasados em controles e procedimentos de segurança da informação. (ABNT, 2005)

2.5.8.2 Processamento correto nas aplicações

Objetivo: “Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.” (ABNT, 2005)

As aplicações da empresa devem ter processos de validação na entrada de dados, devem ter controles no processamento interno, para garantir a integridade dos dados e devem possuir validação dos dados de saída. (ABNT, 2005)

2.5.8.3 Controles criptográficos

Objetivo: “Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos.” (ABNT, 2005)

Política para o uso de controles criptográficos devem ser implementados e um gerenciamento de chaves deve ser adotado para que todas as informações sensíveis possam estar protegidas corretamente. (ABNT, 2005)

2.5.8.4 Segurança dos arquivos do sistema

Objetivo: “Garantir a segurança dos arquivos do sistema.” (ABNT, 2005)

Deve-se garantir que somente pessoas autorizadas tenham permissão de instalar *softwares*. No caso de acesso ao código-fonte dos sistemas, deve-se criar procedimentos de forma que uma única pessoa nunca tenha acesso total, mas somente aquilo que for necessário para o desempenho de suas atividades. (ABNT, 2005)

2.5.8.5 Segurança em processos de desenvolvimento e de suporte

Objetivo: “Manter a segurança de sistemas aplicativos e da informação.” (ABNT, 2005)

A gestão de mudanças deve ser implementada para o controle de atualizações dos sistemas. As atualizações devem ser feitas primeiramente num ambiente de desenvolvimento e se corretas, aplicadas no ambiente de produção. (ABNT, 2005)

2.5.8.6 Gestão de vulnerabilidades técnicas

Objetivo: “Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.” (ABNT, 2005)

A organização deve ficar atenta as vulnerabilidades técnicas conhecidas e tomar procedimentos que possam minimizar os riscos: aplicar *patches*, isolar o sistema que possui a vulnerabilidade, monitorar os *logs*. (ABNT, 2005)

2.5.9 Gestão de incidentes de segurança da informação

2.5.9.1 Notificação de fragilidades e eventos de segurança da informação

Objetivo: “Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.” (ABNT, 2005)

Deve-se criar procedimentos para que eventos de segurança da informação sejam notificados o mais rapidamente possível por funcionários, fornecedores ou terceiros. (ABNT, 2005)

2.5.9.2 Gestão de incidentes de segurança da informação e melhorias

Objetivo: “Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.” (ABNT, 2005)

Deve-se criar procedimentos que assegurem respostas rápidas e eficientes no caso de ocorrências de incidentes de segurança da informação. No caso de incidentes que levem a uma ação legal, coleta de evidências serão necessárias. (ABNT, 2005)

2.5.10 Gestão da continuidade do negócio

2.5.10.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação

Objetivo: “Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.” (ABNT, 2005)

Deve-se incluir os requisitos de segurança de informação no plano de continuidade do negócio da organização. Para isto, deve-se analisar os eventos que podem causar interrupção das atividades, verificando a probabilidade e o impacto de tal interrupção, visando a segurança da informação. O plano deve ser testado e atualizados continuamente. (ABNT, 2005)

2.5.11 Conformidade

2.5.11.1 Conformidade com requisitos legais

Objetivo: ”Evitar violações de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação.” (ABNT, 2005)

Deve-se identificar a legislação aplicável para todas as atividades da empresa. Estes requisitos devem ser documentados e atualizados para cada sistema de informação da organização. (ABNT, 2005)

2.5.11.2 Conformidade com normas e políticas de segurança da informação e conformidade técnica

Objetivo: “Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.” (ABNT, 2005)

Gestores de cada área devem garantir que os requisitos de segurança da informação estão sendo executados. (ABNT, 2005)

2.5.11.3 Considerações quanto à auditoria de sistema de informação

Objetivo: “Maximizar a eficiência e minimizar a interferência no processo de auditoria dos sistemas de informação.” (ABNT, 2005)

A auditoria deve ser planejada para que não ocorra interrupções dos processos do negócio. Além disso, as ferramentas de auditoria devem estar protegidas para prevenir o uso impróprio. (ABNT, 2005)

