A falta de segurança, no meio empresarial, da não adoção da iso/iec 27002

The Lack Of Security, In The Business Environment, Of The Non-Adoption Of ISO/IEC 27002

Fernanda Souza Rezende[1]
Cristiano Diniz[2]

Resumo: Este artigo tem como objetivo estudar a importância da norma ISO/IEC 27002 no âmbito empresarial, para mostrar a grande relevância que esta tem no dia-a-dia nas organizações. O método adotado é o estudo na norma no todo e fazendo um comparativo com a visão das empresas em se tratando de vulnerabilidade e ameaças que as preocupam. É perceptível que se as empresas usassem a norma como guia estariam mais preparadas para proteger seus ativos.

Palavras-Chave: Segurança da Informação; ISO/IEC 27002; Políticas de Segurança da Informação.

Abstract: *This article aims to show the importance of ISO/IEC 27002 in the business environment, to demonstrate the great importance it has in the day to day activities of companies. The method adopted is the study of the code of practice as a whole and making a comparison with the companies' view in regards to vulnerability and threats that concern them. It is noticeable that if companies used the code of practice as a guide they would be better prepared to protect their assets.*

Keywords: Information Security, ISO/IEC 27002, Information Security Policies.

[1] Graduada em Sistemas para Internet (Faculdades Promove) e em Marketing (UNA) e cursando o 8° período do curso de Bacharelado em Sistema de Informação na Faculdade Promove. E-mail: fernandasr7@gmail.com

[2] Pós-graduado em Gestão de Segurança da Informação (FUMEC), Graduado em Ciência da Computação (PUC), professor nos cursos de Graduação e Tecnólogos na Faculdades Promove e orientador desta pesquisa. E-mail: cristianodiniz@gmail.com

1 INTRODUÇÃO

Com o uso cada vez mais amplo de dispositivos digitais em meio empresarial, a quantidade de informação e dados salvos pelas empresas nesses dispositivos está cada vez maior. O que ocorre, às vezes por falta de conhecimento do empresário ou por não querer investir muito em tecnologia, é que as informações acabam ficando concentradas em um único lugar. Isto faz aumentar os riscos para que as informações se percam ou sejam modificadas indevidamente.

Um sistema computacional é considerado seguro se houver uma garantia de que é capaz de atuar exatamente como esperado. Segurança como uma condição no qual estamos livres de perigos e incertezas. Ainda afirma que “dentro de uma organização, esta segurança costuma se aplicar a tudo que possui valor”. A segurança é esperada por um simples motivo: evitar e minimizar riscos. Para tanto existe a ISO/IEC 27002, que é um código de práticas para orientação empresarial.

A norma ABNT NBR ISO/IEC 27002 foi preparada para servir como um guia prático para o desenvolvimento e a implementação de procedimentos e controles de segurança da informação em uma organização.

Delimitou-se o tema deste estudoao risco à segurança das informações na não adoção da norma da Associação Brasileira de Normas e Técnicas (ABNT), um estudo sobre a ISO/IEC 27002.

O objetivo geral é mostrar a importância da norma, no âmbito empresarial, assim como os principais itens que compõem a ISO 27002.

A relevância deste estudo consiste em demonstrar em que ponto as empresas estão sendo prejudicadas em não adotar esta norma que tem aceitação global, além de ser um ótimo diferencial de mercado. Tendo em vista que manter a informação segura, confiável, íntegra e sempre disponível aumenta a competitividade e a agilidade na tomada de decisões.

Quanto à metodologia, trata-se de uma pesquisa do tipo exploratória. Utilizou-se como técnica a pesquisa bibliográfica (fontes secundárias) tendo como base a ABNT NBR ISO/IEC 27002.

Para compreensão do tema dividiu-se este artigo em 5 seções. A seção 1 trata da introdução, que delimita a importância do tema; a seção 2 apresenta o conceito e a importância da segurança da informação; a seção 3 descreve a norma, junto com o conceito geral e objetivo; a seção 4 é uma análise de uma pesquisa quantitativa sobre segurança cibernética; e seção 5 com as conclusões.

