UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA – DAELN
CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

DOUGLAS ROBERSON DE BRITO

# COMBATENDO A AMEAÇA *RANSOMWARE* APLICANDO A NORMA NBR ISO/IEC 27001:2013 NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA - PR

2016

DOUGLAS ROBERSON DE BRITO

# COMBATENDO A AMEAÇA *RANSOMWARE* APLICANDO A NORMA NBR ISO/IEC 27001:2013 NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Monografia de Especialização apresentada ao Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do título de "Especialista em Gestão da Tecnologia da Informação e Comunicação"

Orientador: Prof. Msc. Alexandre Jorge Miziara

CURITIBA - PR

2016

**1.**

**2.** UTFPR UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

## TERMO DE APROVAÇÃO

Título da monografia

**COMBATENDO A AMEAÇA *RANSOMWARE* APLICANDO A NORMA NBR ISO/IEC 27001:2013 NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO**

Por

**DOUGLAS ROBERSON DE BRITO**

Esta monografia foi apresentada às **16:15 h** do dia **06/12/2016** como requisito parcial para a obtenção do título de Especialista no CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, da Universidade Tecnológica Federal do Paraná, **Câmpus Curitiba**. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho:

| | | |
|---|---|---|
| **1** | **x** | Aprovado |
| **2** | | Aprovado condicionado às correções Pós-banca, postagem da tarefa e liberação do Orientador. |
| **3** | | Reprovado |

_____

**Prof.** Dr. Roberto Candido
UTFPR - Examinador

_____

**Prof.** Msc. Alexandre Jorge Miziara
UTFPR – Orientador

_____

**Prof. Msc. Alexandre Jorge Miziara**
UTFPR – Coordenador do Curso

* O Termo de Aprovação assinado encontra-se na Coordenação do Curso.

## RESUMO

BRITO, Douglas Roberson de. Combatendo a ameaça *ransomware* aplicando a norma ISO/IEC 27001:2013 na gestão da segurança da informação. 2016. 18 f. Monografia (Especialização em Gestão da Tecnologia da Informação e Comunicação) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2016

Este trabalho apresenta um estudo acerca do atual cenário da Segurança da Informação quanto à evolução e crescimento dos incidentes envolvendo o *ransomware*, um tipo específico de *malware* com características específicas que causam prejuízos monetários substanciais às empresas, demonstrando a relevância desta ameaça para as organizações. Mediante os dados pesquisados e apresentados, foi proposta a adoção de controles apresentados na norma ISO 27001: 2013, norma mundialmente reconhecida que descreve uma gama de controles utilizados para a implementação de um Sistema de Gestão de Segurança da Informação adequado.



**Palavras-chave**: Sistema de Gestão da Segurança da Informação, *Ransomware*, NBR ISO/IEC 27001:2013, *Malware*.

## ABSTRACT

BRITO, Douglas Roberson de. Fighting the *ransomware*'s threat applying the ISO/IEC 27001: 2013 norm in the information security management. 2016. 18 s. Final essay. (Information Technology and Communication Management Specialization) – MBA - Federal University of Technology of Paraná. Curitiba, 2016.

This essay presents a study about the nowadays scenario of Information Security, related to the evolution and rising of the numbers of incidents caused by *ransomwares*, a specific kind of *malware* with unique characteristics which causes substantial monetary losses to several companies, showing the relevance from this threat to the organizations. In front of data obtained through researches and showed here, it was proposed the adoption of controls described in the ISO 27001: 2013 norm, which is a globally recognized norm describing a range of controls, used on implementations of an Information Security Management System.



**Keywords**: Information Security Management System, *Ransomware*, ISO/IEC 27001:2013, *Malware*.

# SUMÁRIO

# 3. INTRODUÇÃO

## 1.1 Contextualização

A informação é um ativo essencial das organizações e faz parte de todos os processos de negócios, tendo, portanto, um valor praticamente imensurável, podendo levar as empresas ao sucesso ou ao fracasso devido aos grandes impactos financeiro, operacional ou de imagem, ocasionados por diversas falhas, erros ou fraudes.

