EMPRAD ENCONTRO DOS PROGRAMAS DE PÓS-GRADUAÇÃO PROFISSIONAIS EM ADMINISTRAÇÃO

ADAPTANDO O MODELO PREPARE PARA GESTÃO DE RISCOS EM CRISES DE TECNOLOGIA

Ruddy Vasquez - Pontifícia Universidade Católica de São Paulo - PUC SP

Lucas Carrazzoni Mirabella - USP - Universidade de São Paulo

Jefferson Luiz Bution - Faculdade de Economia, Administração e Contabilidade - USP

Andrei Carlos Torresani Paza - Faculdade de Economia, Administração e Contabilidade - USP

Lucas Israel Oliveira Testi - Faculdade de Economia, Administração e Contabilidade - USP

Fábio Lotti Oliva

Resumo

O volume de tráfego e dependência de dados faz com que os riscos na área de tecnologia sejam notavelmente crescentes. Em 2017, o ataque cibernético do ransomware Wannacry, que atingiu milhares de organizações em escala mundial, revelou como a gestão de riscos e a gestão de crises podem estar relacionadas. Esta pesquisa tem o objetivo de adaptar um modelo de solução sistêmica para eventos de crise voltados à tecnologia e analisá-lo a luz da estratégia de gestão de riscos. Para isso, estuda o caso de um grande banco privado brasileiro durante o ataque do Wannacry e a aplicabilidade de uma adaptação do modelo PREPARE. Os resultados revelaram a aplicabilidade do modelo e as ações necessárias para que a organização antecipasse possíveis impactos de ataque e ações mitigatórias relacionadas. As constatações das entrevistas trouxeram insumos para propor uma contribuição à metodologia já utilizada pelo banco, com impacto real na organização.

Palavras-chave: Gestão de riscos; segurança da informação; gestão de crise; ataque cibernético; wannacry; ransomware

Abstract

The volume of traffic and data dependency makes the risks in the technology area remarkably increasing. In 2017, the Wannacry ransomware cyber attack, which hit thousands of organizations worldwide, revealed how risk management and crisis management can be related. This research aims to adapt a systemic solution model for technology-oriented crisis events and analyze it in light of the risk management strategy. For this, it studies the case of a large Brazilian private bank during the Wannacry attack and the applicability of an adaptation of the PREPARE model. The results revealed the applicability of the model and the necessary actions for the organization to anticipate possible attack impacts and related mitigation actions. The findings of the interviews provided inputs to propose a contribution to the methodology already used by the bank, with a real impact on the organization.

Keywords: Risk management; information security; crisis management; cyber attack; wannacry; ransomware

Adaptando o Modelo PREPARE para Gestão de Riscos em Crises de Tecnologia

RESUMO
O volume de tráfego e dependência de dados faz com que os riscos na área de tecnologia sejam notavelmente crescentes. Em 2017, o ataque cibernético do *ransomware* Wannacry, que atingiu milhares de organizações em escala mundial, revelou como a gestão de riscos e a gestão de crises podem estar relacionadas. Esta pesquisa tem o objetivo de adaptar um modelo de solução sistêmica para eventos de crise voltados à tecnologia e analisá-lo a luz da estratégia de gestão de riscos. Para isso, estuda o caso de um grande banco privado brasileiro durante o ataque do Wannacry e a aplicabilidade de uma adaptação do modelo PREPARE. Os resultados revelaram a aplicabilidade do modelo e as ações necessárias para que a organização antecipasse possíveis impactos de ataque e ações mitigatórias relacionadas. As constatações das entrevistas trouxeram insumos para propor uma contribuição à metodologia já utilizada pelo banco, com impacto real na organização.

1. INTRODUÇÃO

Um evento é um incidente ou uma ocorrência gerada com base em fontes internas ou externas, que afeta a realização dos objetivos da organização (COSO, 2007). Um subconjunto possível de eventos contém situações de alto nível de incerteza que afetam as atividades básicas ou a credibilidade da organização, exigindo medidas urgentes. Esse subconjunto retrata a definição de crise proposta pela ISO 22301 (2012).

Com a estruturação de uma Gestão de Riscos Corporativos (GRC) a organização estabelece estratégias para identificação e mitigação dos impactos ocasionados pelo evento. Entretanto, quando esse evento atinge um nível crítico de complexidade e impacto, o processo de atuação pertinente é o de gestão de crises (Deloitte, 2015).

No entanto, nas etapas anteriores a materialização desse evento de crise, a organização consegue antecipar-se, através de soluções sistêmicas no processo de gestão de riscos, de forma a mitigar os possíveis impactos aos seus objetivos e operações (Davis, 2005).

No contexto atual, onde um ambiente de tecnologia permeia diferentes modelos de negócio, a necessidade de antecipar e endereçar eventos de crise voltados a tecnologia é urgente (Davis, 2005). Com o desenvolvimento de sistemas cada vez mais complexos, com mais funcionalidades, integrações e componentes, a probabilidade de eventos do tipo considerado "cisne negro" aumenta com o tempo (Masys, 2012 e INCOSE, 2014).

Exemplificando um evento de crise voltado à tecnologia, em maio de 2017 um acontecimento inesperado, sem precedente, e em escala global atingiu milhares de computadores, impossibilitando qualquer atividade e exigindo um pagamento de resgate em criptomoedas. Um *ransomware* (i.e. instruções designadas a criptografar e bloquear as informações de um computador até o pagamento de resgate) chamado *Wannacry* propagou-se pela internet atingindo aproximadamente 230.000 máquinas em todos os continentes (150 países). Diversas organizações foram afetadas, dentre elas instituições de saúde, como NHS (Inglaterra e Escócia), companhias automotivas, como Nissan e Renault (Gales e França), e grandes corporações como FedEx (Estados Unidos), Deutsche Bahn (Alemanha) e Telefónica (Espanha). No Brasil, empresas como Petrobrás e Vivo, além do Tribunal de Justiça de São Paulo também foram impactadas.

