Universidade Federal da Paraíba
Centro de Tecnologia
Departamento de Engenharia de Produção

PROCEDIMENTO DE ANÁLISE DE RISCOS EM *CYBERSECURITY*: APLICAÇÃO EM UMA EMPRESA DE PRODUÇÃO DE GASES INDUSTRIAIS E MEDICINAIS

MARLON UCHÔA DA SILVA

João Pessoa - PB
2021

MARLON UCHÔA DA SILVA

PROCEDIMENTO DE ANÁLISE DE RISCOS EM *CYBERSECURITY*: APLICAÇÃO EM UMA EMPRESA DE PRODUÇÃO DE GASES INDUSTRIAIS E MEDICINAIS

Trabalho de Conclusão de Curso apresentado como parte dos requisitos necessários para obtenção do título de bacharel em Engenharia de Produção pela Universidade Federal da Paraíba.

Orientador: Dr. Luciano Costa Santos

João Pessoa - PB
2021

Catalogação na publicação
Seção de Catalogação e Classificação

S586p Silva, Marlon Uchoa da.
PROCEDIMENTO DE ANÁLISE DE RISCOS EMCYBERSECURITY: APLICAÇÃO EM UMAEMPRESA DE PRODUÇÃO DE GASESINDUSTRIAIS E MEDICINAIS / Marlon Uchoa da Silva. - João Pessoa, 2021.
51f. : il.

Orientação: Luciano Costa Santos.
TCC (Graduação) - UFPB/CT.

1. Cibersegurança. 2. Análise de riscos. 3. Sistemas de informações. I. Costa Santos, Luciano. II. Título.

UFPB/BS/CT CDU 658.5(043.2)

Elaborado por ROSANGELA GONCALVES PALMEIRA - CRB-216

FOLHA DE APROVAÇÃO

PROCEDIMENTO DE ANÁLISE DE RISCOS EM *CYBERSECURITY*: APLICAÇÃO EM UMA EMPRESA DE PRODUÇÃO DE GASES INDUSTRIAIS E MEDICINAIS

MARLON UCHÔA DA SILVA

Trabalho de Conclusão de Curso aprovado em 12 de julho de 2021 como parte dos requisitos para a obtenção do título de bacharel em Engenharia de Produção pela Universidade Federal da Paraíba.

Prof. Dr. Luciano Costa Santos - Orientador - DEP/CT/UFPB

Profª. Drª. Lígia de Oliveira Franzosi Bessa - Examinador Interno - DEP/CT/UFPB

Prof. Dr. Ivson Ferreira dos Anjos - Examinador Interno - DEP/CT/UFPB

João Pessoa - PB
Julho/2021

Resumo

Este trabalho teve como objetivo aplicar um procedimento de análise de riscos em *cybersecurity* em uma empresa multinacional do ramo de gases industriais e medicinais. A empresa em estudo utiliza um sistema de Gerenciamento de Segurança da Informação (GSI) que é padrão para todas as suas unidades por todo o mundo. A fase de identificação de riscos representou o escopo deste estudo e consiste na aplicação de um procedimento composto de três partes: *Business Service Level Description* (BSLD), *Risk Assessment* e *Scan* ou varredura de Vulnerabilidades. Cada um desses procedimentos possui atribuições e objetivos específicos e são baseados em questionários, análises de risco e verificação de vulnerabilidades de aplicativos ou softwares candidatos a inserção na empresa. Foi realizada uma análise individual da aplicação de um dos cada componentes do GSI a um sistema candidato à inserção na empresa. Observou-se que os procedimentos aplicados possuem um caráter extensivo e demorado, o que pode ser uma vulnerabilidade da estratégia de proteção contra *cyber-risks*. Além disso, gestores despreparados podem deixar lacunas importantes dentro da aplicação dos procedimentos, diminuindo a qualidade de análise.

Palavras-chave: cibersegurança, análise de riscos, sistemas de informação.

Abstract

This work aimed to apply a cybersecurity risk analysis procedure in a multinational company in the field of industrial and medical gases. The company under study uses an Information Security Management (ISM) system that is standard for all its units all over the world. The risk identification step represented the scope of this study and consists of the application of a procedure composed of three parts: Business Service Level Description (BSLD), Risk Assessment and Vulnerability scanning. Each of these procedures has specific attributions and objectives and are based on questionnaires, risk analysis and verification of application or software vulnerabilities that are candidates for insertion in the company. An individual analysis of the application of one of the ISM components to a candidate system for insertion in the company was carried out. It was observed that the applied procedures have an extensive and time-consuming character, which may be a vulnerability of the cyber-risks protection strategy. In addition, unprepared managers can leave important gaps within the application of procedures, reducing the quality of analysis.

Keywords: cybersecurity, risk analysis, information systems.

Lista de quadros

Lista de tabelas

Lista de ilustrações

Sumário

1 Introdução

Segundo dados da pesquisa “Os Cinco Pilares de Riscos” de 2019 da empresa Deloitte em parceria com o Instituto Brasileiro de Governança Corporativa (IBGC), apenas três quartos de 160 organizações pesquisadas em todo Brasil apresentaram uma política de gestão de riscos formalizada. Ainda segundo o estudo, os riscos operacionais são os que mais têm processos definidos para mitigação, seguidos pelos riscos financeiros e regulatórios. Os riscos cibernéticos são os que menos apresentam processos definidos de redução e aqueles que figuram como os que as organizações pesquisadas têm menos conhecimento, indicando um nicho emergente de gestão de riscos, tendo em vista o avanço tecnológico empresarial em crescimento (DELOITTE; IBCG, 2019).

A mudança nas relações humanas com a tecnologia, em particular no âmbito corporativo, traz não somente avanço e produtividade, é parte dessa mudança o surgimento de riscos e a necessidade de adequação à nova realidade. Portanto, tem sido motivo de preocupação para os gestores de segurança cibernética os mecanismos de controle de redes e dados internos sigilosos. Dispositivos mal configurados, e má adequação do setor de tecnologia da informação em uma organização pode ser a entrada para intrusos mal-intencionados através de vírus, *malwares* e *ransomwares* (CUSTOIAS; MENDONÇA; CUNHA, 2019).

Risco, vulnerabilidade e ameaça são, portanto, palavras-chave no campo da segurança digital. Portanto, é importante avaliar a vulnerabilidade do sistema cibernético, determinar seu risco para a indústria, descobrir os pontos fracos, definir a resposta adequada aos incidentes prováveis e aumentar a segurança do sistema cibernético (JIAXI; ANJIA; ZHIZHONG, 2006).

Apesar de ser necessário um gerenciamento eficaz das vulnerabilidades, esses processos costumam ser mais reativos por natureza, ou seja, contam com a publicação de vulnerabilidades, criação de assinaturas e o processo de varredura e detecção antes que as mitigações de controle possam ser implementadas. Os sistemas de computadores são vulneráveis a ataques cibernéticos de dentro e de fora da rede do sistema. Durante o processo de produção de produtos de software e design de sites, fornecedores e desenvolvedores criam involuntariamente vulnerabilidades que podem servir de oportunidade para criminosos cibernéticos. Sendo assim, com o crescimento e uso contínuo da Internet, houve uma sofisticação crescente de ferramentas e métodos para identificação e prevenção de novas vulnerabilidades durante o ciclo de vida de desenvolvimento dos sistemas interconectados emergentes (TANG et al., 2018).