Partindo deste ponto, a informação torna-se um recurso estratégico para qualquer organização, de forma fundamental para a geração de conhecimento e tomada de decisão dentro do negócio.

De acordo com Fontes (2011), considerando a informação um ativo de extrema importância para qualquer organização, não se restringindo a qualquer porte ou segmento de mercado, deve ser considerada a necessidade de haver controles adequados por meio dos processos de segurança da informação.

Os controles devem estar alinhados às principais fases da gestão do ciclo da informação que, conforme Sêmola (2003), são: manuseio, armazenamento, transporte e descarte.

Sêmola (2003, p. 9) ainda diz que “toda a informação é influenciada por três propriedades principais: confidencialidade, integridade e disponibilidade, além dos aspectos autenticidade e legalidade que complementam esta influência".

Para uma melhor compreensão, a figura abaixo ilustra as fases da informação, dentro do ciclo, com referência às propriedades básicas da informação confiável:

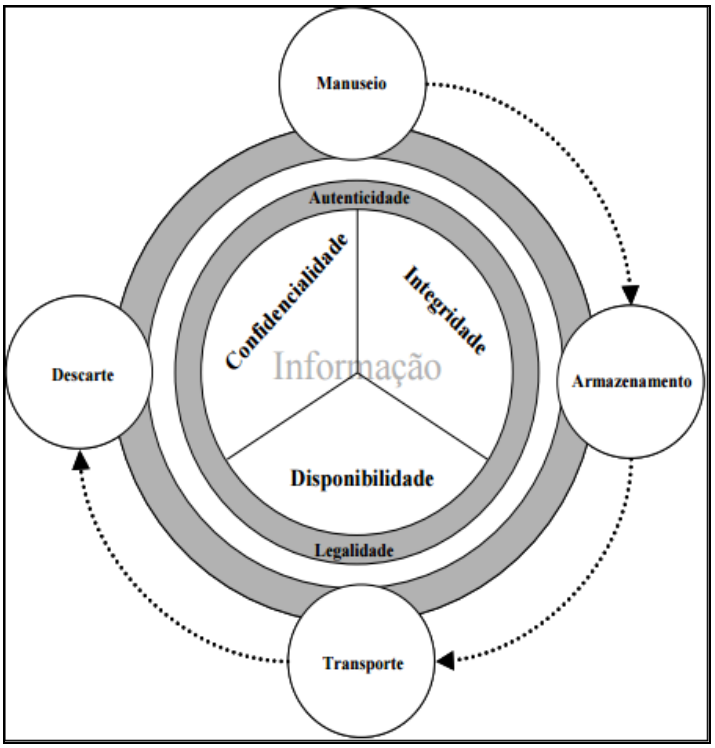


**Figura 1: Ciclo de vida da informação, considerando os conceitos básicos da segurança (SÊMOLA, 2003, p. 11)**

Visando garantir as propriedades da informação descritas por Sêmola, torna-se fundamental que seja aplicada uma política que vise a segurança da informação.

## 1.2 Problema

A proteção da informação torna-se ainda mais necessária diante do atual cenário de riscos e ameaças às informações.

Devido ao grande valor que a informação tem assumido dentre os ativos das organizações, as ameaças também têm aumentado acompanhando o alto interesse de mal-feitores nessas informações.

Nos últimos anos houve um crescimento notável nos incidentes envolvendo as informações corporativas. Em sua pesquisa anual de segurança de informação para o ano de 2015, a PwC reportou que desde 2009 os incidentes de segurança da informação têm aumentando anualmente numa proporção de 66%. Já a Symantec reportou que, no ano de 2015, a cada semana ao menos uma vulnerabilidade do tipo ‘dia zero’ foi identificada, num total de 54 incidentes, representando um aumento de 125% sobre o ano de 2014 (A New Zero-Day Vulnerability Discovered Every Week in 2015, 2016).

