FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

CONCEITOS DE CONTINUIDADE DE NEGÓCIOS APLICADOS À INSTITUIÇÃO DE ENSINO SUPERIOR (IES)

DANIEL PIACENTINI

Americana, SP
2016

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

CONCEITOS DE CONTINUIDADE DE NEGÓCIOS APLICADOS À INSTITUIÇÃO DE ENSINO SUPERIOR (IES)

DANIEL PIACENTINI
pi4centini@hotmail.com

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Segurança da Informação, sob a orientação do Profº Msc. Leandro Halle Najm.

Área de concentração: Gestão da Continuidade de Negócios.

Americana, SP
2016

Piacentini, Daniel
P641 Conceitos de continuidade de negócios aplicados à instituição de ensino superior (IES). / Daniel Piacentini. – Americana: 2016.
56f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Me. Leandro Halle Najm

1. Administração de projetos 2. Gestão de negócios I. Najm, Leandro Halle II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 658.511-4

Daniel Piacentini

CONCEITOS DE CONTINUIDADE DE NEGÓCIOS APLICADOS À INSTITUIÇÃO DE ENSINO SUPERIOR (IES)

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Gestão da Continuidade de Negócios.

Americana, 27 de Junho de 2016.

Banca Examinadora:

Leandro Halle Najm
Mestre
Fatec Americana

Benedito Aparecido Cruz
Graduado
Fatec Americana

Maria Cristina Aranda
Doutora
Fatec Americana

AGRADECIMENTOS

Agradeço primeiramente ao meu orientador Profº Msc. Leandro Halle Najm por me aceitar como orientando, e me mostrar os caminhos a percorrer para que esse trabalho fosse feito da melhor maneira possível. Aos meus pais e irmão pelo apoio e ajuda durante o período desse curso de graduação de Tecnologia em Segurança da Informação. E a minha namorada pela paciência, incentivo e carinho, durante esse período difícil em que foi necessária muita dedicação e disciplina.

DEDICATÓRIA

Dedico este trabalho aos meus pais e irmão, pelo apoio e paciência, aos meus amigos pelas risadas e a minha namorada pelo carinho.

RESUMO

Como qualquer organização, uma instituição de ensino superior possui informações criticas que são tratadas como ativos, e também não está livre de sofrer interrupções em seus negócios, oriundas de diversos riscos e ameaças internas e externas que podem ocorrer neste cenário e explorar suas vulnerabilidades. Mas a verdade é que a maioria das instituições de ensino superior não possui procedimentos, ações a serem tomadas ou documentos que garantam a mínima disponibilidade dessas informações e por consequência a continuidade de seus serviços mais prioritários. Em função ao exposto, deve-se dar importância ao plano de continuidade de negócios dentro deste cenário. Esse trabalho foi desenvolvido com o intuito de demonstrar a relevância da informação como um bem, e da necessidade do uso de medidas de segurança da informação e da gestão de continuidade de negócios para que a mesma esteja disponível, eestudar o contexto de uma instituição de ensino superior e propor ações de continuidade para serviços críticos das mesmas.

Palavras chave: Continuidade de Negócios, Segurança da Informação, Resposta a incidentes.

ABSTRACT

Like any organization, an institution of higher education has critical information which are treated as assets, and is also not free from suffering interruptions in their business, arising from various risks and internal and external threats that may occur in this scenario and exploit their vulnerabilities. But the truth is that most higher education institutions does not have procedures, actions to be taken or documents that guarantee minimum availability of this information and therefore the continuation of its most priority services. So has the importance of business continuity plan in this scenario, and this work was developed in order to demonstrate the relevance of the information as well, and the need to use security measures of information and continuity management business so that it is available, to understand the context of a higher education institution and propose actions continuity for critical services from them.

Keywords: Business Continuity, Information Security, Incident Response.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

IBGE Instituto Brasileiro de Geografia e Estatística.

IES Instituição de Ensino Superior.

PCN Plano de Continuidade de Negócios.

GCN Gestão da Continuidade de Negócios.

TI Tecnologia da Informação.

ABNT Associação Brasileira de Normas Técnicas.

SWOT *Strenght, Weakness, Opportunities, Threats.*

FOFA Força, Oportunidades, Fraquezas, Ameaças.

BS *British Standards.*

DRI *Disaster Recovery Institute.*

SGCN Sistema de Gestão da Continuidade de Negócios.

PDCA *Plan, Do, Check, Act.*

RACI Responsável, Autoridade, Consultado, Informado.

SAMU Serviço de Atendimento Móvel de Urgência.

1 INTRODUÇÂO

Ao longo da história, para Sêmola (2003), a informação foi primordial para que os povos pudessem se modernizar e evoluir em diversas eras, como a industrial, e alcançar seus objetivos, e também, que os mesmos conseguissem se comunicar. Seja essa uma informação sobre o exército inimigo, ou sobre trocas comerciais da época, ainda distante do mundo digital em se vive hoje.

Com o passar do tempo, e o aumento de informação gerada, foi necessária a criação de máquinas, para processar e armazenar essa informação mais rapidamente, pois a mesma se tornou um ativo indispensável para pessoas, empresas e organizações. Com isso, surge a necessidade do avanço da tecnologia que se tem nos dias de hoje, antes a informação que era processada localmente, atualmente trafega através da internet.

O ser humano está cada vez mais dependente da Internet, para demonstrar isso, uma pesquisa do Instituto Brasileiro de Geografia e Estatística, IBGE (2015), diz que mais de 85 (oitenta e cinco) milhões de brasileiros navegaram na Internet em 2013. Mesmo ainda existindo muita gente distante desse universo digital, esse número vem tendo um crescimento galopante. Nos últimos cinco anos foi um aumento de 50% (cinquenta por cento).

Não somente as pessoas estão conectadas, também empresas, governos e instituições de diversos setores estão presentes na rede mundial, e tem a informação como um ativo de maior importância trafegando e sendo armazenada nela. Com isso, surgem os riscos de se comprometer esse ativo, como perda, acesso indevido, quebra de confidencialidade, etc.

Em 2008, durante viagem entre plataformas, a empresa estatal petrolífera Petrobras, teve alguns de seus notebooks furtados, nos quais continham informações sigilosas sobre novas fontes de petróleo e gás. Isso mostra que sim, informações estratégicas saltam os olhos de outrem, além de evidenciar a fragilidade em segurança de uma grande empresa, trazendo sérios problemas como a queda no valor das ações (UOL NOTÍCIAS, 2008).

Não somente “ladrões de informação” ou *hackers* preocupam as instituições, e seus profissionais de segurança da informação, pois elas sempre foram, e serão vulneráveis a uma grande variedade de riscos e ameaças. Riscos que também podem ser gerados das mais diversas formas, como desastres naturais, problemas na infraestrutura, funcionários insatisfeitos ou mal instruídos, e mesmo estando protegidos, os sistemas não tem total garantia sobre quebra de segurança, e quando ela acontece, deve-se estar preparado para uma resposta rápida em dar continuidade aos negócios.

No caso de uma instituição de ensino superior (IES), a interrupção dos negócios pode afetar a continuidade dos estudos de várias pessoas, os alunos podem perder um semestre inteiro de aulas, causando atraso em sua formação. Tanto no caso de uma instituição particular ou pública isso acarreta em mais gastos para o aluno e instituição, podendo se tornar problema do governo, causando má imagem para seus gestores. Por possuir dados pessoais e acadêmicos de alunos, dados esses necessários para sua graduação, e estudos futuros, uma IES não pode negar a importância de um plano de continuidade de negócios.

Ao longo deste trabalho, com base em uma revisão bibliográfica, são apresentados conceitos sobre segurança da informação, gestão de risco, gestão da continuidade, e formulação de um plano de continuidade de negócios (PCN), para ser aplicado principalmente em uma IES.

Sabe-se que a implantação de um sistema de gestão da continuidade dos negócios não é simples, e é um documento específico para cada organização, mas torna este trabalho um passo inicial para que as IES tenham uma referência.

O **objetivo geral** foi estudar os conceitos de segurança da informação, mais especificamente de gestão de continuidade de negócios (GCN), a fim de entender os seus processos, com o intuito de elaborar um plano de continuidade de negócios a ser aplicado a uma IES.

Os **objetivos específicos** do trabalho foram: a) Fazer um levantamento bibliográfico, sobre informação como ativo, segurança da informação, gestão de

riscos e de continuidade de negócios, buscando identificar os principais conceitos necessários para a compreensão da estrutura de um plano de continuidade de negócios para uma instituição de ensino superior; b) Desenvolver um estudo de caso, onde são aplicadas as matrizes de gestão de risco apresentadas no capitulo anterior, conceitos da NBR ISO 22301, e gestão de continuidade de negócios em um cenário de uma faculdade; c) Analisar todo o trabalho para a produção das considerações finais do mesmo.

A **metodologia** utilizada para o desenvolvimento desse trabalho foi uma pesquisa qualitativa, onde um questionário desenvolvido pelo próprio autor foi enviado a profissionais de IES, respondidos, e serviu de base para que, juntamente com os conceitos adquiridos na revisão bibliográfica, se obtivesse a produção do estudo de caso.

O trabalho foi estruturado em 4 capítulos, sendo que o **primeiro** é a introdução, o **segundo** apresenta conceitos e definições sobre a importância da informação como ativo para as organizações, segurança da informação, gestão de risco, e de continuidade de negócios, o **terceiro** é o estudo de caso onde os conceitos são aplicados em um cenário de IES e o **quarto** se reserva as considerações finais do trabalho.

2 INFORMAÇÃO, SEGURANÇA E CONTINUIDADE

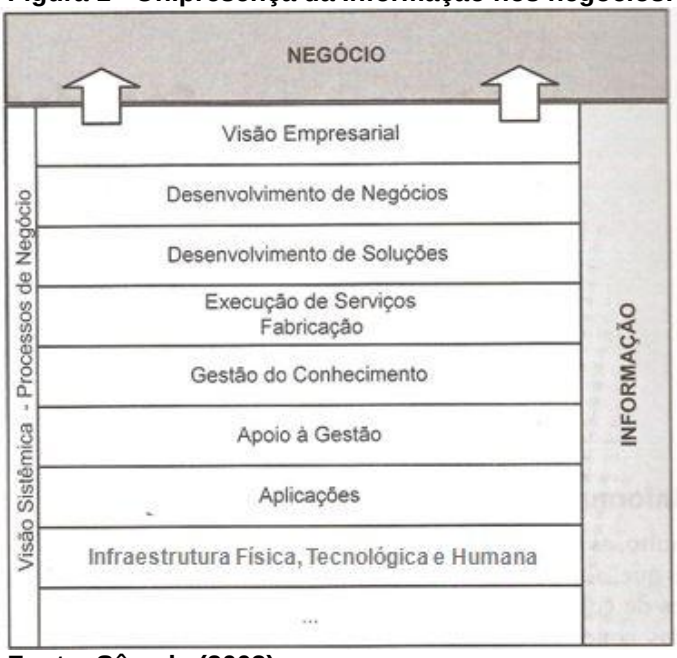
2.1 A INFORMAÇÃO COMO ATIVO

Quando se trata a informação como um bem, devemos saber de sua relevância em várias áreas do negócio, pois, a mesma atua como suporte para qualquer tomada de decisão importante, e pode alterar estrategicamente os caminhos de uma organização.

