ENTREGAR, SERVIR E SUPORTAR COM SGSI

Caroline Santos de Lemos*

César Augusto Borges de Andrade*

RESUMO

Este artigo apresenta aspectos da importância dos ativos para uma organização e a segurança que se deve ter para com os mesmos, uma vez que a organização depende da informação para sua evolução tecnológica e mercadológica. A necessidade de estabelecer medidas políticas e de gestão na instituição são vitais para minimizar a criticidade das informações e evitar danos aos dados sensíveis e a exposição da imagem de uma instituição. As normas ISO 27000 auxiliam na implantação e adoção de um sistema de gestão de segurança da informação para garantir que os serviços possam ser monitorados, entregues, suportados e continuados, além de gerenciar a segurança da informação em uma organização.

Palavras-chave: ISO 27000, Políticas de Segurança de Informação, Sistema de Gestão de Segurança da Informação.

ABSTRACT

This article presents aspects of the importance of the assets for the organization and security that is needed to have with these, once the organization depends of the information to its technological and marketing evolution. The necessity of establishing political and management measures in the institution are vital to minimize the criticism of information and avoid damage to the sensitive data and the exposure of the image of a company. The ISO 27000 assists the implementation and adoption of a system of information security management to guarantee that the services may be monitored, delivered, supported and continued, as also to manage the information security of a company.

Keywords: ISO 27000, Information Security Policies,Management of Information System Security.

1 INTRODUÇÃO

A informação sempre foi um fator para o desenvolvimento humano. Atualmente ela compõe uma peça fundamental para a vida e o desenvolvimento corporativo. Além de ser uma alavan-

* Faculdade JK - Especialização em Gestão de TI na Administração Pública QI 03, Lotes 1 a 4, Avenida Samdu Norte, Taguatinga/DF - CEP: 72.135-030
carolinesantossin,caborges72}@gmail.com

ca para o sucesso de uma organização, as informações contribuem para sua sobrevivência no mercado de trabalho.

Com o advento da tecnologia, muitas informações saíram do papel e passaram a ser armazenadas nos meios digitais, tornando-se um celeiro de dados privilegiados e vitais para uma corporação.

A complexidade no manuseio das informações tornou-se uma das atividades mais críticas em uma organização, uma vez que seus ativos mais valiosos estão expostos a ataques, manipulações e extravios por pessoas más intencionadas.

O cenário de ataques às instituições torna-se atrativo para as empresas concorrentes que buscam obter informações e tirar proveito delas auferindo vantagens frente suas rivais. Organizações podem ser alvos diários de muitos atacantes, pois várias são as formas de atingir seus ativos e até destruir a reputação de uma marca diante de um Mercado global.

O artigo tem como papel fundamental conscientizar organizações a tomar medidas para segurança de seus ativos, no papel de entregar, servir e suportar seus serviços, bem como, a necessidade da gestão da segurança da informação de sua instituição na criação e implantação de políticas, no papel do gestor, apoiando todo o ciclo e implantação de um sistema de gestão de segurança da informação e alinhando a organização de ponta a ponta com as normas e politicas de segurança, com intuito de minimizar riscos e potenciais incidentes.

O restante do artigo está organizado da seguinte maneira. A seção 2 apresenta o tópico de segurança com alguns fundamentos, termos da segurança da informação e ameaças encontradas em redes de computadores de uma corporação. A seção 3 explana alguns conceitos de gestão de segurança da informação em uma organização. A seção 4 define o *framework* COBIT e detalha sua aplicabilidade para a segurança da informação. Na seção 5 são definidos conceitos e aplicabilidades das normas de segurança, com foco nas normas *ISO* 27001 e *ISO* 27002. A seção 6 detalha, conforme as normas, o estabelecimento e gerenciamento de um SGSI. A seção 7 trata de responsabilidades da direção para com o SGSI. A seção 8 trata de auditorias internas. A seção 9 expõe a análise critica do SGSI pela direção. A seção 10 informa como o SGSI pode ser melhorado com ações corretivas e preventivas. Na seção 11 apresenta discussões de alguns trabalhos relacionados e na seção 12 é feita a conclusão do trabalho.

2 SEGURANÇA

Com a acessibilidade as informações e a facilidade da conectividade com o mundo externo, os ativos das organizações tornaram-se vulneráveis e alvos de violação à privacidade e a ataques que visam a inoperação dos serviços.

Para um processo organizacional de segurança da informação confiável, medidas e politicas de segurança devem ser estabelecidas e implantadas pelo gestor da organização.

2.1 Fundamentos da segurança

A segurança da informação busca proteger os ativos de uma organização contra os diversos tipos de ataques e ameaças, fornecer continuidade dos serviços, minimizar riscos, garantir autenticidade, confiabilidade, integridade e não repúdio das informações.

Segundo os autores Coelho, Araújo e Bezerra (2014), a segurança da informação é resultado de um conjunto de controles que devem ser estabelecidos, implementados, monitorados, analisados e continuamente melhorados, com intuito de atender às necessidades de negócios e segurança da organização. A seguir, são detalhados alguns conceitos:

a) Incidente de Segurança: Qualquer evento adverso relacionado à segurança;

b) Ativo: Qualquer coisa que tenha valor para a organização e para os seus negócios;

c) Ameaças: Qualquer evento que explore vulnerabilidades. Causa potencial de um incidente indesejado, que pode gerar danos à organização ou sistema;

d) Vulnerabilidade: Qualquer fraqueza que possa ser explorada e comprometa a segurança de um Sistema de Informação;

e) Risco: Combinação de probabilidade de um evento ocorrer e de suas consequências para a organização;

f) Ataque: Qualquer ação que comprometa a segurança de uma organização;

g) Confidencialidade: Compreende proteção de dados transmitidos contra ataques não autorizados, envolve medidas de controle de acesso e criptografia;

h) Autenticidade: Garantir que uma comunicação é autentica. Origem e destino podem verificar identidade da outra parte envolvida na comunicação;

i) Integridade: Garantia contra ataques aos ativos, por meio de alterações ou remoções não autorizadas; e

j) Não repúdio: Compreende o serviço que previne uma origem ou destino de negar a transmissão de mensagens.