Além do crescimento gradual dos incidentes de segurança da informação, identifica-se que os ataques são normalmente direcionados a certos nichos do mercado. Em setembro de 2014, Bob Bragdon, editor da revista CSO, mencionou:

> "Grandes empresas têm se tornado um alvo mais frequente de infratores, uma vez que provem informações mais valiosas, entretanto, como também implementam medidas de segurança mais efetivas, cibercriminosos estão aumentando os ataques às empresas de médio porte. Infelizmente, estas organizações ainda não possuem práticas de segurança devidamente implementadas e equiparadas às das grandes companhias. " (The Global State of Information Security® Survey 2014, tradução livre).

O que Bob Bragdon identificava em 2014 veio a ser constatado pela Symantec em 2015, já que os ataques às corporações estavam distribuídos de forma semelhante entre grandes e pequenas empresas, com maior ocorrência nas empresas com menos de 250 empregados, representando 43% do total, frente aos 22% dos ataques às médias empresas (251 a 2500 empregados) e 35% dos ataques às empresas com mais de 2500 empregados (Attackers Target Both Large and Small Businesses, 2016).

Uma outra característica percebida, é que o foco dos *malwares* tem sido direcionado para a geração de rendimentos aos malfeitores, ao invés de somente gerarem o prejuízo quanto à informação. Esse novo foco leva ao aumento de *malwares* para caixas-eletrônicos, vírus bancários e *ransomwares*, com destaque para este último tipo de ameaça.

Entre outubro de 2015 e abril de 2016, a Trend Micro bloqueiou 99 milhões ameaças do tipo *ransomware*, e este número está somente relacionado aos clientes da Trend Micro – o atual volume de infecções em todo o ambiente tecnológico global pode ser muitas vezes maior (Part 1: Combatting the *Ransomware* Epidemic Requires Layered Security, 2016). De acordo com a Infosecurity Magazine (*Ransomware* Spikes 14% in Q1, 2016), dados liberados pela Kaspersky Lab mostram que nos primeiros três meses de 2016 houve um aumento de 30% no número atigindos por *ransomwares*, sendo que, no total, foram detetados 2900 novos tipos deste *malware* no mesmo período.

### 1.3 Objetivo

O principal objetivo deste trabalho é realizar um levantamento das atuais práticas de mercado, alinhadas com a norma ISO/IEC 27001:2013, para a gestão da segurança da informação, com foco no combate a um tipo de *malware* que apresenta um grande crescimento de ocorrências nos últimos anos, o *ransomware*.

De forma mais específica, este documento visa apresentar soluções para gestão da segurança da informação que já estão presentes na norma ISO/IEC 27001:2013, demonstrando exemplos descritivos de combate ao *ransomware*.

# 4. FUNDAMENTAÇÃO TEÓRICA

## 2.1 Gestão da Segurança da Informação

Na prática, a gestão da Segurança da Informação é a existência de melhores práticas dentro da organização a fim de assegurar o monitoramento contínuo dos dados e a integridade das informações corporativas.

Como já contextualizado, a informação é um ativo cada vez mais valorizado e impacta diretamente na continuidade dos negócios e na credibilidade das empresas. Por conta disso, as empresas têm buscado soluções para mitigar os riscos inerentes ao acesso indevido ou ao ataque às informações armazenadas nos sistemas computacionais corporativos, cada vez mais utilizados visando o crescimento e aumento da produtividade. Estabelece-se então um conjunto de boas práticas por meio de políticas de segurança gerenciadas em diferentes instâncias com funções e responsabilidades bem definidas. Tudo para assegurar o nível de segurança ideal, ou o mais próximo de, ao negócio.

Este é o conceito de Gestão da Segurança da Informação que envolve a criação de processos voltados à prevenção de acessos indevidos e ao furto dos dados, integridade das informações, e o acesso seguro às informações das companhias com o pronto restabelecimento dos sistemas em casos de interrupções inesperadas.

Para o desenvolvimento de padrões internacionais dos processos, foram definidas as Normas de Gestão da Segurança da Informação, também reconhecidas como série 27000. Essas normas se fundamentam em 10 premissas básicas aplicadas em qualquer tipo de organização, sendo elas:

- ✓ Política de Segurança da Informação;
- ✓ Segurança Organizacional;
- ✓ Classificação e controle dos ativos de informação;
- ✓ Segurança em pessoas;
- ✓ Segurança Física e Ambiental;
- ✓ Gerenciamento das operações e comunicações;
- ✓ Controle de Acesso;
- ✓ Desenvolvimento de Sistemas e Manutenção; e

- ✓ Gestão da continuidade do negócio e a Conformidade.

