RISCOS, AMEAÇAS E VULNERABILIDADES: O IMPACTO DA SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

Eduardo Esteves dos Santos[1]
Tamires Mariana Mayumi Kurosaki Soares[2]

Resumo
Este artigo apresenta a importância da segurança da informação para as organizações, conceitos fundamentais de segurança, noções de risco, ameaça, vulnerabilidade, e o impacto de ataques que exploram tais falhas, que causam prejuízos milionários para as empresas de quaisquer segmentos. E também quais passos são essenciais para a elaboração de uma política de segurança alinhada ao negócio e as boas práticas do mercado, com o intuito de minimizar as vulnerabilidades e mitigar os danos causados por eventuais ataques ao ambiente corporativo.
Palavras-chaves: Segurança da Informação. Organizações. Vulnerabilidade.

Abstract.
This article presents the importance of information security for organizations, fundamental concepts of security, notions of risk, threat, vulnerability, and the impact of attacks that exploit those flaws in which millionaire losses are involved for the target company. And also, what steps are fundamental to the development of a security policy aligned to the business and good practices in the market, in order to minimize vulnerabilities and mitigate the damage caused by attacks in the corporate environment.
Keywords*: Information security. Organizations. Vulnerability.*

Introdução

Com a expansão das redes e da *internet* no meio corporativo nos últimos anos, a informação, que outrora navegava por papéis e serviços de postagens, passou a ser transmitida por meio digital, agilizando processos e estreitando laços entre as empresas, clientes e fornecedores. Com todas as vantagens inimagináveis que a tecnologia e sistemas da informação trouxeram para as organizações, vieram novas e devastadoras ameaçase poderiam levar uma empresa à falência (REUTERS, 2017). Há diversos relatos e reportagens de empresas que tiveram seus dados sequestrados por *hackers* através do método de ataque *Ransomware* (G1, 2017), ou seja, um sequestro de dados em que o pagamento ocorre normalmente através de moedas digitais. Essa é apenas uma das ameaças que cercam o meio corporativo, pois há ataques por vírus, DDoS (*Distributed Denial of Service*), invasão, engenharia social, roubo de senha entre outros métodos e ferramentas que visam explorar seus alvos, pois "todo funcionário da empresa que utilize um computador, um dispositivo de rede, um *tablet* ou um telefone é um alvo em potencial" (LISKA e GALLO, 2017, p. 111).

Pensando nesse cenário hostil, este artigo tem como objetivo levantar questionamentos sobre a importância da segurança da informação no ambiente corporativo e os desafios da implementação de uma política de segurança da informação alinhada ao negócio.

1 Segurança da Informação

[1] Fatec Americana. E-mail: edu.santos89@gmail.com
[2] Idem. E-mail: mayumi.kurosaki@gmail.com

Afinal, por que segurança da informação é tão importante para as empresas? Para responder essa pergunta é necessário entender o conceito e no que é baseado o termo Segurança da Informação.

Segurança da Informação (SI) é definida como "conjunto de orientações, normas, procedimentos, políticas e demais ações que têm por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada" (FONTES, 2006, p. 11). Deste modo, pode ser considerada uma ferramenta criada com o intuito de se locomover junto ao negócio, presente em todo o escopo da organização, protegendo o bem mais valioso para a empresa, a informação.

Para que este bem seja devidamente protegido, é fundamental conhecer os pilares que sustentam a SI: confidencialidade, integridade e disponibilidade (FONTES, 2006):

a) confidencialidade: garantir que somente pessoas autorizadas dentro da empresa tenham acesso à informação.

b) integridade: garantir que a informação se mantenha íntegra, ou seja, que não tenha sido alterada em nenhum estágio, propositalmente ou não.

c) disponibilidade: garantir que a informação esteja disponível no momento em que precise a empresa precise para as atividades de seus colaboradores.

É necessário classificar as informações para que se tenha uma visão ampla do que precisa ser protegido, pois cada informação tem um valor diferente. É necessário analisar e identificar as informações para que se possam classificá-las em níveis. Tais níveis também podem ser utilizados por toda a organização, a fim de padronizá-las (redação). Essa classificação pode ser baseada na utilidade que essa informação tem dentro da empresa, o custo que possui para o negócio, o impacto em sua operacionalização e os riscos envolvidos em caso de vazamento. Com isso, recursos podem ser economizados para assegurar informações sensíveis, evitando gastos desnecessários com informações públicas (KIM e SOLOMON, 2014).