2.2. Redes sob ameaças

Segundo o autor Kurose (2012), alguns problemas atuais à segurança da informação podem ser dados pelos programas maliciosos que se infiltram nos computadores de forma ilícita, *Malwares*, hospedados em redes. Uma vez instalado na rede, o *Malware* pode infectar aparelhos e ser capaz de fazer coisas tortuosas, como apagar arquivos, instalar *Spyware*, que são programas que coletam nossas informações particulares e de comportamento do usuário e enviam a terceiros sem o consentimento e conhecimento do usuário, e ainda, pode comprometer a estrutura da rede envolvendo os equipamentos a se conectarem a diversos aparelhos que têm o objetivo de controlar e influenciar a rede ou provocar ataques contra negação de serviço, conhecidos como *Botnet*, podendo tirar um serviço do ar ou mantê-lo inoperável.

Segundo o autor Kurose (2012), um amplo grupo de ameaças à segurança pode ser classificado como ataque de recusa de serviços, ataque *DoS*, que torna uma rede ou um hospedeiro ou uma parte da infraestrutura inutilizável por usuários verdadeiros. Servidores da *Web*, de *e-mail*, *DNS* (*Domain Name System* - é um sistema de gerenciamento de nomes hierárquico e permite a inscrição de vários dados digitados além do nome do *host* e seu *IP*) e redes institucionais podem estar sujeitos aos ataques *DoS*. Os ataques de negação de serviço mais utilizados na internet são:

a) Ataque de Vulnerabilidade: Envolve envio de mensagens perfeitas a uma aplicação vulnerável ou sistema operacional. Se a sequencia correta de pacotes for enviada o serviço pode parar ou pifar o hospedeiro;

b) Inundação na Largura de Banda: O atacante envia um grande número de pacotes ao hospedeiro, entupindo e impedindo que os pacotes legítimos cheguem ao servidor;

c) Inundação na Conexão: O atacante estabelece um grande número de conexões no hospedeiro-alvo. O hospedeiro fica sobrecarregado com as conexões falsas e para de aceitar conexões legítimas.

Outro ataque que as redes estão propensas a passar, segundo Kurose (2012), é a análise de pacotes. Um analisador de pacote pode estar distribuído em ambientes de conexão com ou sem fios. O atacante analisa os pacotes podendo obter cópias de todos os enviados pela rede. Os pacotes podem ser farejados em busca de informações confidenciais que podem causar prejuízos para uma entidade. Caso não sejam adotadas medidas e controles de segurança adequadas, tais prejuízos podem ser irreparáveis a uma instituição.

3 GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Diante dos cenários de vulnerabilidades, ataques e fragilidades aos ativos expostos que uma instituição está sujeita a sofrer e todos os prejuízos acarretados, o reforço da relevância da gestão de segurança da informação na organização é valido.

Para entregar, servir e suportar os serviços de uma organização, o profissional de segurança deve desenvolver ações alinhadas e pautadas com os melhores frameworks (conjunto de conceitos usados para resolver um problema de um domínio específico), normas e práticas para a proteção e controle da informação.

O papel fundamental na gestão de segurança da informação na organização é o planejamento, execução, monitoramento e a melhoraria continuada da segurança da informação, tomando como direcionador a governança da segurança da informação, que é o alinhador das necessidades do negócio com as soluções tecnológicas e que busca o maior retorno sobre os investimentos e coerência com objetivos de negócios.

Segundo Defenda (2012), para que haja a governança da segurança de informação de forma efetiva, diretores e executivos devem ter um claro entendimento do que esperar das iniciativas e ações de segurança da informação. Deve-se ter um entendimento para direcionar a imple-

mentação de programas de segurança da informação, como avaliar o andamento dessas ações, o seu retorno para organização e como decidir as estratégias e os objetivos de um programa de segurança da informação efetivo.

Defenda (2012) afirma ainda que a governança da segurança da informação, quando desenvolvida apropriadamente, retorna à organização os resultados de alinhamento estratégico, gestão de riscos, gestão de recursos, gestão de desempenho e entrega de valor. Como facilitador dessas ações e soluções, o alicerce da gestão será pautada no *framework* COBIT 5, modelo corporativo para governança e gestão de TI da organização, que será citado nas próximas seções.

4. COBIT

A ISACA (*Information Systems AuditandControlAssociation*), organização mantenedora do COBIT, o descreve como framework de governança de TI e ferramentas de suporte que permitem aos gerentes fazerem a ponte entre os requisitos de controle, questões técnicas e riscos de negócios. Além disso, permite o desenvolvimento de políticas claras e boas práticas para controle de TI nas organizações.

O COBIT 5 ajuda a organização criar valor por meio da TI mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de riscos e de utilização de recursos. O COBIT é genérico e útil para organizações de todos os portes, sejam comerciais, sem fins lucrativos ou públicas. Em sua última versão, baseia-se em cinco princípios básicos para a governança e gestão de TI da organização, quais sejam: atender às necessidades das partes interessadas, cobrir a organização de ponta a ponta, aplicar um modelo único integrado, permitir uma abordagem holística e distinguir a governança de gestão.