Quanto mais informação tiver ao seu comando, melhor pode adaptar-se ao mundo ao seu redor (RHODES-OUSLEY, 2013).

Historicamente a informação esteve sempre presente, desde a revolução elétrica e industrial, até os efeitos da tecnologia da informação (TI) aplicada aos negócios, e cumpria importante papel para a gestão do negócio. Claro que, para tal análise, se devem considerar variáveis culturais, mercadológicas e até macroeconomicas da época, a fim de adequar a projeção dos impactos. Mas é inegável que todas as empresas, independente de tamanho ou segmento de mercado, em todas as épocas, utilizaram a informação objetivando melhor produtividade, redução de custos, ganho de *market share*, aumento de agilidade, competitividade e apoio a tomada de decisão (SÊMOLA, 2003).

Figura 1 - Onipresença da Informação nos negócios.



Fonte: Sêmola (2003)

A Figura 1 explana a presença da informação nos principais processos em uma organização, e com isso confirma sua importância.

Para as empresas e instituições em geral, a informação é um ativo de grande importância dentro uma organização. Conforme citado pela Agência Brasileira de Normas Técnicas (ABNT), na norma NBR ISO/IEC 27002 (ABNT, 2005, p. 10), "A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida.". Além de ter importância, a informação como ativo de uma empresa, obteve grande participação na valorização dos negócios da mesma.

Dantas (2011, p. 21) explica a importância na valorização da informação:

> “Como a informação tem ocupado um papel de destaque no ambiente de negócios, e também tem adquirido um potencial de valoração para as organizações e para as pessoas, ela passou a ser considerada o seu principal ativo.”

Segundo Rainer Jr. e Cegielski (2012), vários aspectos contribuem para o aumento da vulnerabilidade das informações em uma organização, o primeiro deles é a evolução dos recursos de tecnologia da informação. Nos dias atuais, os ambientes são altamente complexos, interconectados, independente e conectados por redes sem fio.

Por ser um ativo tão importante, a informação é muito cobiçada por pessoas mal-intencionadas, e o roubo de alguma informação, ou a falta de acesso à mesma atrapalha a organização de várias maneiras, algumas delas, de forma irreversível. Com isso, percebe-se a necessidade de proteger a informação, e fazer com que a mesma esteja disponível para quem deva acessá-la. Para poder proteger esse ativo, deve-se conhecer primeiro as ameaças e vulnerabilidades que as envolvem, que serão tratadas a seguir.

2.2 AMEAÇAS E VULNERABILIDADES

Como foi visto no capitulo anterior, a informação tem importância primordial nas organizações, e por isso, existem muitos fatores externos interessados e motivados

a obtê-la, e que na tecnologia denomina-se ameaça. A ABNT na norma ISO/IEC 27002:2005 (ABNT, 2005, p.3) conceitua ameaça como “Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização”.

Seguindo o raciocínio de Dantas (2011, p. 31):

> “Essas ameaças podem surgir de várias formas: de eventos da natureza, como terremotos, furacões, enchentes, descargas elétricas, *tsunamis*, etc; de incidentes em instalações, como incêndio, curtos-circuitos, infiltrações; de incidentes de segurança, com roubo, furto, sabotagem, ataques terroristas, etc; e de uma variedade de eventos, que, de uma forma ou de outra, pode vir a afetar os negócios de uma organização.”

Por sua vez, a ameaça se utiliza de uma fragilidade, uma brecha no sistema para que consiga a quebra da segurança. Ameaça é o agente causador dos incidentes de segurança utilizando de um agente passivo, vulnerabilidade, apropriado, Sêmola (2003, p. 18) diz:

> “A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvos de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada.”

Como se pode observar, a ameaça ao acesso indevido à informação existe constantemente no meio tecnológico, e sempre buscando uma exploração da vulnerabilidade. Segundo a ABNT ISO/IEC 27002:2005 (ABNT, 2005, p.3), define-se vulnerabilidade como “Fragilidade de um ativo ou grupos de ativos que pode ser explorada por uma ou mais ameaças”. Portanto, a segurança busca tornar o sistema menos vulnerável possível.

Observa-se que vulnerabilidades se relacionam sempre e diretamente com as fragilidades, e essas podem estar em vários locais, como, política, processos, equipamento e também no fator humano. As vulnerabilidades sozinhas não causam incidentes, pois são passivas, necessitando sempre de um agente causador, ou seja, a ameaça (DANTAS, 2011).

As vulnerabilidades nas organizações podem ter diversas origens como: física, onde a infraestrutura da empresa pode estar comprometida, como um cabeamento desprotegido. Origem organizacional, onde as políticas e processos da instituição não estão sendo seguidos, ou até mesmo defasados. Origem natural, como instalações em locais de risco de terremotos e furacões, dentre outras tantas origens das vulnerabilidades existentes (SÊMOLA, 2003).

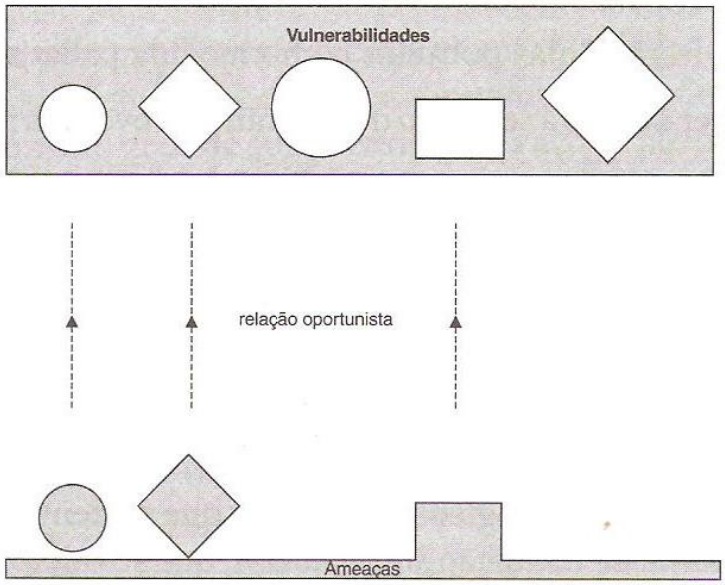
Aquelas ameaças causadas sem a intenção de danificar o sistema, como ações inconscientes e erros de usuários, são chamados de ameaças involuntárias.

E os *hackers, crackers*, sabotadores entre outros, que deliberadamente querem danificar o sistema, são chamadas de ameaças intencionais.

Como foi visto, as origens das vulnerabilidades de uma organização, e, as categorias de ameaças existentes são muito similares, tendo assim, um encaixe entre elas, gerando o incidente de segurança da informação.

A Figura 2 demonstra a relação entre vulnerabilidade e ameaça como peças compatíveis que se encaixam:

Figura 2 – Como peças que se encaixam, ameaças exploram vulnerabilidades.



Fonte: Sêmola (2003)

Como se conceituou acima, as ameaças e vulnerabilidades existentes permitem danificar a informação, e por consequência, a organização que a possui, e quando elas se encontram e se relacionam oportunamente, surge à quebra da segurança da informação para a instituição. Portanto, no próximo capitulo será visto conceitos de segurança da informação.

2.3 SEGURANÇA DA INFORMAÇÃO

“A segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio” (ABNT, 2005).

Para Sêmola (2003), pode-se definir segurança da informação como uma área do conhecimento que tem como objetivo proteger os ativos da informação contra acessos indevidos, mudança indevida e sua indisponibilidade, ainda de forma mais geral, pode-se considerar a segurança da informação como prática da gestão de riscos e incidentes que busca a garantia dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação.

A Figura 3 demonstra a confidencialidade, integridade e disponibilidade como a tríade da segurança da informação:

Figura 3 – Tríade da segurança da informação.

Fonte: Ataíde (2013)

Segundo Dantas (2011, p. 11):

> “Ao se falar em segurança da informação, deve-se levar em consideração essas qualidades da informação, pois toda ação que venha a comprometer qualquer uma dessas qualidades estará atentando contra a sua segurança.”

Como se conceitua na Figura 3, a segurança da informação abrange métodos, políticas, entre outras coisas, tudo para que a informação seja protegida, de tal forma que os objetivos da segurança sejam atingidos.

Os pilares da segurança da informação, confidencialidade, integridade e disponibilidade, são base para todos os programas de segurança em TI, e os profissionais da área, que criam políticas e procedimentos para proteger um sistema, devem levar cada um desses objetivos em consideração (MERKOW; BREITHAUPT, 2014).

- Confidencialidade visa garantir que as informações sejam confidenciais, ou seja, protegidas contra acessos indevidos, e vistas, lidas, processadas, somente por pessoas ou processos que tenham a devida autorização, independente de posição dentro da organização, também que os privilégios dos usuários sejam suficientes e limitados para seus deveres.

- Integridade visa garantir que as informações sejam integras, ou seja, após serem armazenadas, transmitidas, editadas, completamente ou parcialmente deletadas, as informações devem ser verdadeiras e confiáveis. Também garantir que as mesmas não sejam alteradas por usuários não autorizados.

- Disponibilidade é garantir que as informações estejam disponíveis quando for necessária sua utilização, seja por uma pessoa ou processo dentro de uma organização, a indisponibilidade de uma informação importante pode causar a inoperabilidade de um processo, ou talvez de toda a organização (DANTAS, 2011).

Porém, para que se consiga essa tríplice garantia da segurança da informação, é necessário grande esforço da organização como um todo, como afirma Fontes

(2008, p.6): “A proteção da informação exige dedicação de recursos financeiros, de tempo e de pessoas.”.

A segurança da informação existe para toda organização, não somente grandes empresas, mas também instituições públicas e ou usuários domésticos, pois as ameaças se encontram em qualquer lugar, inclusive nas IES. Por isso é necessário angariar recursos e proteger adequadamente a informação que foi classificada como relevante, tornando-a menos vulnerável. Com isso, o próximo capítulo trará um breve conceito de medidas de segurança.