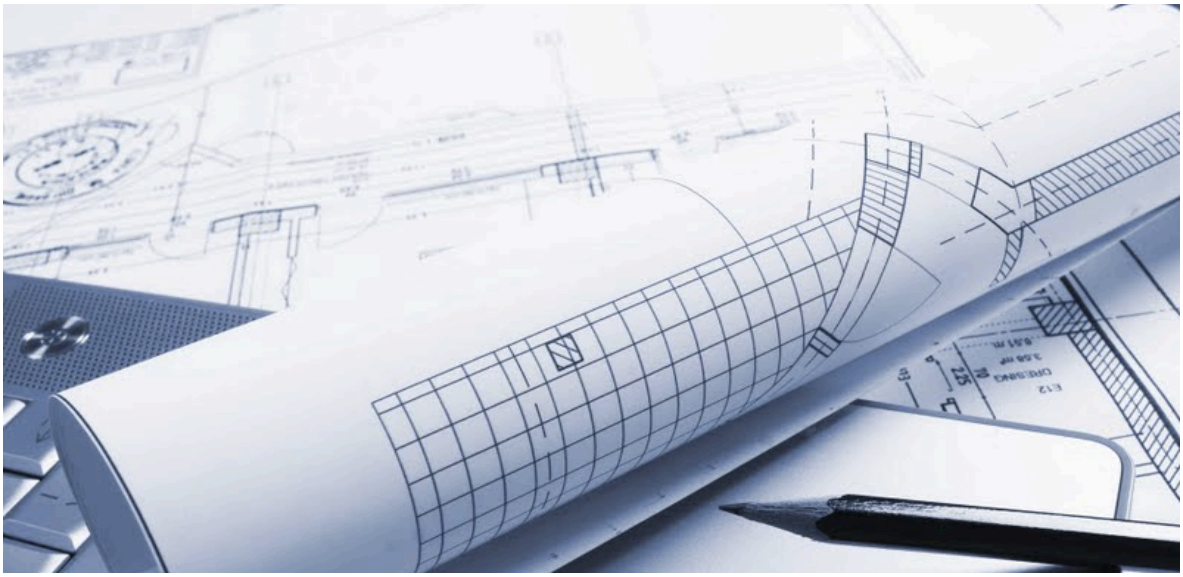
3 ADERÊNCIA DA EMPRESA A ABNT NBR ISO/IEC 27002: 2005

Este capítulo apresenta o questionário que deve ser realizado para verificar o quanto uma organização de pequeno porte está aderente a ABNT NBR ISO/IEC 27002: 2005. Ao mesmo tempo, com os resultados obtidos, será possível conhecer quais pontos são mais relevantes no processo de adaptação da empresa a norma de segurança.

3.1 QUESTIONÁRIO

O questionário abaixo deve ser respondido com o objetivo de ver claramente como está a questão da segurança da informação na organização. Além do questionário, é interessante que aqueles que respondam o questionário separem evidências de suas afirmações (procedimentos e documentação existente, *prints* de tela, etc), para que se possa verificar como determinado atividade está sendo realizada e verificar possíveis falhas.

Para respondê-lo, provavelmente serão necessárias várias pessoas de departamentos diferentes, como TI e recursos humanos. O interessante é ter uma pessoa responsável (provavelmente o gerente de TI) para coletar e agrupar estas respostas.



Questionário

1 Política de segurança da informação

1.1 Politica de segurança da informação
1.1.1 Documento da politica de segurança da informação
1.1.2. Análise crítica da política de segurança da informação

1. Existe uma política de segurança da informação?
   - ○ Sim
   - ○ Não
2. A política de segurança da informação possui o apoio e comprometimento da direção?
   - ○ Sim
   - ○ Não
3. A politica de segurança da informação foi publicada e comunicada para todos os funcionários?
   - ○ Sim
   - ○ Não
4. A politica de segurança da informação foi publicada e comunicada para as partes externas relevantes (fornecedores, terceiros, etc)?
   - ○ Sim
   - ○ Não
5. A politica de segurança da informação possui um gestor?
   - ○ Sim
   - ○ Não
6. A politica de segurança da informação é analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrem?
   - ○ Sim
   - ○ Não
7. Quais campos abaixo são contemplados na política de segurança da informação?
   - ☐ Definição de segurança da informação
   - ☐ Metas globais
   - ☐ Escopo da politica de segurança da informação
   - ☐ Descrição da importância da política para a empresa
   - ☐ Declaração do comprometimento da direção
   - ☐ Análise/avaliação de risco
   - ☐ Definição das responsabilidades gerais e específicas
   - ☐ Procedimento para informar sobre incidentes de segurança da informação
   - ☐ Referências a outros documentos que possam apoiar a politica

- [ ] Controle de versão da política
- [ ] Declaração do comitê de gestão da segurança da informação
- [ ] A periodicidade em que o comitê se reúne
- [ ] Conformidade com a legislação e com requisitos regulamentares e contratuais
- [ ] Requisitos de conscientização, treinamento e educação em segurança da informação
- [ ] Gestão da continuidade do negócio
- [ ] Consequências das violações na política de segurança da informação

2 Organizando a segurança da informação

2.1. Organização interna
2.1.1 Comprometimento da direção com a segurança da informação
2.1.2 Coordenação da segurança da informação
2.1.3 Atribuição de responsabilidades para a segurança da informação
2.1.4 Processo de autorização para os recursos de processamento da informação
2.1.5 Acordos de confidencialidade
2.1.6 Contato com autoridades
2.1.7 Contato com grupos especiais
2.1.8 Análise crítica independente de segurança da informação
2.2 Partes externas
2.2.1 Identificação dos riscos relacionados com partes externas
2.2.2 Identificando a segurança da informação, quando tratando com os clientes
2.2.3 Identificando segurança da informação nos acordos com terceiros

8. Existe um documento que demonstre o apoio da direção em relação a política da segurança da informação?
   - ( ) Sim
   - ( ) Não
9. Existem pessoas de diferentes partes da organização na coordenação da segurança da informação?
   - ( ) Sim
   - ( ) Não