As Normas ISO/IEC 27001 e ISO/IEC 27002 tem origem no Padrão Britânico, que em 1993 criou a Norma BS 7799, até então uma única norma, mas dividida em duas partes. No ano de 2000, a ISO (International Organization for Standardization) publica a norma ISO 17799, baseada na primeira parte da Norma BS 7799, onde se tratava do código de conduta ou o guia de execução para a gestão da segurança da informação. Em 2005, a norma sofreu uma revisão, surgindo a ISO/IEC 17799:2005 e nesse mesmo período foi criada a Família 27000. E como primeira norma, a segunda parte, onde continha os requisitos de auditoria para a certificação de um sistema de gestão de segurança da informação, dando origem à ISO/IEC 27001:2005. Em 2007 a ISO/IEC 17799:2005 passou para o novo padrão e tornou-se a Norma ISO/IEC 27002:2005. Recentemente, em 2013, após extensas revisões as normas foram atualizadas, a ISO 27001 foi substancialmente modificada para ficar em linha com as demais normas de sistemas de gestão, mas a ISO 27002 teve seu processo de revisão ainda mais trabalhoso e demorado, com modificações no número de seções e controles, assim como na estrutura das seções.

## 2.2 A norma ISO/IEC 27001:2013

A norma ISO 27001 é o padrão internacional que especifica o Sistema de Gestão da Segurança da Informação (SGSI), contendo os requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar o SGSI.

O SGSI é um conjunto de atividades voltadas à gestão dos riscos para a informação, denominados riscos à segurança da informação, e assegura que os dispositivos de segurança estão definidos para manterem-se atualizados conforme novas ameaças, vulnerabilidades e impactos ao negócio apareçam.

A norma abrange todos os tipos de organizações (empresas comerciais, orgãos governamentais, organizações não lucrativas etc), de todos os tamanhos e de qualquer indústria ou mercado. Porém, é importante destacar que essa adaptabilidade da norma leva à característica de não determinar uma especificação mandatória de controles, uma vez que os controles variam dentro da vasta gama de organizações que adotam a norma.

## 2.3 A norma ISO/IEC 27002:20013

Dentre as duas normas que tratam da gestão da segurança da informação, a ISO 27002 é a mais antiga, tendo como norma precurssora a BS 7799, há mais de 30 anos.

A norma se trata de um código de práticas – um documento genérico com finalidade de guia, não uma especificação formal tal qual a ISO 27001. A ISO 27002 estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. É um conjunto completo de catorze cláusulas (ou seções) de controle de segurança e 114 controles de segurança que apóia e suporta a ISO 27001. Estes controles são os elementos que definem o que a norma considera importante para um processo, a fim de orientar a forma mais adequada de proteção da informação.

## 2.4 O *Ransomware*

O *ransomware* é um tipo de *malware*, ou seja, um tipo de *software* malicioso destinado a infiltrar-se em um sistema computacional alheio de forma ilícita. O que diferencia o *ransomware* dos demais *malwares* é que, ao invadir o sistema da vítima este tipo de *software* malicioso não visa simplesmente causar danos, mas bloquear o sistema invadido ou os dados contidos no sistema com a determinação de um valor de resgate a ser pago pelo usuário. Daí também explica-se o nome em inglês, com *ransom* significando resgate. Famílias mais modernas de *ransomwares*, coletivamente denominadas crypto-*ransomware*, também trabalham com a encriptação de certos tipos de arquivos ou sistemas e forçam o usuário a pagar o resgate usando canais de pagamento online pela chave de desencriptação.

# 5. METODOLOGIA

A metodologia adotada na elaboração desta monografia é a pesquisa documental. Segundo Fonseca (2002, apud SILVEIRA e CÓRDOVA, 2009 p. 37) a pesquisa documental recorre às mais diversas fontes de informação, tais como: tabelas estatísticas, jornais, revistas, relatórios, documentos oficiais, blogs, relatórios de empresas, etc.