Através da exploração de vulnerabilidades em computadores da organização, esse ataque pôde se espalhar por toda a rede, ocasionando a indisponibilidade de serviços, vazamento de informações e impacto na reputação e valor das marcas. A estimativa de perda financeira com esse ataque ao redor do mundo atingiu bilhões de dólares.

Nesse contexto, este artigo tem o objetivo de adaptar um modelo de solução sistêmica para eventos de crise voltados à tecnologia e analisá-lo a luz da estratégia de gestão de riscos de tecnologia e segurança da informação adotada por um grande banco privado brasileiro durante o ataque do *Wannacry* de 2017.

2. PROBLEMA DE PESQUISA E OBJETIVO

Em maio de 2017 o maior ataque *ransomware* da história atingiu computadores de todo o mundo, afetando operações de diversas empresas, hospitais, órgãos governamentais e de uso pessoal. Esse evento foi singular devido a exposição do ataque e rapidez da infecção, pela primeira vez atingindo máquinas no mundo todo em apenas algumas horas. O evento rapidamente se transformou em crise quando impactou de forma crítica diversos negócios, ocasionando interrupções em operações, vazamentos de informação e consequente perdas financeiras e de imagem das organizações.

O ataque do Wannacry revelou ao ambiente de tecnologia como a gestão de riscos e a gestão de crises podem estar, na prática, fortemente relacionadas. Se por um lado empresas enfrentaram crises, por outro empresas preparadas para ataques no ambiente tecnológico tiveram o impacto em seus negócios amortecido pela rápida ação resultante da preparação.

Ainda, empresas que mitigaram esses riscos não ficaram vulneráveis aos ataques. Em março de 2017, dois meses antes do ataque, a Microsoft havia lançado pacotes para correção da vulnerabilidade no código do Windows que permitiu o ataque desse malware. Isso significa que se grande parte das máquinas tivessem aplicado a atualização necessária, esse ataque não teria o impacto que teve. Do outro lado da balança, argumenta-se que são liberadas correções para vulnerabilidades críticas recorrentemente, e que essas atualizações podem impactar algum serviço essencial da empresa. Vale ressaltar que antes desse ataque diversas empresas não compreendiam os riscos associados a segurança da informação. A história mostra que esse tipo de abordagem é avesso as práticas de gestão de riscos em um mundo dependente de tecnologia, e o tema de segurança de informação deve estar presente na estratégia de todas as empresas e instituições (World Economic Forum, 2020).

A Gestão de Riscos Corporativos, no conceito atual de alinhamento entre estratégia e desempenho, considera que dentre suas funções estão as de reduzir surpresas negativas e aumentar e resiliência do negócio (COSO, 2017). Nesse contexto, a gestão de riscos e a gestão de crises mostram-se complementares, como observado no caso do ataque do wannacry. Apesar disso, a literatura capaz de fazer a ligação entre a gestão do que acorre antes da materialização (risco) e o que sucede (crise) é tímida.

Ao encontro desse problema, este artigo tem o objetivo de adaptar um modelo de solução sistêmica para eventos de crise voltados à tecnologia e analisá-lo a luz da estratégia de gestão de riscos de tecnologia e segurança da informação. Para isso, estuda o caso de um grande banco privado brasileiro durante o ataque do *Wannacry* de 2017 e a aplicabilidade do modelo adaptado nesse contexto.

3. FUNDAMENTAÇÃO TEÓRICA

*3.1.*Gestão de Riscos Corporativos e o Ambiente de Valor

Em 2007 o *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) publicou o documento *Enterprise Risk Management Framework* com o objetivo de auxiliar no desenvolvimento de estruturas abrangentes e diretrizes sobre controles internos para um melhor gerenciamento de riscos corporativos. A estrutura apresentada pelo COSO naquele ano oferece

um enfoque mais vigoroso e extensivo no gerenciamento de riscos corporativos, embora não tenha por meta substituir a estrutura de controles internos das organizações (COSO, 2007).

Em 2017 o COSO propôs uma revisão do modelo na qual a estratégia passou a ter um peso ainda maior na gestão de riscos das organizações. Para o COSO (2017), a Gestão de Riscos Corporativos tem seis principais vantagens: aumentar a gama de oportunidades; identificar e gerenciar riscos em todo o negócio; incrementar resultados positivos e reduzir surpresas negativas; reduzir a variabilidade do desempenho; melhorar o emprego de recursos; aumentar a resiliência do negócio.

Além dos riscos estratégicos, operacionais, de comunicação e de conformidade consolidadas pelo COSO (2007), o COSO (2017) contempla os riscos derivados da possibilidade de que as estratégias não estejam alinhadas com a missão, visão e valores da organização e os riscos resultantes das estratégias selecionadas. Assim, os conceitos mais recentes do COSO convergem para uma gestão de riscos capaz de alavancar a geração de valor através de uma integração com a estratégia e o desempenho. A Figura 1 apresenta o modelo proposto pelo COSO (2017).