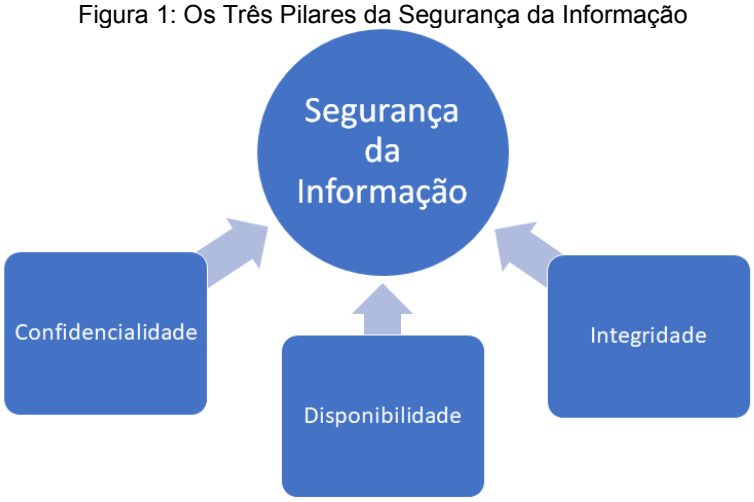
2 SEGURANÇA DA INFORMAÇÃO

Segundo Coelho (2014), segurança da informação "é a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança". Ainda acrescenta que é de necessidade que estes controles precisam ser estabelecidos, implementados, monitorados, analisados e melhorados para que assegurem que os objetivos do negócio e a segurança da informação da organização sejam atendidos de acordo com os parâmetros da norma.

> A segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software. (COELHO, 2014, p 2).

A segurança da informação possui três atributos básicos, de acordo com Dantas (2011), como mostra a figura 1: a confidencialidade que zela a proteção e garantia dos dados, para que nenhum acesso não autorizado tenha acesso às informações; a integridade, por sua vez, é a garantia que os dados serão armazenados e transferidos conforme a entidade enviada; e a disponibilidade que é a garantia que o serviço esteja disponível para o seu uso sempre que for necessário.

Figura 1: Os Três Pilares da Segurança da Informação



Fonte: A autora

Ao longo dos anos, com a evolução da tecnologia, surgiram vários problemas relacionados à segurança da informação. Sendo assim, é aconselhado estabelecer métricas para definição do nível de segurança existente e assim estabelecer as análises para melhoria da situação.

Para melhor assistência existe a família da norma ISO 27000, que é relacionada à segurança de dados digitais ou sistemas em armazenamento eletrônicos. Dentre elas a ISO/IEC 27002, que traz controles de segurança para implementação de um Sistema de Gestão de Segurança da Informação (SGSI).