Embora as soluções para cada aspecto de segurança possam parecer diferentes em seus detalhes, todas compartilham o objetivo de minimizar os riscos para um ativo, reconhecendo suas ameaças internas e externas, identificando suas vulnerabilidades potenciais, realizando avaliações de risco e, em seguida, mitigando as vulnerabilidades. A segurança cibernética associada a cada computador, por exemplo, é multifacetada e essas múltiplas facetas podem ser inter-relacionadas. Como todos os computadores da rede estão interconectados e sua segurança cibernética é interdependente, o esforço total necessário para toda a rede torna-se o de cada computador multiplicado pelo tamanho da organização (CHANG et al., 1999).

O desafio de criar mecanismos padronizados em segurança cibernética mostra-se de suma importância, considerando as constantes mudanças socioeconômicas e tecnológicas, aumento do compartilhamento de informações e ameaças. O Brasil ainda não tem nenhum documento que estabeleça as diretrizes, metas e responsáveis de uma estratégia nacional de segurança cibernética, sendo um desafio muito importante para o país (GALOYAN, 2019).

Neste trabalho são apresentados procedimentos de análise de risco aplicados a uma empresa que interage com o mundo cibernético de forma ativa e compulsória. Os procedimentos adotados nessa organização não são, no entanto, regra para todas as empresas nacionais, embora seja um procedimento consolidado em um grande espaço empresarial. Usando como exemplo a experiência em outra organização pertencente a outro segmento, na qual existiam algumas políticas a serem seguidas de maneira global, os processos poderiam variar de região para região.

1.1 Objetivos

Propõe-se neste trabalho analisar a *cybersecurity* com foco em *cyber-risks* e vulnerabilidade. Portanto, o objetivo geral deste trabalho é aplicar um procedimento para análise de riscos em *cybersecurity* . A partir do objetivo geral, foram definidos os seguintes objetivos específicos:

- Identificar procedimentos na literatura sobre gestão de *cyber-risks* e *cybersecurity* .
- Definir o procedimento de análise de *cyber-risks* que compõe o processo de gerenciamento de segurança da informação.
- Descrever a aplicação do procedimento em uma empresa de grande porte.

1.2 Justificativa

Segundo o estudo de Humayun et al. (2020) há uma necessidade na literatura de mais estudos em segurança cibernética, em especial aqueles voltados para questões específicas como vulnerabilidade. De acordo com os autores, a maioria dos estudos selecionados na revisão teve como alvo apenas algumas vulnerabilidades de segurança comuns, como *phishing*, negação de serviço e *malware*. No entanto, há uma necessidade, em pesquisas futuras, de identificar as principais vulnerabilidades de segurança cibernética, aplicativos direcionados, técnicas de mitigação e infraestruturas, de modo que pesquisadores e profissionais possam ter uma visão melhor sobre o assunto.

Diante da relevância da avaliação, gerenciamento e análise dos riscos dentro do processo de tomada de decisão e operações empresariais, faz-se necessária a exploração aprofundada e o direcionamento dentro do escopo de um tema em voga como a segurança digital nos dias atuais. Uma questão-chave dentro de um processo de gerenciamento de *cyber-risks* são as vulnerabilidades mais frequentes que emergem no processo de análise. Porém, a identificação das vulnerabilidades depende da aplicação de procedimentos estruturados para isso, o que ainda é algo novo para as organizações.

Uma empresa do porte da escolhida como objeto dessa análise necessita de atualização constante dos seus procedimentos em gestão de risco. Portanto, é de suma importância que seus procedimentos sejam estudados de forma aprofundada e crítica, observando as deficiências e espaços para melhorias. Com isso é possível generalizar, em certo grau, os *insights* descobertos para outras organizações que desejem melhorar ou mesmo implementar um sistema de segurança digital.

1.3 Estrutura do trabalho

Este trabalho está organizado da seguinte forma: a seção 2 consiste em um referencial teórico, seguido pela seção 3 de metodologia. Na seção 4 são apresentados os resultados obtidos e discussões. Por fim, na seção 5, são feitas as considerações finais.

2 Fundamentação teórica

2.1 Conceitos e tipos de risco

Riscos representam a probabilidade de o evento causador de perda acontecer, isto é, a probabilidade de um incidente e sua consequência para um ativo. Um incidente é um evento que prejudica ou reduz o valor de um ativo, ou seja, algo que possua valor para um indivíduo, empresa, grupo, etc. A vulnerabilidade, por sua vez, consiste no grau de comprometimento em relação às ameaças. Logo, existem três elementos sem os quais não pode haver risco: ativos, vulnerabilidade e ameaça. Sem ativos não há nada para causar danos, sem vulnerabilidades não há como causar danos e sem ameaças não há causas para danos (REFSDAL; SOLHAUG; STØLEN, 2015).

A relação entre probabilidade e consequência, que juntas determinam a gravidade, são os ingredientes que produzem o risco. As consequências dos riscos terão impacto em um ativo ou em um objeto de valor que se deseja proteger. Portanto, antes de mensurar o impacto dos riscos é de suma importância conhecer que partes e ativos estão envolvidos nesse processo e assim definir as estratégias de gestão (REFSDAL; SOLHAUG; STØLEN, 2015).

De acordo com a norma da ISO/IEC – *Risk management and Risk assessment techniques* - 31010, do ano de 2009, aqueles que realizam avaliações de risco devem ser claros sobre as consequências do risco, a probabilidade de sua ocorrência futura, fatores que possam mitigar as consequências do risco ou que reduzam a sua probabilidade, se o nível de risco é tolerável ou aceitável e requer algum tratamento adicional. Além de métodos e técnicas a serem usados para avaliação de risco, e sua contribuição para o processo de gestão de risco e o contexto em que a organização está inserida, bem como seus objetivos (ABNT, 2009).

A noção de risco é, portanto, baseada em uma combinação de um conhecimento possível e incerteza do objeto estudado e da análise de riscos do ambiente, sendo a incerteza dos resultados e seus elementos que servem de base para importantes para decisões na gestão dos riscos, podendo ser muito significativa e ter consequências relevantes.

A caracterização das incertezas no processo de análise de riscos, por sua vez, tem a vantagem de demonstrar que o conhecimento é incompleto e que as decisões serão tomadas utilizando-se os conhecimentos disponíveis, bem como a análise do grau de incerteza e, enfim, decidindo se o risco é aceitável ou não. Além disso, também permite atuar eficazmente ou de um modo mais eficiente para reduzir a incerteza

resultante, permitindo separar as incertezas aleatórias das intelectuais, que interferem na eficácia no controlo finais, e possibilitando a adaptação do processo de decisão ao tipo e valor das incertezas (ALMEIDA, 2014).