3 Gestão de ativos

3.1 Responsabilidade pelos ativos
3.1.1 Inventário dos ativos
3.1.2 Proprietário dos ativos
3.1.3 Uso aceitável dos ativos
3.2 Classificação da informação
3.2.1 Recomendações para classificação
3.2.2 Rótulos e tratamento da informação

10. Existe um inventário de todos os ativos importantes?
    - ○ Sim
    - ○ Não
11. O inventário possui?
    - ☐ Código do ativo
    - ☐ Descrição do ativo
    - ☐ Tipo do ativo
    - ☐ Formato do ativo
    - ☐ Localização do ativo
    - ☐ Informações sobre cópia de segurança
    - ☐ Informações sobre licença
    - ☐ Importância do ativo para o negócio
12. Todos os ativos e informações possuem um proprietário (pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos)?
    - ○ Sim
    - ○ Não
13. Existem regras para o uso da Internet?
    - ○ Sim
    - ○ Não
14. Existem regras para o uso do e-mail?
    - ○ Sim
    - ○ Não
15. Existe uma política de reclassificação, quando necessário?
    - ○ Sim
    - ○ Não

4 Segurança em recursos humanos

4.1 Antes da contratação
4.1.1 Papéis e responsabilidades
4.1.2 Seleção
4.1.3 Temos e condições de contratação
4.2 Durante a contratação
4.2.1 Responsabilidades da direção
4.2.2 Conscientização, educação e treinamento em segurança da informação
4.2.3 Processo disciplinar
4.3 Encerramento ou mudança de contratação
4.3.1 Encerramento de atividades
4.3.2 Devolução de ativos
4.3.3 Retirada de direitos de acesso

16. Os funcionários estão adequadamente instruídos sobre as suas responsabilidades e papéis pela segurança da informação?
    - ○ Sim
    - ○ Não
17. Os terceiros estão adequadamente instruídos sobre as suas responsabilidades e papéis pela segurança da informação?
    - ○ Sim
    - ○ Não
18. Os fornecedores estão adequadamente instruídos sobre as suas responsabilidades e papéis pela segurança da informação?
    - ○ Sim
    - ○ Não
19. Houve treinamento sobre a política de segurança da informação para os funcionários?
    - ○ Sim
    - ○ Não
20. Houve treinamento sobre a política de segurança da informação para os fornecedores?
    - ○ Sim
    - ○ Não
21. Houve treinamento sobre a política de segurança da informação para os terceiros?
    - ○ Sim
    - ○ Não
22. Existe um processo disciplinar formal para os funcionários que tenham cometido uma violação de segurança da informação?
    - ○ Sim
    - ○ Não
23. Existe um processo disciplinar formal para os fornecedores que tenham cometido uma violação de segurança da informação?
    - ○ Sim
    - ○ Não
24. Existe um processo disciplinar formal para os terceiros que tenham cometido uma violação de segurança da informação?
    - ○ Sim
    - ○ Não
25. O encerramento das atividades inclui requisitos de segurança e responsabilidades legais?
    - ○ Sim
    - ○ Não

26. Existe alguma cláusula no contrato de confidencialidade indicando a continuidade deste contrato após o encerramento das atividades?
    - ○ Sim
    - ○ Não
27. Todos são informados sobre o desligamento de um funcionário, um fornecedor ou um terceiro?
    - ○ Sim
    - ○ Não
28. Existe um processo formal para a devolução de todos os equipamentos, documentos corporativos, *softwares*, dispositivos de computação móvel, cartões de crédito, cartões de acesso, manuais e informações armazenadas em mídia eletrônica entregues a pessoa que está saindo?
    - ○ Sim
    - ○ Não
29. No caso em que um funcionário, fornecedor ou terceiro use seu próprio equipamento, existe um procedimento para assegurar que toda a informação relevante seja transferida para a organização e que seja apagada de forma segura do equipamento?
    - ○ Sim
    - ○ Não
30. Existe um processo de documentar as atividades que este funcionário, fornecedor ou terceiro, antes que ele encerre suas atividades na empresa?
    - ○ Sim
    - ○ Não
31. Os direitos de acesso do funcionário são retirados após o encerramento de suas atividades?
    - ○ Sim
    - ○ Não
32. Os direitos de acesso do fornecedor são retirados após o encerramento de suas atividades?
    - ○ Sim
    - ○ Não
33. Os direitos de acesso do terceiro são retirados após o encerramento de suas atividades?
    - ○ Sim
    - ○ Não

5 Segurança física e do ambiente

5.1 Áreas seguras

5.1.1 Perímetro de segurança física

5.1.2 Controles de entrada física

5.1.3 Segurança em escritórios, salas e instalações

5.1.4 Proteção contra ameaças externas e do meio ambiente
5.1.5 Trabalhando em áreas seguras
5.1.6 Acesso do público, áreas de entrega e de carregamento
5.2 Segurança de equipamentos
5.2.1 Instalação e proteção do equipamento
5.2.2 Utilidades
5.2.3 Segurança do cabeamento
5.2.4 Manutenção dos equipamentos
5.2.5 Segurança de equipamentos fora das dependências da organização
5.2.6 Reutilização e alienação segura de equipamentos
5.2.7 Remoção de propriedade