Para Ferreira e Araújo (2008) as informações podem ser classificadas em três classes: informações públicas, internas e confidenciais.

a) informações públicas são aquelas de conhecimento de todos os funcionários. não é preciso investir em recursos de segurança, pois caso a informações sejam vazadas, não causam impacto ao negócio e nem a organização.

b) informações internas são as de uso interno, e sua divulgação deve ser evitada. Entretanto, se forem vazadas, causam pouco impacto ao negócio.

c) informações confidenciais são as sensíveis, que tem grande valor para a organização. Devem ser restritas para pessoas autorizadas, deve se investir em recursos de segurança, pois se vazadas podem causar grande impacto ao negócio.

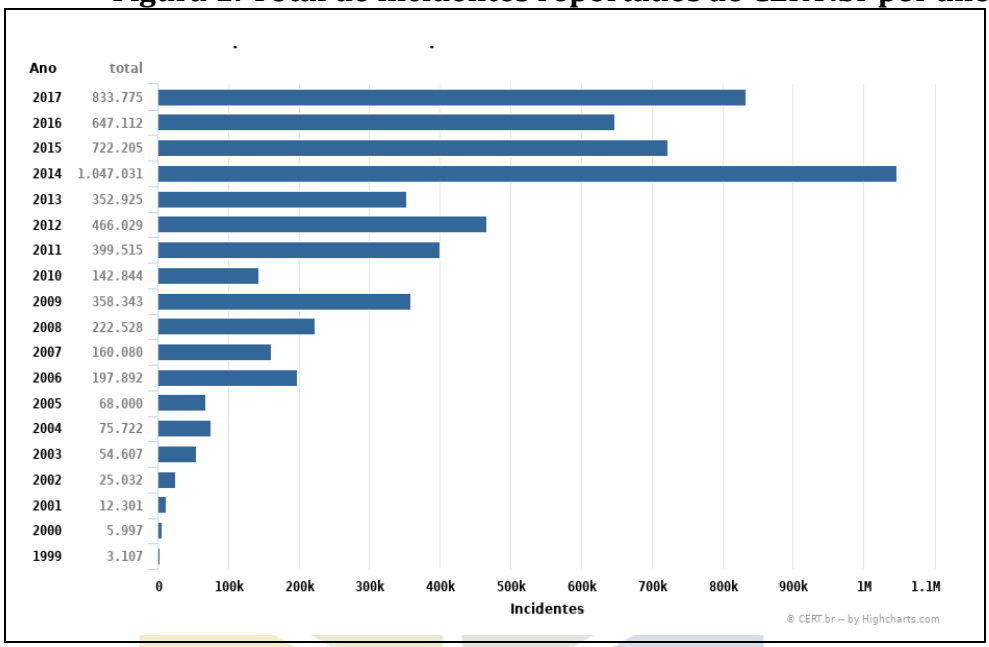
Com as definições apresentadas, pode concluir-se que toda a informação interna ou confidencial deve manter-se segura, ou seja, que elas sejam acessadas somente por pessoas devidamente autorizadas, quando eles precisarem, e, principalmente, que não tenham sido alteradas, pois uma informação alterada poderá causar prejuízos financeiros e jurídicos para as empresas (KIM e SOLOMON, 2014).

2 Riscos nas Organizações

A preocupação crescente quanto à segurança da informação não pode ser vista apenas como um alarde desnecessário que gera gastos à organização. Os crimes contra empresas e indivíduos aumentaram exponencialmente nos últimos anos. De acordo com a análise de incidentes reportados ao CERT.br (CERT.br, 2018), houve, no ano de 2017, 833.755 notificações de incidentes recebidas pela empresa. Este número representa, somente no Brasil,

um aumento de 29% em relação ao ano anterior. Tais ataques variam entre negação de serviço, fraudes, varreduras, *phishings* e ataques aos servidores *web*.

Figura 1: Total de incidentes reportados ao CERT.br por ano



Fonte: CERT.br (2018)

O gráfico apresentado na Figura 1 mostra o crescimento de incidentes com o passar dos anos. Seu crescimento está relacionado com a evolução da tecnologia e sua importância para as organizações. Realizar ataques virtuais tornou-se um viés lucrativo no meio digital, seja para extorquir dinheiro ou roubar informações sigilosas. Outro dado preocupante, que fomenta o número de ataques, é que segundo o estudo "*Norton Cyber Security Insights Report*" da Symantec em 2017 houve um prejuízo de 22,5 bilhões de dólares no Brasil causado por crimes virtuais, deixando o país atrás apenas da China, que teve um prejuízo de 66,3 bilhões de dólares. Tais números acabam despertando interesse para que mais pessoas cometam crimes virtuais, devido à crescente facilidade em realizar ataques, com ferramentas prontas que exigem pouco conhecimento do atacante, e em alguns casos, o pagamento é feito em moedas virtuais como a *bitcoin* que valoriza a cada dia e dificilmente é rastreável.