Neste documento, foi-se majoritariamente utilizado de relatórios empresariais produzidos por organizações reconhecidas no mercado de segurança da informação e prestação de serviços na área.

A pesquisa eletrônica, constituída por informações extraídas de endereços eletrônicos em *sites* de empresas de boa reputação, portanto com procedência aceitável, reconhecida como uma fonte válida (SILVEIRA e CÓRDOVA, 2009 p. 69), também foi base para descrever este trabalho.

Tanto para pesquisa documental quanto para a pesquisa eletrônica adotadas, as fontes são consideradas de segunda mão, já que de alguma forma os dados já foram analisados, tendo sido transcritos para relatórios, infográficos e tabelas estatísticas.

# 6. APLICANDO AS POLÍTICAS DE SEGURANÇA NO COMBATE AO *RANSOMWARE*

## 4.1 A evolução do *Ransomware*

Historicamente, os primeiros casos conhecidos de infecção por *ransomware* ocorreram entre 2005 e 2006 na Rússia. Em 2006 a Trend Micro relatou um incidente involvendo um tipo de *ransomware,* que compactava alguns tipos de arquivos e os sobreescrevia com o arquivo compactado com senha. Um arquivo texto também era criado informando o usuário que os arquivos poderiam ser revistos sob o pagamento de U$300 (*Ransomware*! *Ransomware*! *Ransomware*!, 2006).

Embora inicialmente limitado à região da Rússia, a popularidade e o modelo de negócio rentável do *ransomware* o tornou popular, e em meados de Março de 2012 a Trend Micro observou uma contínua propagação de infecções por *ransomwares* pela Europa e América do Norte (*Ransomware* Attacks Continue to Spread Across Europe, 2012).

Em 2013, um novo tipo de *ransomware* surgiu encriptando arquivos, além do bloqueio do sistema da vítima. Os arquivos criptografados asseguravam que as vítimas seriam forçadas a realizar o pagamento do resgate mesmo após a deleção do *malware*. Devido a essas caraterísticas, esse tipo de *malware* passou a ser chamado de "CryptoLocker". Ainda em 2013 os *crypto-ransomwares* conhecidos como CryptoDefense ou Cryptorbit entram em cena realizando a encriptação de bancos de dados, arquivos web, office, vídeos, imagens, scripts, textos e outros arquivos do tipo não binário, com posterior deleção dos backups existentes.

## 4.2 Os métodos de infecção e distribuição

Os métodos de infecção por ramsonware são diversos e vem se aprimorando com o tempo. Em um caso de 2012 (Compromised Website for Luxury Cakes and Pastries Spreads *Ransomware,* 2012), um site de bolos e biscoitos de luxo da França foi comprometido, se tornando o canal de proliferação do *ransomware* TROJ_RANSOM.BOV, que simulava uma notificação da polícia francesa direcionada ao usuário.

Para a distribuição do CryptoLocker, em 2013, notou-se a utilização de uma campanha massiva de mensagens do tipo spam, os emails enviados continham os arquivos maliciosos que direcionavam a um site para o download de um outro arquivo malicioso, esse fluxo foi detectado pela Trend Micro (CryptoLocker: Its Spam and ZeuS/ZBOT Connection, 2013) e pode ser visualizado abaixo.