O COBIT é orientado para os negócios, o que atende as demandas da administração e gerência, quanto ao equilíbrio dos riscos e investimentos, dos usuários dependentes dos serviços de TI e auditores que validam controles internos à administração. As atividades de TI relacionam riscos de negócios, necessidades de controles e questões técnicas, formando estruturas lógicas e organizadas para a instituição que adere ao modelo de gestão.

O COBIT define suas atividades em quatro domínios que são: Alinhar, Planejar e Organizar (APO), Construir, Adquirir e Implementar (BAI), Entregar, Serviços e Suporte (DSS) e Monitorar, Avaliar e Analisar (MEA). O presente trabalho é pautado no domínio de entrega, serviço

e suporte (processo de gestão) e no processo de gerenciar serviços de segurança (DSS05).

4.1 DSS5 Gerenciar Serviços de Segurança

Segundo o COBIT (2012), o DSS5 tem foco em definir políticas, procedimentos e padrões de segurança de TI, além de monitorar, detectar, reportar e solucionar vulnerabilidades e incidentes de segurança.

O DSS5 também protege informações para manter o nível de risco aceitável para a segurança da informação da organização, de acordo com a política de segurança. Estabelece e mantem as funções de segurança da informação, privilégios de acesso e realiza o monitoramento de segurança.

O DSS05 mantem como práticas:

a) Proteger contra *Malware*;

b) Gerenciar segurança de rede e conectividade;

c) Gerenciar segurança de *endpoints* (entidade em um terminal de uma conexão);

d) Gerenciar identidade e acesso lógico de usuários;

e) Gerenciar acesso físico a ativos de TI;

f) Gerenciar documentos e dispositivos de saída sensíveis; e

g) Monitorar a infraestrutura quanto a eventos relacionados à segurança.

5 NORMAS DE SEGURANÇA DE INFORMAÇÃO

Para Ferreira (2008), a Política de Segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da Segurança da Informação devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação.

Como forma de aplicar políticas de segurança e garantir a conformidade com a gestão, a base das normas de segurança se firma na família da ISO 27000. As normas da família **ISO/IEC** são normas Internacionais desenvolvidas pela *International Organization for Standardization*- ISO, em Genebra, e a *International Eletrotechnical Commission* – IEC. Compõem um conjunto de normas utilizadas para a Gestão de Segurança da Informação e fornecem uma estrutura para a sua implantação. Serão brevemente citadas a seguir as normas 27001 e 27002.

5.1. NBR ISO 27001

A Norma ABNT (2006) foi desenvolvida pelo Comitê Brasileiro de Computadores e Processamento de Dados, e pela Comissão de Estudo de Segurança Física em Instalações de Informática. Essa norma pretende determinar um padrão para a Gestão de Segurança da Informação – SGSI, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação – SGSI de uma organização.

Segundo a Norma ABNT (2006), uma organização que deseja implementar um sistema de gestão de segurança da informação - SGSI deve adotar essa norma como base. A referida norma é utilizada como documento para realizar auditorias, certificação e especificação de um SGSI.

A norma adota o modelo PDCA – *Plan, Do, Check e Act*, para aplicar e estruturar todos os processos do SGSI nos quais:

a) *Plan* (Planejar): estabelecer a politica de segurança da informação, os objetivos, processos e procedimentos do SGSI;

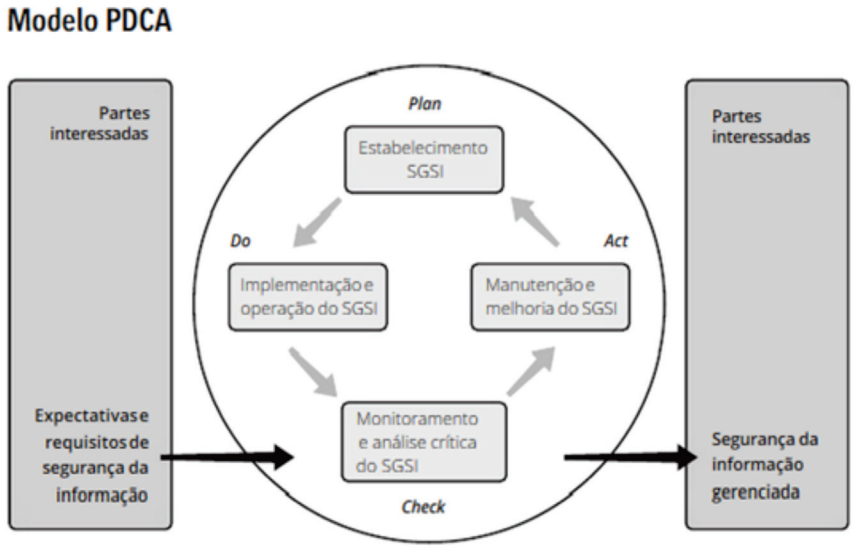
b) *Do* (fazer): implementar e operar a política, os procedimentos, controle e processos do SGSI;

c) *Check* (checar): monitorar, analisar criticamente, realizar auditorias e medir o desempenho dos processos; e

d) *Act* (agir): manter e melhorar, por meio de ações corretivas e preventivas, o SGSI visando seu contínuo aperfeiçoamento.

A figura 1 apresenta a estrutura organizacional com os processos estruturados através do modelo PDCA.

Figura 1 - Modelo PDCA.



