PLANO DE RECUPERAÇÃO DE DESASTRES EM TI COM FOCO NO ERP

FURTADO NETO, João José [1]
MISAGHI, Dr. Mehran [2]

RESUMO

A segurança da informação tem como principal responsabilidade garantir a continuidade e minimizar o risco do negócio. O Plano de Recuperação de Desastres (PRD) é um plano de ação com objetivo de restaurar no menor tempo possível os serviços de Tecnologia da Informação (TI) que sustentam os processos críticos do negócio. Este trabalho tem como objetivo realizar um estudo de caso sobre a aplicação de um PRD baseado em normas e boas práticas de TI apresentadas, podendo ser usado como base para outras empresas. A metodologia aplicada neste trabalho trata-se de uma pesquisa exploratória seguida de um estudo de caso direcionado aos serviços de TI responsáveis por manter disponível o *Enterprise Resource Planning* (ERP) da empresa, para isso, foi necessário a realização das etapas de caracterização do ativo, identificar as ameaças, identificar as vulnerabilidades, determinar as probabilidades, análise de impactos e análise de riscos. Foi identificado que a empresa não possui um PRD, sendo necessário acionar os responsáveis para solucionarem os eventuais problemas que possam ocorrer. Desta forma, este artigo mostra que a implementação de um PRD minimiza os impactos de um desastre, criando a possibilidade de as empresas reagirem de forma adequada em casos de eventos negativos.

Palavras-chave: Plano de Recuperação de Desastres; Segurança da Informação; Tecnologia da Informação; Sistema de Gestão de Segurança da Informação.

1 INTRODUÇÃO

A economia moderna valoriza a aquisição, o processamento e o uso adequado da informação em todas as suas formas e formatos. A Tecnologia da Informação (TI) é responsável por saltos inovadores e melhorias no local de trabalho em vários setores do mercado e desempenha um papel crítico nas organizações empresariais (SISK, 2018). Uma pesquisa da Accenture mostra que 34% das empresas veem o departamento de TI como o principal impulsionador da inovação (NEWMAN, 2016).

[1] Graduando do Curso de Bacharelado em Sistemas de Informação do Centro Universitário UNISOCIESC, jjfurtadoneto@gmail.com;
[2] Professor Doutor em Engenharia Elétrica, Centro Universitário UNISOCIESC, mehran.misaghi@unisociesc.com.br;

Com o crescimento da competitividade do mercado, as empresas têm a necessidade de utilização de um sistema de informação, seja para auxílio no gerenciamento dos processos de negócio ou até mesmo para auxiliar nas tomadas de decisões. Por este motivo, as empresas passam cada vez mais a serem dependentes desses sistemas, tendo a responsabilidade de assegurar a disponibilidade do mesmo, tanto para manter os processos sempre disponíveis quanto para prestação de serviços críticos para os clientes.

Incidentes, falhas e sinistros podem acontecer com qualquer organização a qualquer momento, e como resultado, podem parar todas as operações de negócio por horas ou dias, ocasionando uma possível perda de receita e produtividade, com impacto negativo na confiança dos clientes. Ter um plano de ação em TI caso aconteça qualquer interrupção - seja ela causada por *hackers*, incêndio, falta de energia, desastre natural ou outro tipo de crise -, é extremamente importante para manter a rentabilidade de qualquer negócio (VELEZ, 2017).

A empresa onde esse projeto será aplicado não possui um Plano de Recuperação de Desastres (PRD), e, atualmente isto é indispensável para que os processos críticos da organização não fiquem indisponíveis, mantendo a normalidade das operações sem perder a competitividade no mercado. Todos os processos de negócios da empresa são gerenciados através de um único *Enterprise Resource Planning* (ERP), compras, vendas, faturamento, dados de clientes e fornecedores, estoque, chamados e outros processos e, caso venha a ocorrer algum tipo de desastre, a empresa não possui nenhum plano estratégico para disponibilizar rapidamente o ERP de forma que não prejudique os seus negócios. Melhor dizendo, se o ERP para a empresa também para.

De acordo com os dados disponibilizados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), o total de incidentes de segurança da informação reportados no Brasil vem crescendo desde 1999 com algumas quedas consideráveis, sendo em 2014 o ano em que foram reportados mais incidentes na história do Brasil. Houve uma queda nesse número em 2015 e 2016, entretanto, estes incidentes voltaram a subir em 2017 (CERT.BR, 2020).

Neste cenário, acredita-se que com a implementação de um PRD e seus devidos testes e treinamentos, o mesmo possui a capacidade de minimizar efetivamente as consequências negativas de um desastre se aplicado corretamente.

Aguiar Junior (2007) afirma que, a elaboração de um PRD é um meio o qual traz uma estratégia de recuperação pronta para as empresas no momento em que um incidente gere uma interrupção dos negócios, seja qual for o caráter deste incidente, natural, proposital ou mesmo acidental.

Este estudo surgiu a partir do seguinte problema de pesquisa: Realmente um PRD é eficaz para minimizar as interrupções dos negócios e restaurar rapidamente a normalidade das atividades? Sendo assim, buscando responder a referida questão, a presente pesquisa foi conduzida com o objetivo geral de realizar um estudo de caso sobre a aplicação de um PRD com foco no ERP, para redução dos efeitos resultantes de qualquer interrupção dos processos, garantindo o retorno da operação no menor tempo possível. Para que esse objetivo seja alcançado, criaram-se os seguintes objetivos específicos: estudar normas de TI; descrever Sistema de Gestão de Segurança da Informação (SGSI); explicar Gestão de Riscos; conceituar Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (PRD); avaliar estratégias de continuidade e; apresentar estudo de caso sobre a aplicação do PRD.

A metodologia aplicada neste trabalho trata-se de uma pesquisa exploratória, as estratégias de pesquisas utilizadas serão pesquisas bibliográficas, em livros, artigos científicos, dissertações e publicações. A pesquisa exploratória será seguida de um estudo de caso direcionado aos serviços de TI responsáveis por manter disponível o ERP da empresa, com a ideia de avaliar, classificar e desenvolver um PRD.