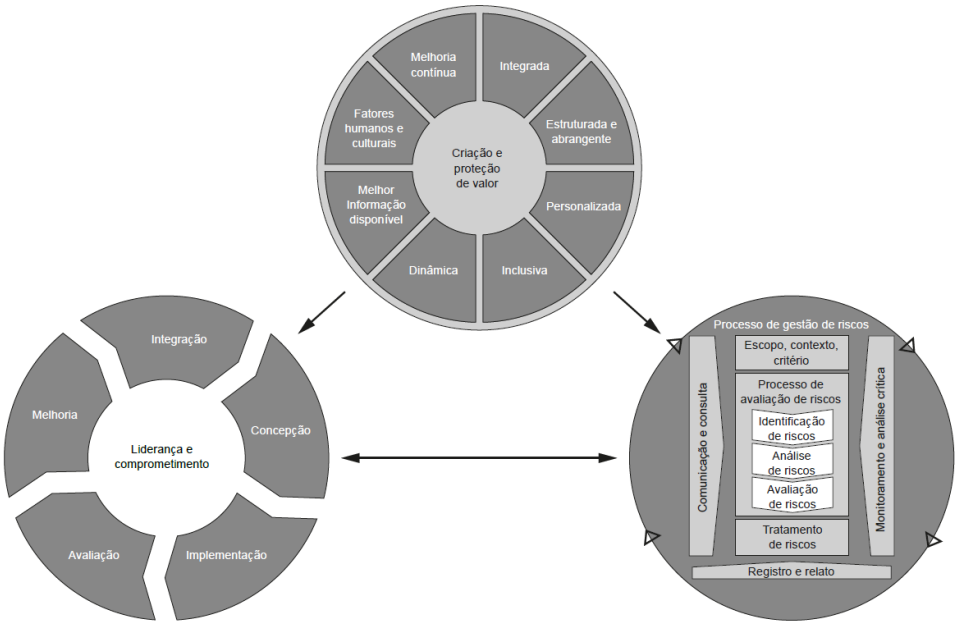
Figura 1. Gerenciamento de Riscos Corporativos Integrado a Estratégia e Desempenho

Fonte: COSO (2017, p.6).

Além do COSO, á o ISO 31000 de 2018 também apresenta um modelo de gestão de riscos com uma visão integrada entre princípios, estrutura e processos para que sirvam como diretrizes para gerenciar os riscos enfrentados pelas organizações. Essas diretrizes podem ser utilizadas ao longo da vida da organização e aplicadas a quaisquer atividades. A Figura 2 apresenta o modelo proposto pela ISO (2018).

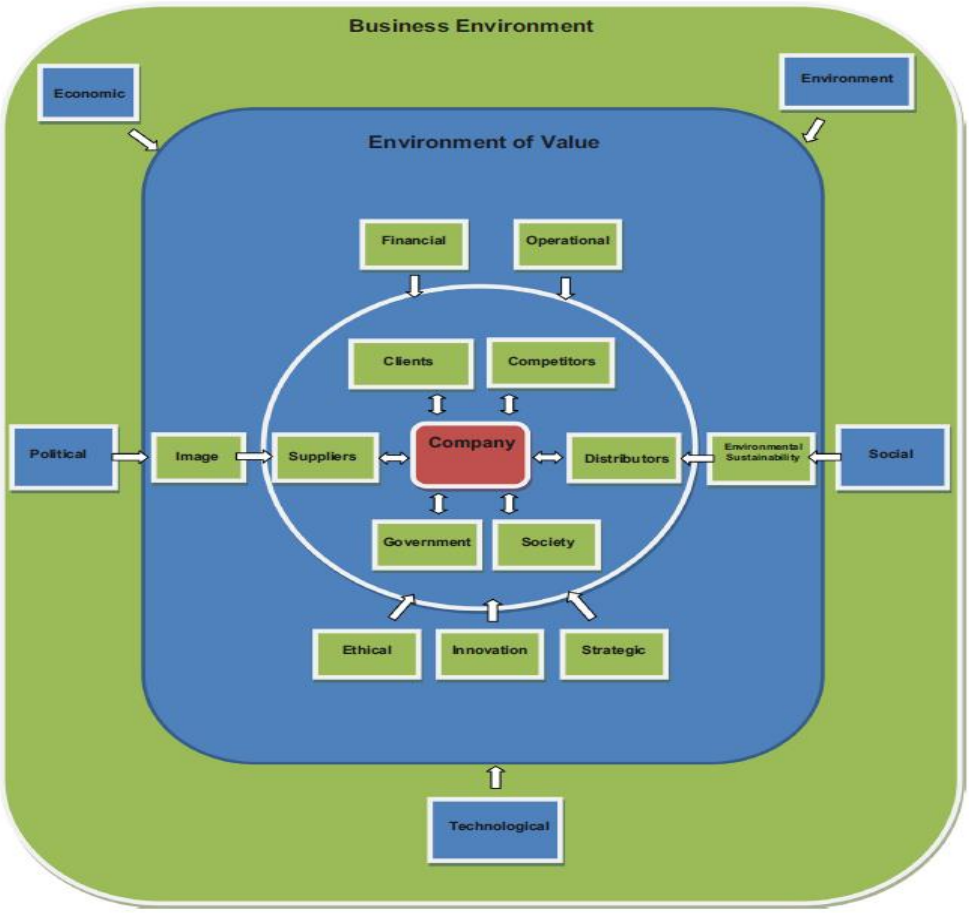
Em relação ao ambiente de valor, Oliva (2016) aborda as relações de risco da organização com seus agentes para definir um nível de maturidade em Gestão de Riscos Corporativos. Nesse modelo, o autor conceitua o Ambiente de Valor como o conjunto dos agentes que tem relações com a organização e que, por tanto, podem gerar valor. Sendo assim, a gestão de risco corporativo tem que avaliar todas essas relações de forma sistêmica para que não haja risco na relação de valor com esses agentes. A Figura 3 apresenta o ambiente de valor de Oliva (2016).