34. É solicitado algum documento (identidade com foto) para entrar na empresa?
    - Sim
    - Não
35. É tirado foto de quem entra na empresa?
    - Sim
    - Não
36. O visitante circula pelas dependências da empresa sozinho?
    - Sim
    - Não
37. Existe uma recepção onde todos devem se identificar?
    - Sim
    - Não
38. Existem perímetros de segurança claramente definidos para o ambiente de TI?
    - Sim
    - Não
39. Existem mecanismos de controle para o acesso ao ambiente de TI?
    - Sim
    - Não
40. Existe monitoramento?
    - Sim
    - Não
41. A entrada e a saída de visitantes é registrada?
    - Sim
    - Não
42. Um funcionário de TI sempre acompanha um visitante no ambiente de TI?
    - Sim
    - Não
43. Os funcionários usam crachá de identificação?
    - Sim

- Não

44. Os fornecedores usam crachá de identificação?
    - Sim
    - Não
45. Os terceiros usam crachá de identificação?
    - Sim
    - Não
46. Existem locais em que o público geral não tem acesso?
    - Sim
    - Não
47. Sobre a localização da empresa, foram levadas em conta: as instalações dos vizinhos, vazamento de água do telhado ou pisos do subsolo?
    - Sim
    - Não
48. Os materiais perigosos são armazenados a uma distância segura da área de segurança?
    - Sim
    - Não
49. Existem equipamentos apropriados de detecção e combate a incêndios?
    - Sim
    - Não
50. Existem áreas seguras?
    - Sim
    - Não
51. Existe controle para acesso a estas áreas seguras?
    - Sim
    - Não
52. Estas áreas são fisicamente trancadas e periodicamente verificadas?
    - Sim
    - Não
53. É permitido o uso de máquinas fotográficas neste ambiente?
    - Sim
    - Não
54. Existem áreas de entrega e carregamento com controle de acesso?
    - Sim
    - Não

6 Gerenciamento das operações e comunicações

6.1 Procedimentos e responsabilidades operacionais

6.1.1 Documentação dos procedimentos de operação

6.1.2 Gestão de mudanças
6.1.3 Segurança de funções
6.1.4 Separação dos recursos de desenvolvimento, teste e de produção
6.2 Gerenciamento de serviços terceirizados
6.2.1 Entrega de serviços
6.2.2 Monitoramento e análise crítica de serviços terceirizados
6.2.3 Gerenciamento de mudanças para serviços terceirizados
6.3 Planejamento e aceitação dos sistemas
6.3.1 Gestão de capacidade
6.3.2 Aceitação de sistemas
6.4 Proteção contra códigos maliciosos e códigos móveis
6.4.1 Controles contra códigos maliciosos
6.4.2 Controles contra códigos móveis
6.5 Cópia de segurança
6.5.2 Cópias de segurança das informações
6.6 Gerenciamento da segurança em redes
6.6.1 Controles de redes
6.6.2 Segurança dos serviços de rede
6.7 Manuseio de mídias
6.7.1 Gerenciamento de mídias removíveis
6.7.2 Descarte de mídias
6.7.3 Procedimentos para tratamento de informação
6.7.4 Segurança da documentação dos sistemas
6.8 Troca de informações
6.8.1 Políticas e procedimentos para troca de informações
6.8.2 Acordos para a troca de informações
6.8.3 Mídias em trânsito 6.8.4 Mensagens eletrônicas
6.8.5 Sistemas de informações do negócio
6.9 Serviços de comércio eletrônico
6.9.1 Comércio eletrônico
6.9.2 Transações on-line
6.9.3 Informações publicamente disponíveis
6.10 Monitoramento
6.10.1 Registros de auditoria
6.10.2 Monitoramento do uso do sistema
6.10.3 Proteção das informações dos registros (logs)
6.10.4 Registros (logs) de administrador e operador
6.10.5 Registros (logs) de falhas
6.10.6 Sincronização dos relógios

55. Existe gerência de mudança?
    - ○ Sim
    - ○ Não
56. Existe um plano de comunicação para todas as pessoas envolvidas na mudança?

- Sim
- Não

57. Existe um documento formal de aprovação das mudanças?
    - Sim
    - Não
58. Quando a mudança é aprovada, exige-se procedimentos de recuperação?
    - Sim
    - Não
59. As mudanças são registradas?
    - Sim
    - Não
60. Existe segregação de funções (impedir que uma única pessoa possa acessar, modificar ou usar ativos sem a devida autorização ou detecção)?
    - Sim
    - Não
61. Se não existe segregação, existe a monitoração das atividades, trilhas de auditoria e o acompanhamento gerencial?
    - Sim
    - Não
62. Existem ambientes de desenvolvimento, teste e produção separados?
    - Sim
    - Não
63. O ambiente de teste emula fielmente o ambiente de produção?
    - Sim
    - Não
64. Existem perfis diferentes para o ambiente de teste e de produção?
    - Sim
    - Não
65. Os dados sensíveis do ambiente de produção são copiados para o ambiente de teste?
    - Sim
    - Não
66. A empresa monitora as atividades dos terceiros no tocante ao que foi acordado e ao que está sendo entregue?
    - Sim
    - Não
67. A transição das atividades para um outro terceiro estão nos acordos?
    - Sim
    - Não
68. As atividades dos terceiros são monitoradas para verificar a aderência junto do que foi acordado?