2.4 MEDIDAS DE SEGURANÇA

É necessário explanar sobre as medidas de segurança da informação, pois é com sua aplicação aos sistemas, é que se alcança a confidencialidade, integridade e disponibilidade, que são os objetivos da segurança da informação. Sêmola (2003, p.49) explica as medidas de segurança:

> “São as práticas, os procedimentos e os mecanismos usados para a proteção da informação e seus ativos, que podem impedir que ameaças explorem vulnerabilidades, a redução das vulnerabilidades, a limitação do impacto ou minimização do risco de qualquer outra forma.”

Depois da definição dada, Sêmola (2003) explica as medidas de segurança, as quais são aplicáveis para que se diminuam os riscos e impactos dos incidentes de segurança da informação, segundo ele as medidas de segurança se categorizam como.

- Preventivas, que são medidas de segurança que visam evitar a ocorrência dos incidentes, e objetivam, por meio de mecanismos, manterem uma segurança da informação já implementada, como por exemplo: Políticas de segurança, instruções e procedimentos de trabalho, palestras de conscientização, treinamento de colaboradores, plano de continuidade de negócios (planejamento).

- Detectáveis, que são medidas de segurança que tem como objetivo identificar condições e indivíduos causadores de ameaças, para que se evite que elas

explorem alguma vulnerabilidade existente, como por exemplo: Análise de riscos, sistema de câmeras de vigilância, alarmes.

- Corretivas, que são ações de medidas de segurança que tem por objetivo, reparar um sistema que já esteja danificado, por sua vez, essa medida acontece quando já houve o incidente de segurança e a quebra da mesma, como por exemplo: Restauração de *backup*, plano de resposta de incidentes, plano de continuidade de negócios (aplicação).

Segundo Sêmola (2003), algumas medidas podem pertencer à categorias diferentes, como foi visto acima. O plano de continuidade de negócios, em sua fase de planejamento e criação, tem as características de medida preventiva, e em uma provável aplicação desse plano, as características passam a ser uma medida corretiva.

Partindo do princípio de que para uma organização, seja ela de grande ou pequeno porte, ou qualquer segmento, é de suma importância que o negócio seja contínuo. A próxima seção, trata sobre os riscos, e a gestão de riscos para que a probabilidade dele acontecer seja controladamente a menor possível.

2.5 GESTÃO DE RISCO

Observa-se que as ameaças e vulnerabilidades no meio tecnológico, existem e querem de alguma forma danificar os sistemas, e o possível encontro destes fatores, gera um risco para a organização. A ABNT ISO IEC 27002:2005 (ABNT, 2005, p.2) diz que risco é “combinação da probabilidade de um evento e de suas consequências.”. No qual evento seria uma ocorrência em um sistema que quebre a segurança do mesmo.

Já para Sêmola (2003, p.50) risco é “Probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios.”. Ou seja, o risco, diretamente se relaciona com a possível quebra, de um ou mais pilares da

segurança da informação, na probabilidade de uma ameaça, encontrar uma fragilidade compatível.

Segundo Dantas (2011, p. 41), conceitua:

> "O risco é compreendido como algo que cria oportunidades ou produz perdas. Com relação à segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas. É medido pela possibilidade de um evento vir a acontecer e produzir perdas."

Seguindo esse conceito, deve-se lembrar que o risco se relaciona com as inúmeras ameaças e vulnerabilidades, que possibilitam a quebra de segurança de um sistema, e também, relaciona-se com a probabilidade que isso aconteça, e as consequências disso.

O número e tipos de ameaças existentes são incontáveis e crescentes, por isso, a segurança necessita de recursos, criatividade dos profissionais, e determinação, para que os riscos sejam diminuídos a um nível aceitável que possa ser gerenciado.

Por esta gama de riscos ser muito grande, não se pode proteger o sistema contra tudo, por isso, existe a priorização dos riscos, que é o tempo gasto, recursos técnicos e financeiros em riscos considerados prioritários para o negócio, já outros riscos, pode-se gastar menos esforços, como terceirizar os riscos, delegar os riscos, adquirir seguros, até mesmo, não fazer nada, e aceitar alguns riscos. Os riscos que ficam fora de sistemas de controle são chamados de riscos residuais (PFLEEGER; PFLEEGER; MARGULIES, 2015)

Sêmola (2003, p. 55), diz que cada organização deve equacionar seus riscos:

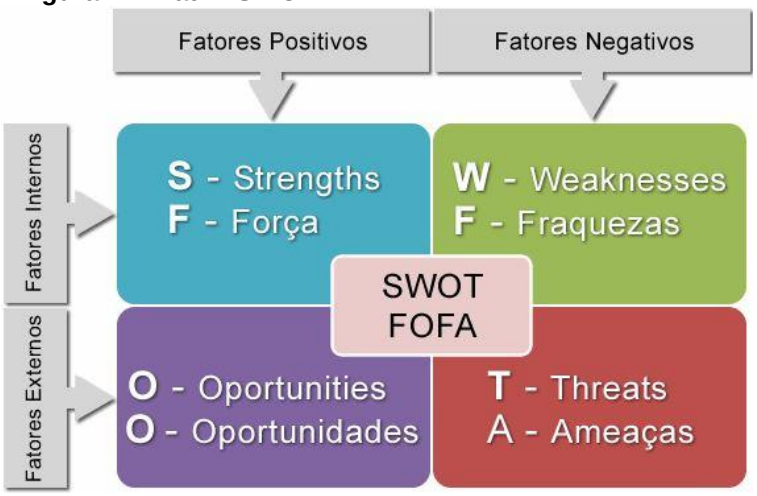
> "Cada negócio, independente de seu segmento de mercado e seu core business, possui dezenas, talvez centenas, de variáveis que se relacionam direta e indiretamente com a definição do seu nível de risco. Identificar estas variáveis passa a ser a etapa do desafio."

Para ajudar as instituições a equacionar suas variáveis, existe um conceito chamado de análise SWOT (*strenghts, weakness, opportunities, threats*), ou FOFA

(forças, oportunidades, fraquezas, ameaças) que propõe uma estratégia para as organizações adequar suas capacidades internas e possibilidades externas. Uma técnica que lista e avalia os pontos fortes (*Strenghts*), e fracos (*Weakness*), da instituição, e também, as oportunidades (*Opportunities*), e as ameaças (*Threats*), do ambiente que a cerca. Os pontos fortes e fracos, são variáveis que as organizações possuem internamente e que ajudam ou atrapalham o alcance dos objetivos. Já as oportunidades e as ameaças são variáveis externas que podem ou não, potencializar ou diminuir os sucessos da mesma (DANTAS, 2011).

A Figura 4 mostra um exemplo de uma matriz de análise SWOT:

Figura 4 – Matriz SWOT.



Fonte: De Paula (2015)

A análise da matriz SWOT é utilizada em uma organização para entendê-la, tanto interna quanto externamente, mas para Dantas (2011, p.50):

> "Essas quatro variáveis formam um cenário bastante utilizado para se compreender o ambiente organizacional, tanto interno quanto externo. Contudo, a compreensão do cenário não deve ser limitada ao emprego da noção SWOT, pois ao final dessa análise tem-se uma fotografia da situação, que é estática, e como sabemos, o ambiente é mutável e oscila de acordo com variáveis que surgem a cada dia."

Portanto, o cenário que a análise da matriz SWOT traz, é um resultado momentâneo, por isso, os profissionais não devem se limitar a essa análise, pois as variáveis nela contidas podem sofrer alguma mudança. Mas sim, utilizar os dados contidos nessa análise para conhecer e estudar melhor os fatores externos, como as ameaças que rondam a instituição.

Uma vez que as ameaças foram identificadas, os riscos devem ser avaliados baseados nessas ameaças, pois cada risco é a combinação entre ameaça explorando uma vulnerabilidade compatível, resultando em danos e quebra de segurança, baseado nessa análise, a defesa da instituição deve ser estrategicamente elaborada (RHODES-OUSLEY, 2013).

Mas existem outras técnicas para que a instituição consiga medir suas variáveis de risco. Uma dessas técnicas é estabelecer níveis dessas variáveis, como, consequências e possibilidades, pois, em geral, com a relação desses parâmetros, podem-se avaliar os riscos, e por consequência, priorizá-los com base em seus respectivos níveis de aceitabilidade. A Tabela 1 mostra um exemplo de níveis de consequências. (DANTAS, 2011).

Tabela 1 – Exemplo de níveis de consequências.

Nível	Descrição	Tipos
1	Insignificante	Nenhum prejuízo na imagem, perdas financeiras irrelevantes, sem impactos sobre os negócios
2	Menor	Pequenos efeitos e facilmente reparados, ações preliminares para tratamento, solução imediata local, perdas financeiras médias
3	Moderado	Efeitos sobre algumas atividades de negócios, possui solução local com ajuda externa, perdas financeiras moderadas
4	Maior	Grandes abalos na imagem, interrupção temporária da atividade de negócio, ajuda externa para tratamento, perdas financeiras elevadas
5	Catastrófico	Morte, interrupção total das atividades, solução externa, danos de difícil reparação, perdas financeiras elevadas

Fonte: Dantas (2011)

Também, é necessário identificar as possibilidades do risco, a Tabela 2 exemplifica os níveis de possibilidades.

Tabela 2 – Níveis de possibilidades.

Nível	Descrição	Tipos
A	Frequente	É esperado que ocorra em mais circunstâncias – possibilidades de incidentes repetidos
B	Provável	Provavelmente ocorrerá em mais circunstâncias – possibilidade de incidentes isolados
C	Ocasional	Poderá ocorrer em algum tempo- possibilidade de algumas ocorrências
D	Remota	Ocorrerá alguma vez – ocorrência pouco provável
E	Improvável	Ocorrerá em circunstâncias excepcionais – praticamente impossível

Fonte: Dantas (2011)

Ainda segundo Dantas (2011), é importante se adotar uma matriz de risco para ilustrar melhor e visualizar a relação entre possibilidades e suas consequências, ajudando assim, a mensurar os riscos mais prioritários. A Tabela 3 exemplifica uma matriz de riscos.

Tabela 3 – Matriz de riscos.