Esse trabalho está estruturado em quatro capítulos. Sendo este uma breve apresentação sobre o tema e apresentação do objetivo da pesquisa e sua justificativa, seguido por uma revisão bibliográfica sobre o PRD, bem como a base e os princípios para esta pesquisa, as etapas de aplicação do PRD e os procedimentos metodológicos adotados e, por fim, as considerações finais.

2 REFERENCIAL TEÓRICO

Neste capítulo são apresentados os embasamentos teóricos referente ao tema proposto, sendo eles: normas de TI, SGSI, gestão de riscos, PCN, PRD e estratégias

de continuidade. Desta forma, orientando para que o objetivo do trabalho seja alcançado.

2.1 NORMAS DE TECNOLOGIA DA INFORMAÇÃO

Uma norma tem a finalidade de harmonizar um conjunto de melhores práticas, levando em consideração estudos, históricos e conhecimentos operacionais, e deve ser aplicada para objetivos específicos. Cada organização tem o dever de determinar as melhores práticas que devem ser aplicadas (ABNT NBR ISO/IEC 27002, 2013).

Na Figura 1 são apresentadas algumas normas brasileiras e também do *National Institute of Standards and Technology* (NIST), ambas com relações a TI e que servirão de apoio no desenvolvimento do projeto, tanto para análises quanto para a elaboração do PRD.

Figura 1 – Principais normas relacionadas a TI

Fonte: O autor (2021).

a) ABNT NBR ISO 31000 (2018): estabelece princípios e orientações genéricas sobre gestão de riscos;
b) ABNT NBR ISO/IEC 22301 (2020): está relacionada a gestão da continuidade de negócios e é relevante a todos os modelos e tamanhos de organizações que tem como objetivo estabelecer, implementar, manter e melhorar o sistema de informação;
c) ABNT NBR ISO/IEC 27001 (2013): especifica requisitos para a implementação de controles de segurança adaptados para as necessidades específicas de organizações ou suas partes;

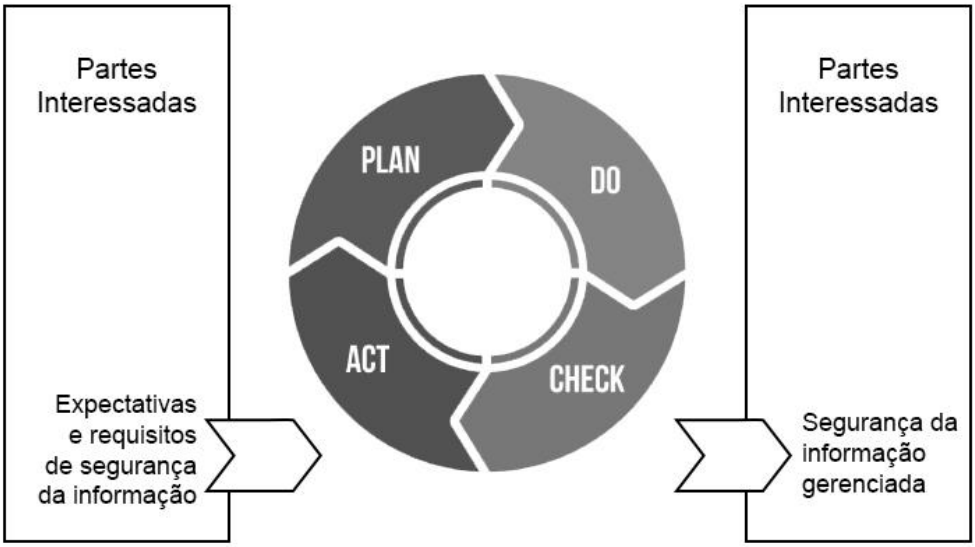
d) ABNT NBR ISO/IEC 27002 (2013): estabelece um guia prático para desenvolver os procedimentos necessários de segurança da informação e práticas de gestão da segurança da informação;
e) ABNT NBR ISO/IEC 27005 (2019): oferece as melhores práticas para o processo de gestão de riscos de uma organização, tratando particularmente os requisitos de um SGSI;
f) NIST SP 800-30 (2012): oferece orientações para a realização de avaliação de riscos dos sistemas de informação e organizações;
g) NIST SP 800-34 (2010): fornece orientações, recomendações e considerações para a contingência dos sistemas de informações;
h) NIST SP 800-37 (2018): apresenta diretrizes para execução do quadro de gestão de riscos para sistemas de informação com o objetivo de prover instruções para a realização das atividades de categorização, seleção, controle, implementação, avaliação, autorização e monitoramento dos controles de segurança.

As normas foram surgindo desde a criação e utilização dos primeiros ativos de TI, tendo como foco a segurança dos mesmos. Nas últimas décadas, estes modelos vêm tomando forma, sendo de origem própria ou até mesmo derivando e evoluindo de outros padrões. Sendo assim, a implementação da segurança da informação não é tendência, e sim uma necessidade determinada por normas e padrões técnicos.

2.2 SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

A norma ABNT NBR ISO/IEC 27001 descreve que a adoção de um SGSI deve ser uma decisão estratégica para uma organização, visto que a especificação e a implementação são influenciadas pelas suas necessidades e objetivos. É recomendável que a implementação de um SGSI seja escalonada conforme as necessidades da organização, por exemplo, um cenário simples exige uma solução de um SGSI simples (ABNT NBR ISO/IEC 27001, 2013). A norma, responsável por providenciar um modelo completo que trata desde o princípio até a melhoria contínua de um SGSI, faz a utilização da metodologia *Plan-Do-Check-Act* (PDCA), que é aplicada para estruturar todos os processos do SGSI.

Figura 2 – Plan-Do-Check-Act (PDCA)



Fonte: Adaptado de ABNT NBR ISO/IEC 27001 (2013).