- ○ Sim
- ○ Não

69. Os terceiros são gerenciados por uma pessoa ou equipe?
    - ○ Sim
    - ○ Não
70. Terceiros têm acesso a informações críticas?
    - ○ Sim
    - ○ Não
71. Existe uma política formal proibindo o uso de *software* não autorizado?
    - ○ Sim
    - ○ Não
72. Os usuários são administradores das máquinas?
    - ○ Sim
    - ○ Não
73. As máquinas dos usuários são auditadas periodicamente para verificar *softwares* não autorizados?
    - ○ Sim
    - ○ Não
74. O antivírus está instalado e atualizado em todas as máquinas?
    - ○ Sim
    - ○ Não
75. Os usuários foram treinados para usar o antivírus em arquivos desconhecidos recebidos por e-mail, acessados na Internet ou dispositivos móveis?
    - ○ Sim
    - ○ Não
76. Existe algum *software* que verifique a existência de códigos maliciosos em página *web*?
    - ○ Sim
    - ○ Não
77. Existe um plano de continuidade do negócio, caso algum código malicioso se espalhe pela empresa?
    - ○ Sim
    - ○ Não
78. Os técnicos da TI assinam lista de discussão e acessam páginas *web* que falam sobre códigos maliciosos?
    - ○ Sim
    - ○ Não
79. É permitido o uso de códigos móveis (código transferido de um computador a outro executando automaticamente e realizando funções específicas com pequena ou nenhuma interação por parte do usuário)?
    - ○ Sim

- ○ Não

80. Existe uma política de *backup*?
    - ○ Sim
    - ○ Não
81. O *restore* é realizado periodicamente para fins de teste do *backup*?
    - ○ Sim
    - ○ Não
82. Existe o registro dos *backups*?
    - ○ Sim
    - ○ Não
83. As cópias são armazenadas em localidade remota?
    - ○ Sim
    - ○ Não
84. As cópias são criptografadas?
    - ○ Sim
    - ○ Não
85. O *software* de *backup* envia e-mail quando há algum erro no *backup*?
    - ○ Sim
    - ○ Não
86. De quanto em quanto tempo é feita uma recuperação para verificar se o *backup* está ok?
    - ○ Sim
    - ○ Não
87. No caso de acesso remoto, utiliza-se VPN com criptografia?
    - ○ Sim
    - ○ Não
88. Existe uma rede de gerência separada?
    - ○ Sim
    - ○ Não
89. Existe um controle no fornecimento dos serviços de rede oferecidos por terceiros?
    - ○ Sim
    - ○ Não

7 Controle de acessos

7.1 Requisitos de negócio para controle de acesso
7.1.1 Política de controle de acesso
7.2 Gerenciamento de acesso do usuário
7.2.1 Registro de usuário
7.2.2 Gerenciamento de privilégios
7.2.3 Gerenciamento de senha do usuário

7.2.4 Análise crítica dos direitos de acesso de usuário
7.3 Responsabilidades dos usuários
7.3.1 Uso de senhas
7.3.2 Equipamento de usuário sem monitoração
7.3.3 Política de mesa limpa e tela limpa
7.4 Controle de acesso à rede
7.4.1 Política de uso dos serviços de rede
7.4.2 Autenticação para conexão externa do usuário
7.4.3 Identificação de equipamento em redes
7.4.4 Proteção de portas de configuração e diagnóstico remoto
7.4.5 Segregação de redes
7.4.6 Controle de conexão de rede
7.4.7 Controle de roteamento de redes
7.5 Controle de acesso ao sistema operacional
7.5.1 Procedimentos seguros de entrada no sistema (*log-on*)
7.5.2 Identificação e autenticação de usuário
7.5.3 Sistema de gerenciamento de senha
7.5.4 Uso de utilitários de sistema
7.5.5 Limite de tempo de sessão
7.5.6 Limitação de horário de conexão
7.6 Controle de acesso à aplicação e à informação
7.6.1 Restrição de acesso à informação
7.6.2 Isolamento de sistemas sensíveis
7.7 Computação móvel e trabalho remoto
7.7.1 Computação e comunicação móvel
7.7.2 Trabalho remoto

90. Nas estações, existe algum aviso informando que somente pessoas autorizadas podem ter acesso?
    - ○ Sim
    - ○ Não
91. Existe um limite de tentativas para entrar na estação?
    - ○ Sim
    - ○ Não
92. Existe o compartilhamento de usuários/senhas?
    - ○ Sim
    - ○ Não
93. A troca de senhas é periódica?
    - ○ Sim
    - ○ Não
94. Existe uma exigência por parte dos *softwares* de uma senha forte?
    - ○ Sim
    - ○ Não
95. Senhas antigas podem ser utilizadas?