	Consequências				
Possibilidade	Insignificante 1	Menor 2	Moderado 3	Maior 4	Catastrófico 5
A (Frequente)	A	A	E	E	E
B (Provável)	M	A	A	E	E
C (Ocasional)	B	M	A	E	E
D (Remota)	B	B	M	A	E
E (Improvável)	B	B	M	A	A

Fonte: Dantas (2011)

Para Rhodes-Ousley (2013), o objetivo de uma gestão de riscos é mitigá-los, porém mitigar os riscos não significa eliminá-los por completo, mas sim, reduzi-los até um nível aceitável, como aceitar os riscos que geram menos consequência é uma das opções para os profissionais de segurança, é necessário confrontar a prioridade dos riscos com os níveis de aceitabilidade dos mesmos, que devem ser definidos pela instituição. A Tabela 4 demonstra os níveis de aceitabilidade dos riscos segundo Dantas (2011).

Tabela 4 – Níveis de aceitabilidade dos riscos.

Risco extremo (E)	Inaceitável- requer ação corretiva imediata
Risco alto (A)	Inaceitável - requer ação corretiva imediata com atenção específica da direção
Risco moderado (M)	Inaceitável- requer monitoramento, ações de mitigação e revisão dos controles pelo gerente Aceitável – requer a revisão e autorização do gerente
Risco baixo (B)	Aceitável- requer procedimentos de rotina

Fonte: Dantas (2011)

A gestão e a análise dos riscos são parte importante para as organizações, pois com isso pode-se tomar melhores decisões, e alimentar as ações necessárias

em uma possível necessidade de continuidade de negócio, pois a seguir será apresentada a norma própria para a GCN, a ISO 22301 feita pela ABNT em 2013.

2.6 ABNT NBR ISO 22301:2013

As organizações, incluindo as IES, necessitam que seus negócios estejam em operação para que não sofram com interrupções inesperadas, e caso isso aconteça é indispensável um planejamento de recuperação com custo e prazo aceitáveis, e para isso, a organização precisa ter um PCN, que é um processo existente na GCN.

A GCN é uma medida importante em segurança da informação, tanto que existe um próprio padrão na ABNT, o ISO 22301:2013, Segurança social – Sistemas de gestão da continuidade de negócios – Requisitos. Com esta norma, as organizações podem fazer melhorias e estruturar seus sistemas de GCN.

Palavras da própria ABNT, em seu catálogo, sobre a norma NBR ISO 22301:2013 (ABNT, 2013).

> “Esta Norma de gestão da continuidade de negócios especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se proteger, reduzir a possibilidade de ocorrência, preparar-se, responder a e recuperar-se de incidentes de interrupção quando estes ocorrerem.”

Esta norma está em vigor, e pode ser considerada uma atualização da *British Standards* (BS) 25999-2, mas na verdade ela a substitui, tendo como maior diferença entre elas a parte de gestão do padrão, onde a ISO 22301 dá mais ênfase na compreensão dos requisitos, definição de objetivos e na medição de desempenho, para que a organização se recupere da melhor forma (ADVISERA, 2016).

O maior benefício da GCN é que, se executada corretamente, a instituição diminui a probabilidade de ter os negócios interrompidos com um incidente em seus sistemas de informação, e mesmo que ele aconteça, a instituição estará preparada para responder ao mesmo. Para sua implementação, a ISO 22301 conta com 11

(onze) seções, divididas em 38 (trinta e oito) capítulos e subcapítulos, sendo alguns deles:

- Geral: Explicativa sobre a norma em si e seu intuito corporativo, seu conteúdo e aplicações.

- O modelo *Plan – Do – Check – Act* (PDCA): Capítulo que explica sobre o modelo PDCA, como utilizá-lo dentro da implementação.

- Contexto da Organização: Onde é mostrado a importância de conhecer a instituição onde a norma será implementada.

- Política: Toda a organização, inclusive a alta direção, deve estar alinhada com a política de continuidade da instituição.

Entre outros assuntos abordados pela norma, que visam planejar uma gestão de continuidade saudável para a instituição.

Com embasamento na norma acima citada, observa-se a importância da GCN dentro da TI, e as organizações tendo em vista a continuidade de suas operações, podem utilizá-la como padrão, e implementá-la. O próximo capítulo trará mais sobre GCN, seus termos e definições.

2.7 GESTÃO DA CONTINUIDADE DE NEGÓCIOS (GCN)

A GCN é um processo importante para qualquer organização, pois, com esse planejamento e gerenciamento correto, os incidentes decorrentes de quebra de segurança, causarão menores danos à mesma. Sêmola (2003, p.99) diz que "Segundo o DRI – *Disaster Recovery Institute*, de cada cinco empresas que possuem interrupção nas suas operações por uma semana, duas fecham as portas em menos de três anos."

Segundo a norma citada anteriormente, ISO 22301 (ABNT, 2013, p.2):

> "A continuidade de negócios contribui para uma sociedade mais resiliente. É possível que seja necessário envolver no processo de recuperação a comunidade em geral, assim como outras organizações e função do impacto no ambiente organizacional."

Como visto acima, para se ter uma sociedade mais resiliente através de uma gestão de continuidade de negócios, toda a comunidade deve estar engajada nessa causa. Assim como em uma organização, a GCN não é fator exclusivo da área de TI.

Fontes (2008, p.80) diz que, “o envolvimento e posterior comprometimento das diversas áreas com a segurança da informação permite que situações que dificilmente seriam identificadas possam ser apontadas e avaliadas.”

De acordo com Marinho (2008), o conceito de que a continuidade de negócios era exclusivo para a área de TI, já foi verdadeiro, quando surgiram os primeiros planos para diminuir o tempo de interrupção dos *mainframes*, pois naquela época, os custos com manutenção dos recursos de informática eram muito altos, e exigia que os profissionais reduzissem o tempo de indisponibilidade. Com o tempo, o PCN começou a ser utilizado em outras áreas de importância para o negócio, e atualmente, funciona para a recuperação de desastres em componente e contingências de processos.

Segundo Fontes (2008, p.86):

> “Mais do que planos de contingência para o ambiente computacional, a organização precisa da continuidade do seu negócio. Evidentemente que para isto o ambiente computacional e de tecnologia são fundamentais. Mas, o mote principal deve ser a continuidade do negócio e não simplesmente a recuperação dos sistemas de informação e computadores. Contemplar pessoas, processos e ambiente físico é fundamental.”

E por ser um conjunto de processos complexos, que envolvem a instituição como um todo, e a norma NBR ISO 22301 (ABNT, 2013) considera a GCN um sistema, e deve ser planejado, para que na sua execução não exista imprevistos. De início, a norma indica a utilização do modelo PDCA para a elaboração do sistema de gestão da continuidade de negócios (SGCN).

Segundo a ABNT NBR ISO 22301 (ABNT, 2013, p.3):

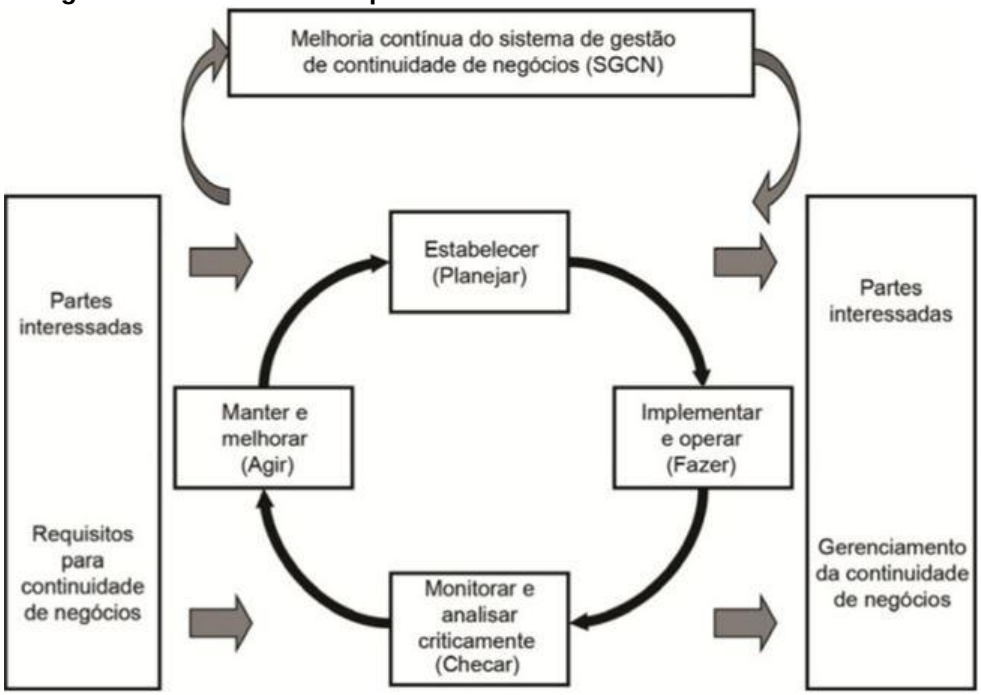
> “Esta norma adota o modelo *“Plan-Do-Check-Act”* para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente,

manter, e melhorar continuamente a eficácia de um SGCN de uma organização.

Isto garante um grau de consistência com outras normas de sistema de gestão [...] suportando assim a implementação consistente e integrada e a operação com sistemas de gestão relacionados."

A Figura 5 demonstra o modelo PDCA.

Figura 5 – Modelo PDCA aplicado a SGCN.



Fonte: ABNT (2013)

A Tabela 5 explica as etapas do modelo P (estabelecer), D (implementar e operar), C (monitorar e analisar criticamente), A (manter e melhorar):

Tabela 5 – Explicação do modelo PDCA.

Plan (Estabelecer)	Estabelecer uma política de continuidade de negócios, objetivos, metas, controles, processos e procedimentos pertinentes para a melhoria da continuidade de negócios de forma a ter resultados alinhados com os objetivos e políticas gerais d a organização.
Do (Implementar e operar)	Implementar e operar a política de continuidade de negócios, controles, processos e procedimentos.
Check (Monitorar e analisar criticamente)	Monitorar e analisar criticamente o desempenho em relação aos objetivos e política de continuidade de negócios, reportar os resultados para a direção para análise crítica, e definir e autorizar ações de melhorias e correções.
Act (Manter e melhorar)	Manter e melhorar o SGCN tomando ações corretivas e preventivas, baseadas nos resultados da análise crítica pela Direção e reavaliando o escopo do SGCN e as políticas e objetivos de continuidade de negócios.

Fonte: ABNT (2013).

Ainda seguindo os conceitos da ABNT (2013), a NBR ISO 22301 reforça alguns pontos, os quais são essenciais para que as instituições consigam gerenciar a continuidade de seus negócios, como:

- Compreender as necessidades da instituição, e a importância de se estabelecer os objetivos e uma política para a GCN;

- Aplicar e operar controles e medidas para eventos de quebra na segurança da informação;

- Monitorizar e avaliar criticamente o desempenho do sistema de GCN;

- Aprimorar continuamente os processos.