As organizações, em busca de soluções de segurança da informação, devem seguir as diretrizes das normas nacionais e internacionais, projetar um SGSI de acordo com seus requisitos, aprovar a gestão e implementá-lo com ajuste contínuo para torná-lo efetivo no atendimento dos desafios dinâmicos de segurança e conformidade (DEY, 2007).

2.3 GESTÃO DE RISCOS

Para identificar as necessidades da organização em relação aos requisitos de segurança da informação e para criar um SGSI que seja eficaz, é necessária uma abordagem sistemática de gestão de riscos de segurança da informação (ABNT NBR ISO/IEC 27005, 2019).

Figura 3 – Diagrama de equação do risco de segurança da informação

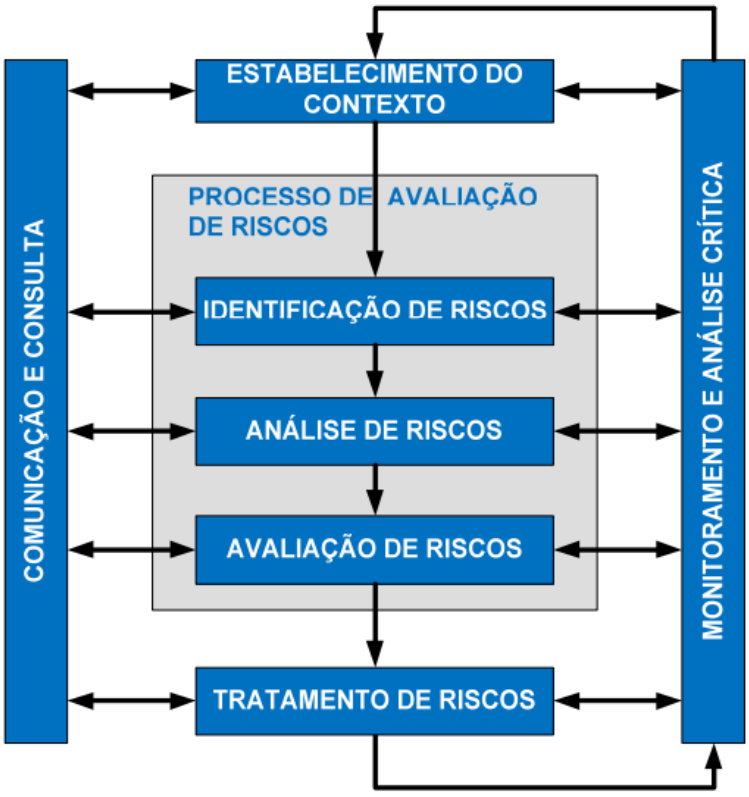
Fonte: Sêmola (2014).

Conforme visto na Figura 3, o risco é a hipótese de que as ameaças explorem as vulnerabilidades, causando impactos aos negócios. Esses impactos podem ser limitados por medidas de segurança, responsável pela proteção dos ativos, impedindo ou dificultando que as ameaças explorem as vulnerabilidades, diminuindo, assim, o risco (SÊMOLA, 2014).

De um modo geral, a gestão de riscos é um método voltado para o controle dos riscos e abrange um conjunto de atividades específicas que tem como objetivo garantir a boa governança, sem que os riscos e surpresas indesejáveis atrapalhem seus objetivos e metas (DANTAS, 2011).

A gestão de riscos é composta por sete etapas, conforme Figura 4.

Figura 4 – O processo de gestão de riscos



Fonte: ABNT NBR ISO/IEC 27005 (2019).

2.4 PLANO DE CONTINUIDADE DE NEGÓCIOS

Na vida cotidiana as pessoas protegem-se ao máximo, através de seguros pessoais, de imóveis, automóveis, saúde, residencial e outros, com o objetivo de proteger-se de situações imprevistas ou mesmo de desastres. Similarmente, é

esperado que os responsáveis das empresas e em especial de TI, tenham a mesma atenção aos ativos críticos, que servem de base de suporte da organização (FERNANDES, 2014).

Consequentemente, pensar em como assegurar a continuidade dos serviços em caso de algum evento que interrompa a operação de um ou mais processos de negócio, se torna uma tarefa essencial para a gestão da segurança da informação. O foco está em garantir a continuidade dos processos e informações cruciais para a sobrevivência da organização, no menor tempo possível, com o objetivo de minimizar os efeitos resultantes de um desastre (SÊMOLA, 2014).

O PCN é um processo, cujo planejamento tem como objetivo assegurar que uma organização resista a um desastre ou qualquer atividade imprevista que provoque danos aos ativos críticos, pondo em risco qualquer processo de negócio (LYRA, 2015). De acordo com a norma NIST SP 800-34, o plano pode ser elaborado englobando somente os processos críticos do negócio ou pode compor todos os processos de uma organização (NIST SP 800-34, 2010).

A metodologia a ser adotada no PCN pode pressupor a criação e administração de planos específicos, sendo eles: Plano de Contingência Operacional (PCO), Plano de Administração de Crises (PAC) e PRD. O PRD, em específico, trata-se de procedimentos previamente definidos para cenários de desastres, ou seja, conjunto de procedimentos para garantir que as atividades críticas retornem à operação dentro do prazo preestabelecido após a ocorrência de um desastre (GUINDANI, 2008).

2.5 PLANO DE RECUPERAÇÃO DE DESASTRES

O PRD é um plano de ação, que tem como principal objetivo restaurar, no menor tempo possível e mesmo com desempenho reduzido, os serviços de TI que sustentam os processos críticos do negócio. A preparação é a peça-chave para um PRD bem-sucedido, por isso é preciso desenvolver uma documentação que abrange ações bem planejadas a serem adotadas antes, durante e após um desastre.

O plano é acionado após o acontecimento de um desastre, podendo ser voluntário (*hackers*, incendiários etc.), involuntário (acidentes, falta de energia etc.) ou natural (terremotos, enchentes, incêndios naturais etc.).

Conforme citado na Seção 2.4, o PCN apresenta uma abordagem completa para uma organização, assegurando desde um grande desastre - um incêndio, por exemplo -, até problemas com fornecedores. Já para se planejar um PRD, somente alguns itens críticos devem ser levados em consideração, tendo como exemplo este projeto, o servidor de banco de dados e da aplicação do ERP da empresa.