A hostilidade deste ambiente conectado e o grande impacto causado pelos atacantes despertou uma nova preocupação para as empresas, pois os riscos e prejuízos são reais e todos estão sujeitos aos ataques. Considerando que "O risco é apenas uma forma de representar a probabilidade de algo acontecer. Trata-se de uma possibilidade. Portanto, pode ou não ocorrer" (DAWEL, 2005, p. 41). Cresce então a demanda das empresas a pensarem em sua segurança digital, criar barreiras com intuito de mitigar os riscos à empresa.

2.1 Ameaças e Vulnerabilidades

Pela definição de Peltier (2010), ameaça é um evento indesejável que pode danificar um ativo, causando impacto nos resultados do negócio. Ele classifica as ameaças em três grupos básicos com base na natureza do agente causador: Ameaças Naturais, que incluem eventos da natureza como enchentes, terremotos e tempestades elétricas; Ameaças Humanas, as quais englobam eventos que sejam causados ou facilitados por um agente humano, de forma

voluntária ou não, tais quais *malwares*, eventos de fraude, e outros erros comuns na área de Tecnologia; e por fim, as Ameaças Ambientais, ação do tempo, poluição e umidade.

Para melhor classificação das ameaças, é possível fazer uma análise individual de cada uma, identificando alguns itens chave, que são: agente ou fonte, que poderá realizar a ação da ameaça; motivação, que procura identificar o que pode levar o agente a realizar tal ação, e por fim, o resultado da ação.

O levantamento de uma lista de ameaças correspondente à cada ativo do processo organizacional é fundamental para a definição de Vulnerabilidades, e, consequentemente, para análise de risco.

Existem diversas formas para realizar este levantamento. Peltier (2010) cita a criação de *checklists*, a análise de histórico de eventos, e por fim, o *brainstorm* com agentes chave dos processos organizacionais para o levantamento da relação de ameaças dos ativos envolvidos em cada etapa dos processos principais da organização.

Vulnerabilidade é uma falha ou fraqueza de um bem, ativo ou processo, que, caso seja explorada por uma ameaça, irá causar algum impacto na organização, podendo ser considerada como a suscetibilidade do sistema ou ativo em relação à determinada ameaça.

Risco pode ser definido como a possibilidade de que uma determinada vulnerabilidade identificada nos processos anteriores tem de ser explorada por uma ameaça. Para o tratamento do risco, é necessário que sejam seguidos alguns passos, sendo eles:

a) análise de risco: subdividida em identificação de riscos, estimativa de riscos e avaliação de riscos.

b) identificação de risco: após a identificação dos ativos que compõe os processos organizacionais, é feita identificação de ameaças e vulnerabilidades relacionadas a estes ativos. com as ameaças e vulnerabilidades identificadas, o próximo passo é a probabilidade de ocorrência de cada ameaça x vulnerabilidade, na qual podem ser utilizados dados de incidentes anteriores. feito isto, a próxima etapa é a análise de impacto, na qual é identificada e classificada, quais as consequências da exploração de determinada vulnerabilidade para a organização.

c) tratamento do risco: com a definição destes dois últimos itens, é possível elaborar a matriz de risco, que serve para identificar a criticidade de um risco, levando em consideração o impacto e a probabilidade de ocorrência do risco, conforme figura 2, que é crucial para a criação e definição dos itens de controle, que visam evitar, tratar ou mitigar os riscos identificados, na forma de políticas de segurança.

Figura 2: Matriz de risco

PROBABILIDADE		IMPACTO		
		BAIXO	MÉDIO	ALTO
		1	2	3
ALTO	3	3	6	9
MÉDIO	2	2	4	6
BAIXO	1	1	2	3

PRIORIZAÇÃO
Muito Alto
Alto
Normal
Baixo
Muito Baixo

Fonte: Adaptado de Peltier (2010)

d) aceitação do risco: para os itens que não serão tratados por meio de políticas de segurança, é necessário fazer o registo de aceitação do risco, bem como a responsabilidade e justificativa da decisão.