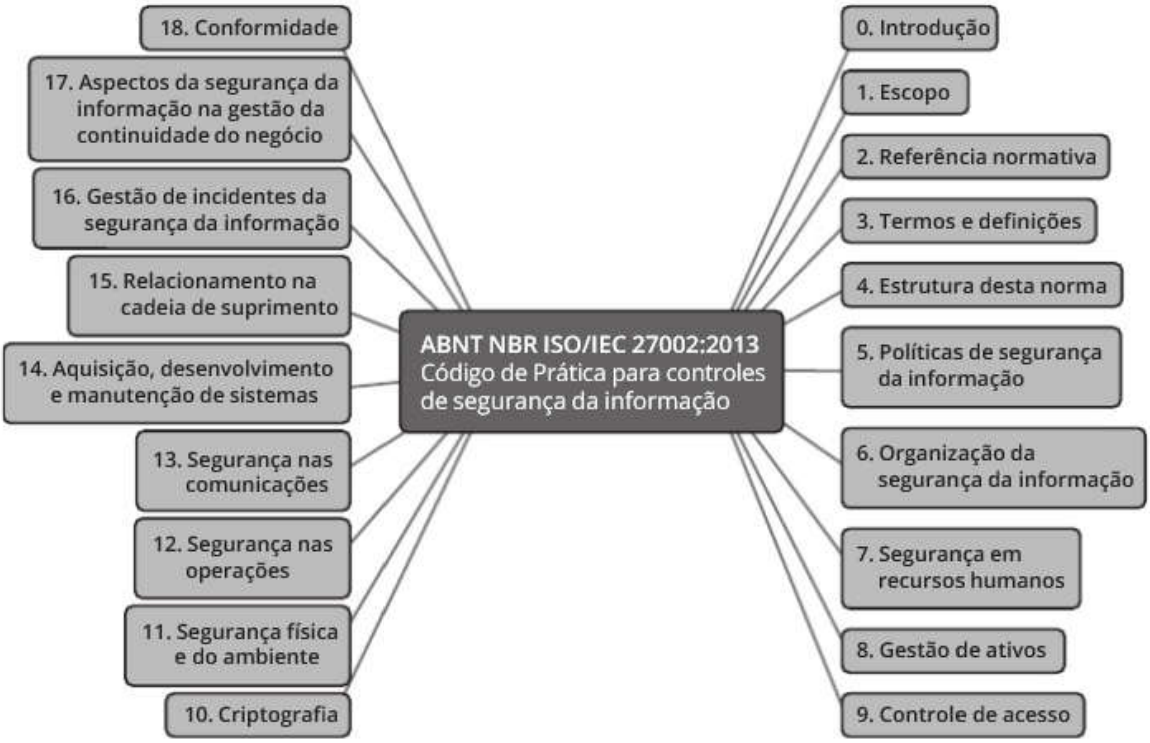
3 NORMA ISO/IEC 27002

A ABNT NBR ISO/IEC 27002 (2013), define como o objetivo, estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança em uma organização.

A norma é estruturada em dezenove capítulos, como mostra a figura 2, sendo que os cinco primeiros dispõem de: temas da introdução, escopo, as referências normativas, os termos e definições, e a estrutura da norma. A partir do capítulo 5, a norma passa a chamar cada capítulo de seção. Assim, encontram-se distribuídos

em quatorze seções, sendo: política de segurança da informação; organizando a segurança da informação; gestão de ativos; segurança em recursos humanos; segurança física e do ambiente; gestão das operações e comunicações; controle de acesso; aquisição, desenvolvimento e manutenção de sistemas de informação; gestão e incidentes de segurança da informação; gestão da continuidade do negócio; e conformidade.

Figura 2 - Sequência Estrutural da Norma



Fonte: Coelho, 2014, p.20

A seção sobre Política de Segurança da Informação, tem como objetivo orientar e apoiar no melhor caminho para a segurança da informação. Esta ainda auxilia no gerenciamento, estabelecendo um documento para melhor acordar as metas, o escopo e a importância da segurança. Este documento deverá ser aprovado pela direção, publicado e comunicado a todas as partes relevantes, pois é nele que são feitos os requisitos de conscientização, as consequências das violações, entre outras.

O sexto capítulo, Organização da Segurança da Informação, tem como objetivo estabelecer os controles para estruturar dentro da organização interna,

como: a responsabilidade e papéis pela segurança da informação; segregação de funções; contato com autoridades; contato com autoridades; contato com grupos especiais; e no gerenciamento de projetos.

Outra seção bastante importante, que muitas vezes passa por despercebido, é a de Segurança em Recursos Humanos, este prevê que dentro da organização é essencial assegurar que as informações de segurança sejam passadas para os funcionários, fornecedores e terceiros, a responsabilidade de cada um destes deve estar documentada de acordo com cada papel na empresa para reduzir riscos de furto, roubo, fraude ou até mesmo mau uso do recurso.

A quarta seção, Gestão de Ativos, tem como objetivo “alcançar e manter a proteção adequada dos ativos da organização” (ABNT, 2013). Ativo, segundo Ramos (2006), é tudo aquilo que possui valor para uma organização. A norma ainda orienta que todos os ativos sejam devidamente identificados e um inventários com os mais importantes seja estruturado e mantido com todas as informações necessárias que permitam recuperar de um desastre, incluindo o tipo do ativo, formato, localização, informações sobre cópia de segurança, informações sobre licenças e a importância do ativo para o negócio.

O capítulo sobre Controle de Acesso tem por objetivo controlar o acesso à informação. Esta seção prevê o gerenciamento de acesso do usuário seja documentada e analisada, para que se tenha uma base nos requisitos necessários como as responsabilidades de cada usuário e seus devidos privilégios, tanto para acessos em locais físicos como em acessos em sistemas operacionais, redes e equipamentos.