A norma NIST SP 800-37 (2018), descreve o PRD como um plano de informação do sistema com foco projetado para restaurar a funcionalidade do sistema, aplicação ou infraestrutura de instalação de computadores em um site alternativo após uma emergência, e complementa informando que se aplica a grandes rupturas, geralmente físicas, para os serviços que negam o acesso a infraestrutura de instalação principal para um período prolongado.

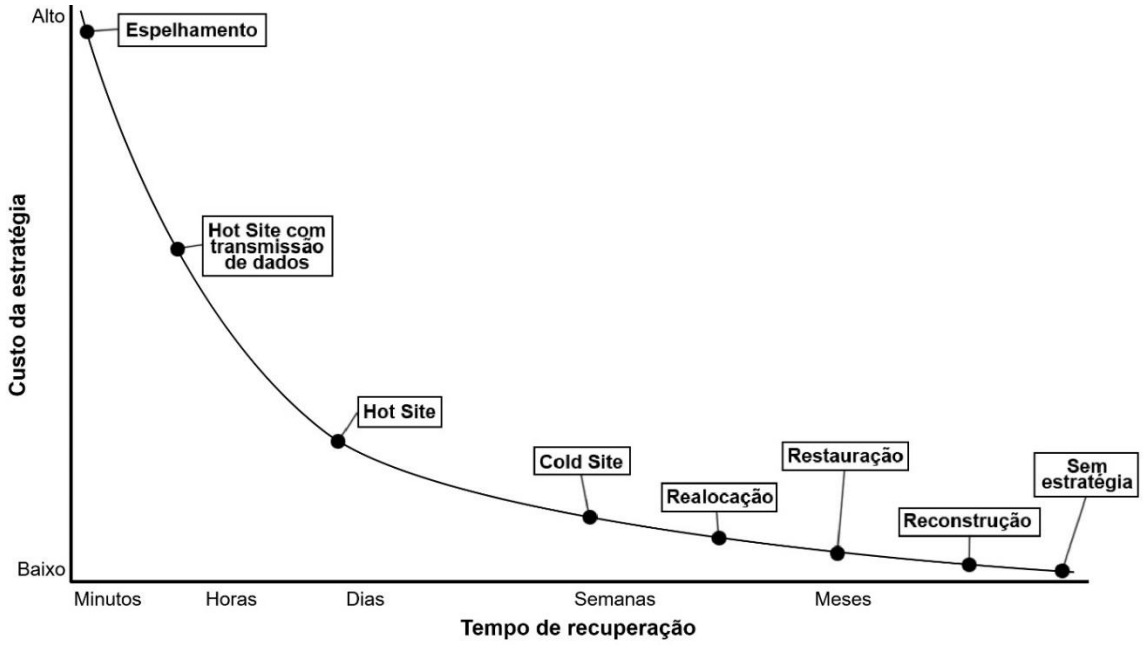
2.6 ESTRATÉGIAS DE CONTINUIDADE

Conforme a norma NIST SP 800-34, a estratégia de recuperação é desenvolvida através da análise dos resultados obtidos da avaliação de riscos e fornece direção na maneira com que a estratégia de continuidade possa ser executada (NIST SP 800-34, 2010).

Guindani (2008), define e orienta a escolha das múltiplas estratégias para a recuperação dos processos e componentes de negócio, dentro dos prazos de recuperação definidos. Com a possibilidade de múltiplas combinações e cada uma com seus benefícios, é difícil agradar todos os gestores, isto é, não existe uma solução correta nem errada, o responsável pelo PCN deve comparar os fatores existentes e o nível de risco que a organização está disposta a correr. As estratégias mais satisfatórias são aquelas que tem a melhor relação custo X benefício, são as que reduzem os riscos e exposições e que também atendem às exigências do negócio e não só de TI.

Independente da estratégia escolhida, o objetivo final deve ser o mesmo, garantir uma recuperação eficiente dos processos de negócio da empresa de acordo com a análise obtida na gestão de riscos e seu tipo de negócio. Na Figura 5, são apresentadas algumas das estratégias de continuidade existentes, levando em consideração o tempo de restauração e o custo.

Figura 5 – Custo da estratégia X tempo de recuperação



Fonte: Adaptado de Guindani (2008).

3 METODOLOGIA

Neste capítulo será apresentado toda a metodologia que se fez necessária para a elaboração de um Plano de Recuperação de Desastres focado no ERP da empresa em questão.

3.1 CARACTERIZAÇÃO DA PESQUISA

Este trabalho foi realizado através de uma pesquisa exploratória, foram utilizados métodos de pesquisas bibliográficas, em livros, artigos científicos, dissertações e publicações. Para que o PRD possa ser validado de forma eficaz, elaborou-se um estudo de caso em uma empresa do setor de tecnologia.

3.2 AMBIENTE DA PESQUISA

O estudo presente neste trabalho foi realizado em uma empresa do setor de tecnologia, situada no município de Joinville, no estado de Santa Catarina, dando início de suas atividades em 1977, após toda sua trajetória e evolução, hoje o *case* de

sucesso é o *outsourcing* de impressão, além disso, a empresa também oferece *softwares*, como ferramentas para organização da cadeia de sistemas de impressão, gestão de documentos e automatização de processos de negócios e também conta com o serviço de *outsourcing* de TI, como *notebooks* e *desktops*.

A organização possui uma ampla infraestrutura de TI para manter o seu negócio. Possui uma variedade de sistemas e aplicações, destacando-se: *Active Directory* (AD), *Dynamic Host Configuration Protocol* (DHCP), *Domain Name System* (DNS), servidores de arquivos, *web*, impressão e banco de dados SQL, *firewall*, antivírus, *Virtual Private Network* (VPN), ERP e *Human Capital Management* (HCM).