2.2 Impacto

Após a identificação das ameaças e vulnerabilidades, é necessário analisar o impacto que cada vulnerabilidade terá, caso seja explorada por uma ameaça. Os principais resultados podem ser classificados da seguinte forma, podendo conter mais que uma consequência no mesmo incidente.

Integridade do sistema e dados refere-se ao requisito de que as informações devem ser protegidas contra modificação imprópria. A integridade é perdida se alterações não autorizadas são feitas nos dados ou no sistema de TI, de maneira intencionais ou acidentais. E se a perda de integridade do sistema ou dos dados não é remediada, o uso do sistema ou dados corrompidos pode resultar em imprecisão, fraude ou decisões erradas. Além disso, a violação da integridade pode resultar em um ataque bem-sucedido contra a disponibilidade ou confidencialidade do sistema. Por todas estas razões, a perda de integridade reduz a garantia de um sistema de TI.

Se um sistema de TI de missão crítica não estiver disponível para seus usuários finais, a missão da organização pode ser afetada. Perda de funcionalidade do sistema e a eficácia operacional, por exemplo, pode resultar em perda de tempo produtivo, impedindo o desempenho dos usuários finais de suas funções na entrega de serviço proposto pela organização.

A confidencialidade de sistemas e dados refere-se à proteção de informações de divulgação não autorizada. O impacto da divulgação não autorizada de informações confidenciais pode incluir desde o comprometimento da segurança nacional até a divulgação de dados da Lei de Privacidade (lei nº 13.709, de 14 de agosto de 2018). O vazamento de dados pode resultar em danos irreparáveis à imagem e credibilidade da empresa no mercado, multas, ou mesmo uma ação legal contra a organização. É crucial que este item seja identificado o mais rápido possível, para que as ações necessárias para remediação sejam tomadas.

Segundo a revista *Security Report,* em 2017, o mundo presenciou um ataque de *Ransomware* que atingiu mais de 150 países, que ficou conhecido como *WannaCry,* o qual exigia o pagamento de U$300,00 em *bitcoins* para recuperar os dados criptografados, conforme mostra a Figura 3. Esses ataques explodiram na mídia convencional (R7, 2017), levando a informação a todas as pessoas do real risco envolvido no meio digital, ligando um alerta de que qualquer pessoa ou empresa poderá ser afetada. Surgiu então uma nova mentalidade dentro das empresas que buscaram alternativas e recursos para a implementação de uma segurança dentro de suas estruturas, não somente a segurança física, mas também a segurança de seus dados digitais. De acordo com a Gartner (2017), espera-se que as empresas invistam em 2018 cerca de 93 bilhões de dólares em segurança, e esse número tende a aumentar nos próximos anos.

Figura 3: WannaCry

Fonte: Tecmundo (2017)

De acordo com Manky (2018), todos os tipos ataques de *Ransonware* seguem uma ideia comum em que os atacantes geralmente procuram explorar sistemas com vulnerabilidades conhecidas, mas que por algum motivo não foram remediadas, e ainda completa frisando a importância que a empresa tem que ter um olhar para dentro de sua estrutura e focar em métodos básicos em segurança para mitigar o número de vulnerabilidades em seu parque tecnológico. E isso leva as empresas definirem uma boa política de segurança.

3 Políticas de segurança da informação

As políticas de segurança da informação são as normas que regem o ambiente da empresa, e como devem ser vistas cada atividade exercida de modo seguro. De acordo com Ferreira e Araújo (2008), para a elaboração de uma política de segurança da informação é necessário seguir quatro etapas fundamentais:

a) levantamento de informações da empresa: quais as normas de segurança já existentes. Como funciona o processo de negócio e como funciona o fluxo da informação dentro da organização.

b) desenvolvimento do conteúdo da política e normas de segurança: definição do gerenciamento da política de segurança, esclarecendo os objetivos e pontos críticos. Atribuindo as responsabilidades, com base no pensamento de que a segurança faz parte de todos os profissionais. Definição dos procedimentos de segurança, como será executada cada processo.