- Sim
- Não

96. Existem programas utilitários de sistema que podem ser capazes de sobrepor os controles dos sistemas e aplicações?
    - Sim
    - Não
97. Nos equipamentos de rede, o usuário é desconectado por tempo de inatividade?
    - Sim
    - Não
98. Existe restrição dos horários de conexão às horas normais de expediente?
    - Sim
    - Não

8 Aquisição desenvolvimento e manutenção de sistemas de informação

8.1 Requisitos de segurança de sistemas de informação
8.1.1 Análise e especificação dos requisitos de segurança
8.2 Processamento correto nas aplicações
8.2.1 Validação dos dados de entrada
8.2.2 Controle do processamento interno
8.2.3 Integridade de mensagens
8.2.4 Validação de dados de saída
8.3 Controles criptográficos
8.3.1 Política para o uso de controles criptográficos
8.3.2 Gerenciamento de chaves
8.4 Segurança dos arquivos do sistema
8.4.1 Controle de *software* operacional
8.4.2 Proteção dos dados para teste de sistema
8.4.3 Controle de acesso ao código-fonte de programa
8.5 Segurança em processos de desenvolvimento e suporte
8.5.1 Procedimentos para controle de mudança
8.5.2 Análise crítica das aplicações após mudanças no sistema operacional
8.5.3 Restrições sobre mudanças em pacotes de *software*
8.5.4 Vazamento de informações
8.5.5 Desenvolvimento terceirizado de *software*
8.6 Gestão de vulnerabilidades técnicas
8.6.1 Controle de vulnerabilidades técnicas

99. No desenvolvimento dos sistemas, são verificados questões de segurança da informação?
    - Sim
    - Não
100. Os sistemas possuem validação dos dados de entrada?

- ○ Sim
- ○ Não

101. Os sistemas possuem validação dos dados de saída?
- ○ Sim
- ○ Não

102. As bibliotecas dos sistemas estão protegidas de acesso não autorizado?
- ○ Sim
- ○ Não

103. O código-fonte dos sistemas está protegido de acesso não autorizado?
- ○ Sim
- ○ Não

104. Existe gerenciamento de mudança nas alterações de versão?
- ○ Sim
- ○ Não

105. Existe gerenciamento de mudança na inclusão de novos sistemas?
- ○ Sim
- ○ Não

106. Os sistemas são testados em ambiente de desenvolvimento?
- ○ Sim
- ○ Não

107. Os sistemas possuem um ambiente de teste que represente a realidade?
- ○ Sim
- ○ Não

108. O banco de dados de teste possui dados do banco de dados de produção embaralhados?
- ○ Sim
- ○ Não

9 Gestão de incidentes de segurança da informação

9.1 Notificação de fragilidades e eventos de segurança da informação
9.1.1 Notificação de eventos de segurança da informação
9.1.2 Notificando fragilidades de segurança da informação
9.2 Gestão de incidentes de segurança da informação e melhorias
9.2.1 Responsabilidades e procedimentos
9.2.2 Aprendendo com os incidentes de segurança da informação
9.2.3 Coleta de evidências

109. Existe um procedimento para informar sobre um incidente de segurança da informação?
- Sim
- Não

110. Existe um procedimento para informar sobre eventos de segurança da informação?
- Sim
- Não

111. Os incidentes de segurança da informação são analisados constantemente com o objetivo de melhorar a segurança da informação da organização?
- Sim
- Não

112. Existe um procedimento para coleta de evidências do incidente de segurança da informação?
- Sim
- Não

10 Gestão de continuidade do negócio

10.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação

10.1.1 Incluindo segurança da informação no processo de gestão da continuidade do negócio

10.1.2 Continuidade de negócios e análise/avaliação de riscos

10.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação

10.1.4 Estrutura do plano de continuidade do negócio

10.1.5 Testes, manutenção e reavaliação de continuidade do negócio

113. Existe uma identificação dos ativos envolvidos em processos críticos?
- Sim
- Não

114. Existe documentação de continuidade do negócio?
- Sim
- Não

115. Os riscos a que a organização está exposta foram elencados?
- Sim
- Não

116. Planos de continuidade relativos à segurança da informação foram desenvolvidos e implementados?
- Sim

- ○ Não

117. Existem procedimentos operacionais que permitam a restauração e recuperação do ambiente crítico em caso de desastres?
- ○ Sim
- ○ Não

118. Os planos de continuidade do negócio englobam cada parte vital da empresa?
- ○ Sim
- ○ Não

119. Os planos de continuidade do negócio foram testados?
- ○ Sim
- ○ Não

11 Conformidade

11.1 Conformidade com requisitos legais
11.1.1 Identificação da legislação aplicável
11.1.2 Direitos de propriedade intelectual
11.1.3 Proteção de registros organizacionais
11.1.4 Proteção de dados e privacidade de informações pessoais
11.1.5 Prevenção de mau uso de recursos de processamento da informação
11.1.6 Regulamentação de controles de criptografia
11.2 Conformidade com normas e políticas da informação e conformidade técnica
11.2.1 Conformidade com as políticas e normas de segurança da informação
11.2.2 Verificação da conformidade técnica
11.3 Considerações quanto à auditoria de sistemas de informação
11.3.1 Controles de auditoria de sistemas de informação
11.3.2 Proteção de ferramentas de auditoria de sistema de informação