Além de todas essas informações citadas acima, a organização necessita de conectividade com a *Internet* para a utilização e disponibilização dos serviços *online*, acesso aos *e-mails* e as atividades comuns realizadas diariamente. A *Internet* é a peça-chave para o funcionamento de muitos serviços, portanto, a empresa dispõe de dois *links* de *Internet* de operadoras distintas, sendo elas Ávato Datacenter e Algar Telecom, e conta também com um *firewall* robusto, capaz de detectar a queda de um dos *links*, garantindo assim a redundância de forma eficaz.

3.3 ETAPAS DA PESQUISA

De acordo com o plano proposto, serão aplicadas somente no servidor de banco de dados as etapas apresentadas na Figura 6.

Figura 6 – Etapas da pesquisa

Fonte: O autor (2021).

Para ajudar a classificar a criticidade dos sistemas e os possíveis impactos, pode ser utilizado a Análise de Impacto no Negócio (BIA - *Business Impact Analysis*), conforme descrito na norma NIST SP 800-34. A BIA trata-se de uma análise da importância dos ativos ou processos da organização, com base nos fatores de "custo de parada" e "tolerância à interrupção". Sendo assim, quanto maior o custo gerado pela interrupção do item avaliado e quanto menor for a tolerância a interrupções, maior será sua criticidade em relação ao negócio.

O servidor MANAGER foi designado por ser identificado como um dos ativos mais importantes da organização, visto que é responsável por armazenar toda e qualquer informação referente a mesma, como estoque, equipamentos, clientes, fornecedores, compras, entre diversos outros processos necessários para o funcionamento integral da organização.

3.3.1 Caracterização do ativo

A caracterização do ativo é o passo inicial e é tão importante quanto os outros, pois permite identificar as limitações, recursos e informações do ativo. O responsável de TI deve disponibilizar as seguintes informações: informações de *hardwares* e *softwares*; usuários que fazem uso do ativo; missão do ativo, descrevendo os processos realizados pelo mesmo; sensibilidade e criticidade do ativo; políticas de segurança; controles operacionais; e relatórios (NIST SP 800-30, 2012). Conforme apresentado no Quadro 1.

Quadro 1 – Caracterização do ativo

Caracterização do ativo	
Identificação	MANAGER
Missão	Hospedar o banco de dados e prover acesso ao ERP da organização
Usuários ativos	Em média 400 usuários simultâneos
Monitoramento de uso	Através da ferramenta Zabbix, gerenciado por empresa terceirizada
Responsáveis pela manutenção e suporte	DBA e Analista de Infraestrutura de TI
Controle de acesso	Permissões de acordo com os níveis de acesso por usuário
Consequências do ativo para a organização	Afeta todos os processos
Registros de incidentes ocorrido anteriormente	Não é feito relatório, porém nunca ocorreu

Procedimentos documentados de operação, manutenção e suporte	Não existe nada documentado
Formato de operações da manutenção e alteração	Não existe nada documentado
Seguro contra roubo, furto, incêndio ou desastre natural	Sim
Treinamento para administradores e usuários	Não
Criticidade	Muito alta
Sensibilidade	Muito alta
Proprietário	Setor de TI
Processos executados	Por se tratar do ERP, é responsável por executar todos os processos da organização
Informações de hardware	Dell PowerEdge R630, 2 processadores Intel Xeon E5-2670 v3 2.30GHz, 64GB RAM, 2x SSD 960GB e 6x HD 480GB

Fonte: O autor (2021).

Nessa primeira etapa, foi realizada uma entrevista com o coordenador de TI, e foram levantadas todas as informações importantes do ativo, com o objetivo de fornecer as informações necessárias para dar continuidade nas próximas etapas.

3.3.2 Identificar as ameaças

Para essa etapa, é necessário reunir dados obtidos através de análises e relatórios de incidentes, dos responsáveis pelo ativo ou dos usuários, de catálogos externos de ameaças, dentre outros documentos, com o objetivo de levantar informações que indiquem potenciais ameaças para o ativo. Deve-se também coletar informações que podem apontar prováveis ameaças relativas ao ativo que não haviam sido identificadas até o momento (ABNT NBR ISO/IEC 27005, 2019).

É fundamental classificar as ameaças e a probabilidade da existência dela para o ativo, de acordo com o apresentado na Tabela 1.

Tabela 1 – Classificação das ameaças

Categoria	**Classificação de existência**		
Humanas/Ambientais/Naturais	**Muito baixa**	**Moderada**	**Muito alta**
Falha não intencional		X	
Falha de *hardware*		X	
Falha de *software*		X	
Falha de conectividade		X	
Falha de fornecimento de energia		X	

Falha no controle de temperatura		X	
Terrorismo cibernético			X
Espionagem		X	
Sabotagem		X	
Atividade criminosa – Roubo de dados			X
Queda de raios		X	
Fogo		X	
Infestação de pragas/insetos	X		

Fonte: O autor, adaptado de NIST SP 800-30 (2012).

Deve-se lembrar que ativos e organizações possuem diferentes tipos de ameaças, por isso, é necessário realizar pesquisas de acordo com a realidade e necessidade do ativo e da organização. Após analisar e validar o relatório de ameaças, o responsável pela segurança da informação entrega aos *stakeholders* para aprovação, caso aprovado, a etapa é concluída e é elaborada a tabela de ameaças qualificadas para explorar as vulnerabilidades do ativo em questão (NIST SP 800-30, 2012).

3.3.3 Identificar as vulnerabilidades

Com a finalização da identificação das ameaças, é importante elaborar uma tabela das possíveis vulnerabilidades, capazes de afetar diretamente os serviços da organização, conforme apresentado no Quadro 2.