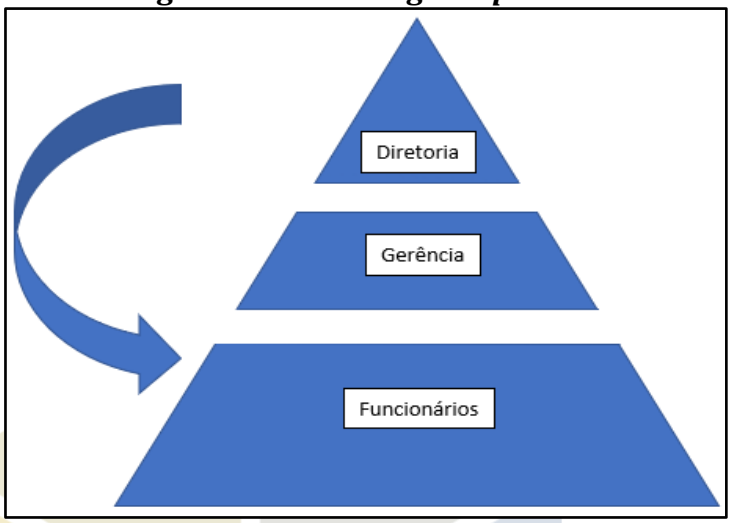
c) elaboração dos procedimentos de segurança da informação: esta etapa visa a formalização da política junto a alta administração, utilizando de técnicas e procedimentos de melhores práticas alinhadas de modo que a segurança não atrapalhe ou crie obstáculos para o negócio.

d) revisão, aprovação e implementação das políticas de segurança da informação e palestras: toda política deve ser revisada periodicamente, pois os processos e tecnologias sofrem mudanças com o tempo. E é de suma importância que todos os profissionais tenham ciência

sobre a existência de uma política de segurança, seja através de palestras, comunicados e integração. E que essas políticas estejam sempre disponíveis para quem quiser consultá-las.

Utilizando a metodologia *Top-Down*, conforme Figura 4, a divulgação da política deve ser atestada pela diretoria da empresa, pois demonstra o comprometimento da política para com seus funcionários.

Figura 4: Metodologia *Top-Down*



Fonte: Adaptado de Ferreira e Araújo (2008).

Para a criação de uma política de segurança mais customizada, é necessário entender quais são os riscos e as ameaças às quais os ativos da empresa estão sujeitos, avaliando suas vulnerabilidades, probabilidades e os impactos que serão causados em meio ao incidente.

3.1 Responsabilidades

O processo de segurança não depende exclusivamente do time de segurança da informação, mas sim de todos os membros da organização que devem estar em sintonia com os processos estabelecidos. A política é composta apenas por regras, mas é fundamental a conscientização de todos os funcionários para que os processos sejam cumpridos.

Ferreira e Araújo (2008) destacam alguns pontos relacionados à atribuição das responsabilidades que todas as áreas da empresa precisam estar cientes, sendo elas:

a) comitê de segurança da informação: equipe responsável por criar procedimentos e realizar a divulgação para os membros da empresa. É recomendável que líderes de outras áreas façam parte desta equipe, pois os valores das informações variam de área para área.

b) proprietário das informações: cabe ao proprietário da informação realizar a liberação do tipo de acesso que cada funcionário poderá ter, sendo necessária uma autorização direta ou designada.

c) usuários da informação: é qualquer funcionário, ou terceiro, que utiliza a informação para a execução de suas atividades, mas que só poderá ser utilizada para o desenvolvimento do negócio.

3.2 Procedimentos de segurança

Após a análise do ambiente, designação das responsabilidades e classificação das informações por níveis, é preciso formalizar a documentação e definir como cada ativo a ser

protegido será realizado. Os procedimentos visam detalhamento de cada processo dos ativos. A seguir alguns exemplos são sugeridos por Ferreira e Araújo (2008):
a) recursos de ti: todo recurso tecnológico da empresa deve ser utilizado apenas por funcionários e terceiros devidamente autorizados, com a finalidade de exercer atividades relacionadas ao negócio.
b) backup: deve existir uma política exclusiva de *backup*, apresentando a periodicidade em que serão efetuados os *backups* e o tempo de retenção alinhado com os responsáveis de cada área da empresa.
c) acesso à *internet*: a maior porta de entrada de arquivos maliciosos tem como origem o acesso irrestrito à *internet*. Deve-se limitar o acesso à *internet* para pessoas autorizadas, sendo monitorado o *login* do usuário, sites acessados e suas respectivas horas.
d) segurança física: em algumas empresas pode ser que os equipamentos de tecnologia estejam em um data-center interno. O acesso para esse espaço deve ser sempre monitorado e permitido somente para pessoas autorizadas, pois há um grande risco ao negócio se houver algum problema nos equipamentos existentes.

4 Conclusão

A política de Segurança da Informação serve como uma barreira, visando a mitigação de riscos para a organização, que também deve estar alinhada com os objetivos que a empresa almeja alcançar e a outros planos já existentes. É fundamental que a política não trave o desempenho das funções, sendo necessária a análise de como deve ser feita a proteção dos dados, e, se necessário, aceitar alguns riscos envolvidos.