Figura 2. Princípios, Estrutura e Processo do Modelo ISO 31000 de 2018



Fonte: ISO 31000 (2018).

Figura 3. Riscos Corporativos no Ambiente de Valor



Fonte: Oliva (2016)

Sobre a maturidade da gestão de risco de uma organização, Oliva (2016) apresenta o resultado de uma pesquisa feita com 243 empresas dentro das 1.000 maiores empresas do Brasil segundo a revista Exame de 2011. Da análise dos resultados das entrevistas o autor classificou 5 níveis de maturidade em Gestão de Riscos Corporativos. Essa classificação começa no nível 1, onde as práticas de gerenciamento de riscos são insuficientes e chega até o nível 5, onda há, por parte da empresa, uma visão sistêmica do gerenciamento do risco, sendo o mais alto nível do modelo. A Tabela 1a seguir mostra algumas das práticas identificadas para cada nível segundo o autor.

Tabela 1. Características dos níveis de maturidade na gestão de riscos corporativos

Níveis de Maturidade	Características
Nível 5 **Gerenciamento de riscos sistêmico**	▪ Empresas com consciência, organização e transparência sobre o gerenciamento de risco. ▪ Tem suporte de consultorias externas, parceiros e institutos de pesquisa para melhorar seu gerenciamento de risco. ▪ Avaliação de risco do seu ambiente de valor, indo além da suas fronteiras.
Nível 4 **Gerenciamento de riscos participativo**	▪ Empresas com alto nível de atenção e organização nos processos de gerenciamento de risco. ▪ Gestão de risco mais descentralizada ▪ Comunicação como parte importante do gerenciamento de risco. ▪ Gerenciamento de risco guiada pela participação da maioria dos funcionários.
Nível 3 **Gerenciamento de riscos estruturado**	▪ Alto nível de organização dos processo de gerenciamento de risco ▪ Uso mais intenso de técnicas, ferramentas e métodos de gerenciamento de risco.
Nível 2 **Gerenciamento de riscos de contingência**	▪ A empresa está ciente dos riscos envolvidos. ▪ Há uso de técnicas, ferramentas e métodos de gerenciamento de risco a grosso modo. ▪ Gerenciamento de risco centralizado e pouco envolvimento dos funcionários.
Nível 1 **Gerenciamento de riscos insuficientes**	▪ Pouca atenção com os riscos corporativos. ▪ Não há uma estrutura dedicada à riscos corporativos. ▪ Práticas não estruturadas para o gerenciamento de riscos.

Fonte: Adaptado de Oliva (2016)

3.2. Gestão de Crises e Modelo PREPARE

Dada a complexidade de operacionalização de um grande banco, é natural estar suscetível a enfrentar os mais diversos desafios nos diferentes setores que o compõe e que podem levar a uma crise. Para Orduña (2002) uma crise é "um acontecimento extraordinário ou uma série de acontecimentos, que afeta de forma diversa a integridade do produto, a reputação ou a estabilidade financeira da organização; ou a saúde e bem-estar dos empregados, da comunidade ou do público geral". Os potenciais eventos de crises devem ser tratadas por meio de uma Gestão de Crises, cujo principal objetivo é gerenciar eventos de grande dimensão que podem comprometer a perenidade e a reputação de negócios (Deloitte, 2015).

O modelo PREPARE foi desenvolvido por Beverly J. Davis em 2005 com o intuito de oferecer, a partir da Janela de Johari, uma conscientização maior e uma melhor prática para o gerenciamento de crises tecnológicas, uma vez que a cibersegurança não é um esforço único, mas um processo contínuo de análise e avaliação. PREPARE é o acrônimo para *Preventive measures*, *Retrospection*, *Protection investment*, *Anticipate*, *Re-evaluate* (Beverly, 2005).

A janela de Johari foi uma criação dos psicólogos Joseph Luft e Harry Ingham que em 1961 propuseram essa ferramenta para um melhor entendimento das relações entre as pessoas. O modelo proposto traz uma visão do que o indivíduo tem conhecimento de si e do que não tem, e o que o outro conhece sobre ele e o que não conhece. O resultado dessas visões é uma matriz com quatro quadrantes conforme a Figura 3.

Figura 3. A janela de Johari

Fonte: Luft e Ingham (1955)

No trabalho de Luft e Ingham (1955), cada quadrante é descrito da seguinte forma:

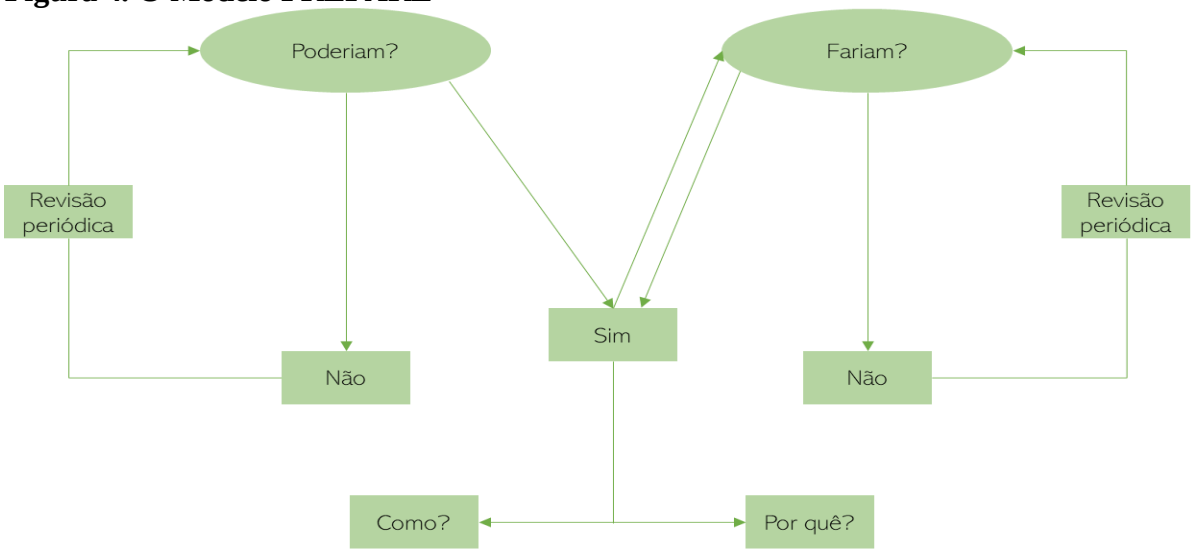
- Quadrante I – Área de livre atividade ou área pública: representa os comportamentos e motivações sabidos por si e pelos outros.
- Quadrante II – Área cega: representa comportamentos que os outros sabem sobre nós, mas não se tem conhecimento.
- Quadrante III – Área evitada ou escondida: representa coisas que sabemos sobre nós, mas que não tornamos público, ou seja, os outros não sabem.
- Quadrante IV – Área de atividade desconhecida: representam os comportamentos que não temos consciência sobre nós e que os outros também não sabem.

Esse modelo de apresentação do que é conhecido entre o indivíduo e o os outros foi ao longo dos anos utilizado em diferentes áreas (e.g. empresarial, tecnológica e educacional) para representar as relações entre os diversos agentes que compõem o ambiente de valor no qual o objeto de estudo está inserido.

A partir da aplicação da Janela de Johari para analisar o risco tecnológico, é possível identificar quais são as possíveis ameaças de possíveis inimigos que podem impactar o negócio da organização. Depois de identificar os potenciais inimigos, o modelo parte da seguinte pergunta: *Os inimigos em potencial poderiam ameaçar a segurança coorporativa?* Em caso negativo, o modelo sugere uma revisão anual. Mas caso a resposta seja positiva, o modelo indica a seguinte pergunta: *Eles fariam?* Caso a resposta para esta segunda pergunta seja negativa, o modelo sugere novamente uma revisão anual. Porém, caso seja positiva, partiríamos para uma

fase onde se discutiria livremente outras duas questões: *Como?* e *Por quê?* A Figura 4 ilustra o modelo PREPARE:

Figura 4. O Modelo PREPARE



Fonte: Adaptado de Beverly (2005).

A parte do "Como?" avalia como a empresa poderia ser atacada, enquanto o "Por quê?" pode revelar os objetivos do ataque, o que inclui qualidades ocultas da organização, conforme descritos no quadrante IV da Janela de Johari. Com o levantamento dessas questões, o PREPARE nos leva a investigar os seguintes pontos: Medidas Preventivas, Retrospecção, Investimento em Proteção, Antecipação e Reavaliação. Assim, o modelo PREPARE propõe uma metodologia de análise preliminar de risco antes que efetivamente o evento se materialize, podendo a organização estar mais preparada para enfrentar futuros ataques.

4. METODOLOGIA

Este artigo emprega o método de estudo de caso para observar a aplicação do modelo PREPARE em um grande banco privado brasileiro. O método de pesquisa utilizado foi a descritiva de caráter qualitativo que, de acordo com Gil (2008, p.28), "têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis."

Os dados foram obtidos através de entrevistas semiestruturadas, que segundo Lakatos e Marconi (2002, p.95) tem maior flexibilidade porque permitem ao entrevistador repetir ou esclarecer perguntas, formular de maneira diferente e especificar significados. O questionário foi dividido em seis grandes tópicos para discussão divididos em duas frentes principais: estrutura e ação. O objetivo foi facilitar o diálogo e incitar o entrevistado para contribuir com resultados tanto primários como a indicação de dados secundários. Os tópicos estruturais de discussão foram:

- A importância do tema de ataques cibernéticos para o banco.
- Visão sobre o nível de maturidade dos processos de gestão de riscos e de crises voltado a tecnologia e sistemas de informações no banco.
- Estruturação dos processos de gestão de crise e gestão de riscos.

E os tópicos que fomentaram a coleta de dados quanto a ação do Wannacry foram:

- Ações realizadas durante o ataque do Wannacry e suas relações com ações já existentes ou novas.

- Incorporação das ações novas implementadas durante o ataque do Wannacry no processo de gestão de riscos.
- Efetividade dos controles existentes antes do ataque do Wannacry para contornar o problema.

As entrevistas foram realizadas com três gestores e líderes de diferentes áreas do banco pesquisado que estiveram diretamente envolvidos nas ações de gerenciamento de risco durante o ataque do *Wannacry*. Foram entrevistados o Superintendente de Risco Operacional em Segurança da Informação e Continuidade de Negócios, o Gerente de Governança de Segurança da Informação e o Analista de Risco Operacional de Segurança da Informação. De acordo com Godoy (1995), procurou-se realizar entrevistas conduzidas no ambiente natural de trabalho e num tom informal.

As análises dos dados coletados seguiram a organização em três etapas como proposto por Bardin (2016, p.125), segundo o qual "As diferentes fases da análise de conteúdo, tal como o inquérito sociológico ou a experimentação, organizam-se em torno de 3 polos cronológicos: 1) a pré-análise; 2) a exploração do material; 3) o tratamento dos resultados, a inferência e a interpretação."