É importante ressaltar que os riscos internos em empresas estão ligados diretamente à operações e processos, o que pode incluir atividades de planejamento, pesquisa e desenvolvimento, compartilhamento de informações e/ou estrutura organizacional (LIN; ZHOU, 2011). Diante disso, a necessidade de administrar riscos passa a ser elemento no mercado competitivo e, dessa forma, surge a necessidade de agregar valor e aperfeiçoar o desempenho das organizações de forma contínua.

Em relação à probabilidade, Laneve et al. (2014) destacam que pode ser representada por exposição dos elementos ou ativos, pela a sensibilidade de propensão dos elementos expostos para determinar o nível de danos e por fim sua capacidade de antecipação e resposta, pois elas influenciarão na sensibilidade dos elementos e nas exposições que eles sofreram.

Um passo importante na gestão do risco consiste em classificar o tipo de risco enfrentado. Seguindo a classificação de Brasiliano (2016), podemos dividir os riscos em quatro grupos principais:

- Riscos estratégicos: associado à tomada de decisões dos escalões mais altos da organização. Estão relacionados à geração de lucros ou perdas significativas para organização.
- Riscos operacionais: relacionados à ocorrência de falhas, deficiências ou inadequações de processos internos e/ou pessoas, eventos e sistemas externos.
- Riscos legais e de conformidade: relacionados a desobediências legais ou regulamentares de mudanças na legislação, ou ainda do descumprimento de contrato sendo necessário cada nicho de negócio conhecer suas adequações.
- Riscos financeiros: trata da gestão e do controle ineficaz dos meios financeiros da organização e possíveis efeitos de elementos externos.

Embora essa classificação seja útil para identificar o risco a princípio, não existe uma classificação consensual para todas as organizações. O que o gestor de risco deve estar atento é que uma classificação deve ser desenvolvida de acordo com as características de cada organização, contemplando as particularidades da indústria, do mercado e do setor de atuação. Ademais, atualmente as atividades de um departamento de gerenciamento de riscos corporativos abrange diversas disciplinas que são comuns a uma ampla gama de funções administrativas. Portanto, o processo de gerenciamento de risco deve ser sistêmico e contínuo, consistindo em identificação de exposição,

medição, análise, controle, prevenção, redução, avaliação e financiamento de riscos (BRASILIANO, 2016).

2.2 *Cybersecurity e cyber-risks*

A Agência de Segurança Cibernética e Infraestrutura (CISA) define segurança cibernética (*Cybersecurity*) como a arte de proteger redes, dispositivos e dados contra acesso não autorizado ou uso criminoso e a prática de garantir a confidencialidade, integridade e disponibilidade de informações. Tem-se a percepção que agora todas as coisas dependem da informática e da internet, seja na parte de comunicação, de entretenimento, de transporte, compras, saúde e em diversas outras áreas. Segundo o Departamento de Defesa dos Estados Unidos (2018), embora o custo de execução de um ataque cibernético seja relativamente pequeno, os riscos e suas consequências financeiras podem ser significativas para as organizações. De acordo com Humayun et al. (2020), a segurança cibernética pode ser definida como:

> [...] a coleção de ferramentas, técnicas, políticas, medidas de segurança, diretrizes de segurança, estratégias de mitigação de risco, ações, treinamento, boas práticas, garantia de segurança e tecnologias mais recentes que podem ser usadas para proteger o espaço cibernético e os ativos dos usuários.

Os riscos de um ataque cibernético, por sua vez, são divididos em *Hacker*, *Attacker*, ou *Intruder*, que podem ser definidos como pessoas que buscam métodos de explorar fraquezas de sistemas ou softwares para seu ganho pessoal. Um ataque *Hacker* pode significar assumir o controle de um computador remoto por meio de uma rede ou *cracking* de *software*. Esses *hackers* são chamados de cracker ou *black-hat hacker* ou simplesmente "criminosos". Os *intruders* são basicamente usuários não autorizados de um computador, um segundo usuário legítimo "indevido" que faz uso indevido de seus privilégios e um terceiro "usuário clandestino" que se apodera do controle de supervisão do sistema e o usa para suprimir informações de auditoria. Um *attacker*, por sua vez, viola computadores e redes de computadores executando atividades maliciosas para destruir, expor, alterar, desabilitar, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um ativo. (ASHOOR; GORE, 2011; CISA, 2021).

O uso dos *malwares*, arquivos ou programas indesejados, podem causar danos a um computador ou uma rede de computadores comprometendo os dados armazenados, neles estão incluídos os vírus. Os principais riscos de um ataque cibernético podem ser por *phishing*, em que o atacante envia para vários destinatários *e-mails* com uma mensagem falsa, induzindo o usuário a clicar em um site infectado ou baixar um *malware* que infecta um computador ou uma rede de computadores. Seguindo a mesma ideia, mas usando um ataque de voz, a vítima recebe ligação ou contato por

algum aplicativo de comunicação, no qual o atacante presta um serviço falso e o utiliza para adquirir as senhas da vítima (CISA, 2021).

Pode-se citar ainda os *worms* e Cavalos de Tróia, muito usados através de anexos de *e-mail* e páginas falsas na web. Por último, as vulnerabilidades, que são falhas no *software*, *firmware* ou *hardware*, que podem ser exploradas por um invasor para realizar ações não autorizadas em um sistema. Eles podem ser provindos de erros na programação de infraestrutura do software ou ser aproveitada a oportunidade que o *malware* expôs aos sistemas com suas fraquezas (CISA, 2021).

A Agência Nacional de Segurança dos Estados Unidos (NSA, 2020) examinou as tendências que contribuem para a frequência e eficácia dos ataques, como a semelhança entre as ferramentas, estratégias e técnicas usadas por vários atores, o que reduz a confiabilidade do uso desses fatores para identificar os responsáveis por invasões de rede de computadores. Os sites de *hackers* prevalecem na Internet, e ferramentas de compartilhamento são comuns. Isso faz com que os intrusos não relacionados exibam características técnicas semelhantes, tornando difícil diferenciar, detectar e identificar atacantes específicos por causa dessas assinaturas de atacantes combinadas (NSA, 2020).

Esses impactos podem ser em maior ou menor grau de acordo com o nível de proteção, seja informações pessoais regulamentadas ou segredos comerciais. Desse modo, as tecnologias utilizadas para detectar ataques são um reflexo direto do compromisso e do investimento da empresa nessa área e do nível de sofisticação daqueles que tentam penetrar na defesa aplicada (ULSCH, 2014).

É importante ressaltar, por fim, que o recurso à informação é essencial para as organizações. Existem consequências importantes como manter informações de qualidade para apoiar nas decisões corporativas, agregar valor ao negócio com estratégias para atingir benefícios eficientes e inovadores, alcançar excelência operacional por aplicações confiáveis e eficientes, conhecer os riscos e manter em um nível aceitável, otimizar custos e serviços e cumprir leis, regulamentos (ISACA, 2012).