120. A segurança da informação está de acordo com os requisitos legais vigentes?
- ○ Sim
- ○ Não

121. As ferramentas de auditoria estão armazenados em local seguro?
- ○ Sim
- ○ Não

4 CONCLUSÕES

Segurança da informação é uma pauta que não deve estar fora das reuniões das organizações. O principal objetivo deste trabalho foi criar uma ferramenta simples, em forma de questionário, para que qualquer organização possa verificar sua aderência com a ABNT NBR ISO/IEC 27002:2005.

Ter uma política de segurança da informação permitirá um alinhamento para que todos percebam a importância deste tema. Mas não basta ter uma política maravilhosa, se esta não está sendo utilizada e apoiada pela diretoria ou se funcionários, fornecedores e terceiros não possuem conhecimento dela.

O apoio da diretoria é de fundamental importância para garantir que a política de segurança da informação não é mais um papel que a TI fez para atrapalhar a vida dos usuários.

Além disso, um item importante a ser visto é a questão da criação do comitê gestor de segurança da informação, porque sem o apoio das outras áreas, a TI não irá conseguir melhorar a segurança dentro da empresa.

Itens como documentação, procedimentos, gestão de mudanças e gestão da capacidade são simples de implementar (não requerem recursos extras) e podem ser feitos em arquivos texto ou planilhas eletrônicas. O importante é criar procedimentos de atualização de documentos (controle de versão) e criar procedimentos simples para que mudanças não ocorram sem registro e que previsões de capacidade dos ativos da rede sejam feitos sempre visando o crescimento da organização. A segregação de funções ajuda no sentido de que uma única pessoa não terá acesso total a determinado ativo da rede (exemplo: criar uma regra de *firewall* e aplicá-la sem o conhecimento de ninguém).

As alterações devem ser feitas, sempre que possível, em ambientes de teste, para que se possa analisar todo o impacto e corrigir possíveis falhas antes de serem aplicadas no ambiente de produção.

O treinamento dos usuários em relação a segurança da informação deve ser realizado no momento da contratação e periodicamente, para todos. Uma questão importante é sempre ter uma lista de chamada para estes treinamentos, para que possa ser usada como evidência caso o usuário alegue que “não sabia” quando um incidente de segurança ocorre. Os treinamentos podem ser feitos pelo próprio

pessoal da TI junto com o RH, para que custos extras não sejam gerados.

No momento da contratação de funcionários, fornecedores e terceiros, não se deve esquecer que estes precisam assinar um acordo de confidencialidade caso tenham acesso a informações privilegiadas da organização. Além disso, verificar a autenticidade das informações passadas pelos candidatos pode ser uma boa prática.

No momento de encerramento das atividades, tudo que o funcionário tiver em sua posse e que pertence a organização deve ser devolvido formalmente (deve existir um procedimento para esta atividade). Além disso, a TI sempre deve ser informada quando um funcionário muda de setor ou quando este é dispensado ou resolve se desligar da organização, para que os acessos sejam retirados imediatamente (principalmente os acessos externos). Um e-mail formal para toda a organização também deve ser enviado, para que o ex-funcionário não tenha acesso as dependências da empresa após o encerramento de suas atividades.

Os usuários só devem ter acesso a dados que permitam a execução de suas atividades. Controles de acesso devem ser criados e mantidos pela TI. Caso mudanças ocorram, deverá existir procedimentos formais para que os setores façam as solicitações ao pessoal da TI.

Processos disciplinares devem ser estabelecidos e aplicados, quando necessário, para que os usuários percebam o nível de importância da segurança da informação para a organização.

Para que se consiga proteger os ativos é necessário ter conhecimento deles, então o inventário é de suma importância para a questão da segurança da informação. O inventário deve ser criado e mantido a partir de procedimentos criados pela equipe de TI.

Quanto à classificação da informação, este é um item que irá exigir um esforço maior da organização, uma vez que primeiramente terá que se decidir quem é o proprietário do ativo e este irá dizer o grau de sensibilidade do mesmo. Caso a organização ache interessante, ela pode, num primeiro momento, deixar a classificação para uma próxima oportunidade e assumir este risco.

Quanto a segurança física, controles simples como recepcionista, solicitação de documentos para visitantes, crachás de visitantes, acompanhamento do visitante dentro das dependências da organização, crachá para todos os funcionários, separação física e controlada das áreas de acesso público e áreas restritas, podem

garantir que pessoas não autorizadas tenham acesso a informações privilegiadas da organização. Além disso, controles mais fortes (senha individual) para acesso a área dos equipamentos de TI podem garantir que somente o pessoal de TI manipule informações importantes da empresa.