Criptografia (ou escrita escondida) vem no décimo capítulo com o objetivo de garantir o uso concreto e adequado da criptografia para proteger o sigilo, a autenticidade e a integridade da informação.

A seção de Segurança Física e do Ambiente tem como objetivo de prevenir o acesso físico não autorizado tem área definidas na organização. É de

responsabilidade da empresa definir quem são e onde as pessoas autorizadas podem ter acesso e deixar documentado claramente.

Segurança nas Operações, no décimo segundo capítulo, tem por objetivo garantir a operação segura e correta dos recursos e de processamentos da informação. Esta ainda possui sete categorias, uma delas a de documentação dos procedimentos de operação que diz que os procedimentos de operação sejam documentados e disponibilizados a todos os usuários que necessitem deles.

No capítulo de Segurança nas Comunicações são encontradas duas categorias que tratam dos controles necessários para a segurança das comunicações. A categoria de gerenciamento de segurança em redes tem por objetivo assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam. Já a categoria de equipamento tem o objetivo de manter a segurança da informação transferida dentro da organização e com qualquer entidade externa, que convém estabelecer políticas para proteção da troca de informações.

Aquisição, Desenvolvimento e Manutenção de Sistemas tem como objetivo assegurar que a segurança da informação é parte complementar do ciclo de vida dos sistemas de informação, que também inclui os requisitos para sistemas que fornecem serviços sobre as redes públicas.

Relacionamento na Cadeia de Suprimento visa tratar os processos de segurança nos relacionamentos com os fornecedores e possui duas categorias. A primeira segurança da informação na cadeia de suprimentos que define que deve ser assegurado a proteção dos ativos da organização e acessados pelos fornecedores e a segunda categoria, gerenciamento de entrega do serviço do fornecedor que mantém o nível acordado de segurança da informação e de entrega de serviços em consenso com os acordos com os fornecedores.

O décimo sexto capítulo, Gestão de Incidentes da Segurança da Informação, tem o objetivo de assegurar um aspecto compacto e satisfatório para gerenciar os

incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

No capítulo de Aspectos da Segurança da Informação na Gestão de Continuidade do Negócio possui duas subseções: continuidade da segurança da informação que tem o objetivo de não permitir a interrupção das atividades do negócio; redundância assegura a disponibilidade dos recursos de processamento da informação.

O último capítulo, Conformidade, tem por objetivo segundo a ABNT NBR ISO/IEC 27.002 (2013) “evitar violação de quaisquer obrigações legais, estaduais, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação.

4 A NECESSIDADE DAS ORGANIZAÇÕES

Em 2015 a empresa EY[3] fez uma pesquisa com 1.755 organizações do mundo todo. O objetivo final da empresa com a pesquisa é melhorar soluções de segurança cibernética. 88% das empresas, que responderam o questionário, não acham que a sua segurança da informação atenda totalmente às necessidades da organização. Kessel e Allan (2015, p.2), explicam que “na pressa, muitas precauções foram negligenciadas, e riscos subestimados”.

Na figura 3 é apontado um quadro com as respostas quantitativas de uma das questões do questionário representando as vulnerabilidades e ameaças para as empresas que participaram da pesquisa avaliarem com notas de acordo com prioridades no que se refere ao aumento do risco.

[3]**EY,** a antiga Ernst & Young, é uma das quatro maiores empresas de serviços profissionais do mundo (as big four), presente em 150 países, em 728 escritórios, e com mais de 190 mil funcionários. A firma, com sede em Londres, presta serviços de auditoria, elisão fiscal, consultoria e transações corporativas.

Figura 3 - Vulnerabilidade e Ameaça

Quais ameaças e vulnerabilidades mais aumentaram seu risco de exposição nos últimos 12 meses? (Dê uma nota para todos os itens, sendo 1 a de maior prioridade, e 5, a de menor prioridade)

*Ameaça é definida como o potencial de ocorrência de uma ação hostil proveniente de atores em um ambiente externo.