Quadro 2: Identificação de vulnerabilidades

Ameaça	Vulnerabilidade	Comentário
Falha não intencional	Falta de treinamento para analistas	Funcionários não recebem treinamento
Falha de hardware	Falta de peças de reposição, equipamento sem garantia ou fora de linha do fabricante	Nunca houve ocorrência
Falha de software	Falta de aplicação de atualizações	Nunca houve ocorrência
Falha de conectividade	Falta de equipamentos de rede reservas para substituição em caso de falhas	Em caso de falta, a comunicação com o servidor será perdida
Falha de fornecimento de energia	Falta de energia ou *nobreak* com autonomia reduzida	Caso a energia não volte até 1 hora, será necessário o desligamento do ativo
Falha no controle de temperatura	Queima de ar-condicionado	Em caso de falha, existe um ar-condicionado redundante

Terrorismo cibernético	Falta de especialista em *firewall*	Tentativas de ataques e acessos não autorizados
Espionagem	Acesso remoto concedido para terceiros responsáveis pela manutenção	Acessos não monitorados
Sabotagem	Funcionários com privilégios avançados	Número de administradores elevado
Atividade criminosa - Roubo de dados	Extração de dados confidenciais	Roubo de dados pelos funcionários ou criminosos
Queda de raios	Falha no supressor de surto	Raios podem provocar oscilações que causem danos
Fogo	Combate a incêndio feito manualmente	Não possui sistema automático de combate a incêndios, somente detector de fumaça e temperatura
Infestação de pragas/insetos	Falta de dedetização	Nunca houve ocorrência

Fonte: O autor, adaptado de NIST SP 800-30 (2012).

Sêmola (2014) afirma que o objetivo da identificação das vulnerabilidades, é encontrar falhas ou fraquezas com a possibilidade de serem exploradas por ameaças oportunas ao ativo analisado.

3.3.4 Determinar as probabilidades

O objetivo desta etapa é realizar a classificação das probabilidades de explorar as potenciais ameaças através das vulnerabilidades identificadas para o ativo na etapa anterior. Portanto, deve-se montar uma tabela para classificar as probabilidades como muito baixa, baixa, moderada, alta e muito alta, conforme apresentado na Tabela 2.

Tabela 2: Classificação da probabilidade de exploração de vulnerabilidades

Ameaça	**Vulnerabilidade**	**Probabilidade**				
		Muito baixa	**Baixa**	**Moderada**	**Alta**	**Muito alta**
Falha não intencional	Falta de treinamento para analistas				X	
Falha de *hardware*	Falta de peças de reposição, equipamento sem garantia ou fora de linha do fabricante		X			
Falha de *software*	Falta de aplicação de atualizações		X			
Falha de conectividade	Falta de equipamentos de rede reservas para substituição em caso de falhas		X			

Falha de fornecimento de energia	Falta de energia ou *nobreak* com autonomia reduzida				X
Falha no controle de temperatura	Queima de ar-condicionado		X		
Terrorismo cibernético	Falta de especialista em *firewall*				X
Espionagem	Acesso remoto concedido para terceiros responsáveis pela manutenção			X	
Sabotagem	Funcionários com privilégios avançados		X		
Atividade criminosa – Roubo de dados	Extração de dados confidenciais		X		
Queda de raios	Falha no supressor de surto		X		
Fogo	Combate a incêndio feito manualmente		X		
Infestação de pragas/insetos	Falta de dedetização	X			

Fonte: O autor, adaptado de NIST SP 800-30 (2012).

3.3.5 Análise de impactos

O objetivo da análise de impacto é mostrar os eventos negativos que podem levar a danos ou perdas dos recursos de informação, proporcionando à organização margem de impacto em alguns casos. Portanto, é necessário conduzir uma avaliação combinada de ameaças, vulnerabilidades e impactos, identificar aspectos relevantes e determinar onde aplicar esforços para eliminar ou reduzir as probabilidades de ameaças e vulnerabilidades, com o propósito de evitar possíveis problemas no funcionamento dos negócios da empresa (NIST SP 800-37, 2018).

Portanto, deve-se identificar os níveis de impactos consequentes das ameaças, classificando-os em níveis, muito baixo, baixo, moderado, alto e muito alto, conforme elaborado na Tabela 3.

Tabela 3 – Análise de impacto

Ameaça	**Impacto**				
	Muito baixo	**Baixo**	**Moderado**	**Alto**	**Muito alto**
Falha não intencional			X		
Falha de *hardware*					X
Falha de *software*			X		
Falha de conectividade					X

Falha de fornecimento de energia				X
Falha no controle de temperatura			X	
Terrorismo cibernético		X		
Espionagem	X			
Sabotagem	X			
Atividade criminosa – Roubo de dados	X			
Queda de raios	X			
Fogo			X	
Infestação de pragas/insetos	X			

Fonte: O autor, adaptado de NIST SP 800-30 (2012).

A análise de impacto também pode ser medida através da elaboração de um questionário, que deve ser respondido pelo responsável do ativo em questão. O objetivo do questionário é conceituar o impacto adverso em relação à degradação ou perda dos fundamentos da segurança da informação, confidencialidade, integridade e disponibilidade.

Existem entrevistas e questionários que podem ser encontrados em cursos ou livros, porém, não existem *templates* prontos para um questionário correto, ele deve ser projetado de acordo com o conhecimento do ativo e da forma como trabalha a organização. (ALEVATE, 2014).

O questionário realizado com o Gerente de TI, responsável pelo ativo analisado, é apresentado no Quadro 3.

Quadro 3: Questionário do impacto do ativo

Questionário do impacto do ativo	
1. Período de utilização:	Dias: todos os dias úteis Horas: 06h às 20h
2. Este ativo é obrigatório para o funcionamento da organização:	Sim
3. Período de pico de utilização:	Meses: todos Dias: 1 2 3 4 5 6 7 25 26 27 28 29 30 31 Horas: 06h às 22h
4. Tempo de inoperância tolerável:	30 minutos
5. Período de inoperância específico para manutenções:	Dias úteis: 23h às 05h Finais de semana e feriados: 24h
6. Quanto de perda a paralisação deste ativo causaria e empresa (valor estimado):	30 minutos: R$ 10.000,00 1 hora: R$ 20.000,00 2 horas: R$ 40.000,00 3 horas: R$ 60.000,00 4 horas: R$ 80.000,00 5 horas: R$ 110.000,00 6 horas: R$ 200.000,00 1 dia: R$ 480.000,00

7. A indisponibilidade deste ativo resultaria em algum tipo de multa:	Sim, atendimentos feitos fora do SLA gerariam multas.
8. A indisponibilidade deste ativo evitaria disponibilizar algum serviço aos clientes: Se sim, quais:	Sim. Portal do Cliente, envio de faturas, peças e material de consumo.
9. A indisponibilidade deste ativo causaria qual impacto a imagem da organização:	Grande perda financeira e perda de confiança dos clientes.
10. A indisponibilidade deste ativo causaria qual impacto aos colaboradores:	Grande perda de produtividade e retrabalhos.