Quanto as estações de trabalho, retirar a permissão de administrador dos usuários garante que ninguém irá instalar *software* sem a autorização da TI. Ainda sobre estações, sempre solicitar um usuário e senha para acesso ao sistema operacional e que esta senha não seja de fácil adivinhação e que seja trocada periodicamente. A primeira senha deve ser criada pela TI de forma aleatória e deve exigir a sua troca sempre na primeira vez que o usuário realizar o *lo-gon*. Testes para verificar o nível da senha devem ser realizados periodicamente também.

O uso de *softwares* que verifiquem códigos maliciosos devem estar presentes em todos os equipamentos necessários e sempre atualizados, para que não deem a equipe de TI uma falsa sensação de segurança.

Procedimentos de *backup* e de *restore* de informações críticas devem ser realizados periodicamente (de acordo com o nível de sensibilidade da informação). Se possível, alguns *backups* devem ser mantidos fora das instalações da organização (para o caso de desastres) e devem ser criptografados (para que no caso de perda, pessoas não autorizadas não tenham acesso).

No caso de acesso remoto, tanto de funcionários, como de fornecedores e de terceiros, o uso de VPN deve ser obrigatório para garantir que as informações trocadas não possam ser capturadas por alguém não autorizado.

O monitoramento dos sistemas e dos ativos de rede devem ser realizados o tempo todo, para que a TI seja sempre a primeira a saber de algum problema ocorrido. O registro dos *logs* devem ser enviados para um servidor de *logs* e o armazenamento deve estar de acordo com a política de segurança da informação.

Mesmo com todos estes cuidados, incidentes de segurança podem ocorrer, neste caso, é importante que haja procedimentos formais para que qualquer pessoa da organização ou que preste serviço pra mesma consiga informar o ocorrido o mais rápido possível para que a equipe de TI tome as devidas providências. Os incidentes devem ser registrados e serão analisados periodicamente para se verificar quais itens podem ser melhorados na questão de segurança da informação da organização.

Poucas empresas possuem um plano de continuidade do negócio. Mesmo

que não exista, é responsabilidade da TI apresentar para o comitê gestor de segurança da informação os ativos que precisam ser replicados, as informações chaves que precisam estar acessíveis em caso de desastres, para que a organização consiga funcionar.

Todas estas atividades devem estar em conformidade com a legislação vigente e auditorias internas e externas devem ser realizadas periodicamente, para que problemas possam ser apontados e melhorias possam ser realizadas, afinal de contas, segurança da informação não é um produto acabado, mas um processo contínuo dentro da organização.

Como continuidade do presente estudo, sugere-se que o questionário seja aplicado em várias organizações para que se possa melhorá-lo. Além disso, que seja criado, a partir do questionário, pontuações que possam mostrar de forma gráfica o nível de aderência da organização a ABNT NBR ISO/IEC 27002:2005.

REFERÊNCIAS

ALEXANDRIA, João Carlos **Soares de. Gestão da segurança da informação – uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica.** 2009. 193 p. Tese (doutorado em Ciências na Área de Tecnologia Nuclear – Aplicações) – Programa de Pós-Graduação em Tecnologia Nuclear, IPEN, São Paulo.

ASSOCIAÇÃO BRASILEIRA DE NORMAS E TÉCNICAS – **ABNT NBR ISO/IEC 27002:2005** – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da Informação. Rio de Janeiro: ABNT, 2005.

BUKOWITZ, Wendi R.; WILLIAMS, Ruth L. **Manual de Gestão do Conhecimento**: ferramentas e técnicas que criam valor para a empresa. Porto Alegre: Bookman, 2002.

BURGHI M. Pequena empresa não investe em proteção. ***Jornal da Tarde.*** São Paulo, 13 jun. 2009. Seção Economia. Ataque Virtual. Disponível em: <http://txt.jt.com.br/editorias/2009/06/13/eco-1.94.2.20090613.4.1.xml>. Acesso em 10 Nov. 2011.

CAVALCANTI, Marly. **Gestão Estratégica de Negócios**: Evolução, Cenários, diagnóstico e ação. 2. ed. São Paulo: Cengage Learning, 2011.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT. Disponível em <http://www.cert.br/stats/incidentes/2011-jul-sep/tipos-ataque-acumulado.html>. Acesso em: 31 Nov. 2011.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT. Disponível em <:http://www.cert.br/stats/incidentes>. Acesso em: 31 Nov. 2011.

COMER, Douglas E. **Redes de Computadores e Internet**. 4. ed. Porto Alegre: Bookman, 2007.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação – Guia Prático para Elaboração e Implementação**. 2. ed. Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Editora Atlas, 2010.

KUROSE, James F.; ROSS, Keith W.. **Redes de computadores e a Internet: uma abordagem top-down**. 5. ed. São Paulo: Pearson Addison Wesley, 2010.

STALLINGS, Willian. **Redes e Sistemas de Comunicação de Dados**. Rio de Janeiro: Elsevier, 2005.

WADLOW, A.Thomas. **Projeto e Gerenciamento de Redes Seguras**. Rio de Janeiro: Editora Campus, 2000.

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ. **UTFPR: Normas para elaboração de trabalhos acadêmicos**. Curitiba: UTFPR, 2008.