Fonte: (NORMA ABNT ISO/IEC 27001)

A seção que trata do objetivo da norma cita que, o SGSI é projetado para assegurar a seleção de controles de segurança adequados, proteger os ativos de informação e proporcionar confiança às partes interessadas. Os requisitos são genéricos e se aplicam a qualquer organização. A exclusão de qualquer dos requisitos especificados nas seções 4 a 8 da norma NBR ISO 27001 não são aceitáveis, caso uma organização reivindique conformidade com a norma. A necessidade de exclusão de algum controle precisa ser justificada e as evidencias precisam ser providas para os riscos aceitos.

A norma ISO 27001 utiliza como referencia a ISO 27002, que é indispensável para a sua aplicação.

5.2. NBR ISO 27002

A norma ABNT (2005) estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos pela norma provêm diretrizes gerais sobre as metas geralmente aceitas para a gestão de segurança da informação. Ela funciona como um código de boas práticas para a segurança da informação, sugerindo que a informação seja protegida.

A proteção deve ser feita a partir de implementação de um conjunto de controles adequados, políticas, processos, procedimentos, estrutura organizacionais e funções de software e hardware.

Segundo a ISO, esses controles têm por finalidade atender aos requisitos identificados por meio de uma análise e avaliação dos riscos da organização. A norma está organizada da seguinte forma:

a) Objetivo do controle: Define o que deve ser alcançado;

b) Controle: Define o controle a ser implementado para atender o objetivo do controle;

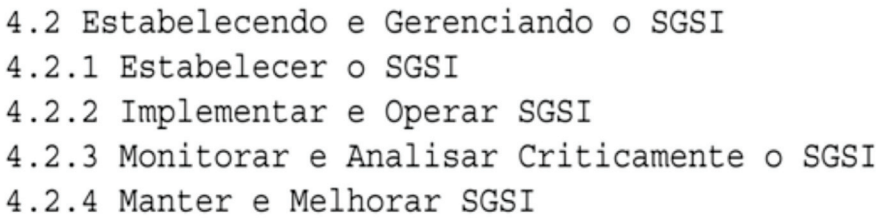
c) Diretrizes: Apresenta informações mais detalhadas para apoiar a implementação do controle; e

d) Informações adicionais: São informações que podem ser consideradas na implementação do controle, como aspectos legais e referência a outras normas.

6. ESTABELECENDO E GERENCIANDO UM SGSI

Este item apresenta as etapas de implantação que uma organização deve estabelecer quando desejam implementar um SGSI em seus ambientes de trabalho, implantando a gestão de segurança da informação para a organização, monitoramento e controlando os Sistemas no ambiente corporativo, propondo a aplicação de ferramentas que auxiliam a segurança da informação, avaliando e assegurando os ativos, controle de acessos, entre outras politicas de segurança.
A seção número 4 da norma ISO 27001 especifica os requisitos gerais para estabelecer um SGSI. A figura número 2 mostra a estrutura da sessão 4 da norma. A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro de um contexto das atividades de negócio globais da organização.

Figura 2. Requisitos para estabelecer SGSI.



Fonte: Elaborada pela autora.

6.1 Estabelecer o SGSI (Plan)

Segundo a norma ABNT (2006), para estabelecer um SGSI uma organização deve:

a) Definir o escopo e os limites do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologias, inclusive detalhes e justificativas para a exclusão de escopo (qualquer exclusão dos requisitos das seções 4, 5, 6, 7 ou 8, não são aceitáveis quando a organização reivindicar conformidade). Qualquer exclusão de controle deve ser devidamente justificada e as evidências de que os riscos associados foram aceitos pelas pessoas responsáveis precisam ser fornecidas. Onde quaisquer controles sejam excluídos, reivindicações de conformidade a esta Norma não são aceitáveis, a menos que tais exclusões não afetem a capacidade da organização, e/ou responsabilidade de prover segurança da informação que atenda os requisitos de segurança determinados pela análise/avaliação de riscos e por requisitos legais e regulamentares aplicáveis.

b) Definir uma política de SGSI nos termos das características do negócio, da organização, de sua localização, de seus ativos e tecnologias que:

- Inclua uma estrutura para definir objetivos e estabeleça um direcionamento global e princípios para ações relacionadas com a segurança da informação;

- Considere requisitos de negócio, legais e ou regulamentares, e obrigações de segurança contratuais;

- Esteja alinhada com o contexto estratégico de gestão de risco da organização;

- Estabeleça critérios em relação os riscos que serão avaliados; e

- Tenha sido aprovada pela direção;

c) Definir abordagem de análise e avaliação de riscos da organização:

- Identificar uma metodologia de análise e avaliação de riscos que seja adequado ao SGSI e aos requisitos legais, regulamentares e de segurança da informação, identificados para o negócio; e

- Desenvolver critérios para aceitação de riscos e identificar os níveis aceitáveis de riscos.

d) Identificar riscos:

- Identificar os ativos dentro do escopo do SGSI e seus respectivos proprietários;

- Identificar as ameaças para com esses ativos;

- Identificar as possíveis ameaças a esses ativos; e

- Identificar os impactos que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos de uma organização.

e) Analisar e avaliar riscos:

- Avaliar os impactos para o negócio da organização que podem resultar de falhas de segurança, levando em consideração perda de confidencialidade, integridade ou disponibilidade dos ativos;

- Avaliar a probabilidade real da ocorrência de falhas de segurança;

- Estimar níveis de riscos; e

- Determinar se os níveis são aceitáveis ou se requerem tratamento utilizando os critérios para aceitação de riscos estabelecidos.

f) Escolher e avaliar as opções de tratamento de riscos:

- Aplicar controles apropriados;