2.3 Gestão de riscos cibernéticos

A implementação do processo de gerenciamento de riscos em uma organização deve ser baseada em estruturas de gerenciamento de riscos, compromissos no seu gerenciamento, criação e uso de políticas, integração nos processos organizacionais e manutenção de comunicações internas e externas. Dessa forma, o processo global de avaliação de risco consiste em: identificação, em que o risco é reconhecido e descrito; análise, que é processo de compreender a natureza do risco e determinar o seu nível; e

avaliação de riscos, em que é possível comparar os resultados da análise de riscos com os critérios para determinar se sua magnitude é aceitável ou não (ABNT, 2009).

Segundo Refsdal, Solhaug e Stølen (2015), a gestão de riscos é também formada por etapas de reconhecimento do ambiente, comunicação e consultoria que visam fornecer, compartilhar, ou obter informações interagindo com as partes interessadas em relação à gestão de riscos. Essas informações servirão de base para tomada de decisões internas (reorganização, estratégias ou ações sobre os riscos) ou externas (legislação, situação do mercado). Essas decisões poderão estar relacionadas à existência, natureza, forma, probabilidade, significância, avaliação, aceitabilidade e tratamento, mas para que isso ocorra é necessário ter uma equipe dedicada, planos de processos definidos que possam garantir o fortalecimento da gestão de riscos e divulgação de seus resultados.

O gerenciamento de riscos envolve inicialmente as etapas de identificação e análise, que podem ser feitas por meio de um *brainstorming* (encontros para troca de ideias) ou uso de dados históricos. Essa escolha deve ter como objetos de análise os custos e benefícios dos tratamentos identificados. Existem quatro opções principais para o tratamento de risco: *(i)* redução das ocorrências de riscos e suas consequências; *(ii)* retenção de risco, ou seja, aceitar o risco informado de acordo com seus padrões organizacionais; *(iii)* prevenção de riscos, e; *(iv)* compartilhamento de riscos através de seguro ou subcontratos com outras empresas (REFSDAL; SOLHAUG; STØLEN, 2015).

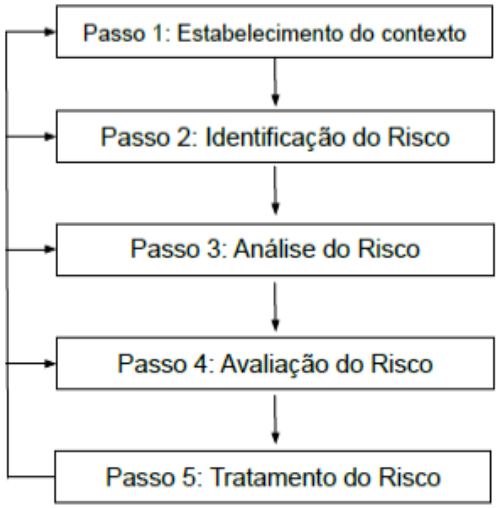
As etapas de monitoramento e revisão de riscos estão mais focadas na identificação dos riscos e nas medidas que a organização deve implementar para tratá-los, sendo o monitoramento uma verificação contínua, supervisionada observando a criticidade. A atividade de revisão consiste em determinar a pertinência, adequação e eficácia do processo e estrutura de uma gestão de riscos, bem como os seus riscos e tratativas. Monitoramento e revisão garantem a eficácia e eficiência dos controles, obtendo informações de melhorias, aprendendo através de análises de incidentes, mudanças, sucessos e fracassos e identificando riscos emergentes (REFSDAL; SOLHAUG; STØLEN, 2015).

O Sistema de Gestão de Segurança da Informação (SGSI) adotou um modelo conhecido como *"Plan-Do-Check-Act"* (PDCA), que é aplicado como modelo para estruturar todos os seus processos (ABNT, 2009). *Plan* (planejar) consiste em estabelecer políticas, objetivos, processos e procedimentos que são importantes para a gestão de risco e a melhorias, produzindo objetivos da organização; *Do* (fazer) consiste em implementar e operar a política, controle, processos e procedimentos; *Check* (checar) consiste em monitorar e analisar, medindo o desempenho do processo em relação à política, apresentando uma análise crítica para a direção; *Act* (agir) é relativo às ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI ou outras informações para melhorar de forma contínua o processo de uma gestão de

riscos.

A Figura 1 a seguir exemplifica o processo de gestão de risco nas suas etapas essenciais (REFSDAL; SOLHAUG; STØLEN, 2015).

Figura 1 – Etapas da gestão de risco



Fonte: Refsdal, Solhaug e Stølen (2015)

Segundo Refsdal, Solhaug e Stølen (2015), o processo de avaliação de risco é dividido em cinco partes. O primeiro passo é estabelecer um contexto, preparando-se para as atividades subsequentes, a partir da documentação do contexto externo e interno de relevância para a avaliação em questão. O passo seguinte consiste em identificar, descrever e documentar os riscos e suas possíveis causas. Após serem identificados é necessário estimar e determinar o nível dos riscos identificados na fase de análise ou terceiro passo. Com o risco devidamente identificado e analisado é possível evoluir para o quarto passo em que são exercidas as atividades que envolvem a comparação dos resultados da análise de risco com os critérios de avaliação de risco para determinar quais riscos devem ser considerados para tratamento. Por fim, o quinto e último passo consiste em identificar e selecionar meios de mitigação e redução de risco.

Diante das proposições da literatura, fica claro que a gestão de risco se configura como um processo contínuo de identificação, avaliação, resposta e gerência. De tal modo, organizações devem compreender que existe a probabilidade de que um evento ocorra e com isso os seus possíveis impactos. As organizações podem determinar o nível de risco que são aceitáveis para atingir seus objetivos organizacionais e podem expressar isso como sua tolerância ao risco (NIST, 2018).

A Estrutura de Segurança Cibernética do *National Institute of Standards and*

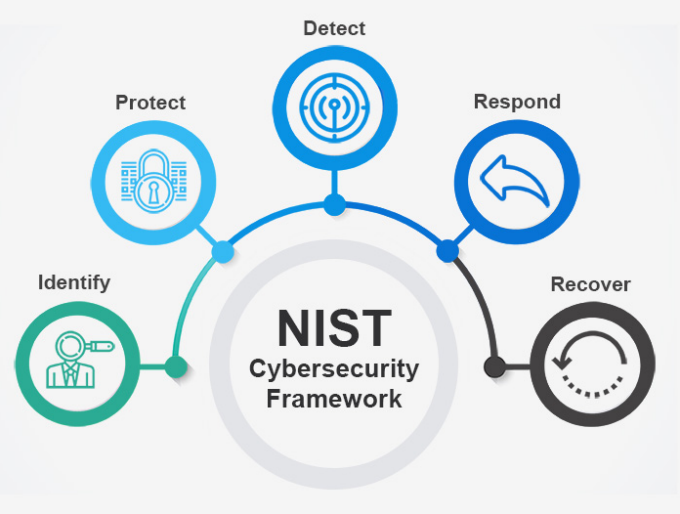
Technology (NIST), nos Estados Unidos, procura solucionar a falta de padrões no que diz respeito à segurança cibernética, fornecendo "uma taxonomia de alto nível dos resultados de segurança cibernética e uma metodologia para avaliar e gerenciar esses resultados". Segundo essa estrutura, a gestão do risco consiste em três componentes principais (TELES, 2020; NIST, 2018):