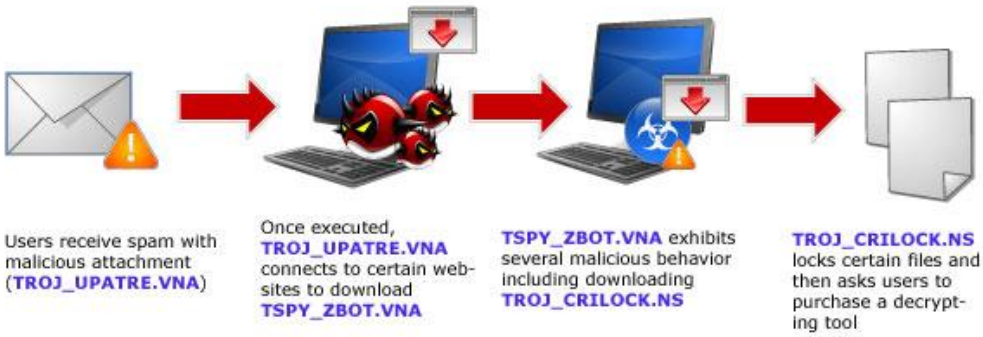


Figura 2 - Cadeia de infecção do CryptoLocker

Ao fim de 2013, uma nova variante do CryptoLocker – WORM_CRILOCK.A – emerge com a característica de se espalhar através de dispositivos removíveis, e essa característica foi notável para a dispersão desse tipo de *malware*.

Em 2015, o kit de exploração Angler se destacou como um dos kits de exploração mais utilizados para disseminar *ransomwares*, o kit foi amplamente utilizado em ataques de *malvertising*. Já em Fevereiro de 2016, o *ransomware* RANSOM_LOCKY.A foi identificado e este *malware* se destacou pelo método de distribuição, inicialmente se apresentando através de macros em um documento Word, posteriormente se alastrando através de pontos de exploração identificados no Adobe Flash e no Kernel do Windows (Locky *Ransomware* Spreads via Flash and Windows Kernel Exploits, 2016). No mês seguinte, a ameaça RANSOM_PETYA.D se apresentava através de serviços de armazenamento como o Dropbox.

## 4.3 A adoção de políticas de Segurança da Informação

Não é possível determinar somente uma solução que acabe com os riscos ligados a ataques de *ransomware*, não existe uma ‘bala de prata’ que elimine essa ameaça.

A abordagem mais eficaz no combate ao *ransomware*, assim como qualquer software malicioso, é a implementação de camadas de segurança que atrapalham a exploração de diferentes vulnerabilidades que cada organização, independentemente da linha de negócio ou porte, possa ter. Exemplos de tais camadas incluem:

- Conscientização de segurança;
- Monitoramento e gerenciamento de eventos de segurança;
- Proteção de e-mail, acesso à internet e rede corporativa;

- Cópias de segurança de dados relevantes;
- Software e hardware atualizados; e
- Políticas de segurança informação definidas.

A implementação da ISO 27001 provê um conjunto de controles que visa a cobertura de todas essas camadas.

No Anexo A da ISO 27001 estão descritos controles e seus respectivos objetivos que são comumente selecionados como resultado da avaliação de riscos, permitindo o tratamento para mitigar o risco. A avaliação de riscos (muitas vezes chamada de análise de riscos) é provavelmente a parte mais complicada da implementação da ISO 27001; entretanto é a etapa mais importante no início do projeto de segurança da informação – ela define os fundamentos para a segurança da informação em sua organização.

No caso de nosso estudo, os riscos identificados estão alinhados aos incidentes de *ransomware* conhecidos até a data desta publicação, conforme alguns exemplos já descritos.

Os controles contidos na ISO 27001 que ajudam na proteção contra o *ransomware* são:

Controle A.6.2.1 (Política para o uso de dispositivo móvel) – Como mencionado neste documento, durante a evolução do *ransomware*, a estratégia do uso de dispositivos móveis para a distribuição desse dos *malware*s foi adotada a partir de 2013, mediante esta ameaça, os usuários precisam ter pleno conhecimento de que não devem conectar em seus equipamentos dispositivos móveis de origem desconhecida. Essa recomendação, dentre outras, se faz necessária em uma política que apoia a segurança da informação no gerenciamento dos riscos decorrentes do uso dos dispositivos móveis.