Fonte: O autor, adaptado de Alevate (2014).

3.3.6 Análise de riscos

Após todos os dados levantados nas etapas anteriores, por fim, é realizada a análise de riscos. É imprescindível que nessa fase de análise de riscos, seja levado em consideração todas as ameaças identificadas na etapa de identificação de ameaças, e também, os dados apurados nas etapas de identificação das vulnerabilidades e análise de impacto, que são necessários para a elaboração da matriz de risco.

O objetivo da análise de riscos é estabelecer o nível do risco, mediante o cálculo da probabilidade de uma ameaça explorar uma vulnerabilidade e da dimensão do impacto na presença de um evento adverso, sendo assim, a função do cálculo para determinar o peso do risco é a multiplicação dos valores atribuídos para a probabilidade de ocorrer ameaças pelo tamanho do impacto após a exploração da ameaça (NIST 800-30, 2012).

Para determinar o peso do risco, foi desenvolvida uma matriz de risco conforme apresentado na Tabela 4.

Tabela 4 – Análise de riscos

Ameaças	**Probabilidade** *Muito baixa = 0.1* *Baixa = 0.2* *Moderada = 0.5* *Alta = 0.8* *Muito alta = 1.0*	x	**Impacto** *Muito baixo = 4* *Baixo = 20* *Moderado = 79* *Alto = 95* *Muito alto = 100*	**=**	**Peso do risco** *Muito baixo = 0-4* *Baixo = 5-20* *Moderado = 21-79* *Alto = 80-95* *Muito alto = 96-100*
Falha não intencional	0.8	x	79	=	63,2
Falha de *hardware*	0.2	x	100	=	20
Falha de *software*	0.2	x	79	=	15,8

Falha de conectividade	0.2	x	100	=	20
Falha de fornecimento de energia	0.8	x	100	=	80
Falha no controle de temperatura	0.2	x	79	=	15,8
Terrorismo cibernético	0.8	x	20	=	16
Espionagem	0.5	x	20	=	10
Sabotagem	0.2	x	20	=	4
Atividade criminosa – Roubo de dados	0.2	x	20	=	4
Queda de raios	0.2	x	20	=	4
Fogo	0.2	x	95	=	19
Infestação de pragas/insetos	0.1	x	20	=	2

Fonte: O autor, adaptado de NIST SP 800-30 (2012).

Toda e qualquer empresa possui suas próprias características, objetivos e planos específicos, em razão disso, precisa encontrar o nível de risco mais adequado para operar. Dentro desse cenário, a análise de riscos é a ferramenta perfeita para mensurar a situação de segurança atual (SÊMOLA, 2014).

4 RESULTADOS E DISCUSSÕES

De acordo com a pesquisa realizada utilizando como base o ativo MANAGER, servidor responsável pelo banco de dados e aplicação do principal sistema utilizado na empresa, bem como as etapas de aplicação do PRD, foi identificado que atualmente a empresa não possui um PRD, portanto, no surgimento de um problema no servidor, os responsáveis são acionados para solucionarem de forma correta e mais rápida possível. Também foi identificado que o único método de prevenção e segurança que a empresa possui, é o *backup* do banco de dados, realizado diariamente às 23 horas.

No setor de Faturamento, por exemplo, onde são geradas as faturas dos clientes, em uma situação em que ocorra uma paralisação do sistema, a empresa fica sem meios para gerá-las, causando atrasos no envio das faturas para os clientes.

Outro exemplo é o setor de Mesa de Operação, onde é feito todo o mapeamento dos chamados dos clientes para os técnicos de todo o Brasil, sendo

necessário a realização de trabalho manual em caso de falta de sistema, através do uso de telefone fixo ou móvel e, utilizando plataformas de edição de texto e planilhas para controle dos chamados abertos pelos clientes.

Após realizar e evidenciar todas as análises efetuadas no presente trabalho, foi realizada uma reunião com os responsáveis de TI, a fim de criar estratégias para solucionar os possíveis problemas de paralisação do ativo. Ao fim, foi possível chegar à seguinte conclusão para a proposta de PRD.

Aquisição de um novo servidor para utilizá-lo em *colocation*, serviço prestado por uma empresa terceira de *data center*, que seria a Ávato Datacenter, mesma empresa que já disponibiliza o serviço de *Internet*, localizada na mesma cidade, com ampla infraestrutura de conectividade de *Internet*, climatização e energia elétrica.

Adquirir o serviço de *LAN to LAN* oferecido também pela Ávato Datacenter, em outras palavras, criando uma *Metropolitan Area Network* (MAN), em português, Rede Metropolitana, disponibilizando um *backbone* de fibra ótica próprio para comunicação direta com o servidor em *colocation*, o *backbone* utiliza a topologia anel, garantindo dupla abordagem através de diferentes rotas.

Migração do servidor atual do formato físico para virtualizado, facilitando o gerenciamento, otimização de recursos, manutenção do servidor e simplificando operações de *backup*. Utilização deste mesmo formato virtualizado no servidor utilizado em *colocation*.

E por fim, implementação do *SQL Server Always On* nos dois servidores, o *Always On* se trata de uma arquitetura de alta disponibilidade, sua implementação é complexa, sendo necessária a contratação de serviço especializado terceirizado. Garantindo, assim, replicação instantânea do banco de dados do ERP, com *delay* em média de 15 segundos de perda de dados em caso de um desastre no servidor principal.