- O núcleo da estrutura: um conjunto de atividades e resultados de cibersegurança desejados, usando linguagem acessível. O núcleo orienta as organizações no gerenciamento e na redução de riscos de segurança cibernética, complementando as metodologias existentes de segurança cibernética e gerenciamento de riscos.
- O perfil da estrutura: o alinhamento exclusivo de uma organização de seus requisitos e objetivos organizacionais, propensão ao risco e recursos com os resultados desejados do núcleo da estrutura. Os perfis são usados principalmente para identificar e priorizar oportunidades para melhorar os padrões de segurança e mitigar os riscos em uma organização
- As camadas de implementação da estrutura: fornece um contexto sobre como uma organização vê o gerenciamento de riscos de segurança cibernética, orienta-os a considerar qual é o nível de rigor apropriado para eles e é frequentemente usado como uma ferramenta de comunicação para discutir o apetite ao risco, a prioridade da missão e o orçamento.

A partir disso são definidas as atividades inerentes aos padrões de segurança cibernética. São elas: Identificar, Proteger, Detectar, Responder e Recuperar (conforme mostra a Figura 2). A função Identificar diz respeito ao entendimento organizacional do risco de segurança cibernética para sistemas, pessoas, ativos, dados e recursos. A função Proteger descreve as defesas na entrega de serviços e limites críticos de infraestrutura. Detectar refere-se à identificação de ocorrências de eventos de segurança cibernética em tempo hábil. A função Responder está relacionada às ações após um incidente de segurança para melhorar a resposta e reduzir o impacto de um evento. A função Recuperar diz respeito ao restabelecimento de recursos ou serviços que foram prejudicados durante um ataque cibernético (TELES, 2020; NIST, 2018).

A fim de apresentar uma visão mais clara e abrangente da etapa inicial em um modelo de gerenciamento de riscos, este trabalho abrange principalmente a etapa Identificar do modelo NIST. Nesse estágio estão incluídas subcategorias que abrangem gerenciamento de ativos, *risk assessment*, governança, questões voltadas ao ambiente de negócios e estratégias de gestão de risco.

Figura 2 – Modelo NIST de *cybersecurity*



Fonte: InfoSec (2021)

2.4 Ferramentas para análise de riscos cibernéticos

Segundo Ali, Warren e Mathiassen (2017), o gerenciamento de risco usa várias descobertas para vincular riscos e resoluções. Nesse contexto, risco refere-se à probabilidade de ocorrência e ao impacto de um resultado adverso, enquanto a resolução refere-se a recursos e esforços para evitar, transferir, prevenir, mitigar ou assumir os riscos. As descobertas, por sua vez, vinculam riscos específicos a uma ou mais resoluções apropriadas. A qualquer momento, os gerentes de uma organização identificam e avaliam os riscos que podem ocorrer, sua probabilidade e seu impacto potencial. Eles então exploram e avaliam quais resoluções, se aplicadas, evitariam, transfeririam, preveniriam, mitigariam ou os ajudariam a assumir os riscos que podem ser encontrados no futuro.

Para Dikmen, Birgonul e Arikan (2004) muitas ferramentas de suporte à gestão de riscos dividem-se em qualitativa e quantitativa, a depender da fase em andamento. Muitas dessas ferramentas são baseadas em análises quantitativas de risco em uma fase e em outras são realizadas sem uso de *softwares*. Portanto, registros de risco e ferramentas de avaliação de risco que são propostos como sistemas de apoio à decisão que só podem ser usados em estágios específicos de um projeto.

Em um estudo de práticas de gestão de riscos em projetos ágeis, Tavares, Silva e Souza (2019) observaram que, os subcomponentes classificados como artefatos (Plano de contingência, Incremento, Protótipo, Repositório de risco, Especificação técnica, Biblioteca de código de *software*, etc.) são os mais importantes para a realização de um gerenciamento eficaz de riscos em projetos ágeis, seguido por eventos, funcionalidades,

funções e técnicas e métodos. A razão é que os artefatos são responsáveis por registrar os riscos e seus planos de exposição e resposta, sendo possível identificar, analisar, planejar respostas e monitorar riscos.

Muitas ferramentas estão disponíveis para gestão de riscos em suas várias fases. Hernández, Carreño e Castillo (2018) buscam destacar essas ferramentas, em particular aquelas associadas a projetos bem-sucedidos. Os autores destacam que em um processo de gerenciamento de risco deve-se primeiro considerar as ferramentas que são mais comumente usadas, assim a organização estará mais perto do estado atual da prática em campo. No topo da lista de ferramentas mais usadas estão a simulação, em primeiro lugar, seguida pela Avaliação de Responsabilidade e Avaliação de Impacto de Risco. Outro resultado importante refere-se às ferramentas que estão associadas a um gerenciamento de projeto de melhor desempenho, ou que são utilizadas por profissionais que já possuem um bom processo de gestão de risco. Entre essas ferramentas estão algumas que serão objeto de estudo nesse trabalho, a saber: revisão periódica de documentos, avaliação de impacto de risco, *checklists*, atribuição de responsabilidade, entre outras (HERNÁNDEZ; CARREÑO; CASTILLO, 2018).

No contexto de riscos cibernéticos, a identificação de ameaças maliciosas deve ser feita prestando atenção especial à interface com o ciberespaço e à superfície de ataque documentada Refsdal, Solhaug e Stølen (2015). Para isso, pode-se envolver pessoas com conhecimento de primeira mão sobre o alvo da avaliação, o que pode ser feito, por exemplo, por meio de questionários, listas e banco de dados com foco nas ciber-ameaças, vulnerabilidades e incidentes que causam riscos inaceitáveis. Com isso, pode-se fazer uso da descrição do alvo da avaliação, investigando onde e como os ataques podem ser lançados com foco nas ciber-ameaças, vulnerabilidades e incidentes que causam riscos inaceitáveis.

Embora questionários sejam muito úteis para extrair informações e conhecimento das pessoas, ao utilizá-los não há possibilidade de perguntas de acompanhamento ou de esclarecimentos que poderiam ser feitos em reuniões presenciais ou *brainstormings*. Além disso, o sujeito tem pouca oportunidade de se aprofundar em questões que não são abordadas no questionário, o que pode causar perda de informações importantes (REFSDAL; SOLHAUG; STØLEN, 2015).