Controle A.7.2.2 (conscientização, educação e treinamento em segurança da informação) – Este controle assegura que "todos os empregados recebam conscientização, educação e treinamento adequado e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções". Sem o treinamento apropriado, não existe tecnologia resistente o suficiente às ameaças de *ransomware*. Um dos mais comuns métodos de distribuição do *ransomware*, e de softwares maliciosos em geral, é através de emails maliciosos. Em seu relatório de análise dos incidentes de vazamento de informações de 2015, a empresa Verizon identificou um crescimento, frente a 2014, de 7% dos casos onde os usuários abriram mensagens do tipo *phishing* e 1% de aumento dos usuários que clicaram no

anexo ou link contido na mensagem (Verizon's 2016 Data Breach Investigations Report, 2016). A gravidade dessa ação dos usuários é ainda mais representativa quando nota-se, no mesmo relatório, que a empresa identificou que 9576 incidentes ocorreram por esse método. Além do *phishing*, a exploração pode ser causada por ações de engenharia social e download de websites comprometidos. Empregados precisam se preparar para estarem atentos a estes ataques.

Controle A.12.3.1 (Cópia de segurança de informações) – Como descrito nos objetivos deste controle, "Cópias de segurança …devem ser realizadas e testadas regularmente". Após a conscientização dos usuários, esse talvez seja um dos controles mais eficientes contra o *ransomware*. Entretanto, esse software malicioso muitas vezes tem a habilidade de se espalhar por diretórios de rede e cópias de segurança, visando a destruição das informações de backup. Logo, a validação destas cópias e a manutenção das cópias em dispositivo segregado e fora da rede é essencial para assegurar o sucesso da restauração quando necessário.

Controle A.12.4.1 (Registro de eventos) – O *ransomware* é um tipo de software malicioso sofisticado. A análise do comportamento do sistema pode ser crucial para a detecção do incidente em tempo hábil. Este controle sugere não apenas a criação de logs de evento, mas também revisões regulares.

Controle A.12.6.1 (Gestão de vulnerabilidade técnicas) – O conhecimento de vulnerabilidades do sistema é essencial para se proteger contra este ou qualquer tipo de ameaça.

Controle A.12.6.2 (Restrições quanto à instalação de software) – Em conjunto com a gestão de vulnerabilidade técnicas, deve-se implementar regras definindo critérios para a instalação de software pelos usuários, visto que estes são uma porta de entrada significante dos *malware*s, conforme já citado no controle A.7.2.2.

Controle A.13.1.3 (Segregação de redes) – A rápida proliferação da criptografia de arquivos na rede causada pelo *ransomware* pode ser contida se a rede for organizada por segmentos. Além de que, com menos tráfego de sinalização passando por todos os segmentos de rede, é mais difícil para um atacante mapear a estrutura da rede, falhas em um segmento são menos prováveis de se propagar, e um melhor controle de acesso pode ser estabelecido considerando o acesso de visitantes ou acesso a informações e ativos sensíveis.

Controle A.12.2.1 (Controles contra softwares maliciosos) – Adicionalmente aos controles acima recomendados, os softwares anti*malware* estão melhorando no

reconhecimento e combate a ataques de *ransomware*, logo é importante manter soluções adequadas de proxy, firewall, dentre outras.

# 7. CONSIDERAÇÕES FINAIS

A evolução do *ransomware* é vista pelos especialistas como uma das maiores ameaças, e mais eficaz ataque em nossos sistemas, em todos os tempos. O combate é sem fim, e é por isso que se faz necessária a prevenção, com a implementação de estrutura de segurança da informação, e melhoria contínua dos controles.

O objetivo específico deste trabalho foi a seleção de controles da ISO 27001: 2013 baseada em análise de riscos apresentados pelo *ransomware*, de forma a proteger a confidencialidade, integridade e disponibilidade das informações. A ISO 27001 não foca apenas em controles de TI, mas também em controles para assegurar a conscientização de todos os empregados, técnicos ou outros, sobre softwares maliciosos.

Aqui indicamos 8 dentre 114 possíveis controles, e adequadamente alinhada com as ameaças, a ISO 27001 se mostra como a ferramenta ideal para proteção contra *ransomware* ou qualquer outro tipo de software malicioso.

# REFERÊNCIAS

FONTES, Edison Luiz G. **Políticas e Normas Para A Segurança Da Informação.** Rio de Janeiro: Editora Brasport, 2011.

InfoSecurity Magazine. ***Ransomware* Spikes 14% in Q1.** Disponível em: < http://www.infosecurity-magazine.com/news/*ransomware*-spikes-14-in-q1/>. Acesso em: 18 de Setembro de 2016, 22:00.