De nada adianta a implementação de uma política quando não há a conscientização de que todos os membros da empresa são responsáveis pelas informações que são geradas devidas as suas atividades. Para isso, cabe aos membros do comitê de segurança que realizem palestras, informativos e programas de integração que foquem na importância de manter as informações seguras.

Pequenos atos e a mudança da cultura das pessoas e da própria empresa surtem mais efeitos que realizar um investimento em tecnologia cara, pois basta um clique errado ou mal-intencionado para que a ameaça se instale dentro da organização. A segurança deve tornar-se um hábito na empresa, trabalhada de forma individual em cada membro da organização, de forma que a preocupação com a segurança da informação esteja presente em cada etapa dos processos do negócio (DAWEL, 2005).

Referências

CERT.BR. Disponível: <https://www.cert.br/stats/incidentes/2017-jan-dec/analise.html>. Acesso: 12 maio 2018.

DAWEL, G. **A segurança da informação nas empresas.** 1. ed. Rio de Janeiro: Editora Ciência Moderna, 2005. 110 p. v. 1.

FERREIRA, F. N. F e ARAÚJO, M. T. **Política de segurança da informação: Guia prático para elaboração e implementação**. 2. ed. Rio de Janeiro: Editora Ciência Moderna, 2008. 260 p. v. 1.

FOLHA DE SÃO PAULO. Disponível: <http://www1.folha.uol.com.br/mundo/2017/06/1896398-novo-ciberataque-afeta-empresas-de-diversos-paises.shtml>. Acesso: 6 out. 2018.

FONTES, E. **Segurança da informação: O usuário faz a diferença.** 1. ed. São Paulo: Editora Saraiva, 2006. 172 p. v. 1.

FORTNET. Disponível: <https://www.fortinet.com/blog/industry-trends/ten-best-practices-for-outsmarting-ransomware.html>. Acesso: 7 out. 2018.

G1. Disponível: <http://g1.globo.com/jornal-nacional/noticia/2017/05/ciberataques-em-escala-mundial-atingem-empresas-e-afetam-o-brasil.html>. Acesso: 6 out. 2018.

GARTNER, D. Disponível: <https://www.gartner.com/newsroom/id/3784965>. Acesso: 14 maio 2018.

HUNTER, R. e WESTERMAN, G. **O risco de TI.** São Paulo: Makron Books, 2008.

KIM, D. e SOLOMON, M. G. **Fundamentos de segurança de sistemas da informação.** 1. ed. São Paulo: Grupo Editorial Nacional, 2014. 410 p. v. 1.

LISKA, Ae GALLO, T**.** ***Ransomware*****: Defendendo-se da extorsão digital.** 1. ed. São Paulo: Novatec, 2017. 224 p. v. 1.

PELTIER, T. R**.** ***Information security risk analysis***, 3.ed. *Auerbach Publication*, 2010. 331 p. v. 1

R7. Disponível: <https://noticias.r7.com/tecnologia-e-ciencia/risco-cibernetico-ataques-hackers-deixam-empresa-em-alerta-no-mundo-todo-29062017>. Acesso: 6 out. 2018.

REUTERS. Disponível: <https://www.reuters.com/article/us-bitcoin-exchange-southkorea/south-korean-cryptocurrency-exchange-to-file-for-bankruptcy-after-hacking-idUSKBN1ED0NJ>. Acesso: 15 ago. 2018.

SANTANDER. Disponível: <https://www.santander.com.br/document/wps/politica_seguranca_informacao_fev_13.pdf>. Acesso: 14 maio 2018.

SECURITY REPORT. Disponível: <http://www.securityreport.com.br/overview/mercado/solucoes-para-o-wannacry-uma-segunda-onda-de-ataques/#.W61vzmhKjIU>. Acesso: 6 out. 2018.

STONEBURNER G, GOGUEN A, FERINGA A (2001) ***Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology.*** *Special Publication*, 800(30)

SYMANTEC. Disponível: <https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf>. Acesso: 14 maio 2018.

TECMUNDO. Disponível: <https://www.tecmundo.com.br/malware/116652-wannacry-ransomware-o-mundo-chorar-sexta-feira-12.htm> Acesso: 7 out. 2018.

TECNOBLOG. Disponível: <https://tecnoblog.net/217587/ataque-ransomware-petya>. Acesso: 15 maio 2018.