5. ANÁLISE DOS RESULTADOS

O banco estudado está entre as maiores instituições financeiras do Brasil e atua oferecendo serviços para pessoas físicas e jurídicas través de milhares de agencias no Brasil, dezenas de milhares de funcionários e milhões de clientes. Nos últimos anos o constante avanço da tecnologia dentro do mercado financeiro propiciou o surgimento de um novo tipo de concorrente, as chamadas *Fintech*, que, através de sua agilidade e soluções digitais, começaram a motivar uma transformação nos bancos tradicionais para uma nova era digital. Para adequar-se à essa constante evolução tecnológica, o banco definiu seis prioridades estratégicas que irão direcionar seu crescimento nos próximos anos, dentre os quais estão elencados a Transformação Digital e a Gestão de Riscos.

As entrevistas foram conduzidas com a intenção de capturar de pessoas chaves no processo de Gestão de Riscos de Tecnologia e Segurança da Informação a estrutura necessária e quais ações foram fundamentais na mitigação do ataque do *Wannacry*. Para tal, a abordagem utilizada na entrevista foi a de perguntas semiestruturadas para que o entrevistado pudesse contribuir com sua avaliação sobre o tema e também pudesse enriquecer o trabalho com informações complementares.

Analisando os resultados obtidos, houve um consenso quanto a importância do tema de ataques cibernéticos para o Itaú Unibanco. Nas entrevistas, destacamos a existência de diferentes Comitês de Risco, envolvendo os executivos para endereçar assuntos voltados a tecnologia e segurança da informação, além de investimentos priorizados pelo banco com a intenção de mitigar riscos associados a vazamento de informação e ataques cibernéticos.

Em relação a estruturação das áreas de gestão de riscos e crise no Itaú, dado a percepção dos entrevistados, esses processos se enquadram em um grau elevado de maturidade, devido a controles e procedimentos estruturados, aparando-se em normas, diretrizes e frameworks internacionais (COBIT, NIST, OWASP) e de mercado. Além disso, os papéis e responsabilidades estão definidos através de políticas, e difundidos em comitês e práticas diárias institucionais. A Tabela 2 apresenta um resumo das principais avaliações dos entrevistados.

Tabela 2. Resumo das principais avaliações dos entrevistados

	Importância do tema para o banco	Maturidade gestão de riscos	Maturidade gestão de crises	Proporção entre ações de risco frente a crise	Ações principais
#1	Alta	4	3	100%	A. Controles de monitoração de ataques cibernéticos B. Controles de correção de vulnerabilidades e resposta a incidente
#2	Alta	4	4	80%	A. Controles implantados, priorizados e antecipando a materialização B. Investimentos voltados a segurança da informação e riscos C. Gestão de crise pronta para seguir manual e orquestrar processo
#3	Alta	5	4	85%	A. Controles mapeados e implantados B. Atuação rápida e orquestrada entre segurança e tecnologia

A coordenação entre esses processos de gestão de riscos e crise se dá de forma definida, através de metodologias e manuais internos, com as responsabilidades estabelecidas. O direcionamento da gestão de riscos é voltado a proatividade, com papel de melhoria e desenvolvimento de processos, com a intenção de criar um ambiente de controles mais robusto. Diante do contexto de segurança da informação, foi reforçado por dois entrevistados a necessidade da resiliência desse ambiente de controle. Quanto ao direcionamento da gestão de crise, dá-se ênfase na orquestração e invocação dos planos necessários.

No contexto das entrevistas surgiram informações que, em 2017, bilhões de transações foram realizadas nos canais digitais do banco, milhões de acesso por mês foram feitos ao *internetbank* via celular e petabytes de informações foram armazenadas em seus servidores. Foi destacado que com o aumento da informatização das operações financeiras, o banco passou a ter um risco maior na parte tecnológica, não só pela grande quantidade de informações dos seus clientes gerando um risco operacional e financeiro, mas também por um eventual ataque cibernético que poderia levar ao vazamento de informações de seus clientes. Ambos os eventos colocariam em risco a reputação do banco e, segundo o *Basle Committe on Banking Supervision* (1997), o risco de reputação é particularmente danoso para os bancos, uma vez que a natureza de seus negócios requer a manutenção da confiança de depositantes, de credores e do mercado geral.

5.1. Adequação do modelo PREPARE

Diante do evento do *Wannacry*, foi consenso entre os entrevistados a participação majoritária do processo de gestão de riscos para mitigação da crise, e o não impacto nas operações. A gestão de riscos analisa toda a cadeia de valor, atuando na prevenção, monitoração para detecção rápida, mitigação dos impactos e recuperação. Na perspectiva dos entrevistados, os controles principais que atuaram durante o evento já haviam sido estabelecidos previamente, de forma proativa e antecipando a materialização de riscos. Complementando essas ações, a atuação em conjunto e mobilização das equipes em fóruns prioritários também auxiliaram na mitigação do risco, caracterizando-se no processo de resposta a incidentes de tecnologia e segurança da informação.

Nesse contexto, foi realizada a adequação do modelo proposto por Davis (2005) no cenário do Banco durante o evento do *Wannacry*, por meio da formalização das ações e medidas sistêmicas tomadas para enfrentar essa crise tecnológica. A análise foi baseada, principalmente, na identificação dos agentes e na pergunta de "Como?" o evento poderia impactar os objetivos da empresa.