PwC US. **The Global State of Information Security® Survey 2015.** Disponível em: < http://www.pwc.com/us/en/press-releases/2014/global-state-of-information-security-survey-2015.html>. Acesso em: 07 de Setembro de 2016, 22:20.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva.** 1.ed. Rio de Janeiro: Campus, 2003.

SILVEIRA, Denise Tolfo. CÓRDOVA, Fernanda Peixoto. **A pesquisa científica**. In Métodos de pesquisa / [organizado por] Tatiana Engel Gerhardt e Denise Tolfo Silveira – UAB/UFRGS, SEAD/UFRGS. – Porto Alegre: Editora da UFRGS, 2009.

SYMANTEC. **A New Zero-Day Vulnerability Discovered Every Week in 2015**. Disponível em: <https://www.symantec.com/content/dam/symantec/docs/infographics/istr-zero-day-en.pdf>. Acesso em: 21 de agosto de 2016, 16:30.

SYMANTEC. **Attackers Target Both Large and Small Businesses.** Disponível em: < https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf>. Acesso em: 28 de Agosto de 2016, 22:30.

Trend Micro Blog. ***Ransomware*! *Ransomware*! *Ransomware*!.** Disponível em: < http://blog.trendmicro.com/trendlabs-security-intelligence/*ransomware*21-*ransomware*21-*ransomware*21/>. Acesso em: 14 de Novembro de 2016, 08:00.

Trend Micro. **Part 1: Combatting the *Ransomware* Epidemic Requires Layered Security.** Disponível em: < http://blog.trendmicro.com/combatting-the-*ransomware*-epidemic-requires-layered-security/>. Acesso em: 08 de Setembro de 2016, 08:00.

Trend Micro Blog. ***Ransomware* Attacks Continue to Spread Across Europe.** Disponível em: < http://blog.trendmicro.com/trendlabs-security-intelligence/*ransomware*-attacks-continue-to-spread-across-europe/>. Acesso em: 15 de Novembro de 2016, 12:08.

Trend Micro Blog. **Compromised Website for Luxury Cakes and Pastries Spreads *Ransomware*.** Disponível em: < http://blog.trendmicro.com/trendlabs-security-intelligence/compromised-website-for-luxury-cakes-and-pastries-spreads-*ransomware*/>. Acesso em: 17 de Novembro de 2016, 23:18.

Trend Micro Blog. **CryptoLocker: Its Spam and ZeuS/ZBOT Connection.** Disponível em: < http://blog.trendmicro.com/trendlabs-security-intelligence/cryptolocker-its-spam-and-zeuszbot-connection/>. Acesso em: 17 de Novembro de 2016, 23:45.

Trend Micro Blog. **Locky *Ransomware* Spreads via Flash and Windows Kernel Exploits.** Disponível em: < http://blog.trendmicro.com/trendlabs-security-intelligence/locky-*ransomware*-spreads-flash-windows-kernel-exploits/>. Acesso em: 28 de Novembro de 2016, 22:24.

Verizon's website. **Verizon's 2016 Data Breach Investigations Report.** Disponível em: < http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf>. Acesso em: 29 de Novembro de 2016, 22:24.

# ANEXOS

## ANEXO A – GLOSSÁRIO

**C**

**Criptografia**: conjunto de princípios e técnicas empregado para codificar a escrita, torná-la ininteligível para os que não tenham acesso às chaves de segurança.

**D**

Incidente ou falha de segurança **‘DIA-ZERO’**: Uma falha que ficou sendo conhecida publicamente antes mesmo que o desenvolvedor do software (ou hardware) lançasse uma atualização para corrigi-la, sendo a partir daí explorada por criminosos.

**M**

**Malvertising**: é um tipo de anúncio publicitário online que geralmente é usado para espalhar *malwares* na internet.

***Malware***: Termo do inglês para Software malicioso, um software destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não).

**P**

**Phishing**: termo oriundo do inglês (fishing) que quer dizer pesca, é uma forma de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais de diversos tipos.