Além desses pontos, a ABNT (2013) recomenda que para uma GCN mais eficaz é recomendado que se tenha a definição de papéis e responsabilidades, com pessoas e equipes, capazes de gerenciar a continuidade do negócio, e também com a autoridade necessária para a tomada de decisão.

Para a delegação dessas responsabilidades, pode-se utilizar a matriz RACI (responsável, autoridade, consultado, informado). Segundo Palma (2013), “RACI é uma ferramenta utilizada para atribuição de responsabilidades, dentro de um determinado processo, projeto, serviço ou mesmo no contexto de um departamento.”. Dentro dessa matriz temos os termos.

Responsável (R) é a pessoa ou equipe responsável por executar o processo ou atividade. Autoridade (A) é a pessoa ou equipe dona do processo ou atividade, somente podendo existir uma autoridade para cada linha da matriz. Consultado (C) é a pessoa ou equipe a ser procurada caso haja necessidade de aconselhamento ou maior conhecimento no processo ou atividade. Informado (I) é a pessoa ou equipe que deve ser informada ao fim da atividade ou processo. A Tabela 6 exemplifica uma matriz RACI.

Tabela 6 – Exemplo de matriz RACI

	Dono do processo	Analista 1	Técnico	Analista de Qualidade
Atividade 1	A/R	C	I	C
Atividade 2	A	R	I	C
Atividade 3	A	R	I	I
Atividade 4	A	C	I	R
Atividade 5	A	R	I	I

Fonte: Palma (2013)

Como foi citada acima, a GCN é um sistema, composto por processos, conforme Marinho (2008, p.6) “não se limita a um, dois ou a um conjunto de componentes ou processos. Ela pode ser implementada em qualquer situação ou ambiente que exija redução no tempo de resposta a eventos.”. Dentre eles, está o PCN, e o plano de contingência. Ainda segundo Marinho (2008), é comum, profissionais e gestores confundirem o conceito desses planos, especialmente em áreas relacionadas a TI, alguns acreditam que possuir uma contingência, já é o bastante para garantir a continuidade dos negócios em uma eventual interrupção. Por isso, a seguir conceitos de plano de contingência e PCN.

2.7.1 PLANO DE CONTINGÊNCIA

Para Sêmola (2003, p.103), o plano de contingência deve estar direcionado para os interesses da instituição. De acordo com ele os planos “são desenvolvidos para cada ameaça considerada em cada um dos processos do negócio pertencente ao escopo, definindo em detalhes os procedimentos a serem executados em estado de contingência”.

Segundo Fontes (2008), o plano de contingência é traçado para acontecimentos onde existe perda de recursos, porém esses recursos podem ser retomados de uma maneira que cause menor dano para a instituição, como por exemplo, ter dois servidores com um mesmo serviço, no caso da parada de um deles, o outro assume suas funções. Para a contingência das instituições, existem algumas estratégias que podem ser utilizadas como forma de se ter a redundância necessária, como:

- *Hot-site*, estratégia “quente”, a qual deve estar pronta para entrar em operação e assumir os serviços assim que ocorrer uma interrupção. Essa estratégia se aplica quando o tempo de tolerância é mínimo. Aplicado a um servidor de banco de dados, por exemplo, o tempo tolerado seria de milissegundos.

- *Warm-site*, esta estratégia se aplica a recursos com maior tolerância de tempo de paralisação, podendo haver maior indisponibilidade do mesmo, até a atividade retornar ao funcionamento. Como por exemplo, um serviço de envio e recebimento de emails, que pode ficar parado por minutos.

- Realocação de operação, como o próprio nome diz, esta estratégia tem como objetivo mudar a atividade atingida pelo incidente, para outro local, seja um ambiente físico, equipamento ou link, que pertencem à mesma instituição, sendo possível, somente com a existência de “folga” de recursos que podem ser alocados em situações de interrupção. Um exemplo é um tráfego de dados redirecionados de um roteador com problema para outro roteador.

- *Bureau* de serviços é uma estratégia que considera a possibilidade de transferir as atividades em questão para um ambiente terceirizado, requerendo assim, um tempo maior para a transferência da mesma.

- Acordo de reciprocidade, onde organizações que possuam infraestrutura, tecnologia e humana semelhantes, propõem um acordo formal entre si para uma alternativa de continuidade operacional.

- *Cold-site*, é uma alternativa de contingência partindo de um ambiente com infraestrutura física e comunicação mínimas, desprovido de recursos de processamento de dados, portanto, é aplicável a ocorrência com tolerância de perda de disponibilidade maior ainda.

- Auto-suficiência, que na verdade, é uma estratégia impensada, na qual muitas vezes, é a melhor, ou a única opção de contingência para certos recursos. Ela ocorre quando nenhuma outra estratégia se mostra aplicável, pelo motivo dos impactos não serem significativos, ou pela falta de recursos financeiros ou técnicos.

A instituição deve estar disposta a correr os riscos, por isso a analise dos mesmos serve como subsidio para a escolha dessa estratégia (SÊMOLA, 2003).

Como foi visto, têm-se várias estratégias de contingência existentes para a continuidade do negócio, mas não somente um plano de contingência garante isso. Como dito por Marinho (2008, p.3): “Uma empresa inteira duplicada, não vai funcionar como a original, se as pessoas que executam suas atividades não estiverem comprometidas ou treinadas para atuar em cenários de contingência e continuidade”.

2.7.2 PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

O PCN, assim como o plano de contingência, faz parte de um sistema maior chamado GCN, e é uma forma das instituições conseguirem uma garantia de que as atividades sigam em funcionamento em caso de incidente de segurança.

Marinho (2008, p.126) conceitua PCN como:

> “É a metodologia que desenvolve estratégias alternativas para uma atividade de processos ou funcionamento de componentes de negócio, minimizando os possíveis impactos acarretados pela interrupção das atividades imposta por um evento indesejável e que ocasione algum tipo de perda financeira ou não.”

De acordo com a ABNT NBR ISO 22301 (2013, p.6), a definição de PCN é “procedimentos documentados que orientam as organizações a responder, recuperar, retomar e restaurar a um nível predefinido de operação após a interrupção.”

Segundo a PwC Brasil (2013), é preciso que haja uma mobilização de toda a organização para que a continuidade de negócios, no caso da ocorrência de um evento, e ainda conceitua: “um plano de continuidade (PCN) descreve as ações e processos necessários para recuperar as operações em caso de ruptura”.

O primeiro passo para a elaboração de um PCN é a vontade da empresa ou instituição, que tem que querer a construção desse plano. Independentemente do

motivo dessa vontade, ela precisa existir. Assim que a instituição resolve elaborar o PCN, e ele começa a fazer parte dos objetivos, deve-se iniciar o desenvolvimento desse plano (FONTES, 2008).

Ainda seguindo conceitos de Fontes (2008), são recomendados alguns passos para a elaboração de um PCN, são eles:

Definição do escopo e do cenário é a primeira etapa para a elaboração do plano, analisar os ambientes, recursos, ameaças e também as situações de interrupção que possam vir a causar descontinuidade nos negócios e necessitam constar no PCN, e tornar o plano inicial mais viável, e entender que um PCN completo para uma organização, só é possível com a junção de planos menores.

Avaliação de ameaças e riscos, que para Fontes (2008, p.93) “esta etapa não é obrigatória, porém é recomendável que ela seja executada.”. Levando em consideração o cenário, devem-se analisar as ameaças e os riscos, e a situação da instituição perante as mesmas.

Análise de impacto no negócio, uma etapa na qual, a instituição precisa reconhecer qual o potencial impacto caso um conjunto de recursos ou serviços sejam interrompidos. Não somente impactos financeiros são considerados, mas também, impactos operacionais ou de imagem para a instituição, e nesta etapa também se tem a noção do tempo de indisponibilidade que o negócio suporta.

Identificação de soluções, esta etapa se baseia nas informações colhidas nas etapas anteriores, e avaliam-se todas as alternativas existentes para que aconteça a continuidade dos negócios.

E por fim, a elaboração do plano, etapa na qual é construído um conjunto de manuais e documentos que formam o PCN e que deverão ser seguidos em caso de necessidade de contingência. Este plano deve conter instruções e atividades para que os envolvidos executem uma forma alternativa de seguimento nos negócios.

Assim também, conforme a ABNT NBR ISO 22301 (2013, p.26) diz que “A organização deve estabelecer procedimentos documentados para responder a incidentes de interrupção, e como irá continuar ou recuperar suas atividades dentro de um prazo pré definido.”. Segue alguns requisitos que para a ABNT (2013) são essenciais em um PCN:

a) Responsabilidades e funções definidas para pessoas e equipes com autoridade;

b) um processo que ativa a resposta ao evento ocorrido;

c) gerenciamento de imediato para impactos que podem piorar serviços prioritários;

d) detalhes sobre comunicação entre instituição e funcionários;

e) estratégias de como continuar ou recuperar os negócios e atividades prioritárias dentro do prazo.

Com os conceitos de PCN apresentados, assim como os outros conceitos dados anteriormente, pode-se iniciar a produção do estudo de caso do mesmo, que será apresentado no próximo capítulo.

3 ESTUDO DE CASO

3.1 CENÁRIO DO ESTUDO

Após a realização da pesquisa bibliográfica foi proposto um estudo de caso, com a aplicação dos conceitos sobre GCN aprendidos para a elaboração de um PCN de serviços importantes em uma IES.

O cenário de uma IES foi escolhido devido à diversidade de variáveis existentes nesse meio, como alunos, professores, gestores, cursos, implicações governamentais, sistemas de informação e ativos, eletrônicos ou não. E também por perceber que diversas instituições desse segmento não possuem um PCN, e assim como qualquer organização está sujeita a incidentes e interrupções e seus serviços, o que pode ser algo muito desastroso.

Neste trabalho não será especificada nenhuma IES, e sim, foi feito acerca de um conjunto de IES. As informações coletadas são oriundas de diferentes instituições públicas e privadas, e serão analisadas e processadas com a intenção de identificar pontos em comum e que o PCN elaborado possa ser aplicado de forma genérica em qualquer IES.

3.2 MÉTODO DE PESQUISA

A pesquisa foi embasada em um questionário desenvolvido e enviado a profissionais de quatro diferentes instituições, que pode ser visto no Anexo A, e em suas respectivas respostas que podem ser vistas no Anexo B. Esse questionário foi desenvolvido e pensando para obter informações importantes sobre medidas de segurança, as ameaças que permeiam o cenário de uma IES, os riscos que a envolvem, e como a instituição se protege contra os malefícios, e as possíveis interrupções que possam vir a ocorrer para a mesma, assim como processo de backup, e continuidade tanto lógico quanto físico. As informações oriundas deste questionário ajudaram a entender como planejar e aplicar os conceitos de GCN a uma IES.