Seguindo o modelo da Janela de Johari, foram identificados os agentes de valor no contexto desse ataque, e as informações disponíveis e não disponíveis para cada grupo. A importância dessa matriz se dá pela identificação de pontos vulneráveis frente aos agentes do ambiente de valor proposto por Oliva (2016), segregando os riscos associados nessas relações. Ressalta-se aqui que a segunda coluna dessa matriz é composta por áreas de bastante incerteza por parte da organização. Isso faz com que seja importante a análise de exposição aos riscos nessas áreas, e a relação de possíveis controles mitigatórios.

Figura 8. Janela de Johari (Joseph Luft e Harry Ingham, 1955) aplicado ao cenário do Banco frente ao Wannacry

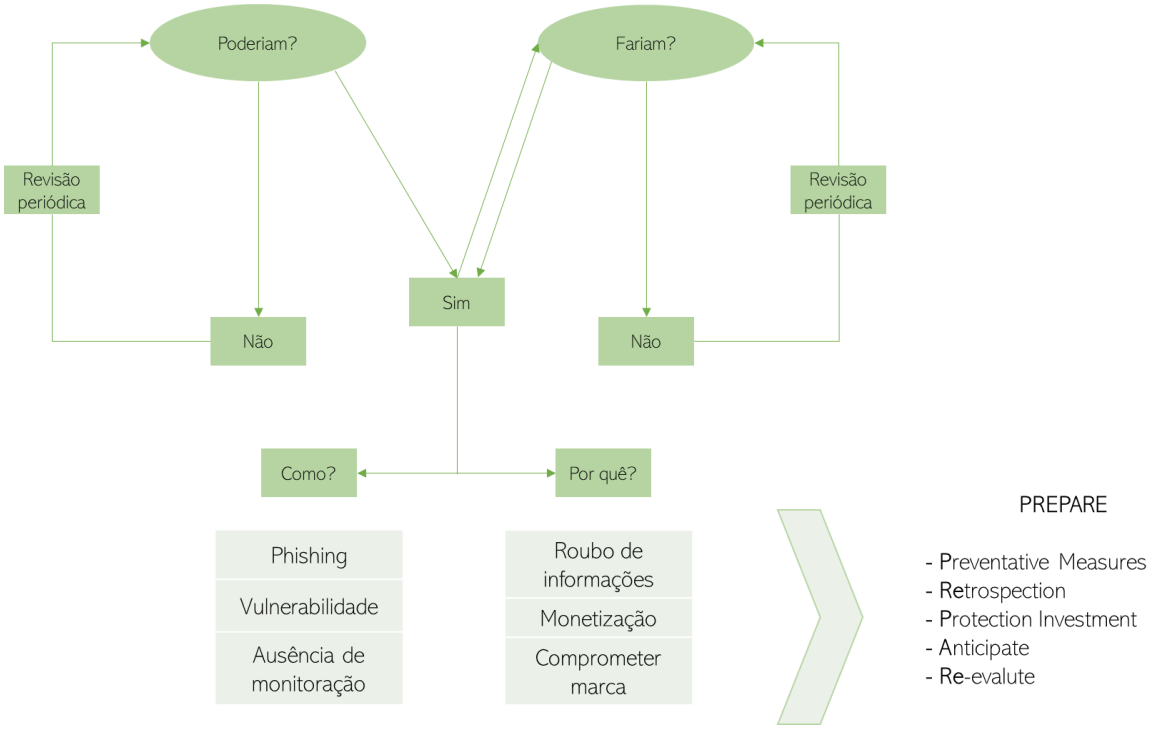
Fonte: Adaptado de *Luft and Ingham* (1955)

Uma vez identificado os agentes de valor e os principais riscos na janela de Johari, utilizamos o modelo PREPARE partindo das duas perguntas a seguir e, a partir delas, a Figura 9 apresenta o modelo aplicado ao Banco.

1° Poderiam: Podem hackers invadir os sistemas de informação do Banco para comprometer operações e roubarem dados?

2° Fariam: Hackers fariam a invasão dos sistemas de informação do Banco para comprometer operações e roubarem dados?

Figura 9. Modelo PREPARE (Davis, 2005) aplicado ao cenário do Banco frente ao Wannacry



Fonte: Adaptado de Beverly (2005)

Vale destacar que no momento em que as duas perguntas acima forem respondidas com "Sim", o modelo segue para as etapas de entendimento das motivações e maneiras de exploração do risco identificado através das perguntas abaixo:

3º Como: Como hackers fariam a invasão dos sistemas de informação do Itaú Unibanco para comprometer operações e roubarem dados?

4º Por quê: Por que hackers fariam a invasão dos sistemas de informação do Itaú Unibanco para comprometer operações e roubarem dados?

Ao aplicar o modelo PREPARE obtivemos as ações necessárias para se antecipar a possíveis impactos do ataque *Wannacry*. Para cada resposta elencada na aplicação desse modelo, temos possíveis ações mitigatórias, associadas as premissas do PREPARE (medidas preventivas, retrospecção, investimento em proteção, antecipação e reavaliação).

Respondendo à pergunta **"3º Como"**, constatamos por exemplo, a necessidade de controle para gestão de vulnerabilidades, que contempla a aplicação de atualizações de segurança no ambiente tecnológico para prevenção a ataques cibernéticos.

COMO?	PREPARE	AÇÃO
Através de exploração de vulnerabilidades	Medidas preventivas para se antecipar a exploração de vulnerabilidades	Aplicação de controles para gestão de vulnerabilidades: atualização de segurança periódica no ambiente tecnológico do Banco

Respondendo à pergunta **"4º Por quê"**, constatamos por exemplo, a necessidade de controle de segurança adicionando uma camada de proteção nos dados bancários de clientes, evitando assim a monetização do hacker ao tentar vender essas informações.