CONSIDERAÇÕES FINAIS

O modelo proposto de PRD no presente trabalho, tem como base as normas e boas práticas de segurança da informação e pode ser utilizado como base em qualquer empresa que necessite.

Realmente um PRD é eficaz para minimizar as interrupções dos negócios e restaurar rapidamente a normalidade das atividades? Sim, o estudo concluiu que a implementação de um Plano de Recuperação de Desastres pode minimizar os impactos de um desastre, possibilitando às empresas reagirem de forma rápida e segura em casos de eventos negativos.

Este trabalho demonstra a importância da implantação do PRD nas organizações e as etapas que os responsáveis de TI devem realizar para elaborar planos, aplicar medidas de segurança contra os prováveis riscos que a organização possa ser afetada, por meio das etapas de caracterização do ativo, identificação das ameaças e vulnerabilidades, determinação das probabilidades e análise dos impactos e riscos, com a possibilidade de restaurar as atividades após um evento negativo de maneira planejada e organizada.

Como sugestão para futuros trabalhos, seria a aplicação da proposta de PRD apresentada neste trabalho, bem como a avaliação dos processos realizados, com a finalidade de analisar a eficácia do plano.

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela minha vida, e por me permitir ultrapassar todos os obstáculos encontrados ao longo da realização deste trabalho.

Aos meus pais e esposa, que me incentivaram nos momentos difíceis e compreenderam a minha ausência enquanto eu me dedicava à realização deste trabalho.

Ao professor Dr. Mehran Misaghi, por ter sido meu orientador e ter desempenhado tal função com dedicação e amizade.

Aos professores, pelas correções e ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação profissional ao longo do curso.

Às pessoas com quem convivi ao longo desses anos de curso, que me incentivaram e que certamente tiveram impacto na minha formação acadêmica.

REFERÊNCIAS

ABNT NBR ISO 31000. 2018. **Gestão de riscos - Diretrizes.** Disponível em: <https://www.apostilasopcao.com.br/arquivos-opcao/erratas/10677/66973/abnt-nbr-iso-31000-2018.pdf>. Acesso em: 12 de agosto de 2020.

ABNT NBR ISO/IEC 22301. 2020. **Segurança e resiliência - Sistema de gestão de continuidade de negócios - Requisitos.** Disponível em: <https://www.target.com.br/produtos/normas-tecnicas/43062/nbriso22301-seguranca-e-resiliencia-sistema-de-gestao-de-continuidade-de-negocios-requisitos>. Acesso em: 29 de novembro de 2020.

ABNT NBR ISO/IEC 27001. 2013. **Tecnologia da Informação - Técnicas de Segurança - Sistemas de gestão de segurança da informação - Requisitos.** Disponível em: <https://www.coursehero.com/file/35223357/ABNT-NBR-ISO-IEC-27001-1-2013pdf/>. Acesso em: 02 de agosto de 2020.

ABNT NBR ISO/IEC 27002. 2013. **Tecnologia da Informação - Técnicas de Segurança - Código de Prática para a Gestão da Segurança da Informação.** Disponível em: <http://www.professordiovani.com.br/AdmRedes/NBRISO-IEC27002.pdf>. Acesso em: 02 de agosto de 2020.

ABNT NBR ISO/IEC 27005. 2019. **Tecnologia da Informação - Técnicas de Segurança - Gestão de riscos de segurança da informação.** Disponível em: <https://br1lib.org/ireader/11682019>. Acesso em: 03 de agosto de 2020.

ALEVATE, W. da R. **Gestão da continuidade de negócios.** Rio de Janeiro, RJ: Elsevier, 2014.

CERT.BR. 2020. **Total de Incidentes Reportados ao CERT.br por Ano.** Disponível em <https://www.cert.br/stats/incidentes/>. Acesso em: 23 de fevereiro de 2020.

DANTAS, M. L. **Segurança da informação: uma abordagem focada em gestão de riscos.** Olinda, PE: Livro Rápido, 2011.

AGUIAR JUNIOR, U. F. de. **Plano de recuperação de desastres: uma pesquisa-ação em empresa do setor energético.** Guaratinguetá, 2007.

DEY, M. **Information security management: a practical approach.** 2007.

FERNANDES, L. M. F. **Planeamento de Estratégias de Salvaguarda e Reposição de Dados/Informação baseado em Algoritmo de Optimização de requisitos Multidimensionais.** Lisboa: 2014.

GUINDANI, A. 2008. **Gestão da Continuidade dos Negócios.** Disponível em: <http://ssystem08.upis.br/repositorio/media/revistas/revista_integracao/gestao_continuidade.pdf>. Acesso em: 04 de fevereiro de 2020.

LYRA, M. R. **Governança da segurança da informação.** Brasília, DF: 2015.

NEWMAN, D. 2016. **The changing role of it in the future of business.** Disponível em: <https://www.forbes.com/sites/danielnewman/2016/07/26/the-changing-role-of-it-in-the-future-of-business>. Acesso em: 23 de março de 2020.

NIST SP 800-30. 2012. **Guide for Conducting Risk Assessments.** Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>. Acesso em: 05 de agosto de 2020.

NIST SP 800-34. 2010. **Contingency Planning Guide for Federal Information Systems.** Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>. Acesso em: 06 de agosto de 2020.

NIST SP 800-37. 2018. **Risk Management Framework for Information Systems and Organizations.** Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>. Acesso em: 10 de agosto de 2020.

SÊMOLA, M. **Gestão da Segurança da Informação: uma visão executiva.** Rio de Janeiro, RJ: Elsevier, 2014.

SISK, A. 2018. **Importance of Information Technology in the Business Sector.** Disponível em: <https://bizfluent.com/about-6744256-importance-information-technology-business-sector.html>. Acesso em: 08 de abril de 2020.

VELEZ, C. 2017. **Desastres tecnológicos: As empresas estão preparadas para a recuperação?** Disponível em: <http://cio.com.br/gestao/2017/12/05/desastres-tecnologicos-as-empresas-estao-preparadas-para-a-recuperacao>. Acesso em: 19 de maio de 2020.