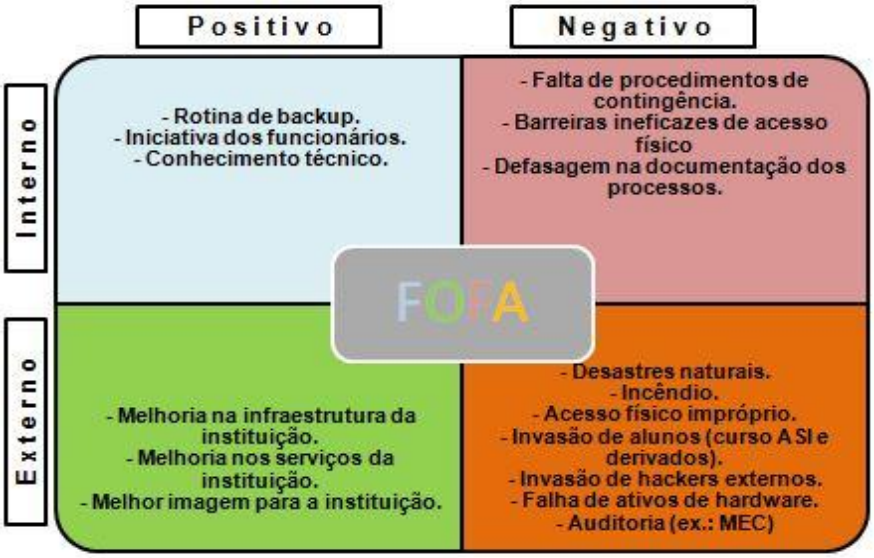
Por questões de privacidade, para não comprometer nenhum profissional e nenhuma instituição, neste trabalho não foram citados os nomes dos colaboradores, e nem das instituições de onde vieram tais informações. Apesar de o cenário de uma IES ser conhecido, as informações obtidas na pesquisa ajudam e são de grande importância para a confecção do PCN, visto que são profissionais que estão presentes em seu cotidiano.

3.3 ANÁLISE DA MATRIZ SWOT (FOFA)

A análise da matriz SWOT (FOFA) ajuda a conhecer as variáveis existentes dentro do cenário de IES, com base nas respostas obtidas do questionário, podem-se avaliar as forças, oportunidades, fraquezas e ameaças que se apresentam.

A Figura 6 corresponde à matriz FOFA em ambiente de IES.

Figura 6 – Matriz FOFA em IES.



Fonte: Autoria própria

Com a matriz acima se visualiza melhor as forças como rotinas de backup já existentes, iniciativa dos funcionários em melhorar serviços e processos, e por se tratar do cenário de IES, conhecimento técnico dos profissionais e professores. Oportunidades como melhoria na infraestrutura, melhoria no atendimento e serviços, e trazer uma imagem mais positiva para a instituição.

Fraquezas como falta de contingência, barreiras de proteção ineficazes e defasagem da documentação dos processos. Ameaças como desastres naturais, incêndio, acesso físico impróprio, alunos de cursos derivados da TI tentando invadir os sistemas, assim como invasões externas, e problemas com ativos físicos, com isso, pode-se obter informações para o entendimento dos riscos que permeiam este cenário para o gerenciamento dos mesmos.

3.4 ANÁLISE DOS RISCOS

Esta etapa é muito importante, pois nela se analisa os riscos inerentes ao cenário de IES, e recomenda-se que ela seja executada e as informações adquiridas sirvam de base para a elaboração do PCN. Com as fraquezas e ameaças vistas na análise da matriz FOFA, juntamente com as respostas do questionário, tem-se os seguintes riscos.

- Falha no sistema acadêmico (notas e faltas): A ocorrência desse risco afeta a todos dentro da instituição, professores, pois utilizam este sistema para o lançamento das notas e faltas e fechamento de semestre. Alunos, que utilizam o sistema para verificação das informações, e secretaria acadêmica, que usa o sistema no atendimento ao público.

- Falha no serviço de telefonia: Este risco, se ocorrer, impossibilita a secretaria acadêmica de realizar o atendimento ao público (alunos e clientes), além de afetar a comunicação entre departamentos da instituição.

- Acidente envolvendo alunos e professores: É um risco muito grave, que pode ocorrer devido a desastre natural, ou eventos involuntários, causando desgaste na imagem da instituição.

- Indisponibilidade nos laboratórios de aula: Risco que pode ocorrer de diversas formas, causando uma perda de aula para alunos e professores que utilizam os mesmos, visto que ocorreria uma inconsistência no conteúdo do plano de ensino a ser ministrado.

- Falha no sistema da biblioteca: Causa indisponibilidade nas informações disponíveis neste sistema, e se ocorrer uma perda ou corrupção de dados, perde-se o registro de empréstimo e devolução dos livros.

- Indisponibilidade do local da instituição: Pode ocorrer devido a desastre natural, ou outro evento, com risco de todo corpo de alunos ficarem sem aula por período indeterminado dependendo da gravidade do incidente.

- Falha na impressora e/ou falta de tinta na impressora da secretaria: Riscos que causam a impossibilidade de impressão de documentos importantes como atestados e declarações, que podem vir a impossibilitar um ex-aluno, ou professor de receber documentos oficiais, para concursos, pós-graduação, entre outros.

- Falha no sistema de arquivos (documentos): Pode causar perda ou indisponibilidade em documentos importantes para a instituição como históricos escolares, documentação de professores, documentos para auditoria, entre outros.

- Falta de professores para ministrar aulas: Um risco comum devido a vários fatores, como congressos, palestras, problemas de saúde etc. Causa a perda de aula para os alunos, que pode acarretar em inconsistência no conteúdo do plano de ensino da disciplina. A Tabela 7 demonstra os riscos acima citados.

Tabela 7 – Riscos, consequências e possibilidades.

	Riscos	Consequências	Possibilidade
1	Falha no sistema acadêmico (notas e faltas)	Maior	Remota
2	Falha no serviço de telefonia	Menor	Ocasional
3	Acidente envolvendo alunos e professores	Catastrófico	Improvável
4	Indisponibilidade nos laboratórios de aula	Insignificante	Remota
5	Falha no sistema da biblioteca	Menor	Remota
6	Indisponibilidade no local da instituição	Catastrófico	Improvável
7	Falha na impressora da secretaria	Menor	Provável
8	Falta de tinta na impressora da secretaria	Menor	Provável
9	Falha no sistema de arquivos (documentos)	Maior	Remota
10	Falta de professores para ministrar aulas	Menor	Remota

Fonte: Autoria própria

Com os riscos já apresentados, os mesmos foram enumerados aleatoriamente, com seus respectivos níveis de consequência e possibilidade definidos, a fim de servir informações necessárias para elaboração da matriz de riscos demonstrada na Tabela 8.

Tabela 8 – Matriz de risco em IES.

	Consequências				
Possibilidade	Insignificante	Menor	Moderado	Maior	Catastrófico
Frequente					
Provável		7 / 8 (A)			
Ocasional		2 (M)			
Remota	4 (B)	10 / 5 (B)		1 / 9 (A)	
Improvável					3 / 6 (A)

Fonte: Autoria própria

Com os riscos já devidamente distribuídos na matriz de risco, levando em consideração sua possibilidade de acontecimento e as consequências nos negócios caso ocorram, observa-se a relação entre essas medidas resultando no nível de aceitabilidade dos riscos, sendo eles, risco extremo (E) risco alto (A) são inaceitáveis e necessitam de ação corretiva imediata, risco moderado (M) pode ser inaceitável e requerer algum tipo de controle ou aceitável com a devida autorização, e o risco baixo (B) que é aceitável e controlado por procedimentos de rotina. A disposição dos riscos nos níveis de aceitabilidade é demonstrada pela Tabela 9.

Tabela 9 – Aceitabilidade dos riscos.

Risco Extremo (E)
Nenhum
Risco Alto (A)
Falha no sistema acadêmico (notas e faltas)
Acidente envolvendo alunos e professores
Indisponibilidade no local da instituição
Falha na impressora da secretaria
Falta de tinta na impressora da secretaria
Falha no sistema de arquivos (documentos)
Risco Moderado (M)
Falha no serviço de telefonia
Risco Baixo (B)
Indisponibilidade nos laboratórios de aula
Falha no sistema da biblioteca
Falta de professores para ministrar aulas

Fonte: Autoria própria

Levando em consideração essa análise de riscos, nota-se a inexistência de problemas tidos como riscos extremos, devido ao fato de que os riscos mais impactantes não ocorrem com a frequência necessária para receberem esse nível de aceitabilidade. Como já foi dito, a fase de análise de riscos fornece embasamento para próxima etapa, a elaboração do PCN.

3.5 ELABORAÇÃO DO PLANO DE CONTINUIDADE

A elaboração do PCN é parte importante para a GCN, assim como a reflexão sobre as contingências necessárias para os serviços e ativos mais críticos. Neste estudo, o processo de desenvolvimento pertence à etapa de planejamento do ciclo PDCA, visto anteriormente.

Lembrando também, que o PCN se encaixa como medida de segurança da informação corretiva, em caso de necessidade de ativação, mas neste caso, ele será exclusivamente uma medida de segurança preventiva, haja visto que é a etapa de desenvolvimento do PCN.

Conforme o referencial bibliográfico recomenda-se a delegação de funções, responsabilidades e autoridades para melhor organização das atividades e procedimentos pertencentes ao PCN, portanto esse será o primeiro passo para a elaboração do mesmo.

3.5.1 DELEGANDO FUNÇÕES

Entende-se que é importante para iniciar a elaboração de um PCN a definição de grupos que exercem papéis importantes dentro da gestão do PCN, como mostra a Tabela 10.

Tabela 10 – Definição de grupos.

Coordenador do plano	Grupo de atuação	Grupo de apoio
Diretor da instituição	Equipe de TI	Equipe de TI
	Secretaria	Secretaria
	Equipe de Manutenção	Equipe de Manutenção
		Professores

Fonte: Autoria própria

Cada um desses grupos tem suas atribuições dentro do gerenciamento do PCN, o coordenador do plano te como tarefas nomear pessoas para o plano, garantir documentação, disponibilizar recursos para o plano, entre outras. O grupo de atuação tem como tarefas planejar ações de resposta relacionadas à sua área, orientar o resto da equipe quanto aos procedimentos, entre outras. O grupo de apoio, como o próprio nome diz, garante apoio ao plano, executa tarefas de manutenção, entre outras.