- Aceitar riscos consciente e objetivamente, desde que satisfaçam as políticas;
- Evitar riscos; e

- Transferir os riscos associados ao negócio a outras partes, como seguradoras ou fornecedores.

g) Selecionar objetos de controle e controles para tratamentos de riscos:

- A seleção de objetivos de controles e controles deve atender aos requisitos identificados pela análise e avaliação de riscos e pelo processo de tratamento de riscos;

- Devem ser considerados os critérios para aceitação de riscos, como também os requisitos legais, regulamentares e contratuais.

h) Obter aprovação da direção dos riscos residuais propostos;

i) Obter autorização da direção para implementar e operar o SGSI; e

j) Preparar uma declaração de aplicabilidade. Deve conter no documento:

- Objetivos de controle, os controles selecionados e as razões para sua seleção;

- Os objetivos de controle e os controles atualmente implementados; e

- A exclusão de quaisquer objetivos de controles e controles e a justificativa para exclusão.

Em conformidade, a norma ISO 27002 em sua seção de número 4 especifica a análise/avaliação e tratamento de riscos. Essa seção especifica o primeiro passo dado por uma organização para seleção de controles para implementar e traz como recomendação:

a) Análise/avaliação de riscos com enfoque sistemático de estimar a magnitude do risco (análise de riscos) e o processo de comparar os riscos estimados contra os critérios de risco para determinar a significância do risco (avaliação do risco);

b) Análise/avaliação de riscos sejam realizadas periodicamente, para que possam ser contempladas as mudanças nos requisitos de segurança da informação e na situação de riscos;

c) Análise e avaliação de riscos tenham um escopo claramente definidos;

A organização deve definir critérios para avaliar se os riscos podem ou não ser aceitos, antes

mesmo de considerar o tratamento de um risco. Além disso, para cada risco identificado, uma decisão para o tratamento do risco precisa ser tomada, como:

a) Aplicar controles para reduzir os riscos;

b) Conhecer e aceitar os riscos;

c) Evitar riscos, não permitindo ações que causem ocorrência de riscos; e

d) Transferir os riscos associados para outras partes, como seguradoras ou fornecedores.

Em conformidade, a norma ISO 27002, em sua seção número 5, especifica a criação de politica de segurança da informação. Na qual, informa conveniência da direção em estabelecer uma política clara, alinhada com objetivos de negócio. Ainda, demonstra apoio e comprometimento com a segurança da informação por meio de publicação e manutenção de uma política de segurança da informação para toda a organização. O documento da política de segurança da informação, dentre outras coisas deve conter:

a) Uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação;

b) Uma declaração do comprometimento da direção;

c) Uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco; e

d) Definição das responsabilidades gerais e específicas na gestão da segurança da informação.

6.2. Implementar e Operar o SGSI (Do)

Na seção de implementar e operar um SGSI, a organização deve:

a) Formular um plano de tratamento de risco, que identifique a ação de gestão apropriada, recursos, responsabilidades e propriedades para gestão dos riscos de segurança;

b) Implementar o plano de tratamento de riscos, para que possam ser alcançados objetivos de controle identificados que incluam considerações de financiamento e atribuição de papéis e responsabilidades;

c) Implementar os controles selecionados para atender objetivos de controle;

d) Definir como medir a eficácia dos controles selecionados, e especificar como essas medições serão aplicadas para avaliar a eficácia dos controles de modo a produzir resultados comparáveis e reproduzíveis (a medição dos controles permite aos gestores determinar o alcance e satisfação dos objetivos de controle planejado);

e) Implementar programas de conscientização e treinamento;

A organização deve assegurar que todo o pessoal que tem responsabilidade atribuída no SGSI seja competente para desempenhar as tarefas requeridas:

- Determinar as competências necessárias para o pessoal que executa trabalhos que afetam o SGSI;

- Fornecer treinamento, ou contratar pessoas competentes para satisfazer as necessidades;

- Avaliar a eficácia das ações executadas; e

- Manter registros de educação, treinamento, habilidades, experiências e qualificações.

A organização deve assegurar que todo o pessoal pertinente esteja consciente da relevância e importância das suas atividades de segurança da informação e como eles contribuem para o alcance dos objetivos do SGSI.

f) Gerenciar as operações do SGSI;

g) Gerenciar os recursos para o SGSI; e

- Provisão de recursos;

A organização deve determinar e prover os recursos necessários para:

- estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI;
- assegurar que os procedimentos de segurança da informação apoiem os requisitos de negócio;
- identificar e tratar os requisitos legais e regulamentares e obrigações contratuais de segurança da informação;
- manter a segurança da informação adequada pela aplicação correta de todos os controles implementados;
- realizar análises críticas, quando necessário, e reagir adequadamente aos resultados destas análises críticas; e
- onde requerido, melhorar a eficácia do SGSI.

- Treinamento, conscientização e competência (citados anteriormente na letra "e");

h) Implementar procedimentos e outros controles capazes de permitir a pronta detecção de eventos de segurança da informação e resposta a incidentes de segurança da informação.