**Vulnerabilidade é definida como existência da possibilidade de ser atacado e sofrer danos.

Fonte: Allan e Kessel (2015, p. 6)

No quadro de vulnerabilidade, o que mais aumenta os riscos segundo as organizações é o fato de ter funcionários displicentes e desinformado. No sétimo capítulo da ISO/IEC 27002 indica que as responsabilidades pela segurança da informação sejam atribuídas antes da contratação e que todos os funcionários e fornecedores sejam adequadamente analisados e ainda que assinem acordos sobre seus papéis e responsabilidades pela segurança da informação. Desta forma nenhuma pessoa envolvida nos processos da empresa estarádesinformada sobre suas responsabilidades.

Com 15% das votações, em segundo lugar está a arquitetura e controles de segurança desatualizados. A ISO/IEC 27002 visa o desenvolvimento e a implementação de procedimentos e controles de segurança da informação para uma organização, com esta qualquer empresa segue preparada e informada para ter seus controles de segurança dentro dos padrões e atualizados, assim como sua arquitetura.

Na seção nove prevê o controle de acesso, isto que preocupa as empresas em segundo lugar com 10%. A norma prevê que seja estabelecida uma política de controle de acesso, direitos de acesso e restrições para papéis específicos dos usuários acessarem seus ativos.

No quadro das ameaças a maior preocupação é o "*Phishing*". Segundo Kurtz (2016), Phishing é uma maneira desonesta que cibercriminosos usam para enganar as pessoas a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Estes criminosos conseguem tais informações através de e-mails e direcionamento de websites falsos. No décimo segundo capítulo da norma, trata sobre a segurança nas operações. Que prevê controles de segurança que atendem à maioria das vulnerabilidades. Deve implementar mecanismos de monitoramento de atividades não autorizadas de processamento da informação.

Ainda no décimo segundo capítulo é descrito a segunda maior preocupação das empresas ainda se tratando das ameaças, *malware*, que é um tipo de software que realiza ações na máquina do usuário sem o seu consentimento podendo roubar

e destruir dados importantes. Na categoria 12.2.1, da norma, tem como objetivo assegurar que as informações e os recursos de processamento da informação estejam protegidos contra *malware*. A norma ainda afirma que os funcionários devem estar conscientes dos perigos e os gestores, onde apropriado, implantar controles para prevenção.

5 CONCLUSÃO

Para a compreensão do tema deste artigo buscou-se, inicialmente, entender a fundo o que a norma compreende. A norma foi projetada para ser referência para organizações terem controles dentro dos processos de implementação do sistema de gestão da segurança da informação. Ela é uma orientação para a implementação de controles de segurança da informação.

Tendo em vista os aspectos observados as pessoas da organização requer mais atenção por parte da empresa, tendo em vista que, as empresas investem em controles tecnológicos para diminuir o risco de incidentes e esquecem que o fator humano é uns dos grandes responsáveis pela falha na segurança.

Seguir os princípios da ISO/IEC 27002 é grande significância para as empresas garantir sua segurança, mas de nada adianta se não ressaltar sua importância para seus colaboradores. Para um início da implementação é necessário realizar ações para mapear e identificar a atual situação, sendo relevante as ameaças, os riscos e as vulnerabilidades. A segurança da informação não é uma despesa, e sim um investimento.

REFERENCIAS

ALLAN, Ken; KESSEL, Paul Van. **Criando Confiança no Mundo Digital**. Disponível em <http://www.ey.com/br/pt/services/giss_2015>. Acesso em: 02/04/2017

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. *Código de prática para a gestão da segurança da informação.* Rio de Janeiro, 2013.

COELHO, Flávia Estélia Silva; et al. **Gestão da Segurança da Informação.** Rio de Janeiro: ESR, 2014. 198p.

DANTAS, Marcus Leal. **Segurança da Informação: Uma Abordagem Focada em Gestão de Riscos**. Olinda: Livro Rápido, 2011. 152 p.

KURTZ, João. **O que é phishing?** Disponível em <http://www.techtudo.com.br/artigos/noticia/2012/01/o-que-e-phishing-e-malware.html> Acesso em: 12/06/2017

Portal ISO 27000. Disponível em <http://iso27000.com.br/> Acesso em: 16/05/2017.

RAMOS, Anderson; et al. **Guia Oficial para Formação de Gestores em Segurança da Informação.** Porto Alegre: Zouk, 2006. 460 p.

SHINEIER, Bruce. **Segurança com: segredos e mentiras sobre proteção na vida digital**. Rio de Janeiro: Campus, 2001.