As equipes pertencentes a esses grupos de apoio também entram como participantes na matriz RACI, para que na ocorrência de um risco, se tenha a definição de papéis e responsabilidades nas atividades e procedimentos necessários para a correção do mesmo, segue a Tabela 11.

Tabela 11 – Matriz RACI genérica.

	Direção	**Secretaria**	**Equipe de TI**	**Equipe de Manutenção**	**Professores**
Falha no sistema acadêmico	C	A / I	R		C
Acidente envolvendo alunos	A / I	R	C	C	I
Indisponibilidade no local da instituição	A / I	R	C	C	I
Falha na impressora da secretaria	I	A	R	C	I
Falta de tinta na impressora	C	A / I	R	C	
Falha no sistema de arquivos	I	I	R / A		C
Falha no serviço de telefonia	I	A / I	I / C	R	C
Indisponibilidade nos laboratórios			R / A	C	I / C
Falha no sistema da biblioteca	I	I	R / A		C
Falta de professores para as aulas	I	R / A			C

Fonte: Autoria própria

Depois de definidos os papéis das equipes para os possíveis riscos que podem acontecer, deve-se documentar as ações, procedimentos, e contingências necessárias para a retomada dos principais serviços de IES.

3.5.2 PROCEDIMENTOS E CONTINGÊNCIAS

Esta etapa apresenta ações a serem tomadas e sugestões de contingência para os riscos anteriormente citados, as equipes responsáveis pela execução dos procedimentos já foram definidas na primeira etapa de elaboração do PCN, portanto, na Tabela 12 se têm os procedimentos e contingências.

Tabela 12 – Procedimentos e contingências.

RISCO	PROCEDIMENTO	CONTINGÊNCIA
Falha no sistema acadêmico	1º Verificar o problema; 2º Restaurar o sistema; 3º Utilizar backup se necessário.	Manter backup do sistema acadêmico; Utilizar o diário de classe dos professores enquanto o problema persistir.
Acidente envolvendo alunos ou professores	1º Ligar imediatamente para o SAMU ou Bombeiros; 2º Informar o responsável pelo aluno ou professor sobre o ocorrido.	Neste caso não existe contingência, a secretaria deve ter um banco de dados com contatos de responsáveis pelos alunos e professores para fazer a notificação.
Indisponibilidade no local da instituição	1º Informar alunos e professores sobre a insdisponibilidade; 2º Ativar contingência.	Contrato de acordo de recíprocidade com outra IES.
Falha na impressora da secretaria	1º Verificar servidor de impressão; 2º Efetuar a troca por outra impressora; 3º Enviar a impressora falha para conserto.	Manter uma impressora funcionando no estoque.
Falta de tinta na impressora	1º Verificar estoque; 2º Efetuar troca do cartucho.	Manter cartuchos carregados no estoque.

RISCO	PROCEDIMENTO	CONTINGÊNCIA
Falha no sistema de arquivos	1º Verificar o problema; 2º Restaurar o sistema; 3º Utilizar backup se necessário.	Manter backup do sistema de arquivos; ter backup das máquinas virtuais para carregar em outro servidor.
Falha no serviço de telefonia	1º Verificar se o problema é local; 2º Acionar a fornecedora do serviço.	Utilizar email corporativo enquanto o problema persistir.
Indisponibilidade nos laboratórios	1º Verificar se há outro laboratório disponível; 2º Notificar os alunos sobre a troca ou perda da aula.	Outro laboratório, ou aceitação do risco.
Falha no sistema da biblioteca	1º Verificar o problema; 2º Restaurar o sistema; 3º Utilizar backup se necessário.	Manter backup do sistema da biblioteca; Utilizar um caderno para marcar os empréstimos enquanto o problema persistir.
Falta de professores para as aulas	1º Notificar os alunos sobre a perda de aula; 2º Informar a direção sobre a falta.	Consultar a disponibilidade de outro professor; aceitar o risco.

Fonte: Autoria própria

Como se pode ver na tabela de procedimentos e contingências proposta, cada risco tem ações a serem tomadas caso ocorram, e também contingências para que o serviço continue minimamente operacional, ou então o risco é aceito. E também observa-se que alguns procedimentos e contingências precisam de atuação externa, como por exemplo, corpo de bombeiros, serviço de atendimento móvel de urgência (SAMU), etc. Por isso, recomenda-se a documentação de contatos críticos.

3.5.3 PONTOS DE CONTATO CRÍTICOS

Observa-se que o planejamento e até mesmo a execução de um PCN, não depende somente de um único setor da instituição, e muitas vezes são necessários pontos de contato com organizações externas. A própria norma ISO 22301 (ABNT, 2013) possui uma sessão onde demonstra a importância da parte de ter a comunicação documentada para uma possível execução do PCN, por isso, segue

uma sugestão de como se documentar contatos críticos tanto externos quanto internos na Tabela 13.

Tabela 13 – Pontos de contato críticos.

CONTATOS INTERNOS				
SETOR	**CONTATO PRIMÁRIO**	**NÚMERO**	**CONTATO SECUNDÁRIO**	**NÚMERO**
Secretaria	nome	xxx-xxxx	nome	xxx-xxxx
TI	nome	xxx-xxxx	nome	xxx-xxxx
Biblioteca	nome	xxx-xxxx	nome	xxx-xxxx
Manutenção	nome	xxx-xxxx	nome	xxx-xxxx
Diretoria	nome	xxx-xxxx	nome	xxx-xxxx

CONTATOS EXTERNOS				
	CONTATO PRIMÁRIO	**NÚMERO**	**CONTATO SECUNDÁRIO**	**NÚMERO**
Bombeiros	nome	xxx-xxxx	nome	xxx-xxxx
SAMU	nome	xxx-xxxx	nome	xxx-xxxx
IES Parceira	nome	xxx-xxxx	nome	xxx-xxxx
Polícia	nome	xxx-xxxx	nome	xxx-xxxx
Empresa de Telecom	nome	xxx-xxxx	nome	xxx-xxxx

Fonte: Autoria própria

Nota-se que é importante obter um ponto de contato com a organização externa, uma pessoa específica que possa resolver o problema em caso de interrupção do serviço respectivo, para que as ações de retomada do serviço aconteçam com maior rapidez.

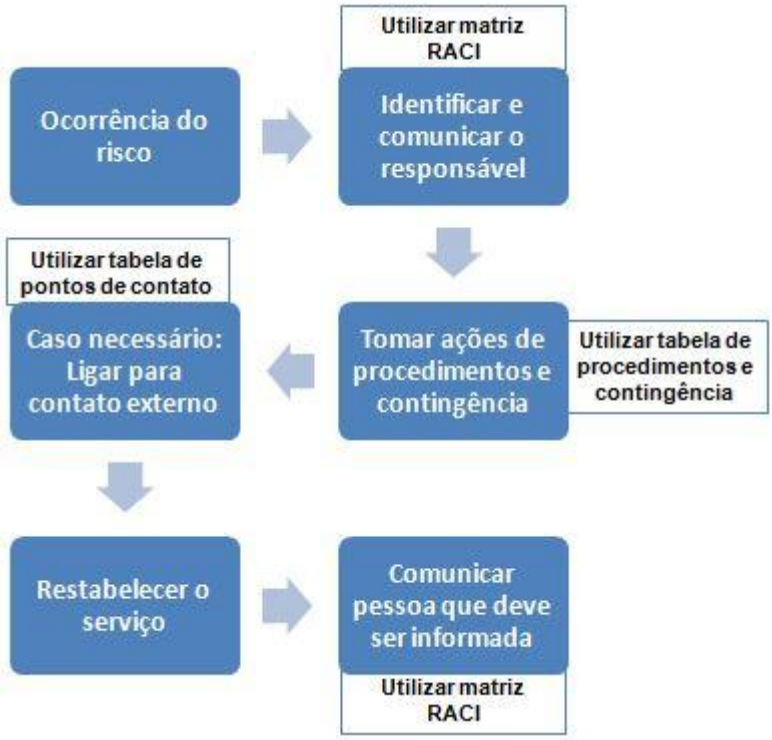
Essa tabela de pontos de contato críticos, assim como as tabelas da matriz RACI e a de procedimentos e contingências são utilizadas no fluxo do plano, caso ocorra um dos riscos já analisados.

3.5.4 FLUXO DO PLANO

Em caso de ocorrência do risco, a instituição deve ter conhecimento de como o PCN ocorre em suas etapas, e de como acontece a utilização das tabelas anteriormente citadas, com isso, se faz necessária a criação do fluxo do plano.

O fluxo demonstra as etapas do PCN desde a ocorrência do risco, até o restabelecimento e comunicação dos participantes que devem ser informados, e durante essas etapas, as tabelas construídas durante este estudo de caso, são usadas como referências para as mesmas, como exemplo, a tabela da matriz RACI, que documenta a pessoa ou equipe responsável por tomar ação para o problema acontecido, ou se necessário realizar um contato externo, utiliza-se a tabela de pontos de contato críticos, como pode ser visto na Figura 7.

Figura 7 – Fluxo do PCN.



Fonte: Autoria própria

Com esse fluxo do plano, e as etapas anteriormente elaboradas, juntamente com as tabelas e análises produzidas, a instituição pode ser capaz de dar continuidade a serviços importantes para seu negócio.

3.5.5 TRABALHOS FUTUROS

Com a complexidade de uma GCN e também a elaboração e desenvolvimento de um PCN, e tudo que envolve a continuidade de negócios, pode-se considerar como trabalhos a serem produzidos futuramente a adequação deste estudo de PCN para uma IES específica, como também a sua aplicação e teste dentro de um

ambiente específico. E também, dentro dessa IES, desenvolver e ministrar o treinamento dos colaboradores participantes do plano.

4 CONSIDERAÇÕES FINAIS

Durante o desenvolvimento deste trabalho, foi possível observar a importância dos conceitos e técnicas da GCN, assim como o PCN, devido ao fato de que nenhuma instituição, de grande ou pequeno porte, por mais medidas e recursos de segurança existentes, não está livre do sofrer interrupções pela ocorrência de riscos.

Durante os estudos realizados, notou-se que a informação atualmente é um bem da organização que a possui, por isso deve ser protegido, como qualquer outro ativo crítico, e deve estar disponível mesmo em caso de interrupção, por isso o PCN é altamente recomendável.

Notou-se também que a elaboração de um PCN é muito complexa, necessita de conhecimento do negócio a ser continuado, da organização como um todo, do entendimento do ambiente, dos processos mais críticos, e dos recursos a serem aplicados, além da vontade da instituição desenvolve-lo, para que assim não sofra com os incidentes de segurança. Observa-se também que a gestão de risco tem importante papel na construção do PCN, pois com ela, a instituição entende melhor os riscos que permeiam o ambiente da instituição, e pode se proteger melhor contra os mesmos.