6.3 Monitorar e Analisar Criticamente (Check)

Na seção de monitorar e analisar criticamente um SGSI, a organização deve:

a) Executar procedimentos de monitoração e análise crítica e outros controles para:

- Prontamente detectar erros nos resultados;

- Prontamente identificar tentativas e violações de segurança bem sucedidas, e incidentes de segurança da informação;

- Permitir à direção determinar se as atividades de segurança da informação delegadas a pessoas ou implementadas por meio te tecnologias de informação são executadas conforme esperado;

- Ajudar a detectar eventos de segurança da informação e assim prevenir incidentes de segurança da informação pelo uso de indicadores; e

- Determinar se as ações tomadas para solucionar uma violação de segurança da informação foram eficazes;

b) Realizar análises críticas regulares da eficácia do SGSI, levando em consideração resultados de auditoria de segurança da informação, incidentes de segurança da informação, resultados da eficácia das informações, sugestões e realimentação de todas as partes interessadas;

c) Medir eficácia dos controles, para verificar se os requisitos de segurança da informação foram atendidos;

d) Analisar criticamente as análises/avaliações de riscos em intervalos planejados e analisar criticamente os riscos residuais e os níveis de riscos aceitáveis identificados, levando em consideração mudanças relativas a:

- Organização;

- Tecnologias;

- Objetivos e processos de negócio;

- Ameaças identificadas;

- Eficácia dos controles implementados; e

- Eventos externos, tais como mudanças nos ambientes legais ou regulamentares, alterações das obrigações contratuais e mudanças na conjuntura social.

e) Conduzir auditorias internas do SGSI a intervalos planejados (ver item 9 do artigo);

f) Realizar uma análise critica do SGSI para a direção em bases regulares para assegurar que o escopo permanece adequado e que são identificadas melhorias nos processos do SGSI;

g) Atualizar planos de segurança da informação para levar em consideração os resultados das atividades de monitoramento e análise crítica; e

h) Registrar ações e eventos que podem produzir impacto na eficácia ou no desempenho de SGSI.

Controle de registros:

Registros devem ser estabelecidos e mantidos para fornecer evidências de conformidade aos requisitos e da operação eficaz do SGSI. Eles devem ser protegidos e controlados. O SGSI deve levar em consideração quaisquer requisitos legais ou regulamentares pertinentes e obrigações contratuais. Os registros devem permanecer legíveis, prontamente identificáveis e recuperáveis. Os controles necessários para a identificação, armazenamento, proteção, recuperação, tempo de retenção e disposição de registros devem ser documentados e implementados.

Devem ser mantidos registros do desempenho do processo e de todas as ocorrências de incidentes de segurança da informação significativos relacionados ao SGSI.

6.4 Manter e Melhorar o SGSI (*Act*)

Na seção de manter e melhorar um SGSI, a organização deve regulamente:

a) Implementar as melhorias identificadas no SGSI;

b) Executar ações preventivas e corretivas apropriadas (será visto no item 11.1 e 11.2 deste artigo);

c) Comunicar as ações e melhorias a todas as partes interessadas com um nível de detalhe apropriado às circunstâncias e, se relevante, obter a concorrência sobre como proceder; e

d) Assegurar-se de que as melhorias atinjam os objetivos pretendidos.

7 RESPONSABILIDADE DA DIREÇÃO

Na seção número 5 da ISO 27001 trata da responsabilidade da direção quanto para com o SGSI. A direção deve fornecer evidências do seu comprometimento com o SGSI mediante:

a) Estabelecimento da política do SGSI;

b) A garantia de que são estabelecidos os planos e objetivos do SGSI;

c) O estabelecimento de papéis e responsabilidades pela segurança da informação;

d) Comunicação à organização da importância em atender objetivos de segurança e conformidade com as políticas, suas responsabilidades para com as leis e a necessidade de melhoria contínua;

e) Prover recursos de forma suficiente para um SGSI;

f) Definir critérios para aceitar riscos e dos níveis de riscos aceitáveis;

g) Garantir que as realizações das auditorias internas do SGSI sejam realizadas;

h) Condução da análise crítica do SGSI pela direção (que será abordado no item 10 deste artigo);

A gestão de recursos complementa a responsabilidade da direção, como provisão de recursos financeiros e assegurar os treinamentos, conscientização e capacitação para todos com responsabilidade definida e atribuída no SGSI. A organização deve assegurar também que o pessoal esteja consciente da importância das suas atividades para o SGSI.

8 AUDITORIAS INTERNAS DO SGSI

Segundo o autor Rodrigues (2011), a auditoria de segurança da informação é uma atividade devida-

mente estruturada para examinar criteriosamente a situação dos controles que se aplicam à segurança da informação, especialmente por meio da análise de objetos e seus pontos de controle, em face da probabilidade de ameaças às informações críticas sobre as quais atuam esses controles.

A seção número 6 da norma ISO 27001 estabelece que a organização deve realizar auditorias internas do SGSI em intervalos planejados para definir se os objetivos de controle, controles, processos e procedimentos do seu SGSI:

a) Atendem aos requisitos dessa norma e a legislação ou regulamentações;

b) Atendem aos requisitos de segurança da informação identificados;

c) Estão mantidos e implementados eficazmente; e

d) São executados conforme esperado.

Um programa de auditoria deve ser planejado levando em consideração a situação e a importância dos processos e áreas a serem auditadas, bem como as auditorias anteriores e seus resultados. Critérios de auditoria, escopo, frequência e métodos devem ser definidos.

Para a seleção de auditores e na execução de auditoria, deve-se assegurar objetividade e imparcialidade dos processos. O responsável pela área a ser auditada deve assegurar que as ações sejam executadas sem demora indevida. E não deve auditar seu próprio trabalho.

As responsabilidades e os requisitos para planejamento e para execução de auditorias para relatar os resultados e a manutenção dos registros devem ser definidos em um procedimento documentado.

9. ANÁLISE CRÍTICA DO SGSI PELA DIREÇÃO

A organização deve analisar criticamente seu SGSI em intervalos planejados para assegurar a sua contínua pertinência, adequação, eficácia, oportunidade de melhoria ou necessidade de mudanças.