POR QUÊ?	PREPARE	AÇÃO
Monetização	Investimento em proteção	Camada adicional de proteção para dados bancários

6. CONCLUSÃO E CONTRIBUIÇÕES

A gestão de crise tem como objetivo mitigar os impactos causados por eventos que, em determinado momento, entraram em desequilíbrio e, assim, ajudar a empresa a minimizar possíveis prejuízos. Quando falamos de gestão de risco, não é possível prever acontecimentos futuros, mas é necessária uma análise prévia de possíveis cenários que auxiliem os gestores a tomarem as melhores decisões. Nesse trabalho propusemos a aplicação do modelo sistêmico de atuação em uma crise de tecnologia para o cenário de um grande banco privado brasileiro, e como a atuação da gestão de riscos, se antecipando ao possível ataque e entendendo a forma de operar dos agentes de valor, contribuiu para a mitigação dos impactos da crise.

Através das entrevistas, podemos perceber a estruturação do processo de gestão de riscos no banco e o modelo que assume para antecipar esses possíveis riscos conforme observado nas ações para conter o *Wannacry*, dado que os controles e processos já existentes contribuíram de forma majoritária para a mitigação dos impactos. Cabe ressaltar que todos os entrevistados, quando questionados sobre a percepção do grau de maturidade da gestão de risco do banco, além de já terem familiaridade com a terminologia, consideraram alto o nível de maturidade.

Com relação a análise de riscos, a dinâmica do Banco já incorporava as práticas estudadas no modelo PREPARE/Johari dentro da sua metodologia interna. As constatações das entrevistas nos deram insumos para propor uma contribuição à metodologia já utilizada pelo Banco, adaptando o modelo PREPARE/Johari para o caso Wannacry. Com a adaptação do modelo sugerido neste artigo, espera-se contribuir para o estudo do tema e possibilitar a utilização desse modelo tanto no banco estudado como em outras organizações, como ferramenta para mitigar as consequências de futuros eventos de crise de tecnologia.

REFERÊNCIAS

APIMEC: Associação dos Analistas e Profissionais de Investimento no Mercado de Capitais. Disponível em: https://apimec.mediagroup.com.br/download/2017/Apresentacao_Sao_Paulo.pdf

BARDIN, L. Análise de conteúdo. São Paulo: Edições 70, 2016.

BRENNER, Bill (16 May 2017). "WannaCry: the ransomware worm that didn't arrive on a phishing hook". Naked Security. Sophos. Retrieved 18 May 2017.

BASLE COMMITTEE ON BANKING SUPERVISION, Core Principles for Effective Banking Supervision, 1997

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). Enterprise Risk Management Framework, 2007.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). Enterprise Risk Management – Integrated Framework, 2017.

"Cyber-attack: Europol says it was unprecedented in scale". BBC News. 13 May 2017. Retrieved 13 May 2017

David Gallop, Chris Willy & John Bischoff (2016) How to catch a black swan: Measuring the benefits of the premortem technique for risk identification, Journal of Enterprise Transformation, 6:2, 87-106, DOI: 10.1080/19488289.2016.1240118

DAVIS, B.J. (2005), PREPARE: seeking systemic solutions for technological crisis management. Knowl. Process Mgmt., 12: 123-131. doi:10.1002/kpm.220

Deloitte (2015) "Manual de Gestão de Crises para Relações com Investidores: Comunicação e estratégia para a preservação de valor"

Essays, UK. (November 2018). Risk and Crisis Management. Retrieved from https://www.ukessays.com/essays/management/risk-crisis-management-3229.php?vref=1

GIL, A.C. Métodos e técnicas de pesquisa social. 6. ed. São Paulo: Atlas, 2008.

GODOY, A. S. Pesquisa qualitativa: tipos fundamentais. Revista de Administração de Empresas, São Paulo, v. 35, n. 3, p. 20-29, mai/jun, 1995.

INTERBRAND: Marcas Brasileiras Mais Famosas 2019. Disponível em: https://www.interbrand.com/br/best-brands/best-brazilian-brands/2019/ último acesso 01JUN2020.

ISO 31000 Gestão de Riscos – Diretrizes, 2018.

LAKATOS, E. M.; MARCONI, M. A. Técnicas de pesquisa: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados. 5. ed. São Paulo: Atlas, 2002. – Disponível em https://www.academia.edu/33781900/Marconi-Lakatos_Tecnicas_de_Pesquisa último acesso 01JUN2020

NAKASHIMA, Ellen; Timberg, Craig (May 16, 2017). "NSA officials worried about the day its potent hacking tool would get loose. Then it did". Washington Post. ISSN 0190-8286. Retrieved December 19, 2017.

OLIVA, F. L. A Maturity Model for Enterprise Risk Management. International Journal Production Economics, vol. 173, p. 66-79, 2016.

ORDUÑA, Octavio Isaac Rojas. A comunicação em momentos de crise. Disponível em: http://www.bocc.ubi.pt/pag/orduna-octavio-comunicacao-em-momentos-de-crise.pdf último acesso em 22JUL2021.

PANG, Augustine (2012),"Towards a crisis pre-emptive image management model", Corporate Communications: An International Journal, Vol. 17 Iss: 3 pp. 358 - 378

Risk Acceptance Personality Paradigm: How We View What We Don't Know We Don't Know. Michael J. Massie*, 2011. ARES Corporation, Houston, Texas 77058, doi: 10.2514/6.2011-1455

Y. T. Chua et al., "Identifying Unintended Harms of Cybersecurity Countermeasures," 2019 APWG Symposium on Electronic Crime Research (eCrime), Pittsburgh, PA, USA, 2019, pp. 1-15, doi: 10.1109/eCrime47957.2019.9037589.