Em se tratando de sistemas de detecção, a *QualysGuard* é uma das principais ferramentas em segurança cibernética com foco em riscos de vulnerabilidades de segurança, levando em consideração a gravidade, risco do negócio, pontuações de métricas específicas, *malware* e *patches* disponíveis. Essa ferramenta usa uma abordagem baseada em riscos para priorizar os esforços de remediação e corrigir as vulnerabilidades que afetariam os negócios. Como esta, existem outras ferramentas semelhantes (*Nessus, Saint8, Retina Security Scanner, GFI LANGuard, nCircle® IP360, Security System Analyzer*

2.0, OpenVas, Nexpose) que usam diferentes métricas e abordagens para priorização baseada em risco. A maioria dessas ferramentas usa métricas de pontuação para avaliar o risco que uma vulnerabilidade pode representar para o negócio, seja nas próprias estratégias da ferramenta ou adicionando novas métricas que permitem ao usuário um melhor entendimento do que está acontecendo no ambiente. Além disso, para ter dados mais completos para o gerenciamento de riscos, muitas dessas fazem integração com outros parceiros comerciais de tecnologia para aprimorar ainda mais o gerenciamento de vulnerabilidades que podem afetam uma organização (ROLDÁN-MOLINA et al., 2017).

Duas ferramentas apresentadas neste estudo são baseadas em questionários e outra baseada no sistema *QualysGuard* de varredura de vulnerabilidades, conforme será exposto na próxima seção.

3 Metodologia

O estudo de caso é um método que consiste na investigação qualitativa detalhada de uma ou mais organizações, ou grupos dentro das organizações, com vista a fornecer uma análise do contexto e dos processos envolvidos no fenômeno em estudo (MEYER, 2001). Neste trabalho, utilizou-se a abordagem do estudo de caso para descrever a execução do procedimento proposto em uma empresa de grande porte de forma a testar a aplicabilidade do mesmo.

Trata-se de uma organização multinacional do seguimento de produção de gases industriais e medicinais fundada no Brasil há mais de 100 anos com cerca de 80 mil funcionários, referência na América Latina e no mundo em seu ramo. A empresa está presente na Argentina, Bolívia, Chile, Paraguai, Peru e Uruguai e conta hoje com pelo menos 27 fornecedores de serviços digitais, todos submetidos ao sistema de gerenciamento de riscos cibernéticos adotado pela empresa. Esse sistema é chamado Gerenciamento de Segurança da Informação (GSI) e é utilizado globalmente pela empresa, buscando promover uma cultura de prevenção e gerenciamento contínuo de riscos em que todos os eventos são devidamente reportados e analisados. Esse processo é representativo de vários outros adotados no Brasil, portanto, o estudo de caso deve servir como modelo para o entendimento das práticas de segurança adotadas no mercado brasileiro.

Para efeito de exemplificação do funcionamento do GSI na análise de *cyber-risks* na empresa, suponha que dois fornecedores X e Y ofereçam o mesmo serviço. Ambos serão submetidos ao GSI e aquele que oferecer maior segurança será favorito. Dessa forma, caberá ao gestor lidar com o *tradeoff* preço e segurança. Muitos aplicativos são ofertados por fornecedores que já inseriram outros serviços digitais na empresa. Nesses casos o mesmo sistema de segurança é implementado e a aplicação é submetida ao GSI.

O Gerenciamento de Segurança da Informação (GSI) adotado pela empresa não se concentra apenas em identificar riscos e esteja alinhado com as várias fases propostas na literatura, em particular aquelas apresentadas na Figura 2. Os processos não se concentram em um único setor ou grupo de colaboradores. Dessa forma, um grupo é designado para identificação, mas pode participar e resolver outras fases, outro grupo é responsável pela proteção e assim por diante. Nesse processo há comunicação na horizontal e vertical, isto é, por níveis e áreas. Dessa forma, não existe um único grupo que concentre todas as fases e resoluções de problemas. Portanto, para fins de viabilidade e obtenção dos objetivos propostos, será abordada em particular a fase de

identificação de riscos e seus subcomponentes já explanados anteriormente.

É importante ressaltar que, para a consecução do objetivo geral do trabalho, foram adotadas técnicas de coleta e análise de dados associadas a cada objetivo específico. O Quadro 1 contém um resumo desses componentes e relações.

Quadro 1 - Coleta e análise de dados

Objetivos do trabalho	Fonte de dados	Técnicas de coleta e análise de dados
Identificar procedimentos na literatura sobre gestão de *cyber-risks* e *cybersecurity*	- Livros e artigos sobre o tema - Normas técnicas - *Websites* sobre o tema	- Análise de conteúdo
Definir o procedimento de análise de cyber-risks que compõe o processo de gerenciamento de segurança da informação	- Documentos da empresa - Procedimentos utilizados em experiências anteriores	- Análise documental - Fluxogramas
Descrever a aplicação do procedimento em uma empresa de grande porte	- Documentos da empresa - Demandas dos fornecedores - Normas internas da empresa	- Questionários - Análise documental - Questionários - Análise documental - Sistema de detecção de ameaças (QualysGuard) - Matriz RACI - Análise probabilidade *vs.* impacto - Gráficos de colunas

Fonte: Elaboração Própria.

3.1 Procedimentos de aplicação

O processo GSI adotado pela empresa é realizado em todos os softwares que serão contratados pela organização, seja hospedado na nuvem (*SaaS/Cloud*)[1] ou internamente. A identificação dos riscos e, portanto, o entendimento organizacional do risco de segurança cibernética para sistemas, pessoas, ativos, dados e recursos é feita utilizando-se de documentos descritivos e procedimentos de análise de risco. Os componentes desse processo, referentes à parte que compete o escopo deste trabalho, são: *Business Service Level Description* (BSLD), *Risk Assessment* e *Scan* ou varredura de Vulnerabilidades (*Web* e aplicativo). O Quadro 2 a seguir sintetiza o objetivo de cada parte do processo.

[1] *SaaS*, ou *Software as a Service*, é uma forma de disponibilizar softwares e soluções de tecnologia por meio da internet, como um serviço.

Quadro 2 - Componentes do processo de Gerenciamento de Segurança da Informação (GSI)

Componente	Objetivo
BSLD	*i)* Descrever processos de fornecedores *ii)* Maturidade do fornecedor
Scan de Vulnerabilidades	*i)* Identificar vulnerabilidades existentes em aplicações e seus impactos. *ii)* Direcionar fornecedores para soluções de problemas.
Risk Assessment	*i)* Identificar o maior número de riscos existentes e iminentes; *ii)* Aumentar a capacidade de mitigação de danos

Fonte: Elaboração própria.