As entradas para análise crítica são:

a) Resultados das auditorias do SGSI e análises críticas;

b) Realimentações das partes interessadas;

c) Técnicas, produtos ou procedimentos que poderiam ser usados na organização para melhorar o desempenho e a eficácia do SGSI;

d) Situação das ações preventivas e corretivas;

e) Vulnerabilidades ou ameaças não contempladas adequadamente nas análises/avaliações de risco anteriores;

f) Resultados das medições de eficácia;

g) Acompanhamento das ações oriundas de análises críticas anteriores;

h) Qualquer mudança que poderia afetar o SGSI;

i) Recomendações para melhoria.

As saídas devem incluir quaisquer decisões e ações relacionadas a:

a) Melhoria da eficácia do SGSI;

b) Atualização da análise/avaliação de riscos e do plano de tratamento de riscos;

c) Modificação de procedimentos e controles que afetem a segurança da informação, quando necessário, para responder a eventos internos ou externos que possam impactar no SGSI, incluindo mudanças de:

- Requisitos de negócio;

- Requisitos de segurança da informação;

- Processos de negócio que afetam os requisitos de negócio existentes;

- Requisitos legais ou regulamentares;

- Obrigações contratuais; e

- Nível de riscos e ou critérios de aceitação de riscos.

d) Necessidade de recursos; e

e) Melhoria de como a eficácia dos controles está sendo medida.

10 MELHORIA DO SGSI

O SGSI é melhorado através de auditorias internas e análises críticas da direção. A organização deve continuamente melhorar a eficácia do SGSI por meio do uso da política de segurança da informação, objetivos de segurança da informação, resultados de auditorias, análise de eventos monitorados, ações corretivas e preventivas e análise crítica pela direção. A seção número 8 da norma trata da melhoria contínua em ação corretiva e ação preventiva.

10.1 Ação corretiva

A organização deve executar ações para eliminar as causas de não conformidades com os requisitos do SGSI, evitando repetições.

Procedimentos documentados para ação corretiva devem definir requisitos para identificar não conformidades, determinar as causas de não conformidades, avaliar a necessidade por ações para assegurar que as não conformidades não ocorram novamente, determinar e implementar as ações corretivas necessárias, registrar os resultados das ações executadas e analisar criticamente as ações corretivas executadas.

10.2 Ação preventiva

A organização deve determinar ações para eliminar as causas de não conformidades potenciais com os requisitos do SGSI, de forma a evitar a sua ocorrência. As ações preventivas tomadas devem ser apropriadas aos impactos dos potenciais problemas.

O procedimento documentado para ação preventiva deve definir requisitos como identificar não conformidades potenciais e suas causas, avaliar a necessidade de ações para evitar a ocorrência de não conformidades, determinar e implementar as ações preventivas necessárias, registrar os resultados de ações executadas, analisar criticamente as ações preventivas executadas.

A norma define que, a organização deve identificar mudanças nos riscos e identificar requisitos de ações preventivas focando a atenção nos riscos significativamente alterados.

Também estabelece que, a prioridade de ações preventivas deve ser determinada com base nos resultados da análise e avaliação de riscos.

Ainda, a norma define que ações para prevenir não conformidades frequentemente têm melhor custo-benefício que as ações corretivas.

11 TRABALHOS RELACIONADOS

Existem muitos trabalhos que abordam o tema de Sistema de Gestão de Segurança da Informação, os quais contribuíram significativamente para a elaboração do trabalho. Quatro deles podem ser comparados a seguir.

A autora Souza (2007) detalha conceitos fundamentais de segurança da informação e ferramentas para reduzir o impacto sobre a segurança de redes em uma organização. Além de estabelecer conceitos a partir das normas ISO 27000 para implantar a segurança da informação, o trabalho apresenta um estudo de casos sobre a empresa Tecnicópias Gráficas e Editora Ltda.
Por outro lado, Martins e Santos (2005) especificam normas, processos e metodologias de implantação de um SGSI como: concepção, estabelecimento política de segurança da informação, definição do escopo, análise de riscos, gerenciamento das áreas de riscos, seleção dos controles, implementação e acompanhamento dos indicadores e auditoria do sistema e plano de melhoria.

Os autores Santos e Filho (2013) propõem um modelo de SGSI em conformidade com as normas NBR ISO 27001, 27002 e 27005, guiando na implementação prática de um novo sistema de segurança da informação em uma organização ou na verificação da conformidade de um já existente.

Ainda, Netto (2007) realiza estudos entre empresa, seus ativos, riscos e vulnerabilidades inse-

ridos. Na mesma dissertação, o autor faz pesquisa exploratória para identificar ferramentas e técnicas de gestão de segurança da informação, obtendo resultados de deficiência e carência das instituições e a não motivação em aderir um SGSI.

Em cada um dos trabalhos são abordados assuntos de gestão e implementação de um sistema de gestão de segurança da informação. Ambos discorrem sobre técnicas e normas que auxiliam na implantação de um SGSI em uma organização. Durante a fase de pesquisa foram selecionadas técnicas de melhores frameworks e normas para servir de base nas soluções de um sistema de gestão de segurança da informação, a fim de, entregar os serviços, minimizar riscos, garantir a confidencialidade das informações, autenticidade e disponibilidade.

O presente trabalho busca motivar e conscientizar o leitor a manter os ativos de uma instituição seguros com técnicas para segurança das informações em um ambiente organizacional. Apresenta fatores críticos de ataques e vulnerabilidades em uma organização para roubo de informações ou para tornar os serviços inoperáveis. E ainda, detalha as normas e referências para melhor elaboração de um SGSI, tomando como referência artigos e normas que especificam práticas para implementação de um Sistema de Gestão de Segurança da Informação alicerçados nas normas NBR-ISO/IEC 27001 e NBR-ISO/IEC 27002.