Com o estudo de caso, foi possível perceber que a criatividade e a experiência do profissional que elabora um PCN é de suma relevância, pois ele deve pensar em como responder a riscos e incidentes sem que eles tenham acontecido, e com isso, proporcionar uma melhor segurança a instituição. O compromisso de toda a organização para fazer o PCN, e executá-lo caso seja necessário. A análise do cenário e do negócio a ser continuado. E a necessidade de documentação dos contatos críticos e do plano em si.

Por fim, pode-se dizer que a elaboração de um PCN uma IES, como qualquer outra organização, é muito vantajosa, mas requer recursos tanto técnicos, quanto de trabalho dos colaboradores, e que os setores da instituição se comuniquem constantemente, para que em case do acontecimento de alguma interrupção, o plano flua adequadamente.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT - AGÊNCIA BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2005**. Rio de Janeiro: ABNT, 2005.

_____. **NBR ISO/IEC 22301:2013**. Rio de Janeiro: ABNT, 2013.

ADVISERA.COM. **Fundamentos da ISO 22301**. Disponível em: <http://advisera.com/27001academy/pt-br/o-que-e-a-iso-22301/>. Acesso em: 10 mar. 2016.

ATAÍDE, Thiago C. **Segurança da informação para todos**. Disponível em: <http://seginfoparatodos.blogspot.com.br/2013/07/triade-seginfo.html>. Acesso em: 15 mar. 2016.

DANTAS, Marcus Leal. **Segurança da informação:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

DE PAULA, Gilles B. **Análise SWOT:** conhecendo as cartas do jogo e aumentando as chances de vitória de sua empresa. Disponível em: <http://www.treasy.com.br/blog/analise-swot>. Acesso em: 25 abr. 2016.

FONTES, Edison Luiz Gonçalves. **Praticando a segurança da informação**. Rio de Janeiro: Brasport, 2008.

G1.COM. **Exemplo de garra, mulheres de Bento Rodrigues voltam a produzir geléia**. Disponível em: <http://g1.globo.com/minas-gerais/desastre-ambiental-em-mariana/noticia/2016/03/exemplo-de-garra-mulheres-de-bento-rodrigues-voltam-produzir-geleia.html>. Acesso em: 23 abr. 2016.

G1.COM. **IBGE divulga números do acesso à internet móvel no Brasil**. Disponível em: <http://g1.globo.com/jornal-nacional/noticia/2015/04/ibge-divulga-numeros-do-acesso-internet-movel-no-brasil.html>. Acesso em: 23 abr. 2016.

G1.COM. **Tsunami no Japão: fotos mostram antes e depois de áreas destruídas.** Disponível em: <http://g1.globo.com/mundo/noticia/2016/03/tsunami-no-japao-fotos-mostram-antes-e-depois-de-areas-destruidas.html>. Acesso em: 24 abr. 2016.

JUNIOR, R. Kelly Rainer; CEGIELSKI, Casey G. **Introdução a sistemas de informação**. Rio de Janeiro: Elsevier, 2012

MARINHO, Fernando. **Como proteger e manter seus negócios:** um plano básico para contingências e continuidade nas empresas. Rio de Janeiro: Ciência Moderna Ltda., 2008.

MERKOW, Mark S.; BREITHAUPT, Jim. **Information security:** principles and practices. 2nd Ed. Indianapolis: Pearson, 2014.

PALMA, Fernando. **A matriz RACI é a solução dos seus problemas!**. Disponível em: < http://www.portalgsti.com.br/2013/04/matriz-raci.html>. Acesso em: 17 mai. 2016.

PFLEEGER, Charles P.; PFLEEGER, Shari L.; MARGULIES, Jonathan. **Security in computing**. 5th Ed. Indianápolis: Pearson, 2015.

PWC BRASIL. **Gestão da continuidade de negócios.** Disponível em: <http://www.pwc.com.br/en/gestao-de-riscos-corporativos-e-compliance/assets/folder-gestao-continuada-13.pdf>. Acesso em: 26 abr. 2016.

RHODES-OUSLEY, Mark. **The complete reference:** information security. 2nd Ed. New York: McGraw-Hill Education, 2013.

SÊMOLA, Marcos. **Gestão da segurança da informação:** visão executiva da segurança da informação aplicada ao *security officer*. Rio de Janeiro: Elsevier, 2003.

UOL NOTÍCIAS. **Petrobras confirma furto de dados sigilosos**. Disponível em: < http://economia.uol.com.br/ultnot/2008/02/14/ult4294u1023.jhtm>. Acesso em: 25 abr. 2016.

WAZLAWICK, Raul Sidnei. **Metodologia de pesquisa para ciência da computação**. Rio de Janeiro: Elsevier, 2009.

ANEXO A – QUESTIONÁRIO

QUESTIONÁRIO: PLANO DE CONTINUIDADE DE NEGÓCIOS

Q1. Quais ativos a instutuição têm que são prioritários e não podem sofrer interrupção? *(Ex.: ativos físicos como impressoras, servidores, projetores, e ativos lógicos como aplicações, base de dados, código fonte, etc...)*

Q2. Quais sistemas a instituição considera como prioritários? *(Ex.: web site, ERP, notas e faltas, sistema acadêmico, etc...)*

Q3. Quais dados/informação a instituição considera de alta criticidade?

Q4. Referente à questão acima existe uma rotina de backup para essa informação?

Q5. Se sim, qual a periodicidade da rotina? Qual a mídia de armazenamento do backup? *(Ex.: servidor NAS, Fita LTO, HD Externa, etc...)*

Q6. Em caso de perda de dados, existe um procedimento documentado a ser seguido?

Q7. E caso de falha de conexão com a internet, existe um procedimento formal documentado a ser seguido?

Q8. A instituição tem pontos de contato definidos em caso de incidente? *(Ex.: fornecedores de serviços, empresas de suporte especializado, autoridades legais, MEC, algum órgão educacional, etc..)*

Q9. A instituição tem pessoas chave em seus setores em caso de incidente?

Q10. A instituição tem algum plano de contingencia, caso ocorra algum desastre? *(Ex.: hot site, warm site, cold site, acordo de parceria, etc...)*

Q11. A instituição já sofreu algum incidente que interrompesse a continuidade do negócio?

Q12. Existe algum plano de continuidade de negócios na instituição, no qual, garanta a que a mesma continue operacional em caso de incidente ou desastre? *(Ex.: greve de professores, impossibilidade de alcance físico a instituição, etc...)*

Q13. A instituição aplica medidas de segurança da informação em seus sistemas? Se sim, quais?

Q14. A instituição conhece os riscos existentes em seus sistemas? se sim, quais são eles?

Q15. Em caso de indisponibilidade da utilização do local operacional, existe algum procedimento de utilização de outro local físico?

Q16. A rede de servidores se encontra separado da rede utilizada pelos alunos?

Q17. A Instituição reconhece as ameaças existentes em seu ambiente externo e interno? (ameaças naturais, físicas, humanas, etc...)

ANEXO B – RESPOSTAS

Tabela 14 – Respostas do questionário.

Questão	Instituição	Resposta
Q1	A	Servidores, sistema ERP, web page
	B	Nossos ativos são exatamente estes citados no exemplo acima: impressoras, servidores, projetores, e ativos lógicos como aplicações, base de dados, código fonte.
	C	Impressoras, Servidores e base de dados
	D	Servidor de impressão, backups das VMs, impressora da secretaria, servidor de arquivos, entre outros..
Q2	A	ERP, sistema acadêmico
	B	Nosso ERP (TOTVS) que é responsável por todo nosso financeiro. O sistema ITL que cuida do pedagógico (notas e faltas)
	C	O ERP (TOTVS) que todo os sistemas integrados.
	D	Sistema acadêmico de notas e faltas, sistema da biblioteca, sistema de arquivos.
Q3	A	Informações fiscais, histórico acadêmico,
	B	Nossa base de dados (SQL SERVER), arquivos gerados durante o dia no servidor de arquivos (planilhas, docs. e etc.)
	C	Tudo o que for relacionado principalmente ao aluno
	D	Notas e faltas, histórico escolar, documentos da instituição.
Q4	A	Sim
	B	No SqlServer existe um JOB que todos os dias as 00:00hs ele realiza um backup automático das bases. Os demais itens são feitos manualmente utilizando um arquivo .BAT para os dados da rede.
	C	Sim.
	D	Rotina de backup diária, salva em fita.
Q5	A	Diária. Servidor e HD externo
	B	Todos os dias no final do expediente para os arquivos da rede e as 00h00min para a base de dados. Sempre em HD externo.
	C	Os backups acontecem diariamente em HD Externa vinculada ao servidor principal.
	D	Diária em fita.
Q6	A	não
	B	Em documento não, apenas um acordo entre nós para recuperar o ultimo backup. No HD externo guardamos pelo menos os últimos 10 backups.
	C	Não
	D	Em alguns casos sim, o time de TI possui uma wiki, mas está desatualizada.

Q7	**A**	Não
	B	Existe sim, temos dois links de internet e caso um caia um procedimento é executado para subir o outro.
	C	Não
	D	Não, mas existe um número de telefone de um funcionário da empresa fornecedora.
Q8	**A**	Não
	B	Sim, Empresa responsável pela rede, internet, telefonia e MEC por se tratar de uma instituição de ensino.
	C	Sim
	D	Somente este do link da internet acima citado.
Q9	**A**	Sim
	B	Sim
	C	Sim
	D	Não.
Q10	**A**	Não
	B	Infelizmente não
	C	Não
	D	Não, mas a instituição possui uma equipe que cuida do espaço físico.
Q11	**A**	Sim, queda de energia
	B	Sim, foram coisas como HD de servidor queimado.
	C	Não
	D	Sim
Q12	**A**	Não
	B	Não que eu conheça.
	C	Não
	D	Não.
Q13	**A**	Sim, controle de acesso, Backup
	B	Sim, como toda nossa informação funciona sobre a rede temos uma empresa especializada que cuida disso.
	C	Não
	D	Sim, autenticação, antivírus, rede dividida, entre outras.
Q14	**A**	Sim,
	B	Sim
	C	Não
	D	Alguns, como falha elétrica, desastres naturais, problemas de infraestrutura.
Q15	**A**	Não
	B	Sim
	C	Não
	D	Não que esteja ciente.

Q16	**A**	Sim
	B	Sim
	C	Sim
	D	Sim
Q17	**A**	Sim
	B	Sim
	C	Sim
	D	Sim.

Fonte: Autoria própria