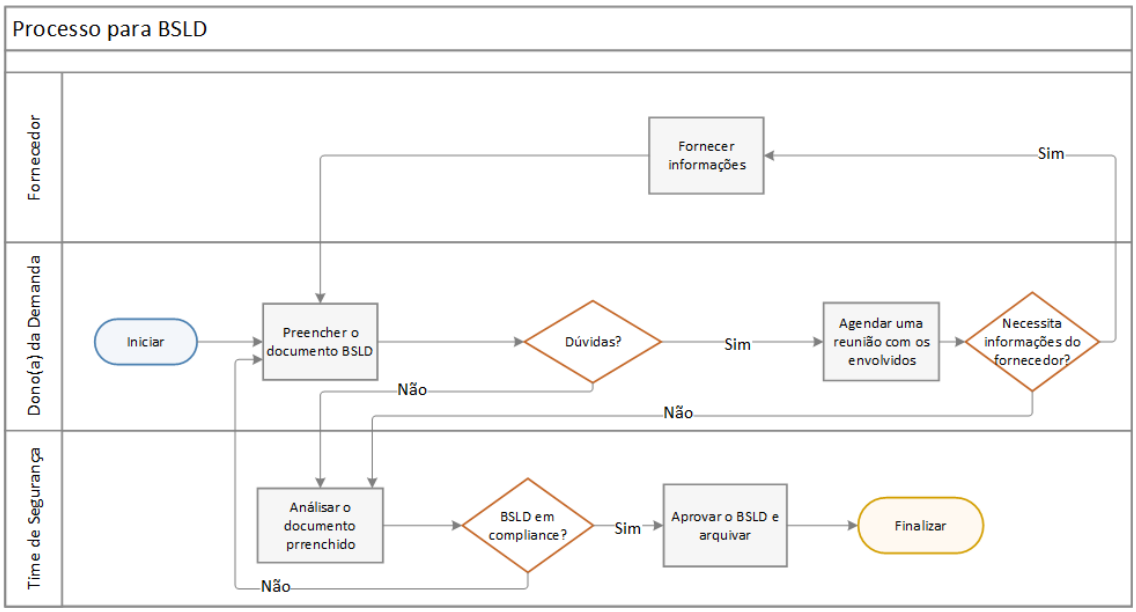
Esses processos servirão para identificar possíveis riscos e ameaças, que deverão ser mitigados ou aceitos, antes da aplicação ser contratada e/ou implantada. Os documentos do BSLD e *Risk Assessment* são enviados para os gestores que devem decidir assumir o risco, caso exista, aprovar ou reprovar o serviço.

3.1.1 BSLD *(Business Service Level Description)*

Nessa etapa há um detalhamento documental através de questionários com perguntas sobre o detalhamento de contratos da empresa fornecedora, continuidade de negócios, isto é, como a empresa propõe garantir o funcionamento adequado do serviço, procedimentos de *backup* e recuperação de dados, arquitetura da aplicação, etc. O objetivo é garantir um entendimento claro entre as partes interessadas quanto aos níveis de serviço, medidas, processos e planos de continuidade em vigor antes de um serviço ser colocado em operação. A Figura 3 detalha através de um fluxograma as etapas dentro do processo de documentação BSLD.

O dono da demanda, isto é, o responsável por acompanhar e executar os processos do sistema GSI, inicia o preenchimento do questionário apoiado pelo suporte do fornecedor. Após o preenchimento, o time de segurança deve analisar o documento. Caso seja aprovado o arquivo BSLD é arquivado, caso contrário uma reunião entre as partes envolvidas é necessária. Essa etapa da identificação, portanto, consiste em documentar riscos e garantir um entendimento claro entre as partes quanto aos níveis de serviço, medidas, processos e planos de continuidade em vigor antes de um serviço ser colocado em operação.

Figura 3 – Fluxograma do procedimento BSLD



Fonte: Elaboração própria

Além de descrever a funcionalidade, nessa fase também são informados os níveis de criticidade e impacto comercial do serviço, indicando a importância da funcionalidade deste serviço para a empresa. A seguir apresenta-se uma descrição dos níveis de criticidade da ausência de um serviço para companhia em cada período de tempo: 1 hora, 8 horas, 48 horas, 72 horas, uma semana e um mês.

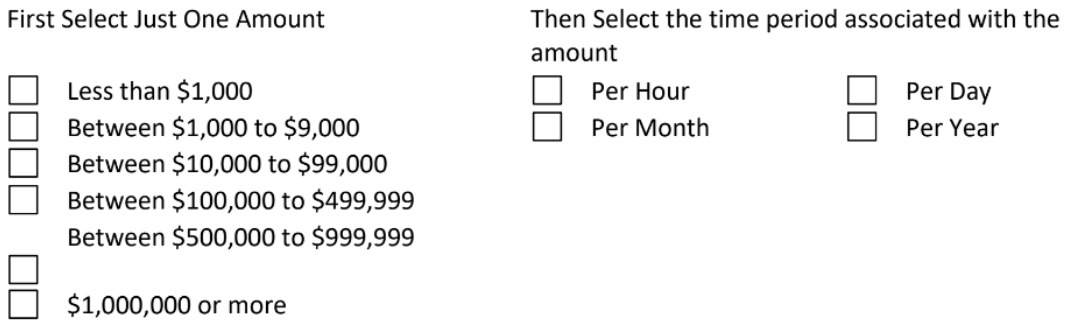
Quadro 3 - Impacto relativo da perda de um aplicativo no processo de negócios

Impacto	Consequência
Catastrófico	Fora do mercado e/ou colocar em risco a segurança pública.
Significativo	Grande impacto na situação financeira de longo prazo da empresa e/ou colocar em risco a segurança pública.
Moderado	Grande impacto da situação financeira de curto prazo da empresa.
Baixo	Nenhum impacto na situação financeira da empresa.

Fonte: Elaboração própria.

Seguindo o mesmo sistema de criticidade é feita a estimativa quantitativa de impacto e perda. Essa estimativa deve variar conforme a decisão do responsável por fornecer as informações de qual métrica utilizar. Feito isso, é possível selecionar o nível apropriado entre os seguintes impactos: redução de produtividade, aumento de custos, demora na obtenção de fundos, redução de renda, penas por atraso, penas de conformidade. Além disso, é necessário determinar as perdas em termos monetários. Isto é, para cada período de tempo específico e utilizando a melhor estimativa possível, estima-se as perdas se esses processos de negócios não puderem ser fornecidos e o prazo associado ao valor de perda. A figura 4 exemplifica esta etapa do procedimento.

Figura 4 – Estimativa de perdas monetárias - BSLD



Fonte: Documentos - BSLD

A etapa de documentação segue com uma descrição de como o aplicativo será monitorado e para quem os alertas serão enviados. Essas questões estão relacionadas à segurança da tecnologia da informação TI, em que o fornecedor deve indicar como a segurança será garantida através de informações como: qual o tipo de autenticação de usuário, quais controles de acesso, senhas, administração do usuário (criação, mudança de departamento, abandono), incluindo uma revisão regular do usuário definido. Nessa etapa técnica o fornecedor é questionado sobre a estrutura do serviço, incluindo a arquitetura do sistema, com explicações sobre interfaces e dependências.

É importante que a empresa contratante saiba também as variações geográficas no processo de negócios ou serviço, caso se aplique. Nesse ponto é necessário que sejam informados os serviços entregues a várias geografias onde a entrega do serviço pode diferir. Entre essas regiões, por exemplo, os componentes regionais podem ser terceirizados em uma região.