12 CONCLUSÃO

Buscando contribuir com a pesquisa em sistema de gestão de segurança da informação (SGSI), este estudo apresenta aos profissionais interessados ou envolvidos na segurança da informação que optam por implantar um SGSI em uma organização, como uma decisão estratégica para suprir suas necessidades e objetivos, exigência de segurança, cobrir a estrutura da organização, bem como, seus processos.

No início, o artigo retrata a evolução tecnológica nas instituições tornando os ativos e serviços, de uma instituição, alvos fáceis para atacantes, impulsionando e incentivando a organização a criar medidas e politicas que auxiliem a gestão da segurança da informação.

Alguns fundamentos básicos da segurança da informação foram abordados para melhor esclarecimento e entendimento das normas citadas ao longo do artigo. Também foram expostos tipos de ameaças sujeitas a serem instaladas em um ambiente de trabalho que possui rede de computadores,

mostrando a relevância de se instalar medidas de contorno de situação, prevenção de incidentes, controles de medição de desempenho, entre outras soluções para gerir a segurança da informação.

Para o bom controle do sistema de segurança da informação, o papel fundamental na organização é o do profissional responsável pela gestão de segurança, que deve estar pautado em *frameworks*, normas e práticas apropriados para entregar, servir e suportar os serviços de uma organização. Com a gestão da segurança e possível planejar, executar, monitorar e melhorar continuamente a segurança da informação, buscando alocar melhor os seus recursos e soluções, trazendo melhor retorno sobre os investimentos e satisfazendo os objetivos do negócio.

O *framework* COBIT 5, mencionado no artigo, auxilia a organização a criar valor por meio da TI. Ele auxilia, por meio dos seus processos, a organização a enxergar o que fazer para que suas necessidades possam ser atendidas.

As atividades do COBIT são definidas em quatro domínios, no qual um deles é alvo do trabalho. No domínio entregar, servir e suportar, que está ligado ao processo de gestão, o DSS5 é destacado para o processo de gerência de serviços de segurança, com foco em estabelecer politicas, procedimentos e padrões de segurança de TI.

As normas que abordam o provimento de um modelo de estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI são a NBR ISO/IEC 27001 e sua referência ISO/IEC 27002.

A norma ISO 27001, que é utilizada como base em uma organização que deseja implementar um SGSI, é como documento para realizar auditorias e certificações. Ela se organiza em um modelo PDCA (Plan- Do- Check e Act) para estruturar todos os seus processos, nos quais cabem os planejamentos de politicas, processos, objetivos e procedimentos, fazer implementações e operações dessas politicas, procedimentos, controles e processos, checar monitorações e analises, desempenho de processos e auditorias e agir para manter e melhorar o SGSI com ações corretivas e preventivas.

A norma traz algumas responsabilidades da direção para com o SGSI e algumas especificações quanto à auditoria de um SGSI e análise crítica pela direção, assegurando a continuidade, eficácia, possíveis melhorias, mudanças e adequações do sistema de segurança.

A implantação de um sistema de gestão de segurança da informação é sem duvida uma solução que viabiliza a eficácia da entrega e suporte dos serviços, garantindo a continuidade das atividades organizacionais de forma a maximizar a segurança do ambiente e entregar resultados satisfatórios com os objetivos do negócio.

REFERÊNCIAS

Associação Brasileira de Normas Técnicas - ABNT. **Norma NBR-ISO/IEC 27001:2006**.

Associação Brasileira de Normas Técnicas - ABNT. **Norma ABNT ISO/IEC NBR 27002:2005.**

COELHO, F. E S. C.; ARAÚJO, L. G. S. A.; BEZERRA, E. K B. **Gestão da Segurança da Informação**: NBR 27001 e NBR 27002. Rio de Janeiro: Escola Superior de Redes, 2014.

COBIT 5. **Modelo Corporativo para Governança e Gestão de TI da Organização**, 2012.

DEFENDA. **Governança da Segurança da informação**. Disponível em: <http://www.defenda.com.br/downloads/Governan%C3%A7a_da_Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o.pdf>. Acessado em 02 de Dez. 2015.

FERREIRA, F. N. F. **Política de Segurança da Informação**: Guia Prático Para Elaboração e Implementação. Rio de Janeiro: Ciência Moderna, 2008.

KUROSE, K. R. **Redes de Computadores e a Internet:** Uma abordagem Top-Down. São Paulo: Pearson, 2012.

MARTINS, A.B.; SANTOS, C.A.S. **Uma Metodologia para Implementação de um Sistema de Gestão de Segurança da Informação**, Revista de Gestão da Tecnologia e Sistemas de Informação, 2005.

NETTO, A.S. **Gestão da Segurança da Informação**: Fatores que Influenciam sua Adoção em Pequenas e Médias Empresas. São Caetano do Sul, 2007.

RODRIGUES, R.W.S.; FERNANDES, J.H.C. **Auditoria e Conformidade de Segurança da Informação**, CEGSIC 2009-2011, 2011.

SANTOS, V.O.; FILHO, R.B. **Um Modelo de Sistema de Gestão da Segurança da Informação Baseado nas Normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008**, Revista Telecomunicações, 2013.

SOUZA, R.M. **Implementação e Técnicas de Segurança da Informação em Conformidade com as Normas ISO 27001 e ISO 27002**, CEATEC, 2007.