Após as caracterizações iniciais é possível seguir com uma definição das responsabilidades da Tecnologia da Informação e dos negócios. Nesse sentido, o fornecedor deve criar uma matriz de responsabilidade RACI (*Responsible, Accountable, Consulted e Informed* [2]), das principais atribuições entre a empresa e o setor de TI, seja ele corporativo, regional ou nacional. São considerados itens como educação do usuário, suporte de primeira linha, manutenção de dados mestre, administração e etc. A seguir temos um quadro exemplo da matriz de responsabilidade que os fornecedores devem providenciar.

[2] Responsável, Prestador de Contas, Consultado e Informado

Tabela 1 – Exemplo de Matriz de Responsabilidade RACI

Referência da Tarefa	Categoria da tarefa	Tarefa	Dono do serviço de TI	TI corporativo	Externos	Time regional	Negócios regionais	Comentários
1	Usuário administrativo	Autorização e definição dos usuários					A, R	-
2	*Master Data*	Manutenção de dados	C				A	-
3	Suporte	Suporte ao usuário	R,A				A	-
4	Novos Lançamentos	Novas ferramentas de melhoria	A, R		R		I	-
5	Segurança e *Backup*	*Microsoft Azure*			R, A			-

Fonte: Elaboração própria.
Nota: R (*Responsible)*, A (*Accountable*), C (*Consulted*) e I (*Informed*).

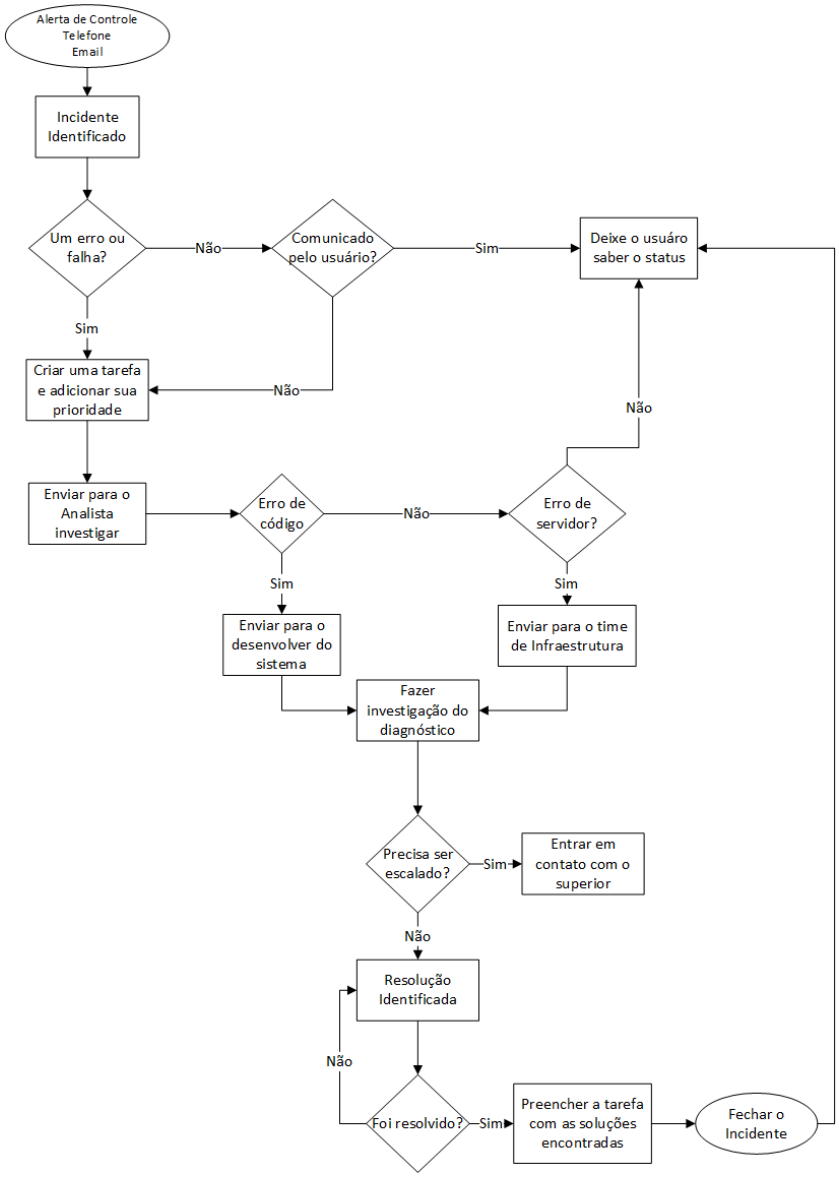
A Matriz RACI ou matriz de atribuição de responsabilidade, é uma ferramenta utilizada para definir e descrever as responsabilidades das partes interessadas de um projeto. *Responsável* ou responsável refere-se ao grupo de pessoas ou responsável geral que será responsáveis por executar as tarefas, desenvolvê-las e entregá-las. *Accontable* ou Prestador de Contas, é o líder ou grupo principal responsável pelo projeto, ou seja, o gerente de projeto que deve tomar as decisões finais. Esse indivíduo ou grupo Fica encarregado de responder perguntas como: quando a tarefa será iniciada? A tarefa foi realizada da forma correta? *Consulted* ou Consultado, como o nome sugere, refere-se a todos aqueles com a experiência ou o poder necessário para a conclusão bem-sucedida do nosso projeto que possam servir de auxílio técnico e/ou intelectual. O grupo *Informed* ou Informado engloba todas as pessoas que devemos manter informados sobre nossas ideias, decisões, progresso e sobre os resultados do projeto (CROSSKNOWLEDGE, 2020).

Além de uma estrutura de divisão de responsabilidades formalizada, o servidor deve oferecer uma visão clara da disponibilidade do serviço, em particular a disponibilidade de uma série de serviços de TI. Esses serviços são constituídos por componentes de infraestrutura e aplicativos. Por exemplo, tecnologia ou serviços de TI de aplicativos combinados com serviços de rede (*LAN, WAN*), local de trabalho (*desktops, laptops*, dispositivos portáteis). No mais, é necessário informar o horário em que o serviço está disponível para que os usuários possam entrar e usar o sistema. Por exemplo, pode-se

estabelecer que o sistema deve estar disponível 24 horas por dia, 7 dias por semana, exceto para interrupções acordadas pelas unidades de serviço comercial.

Por fim, é necessário documentar a existência de um ponto de recuperação anterior ao desastre, em que a recuperação de dados pode ser realizada de acordo com a arquitetura atual e as disposições de *backup*. Além disso, é importante delinear estratégias de enfrentamento de negócios para garantir a recuperação e integridade dos dados, ou seja, recuperação de outras fontes, entrada manual de dados, etc. A Figura 5 exemplifica um plano de recuperação da informação e sua estrutura. Ademais, um resumo de todas as seções de perguntas nesse procedimento está disponível no Apêndice A.

Figura 5 – Exemplo de plano de recuperação de informação



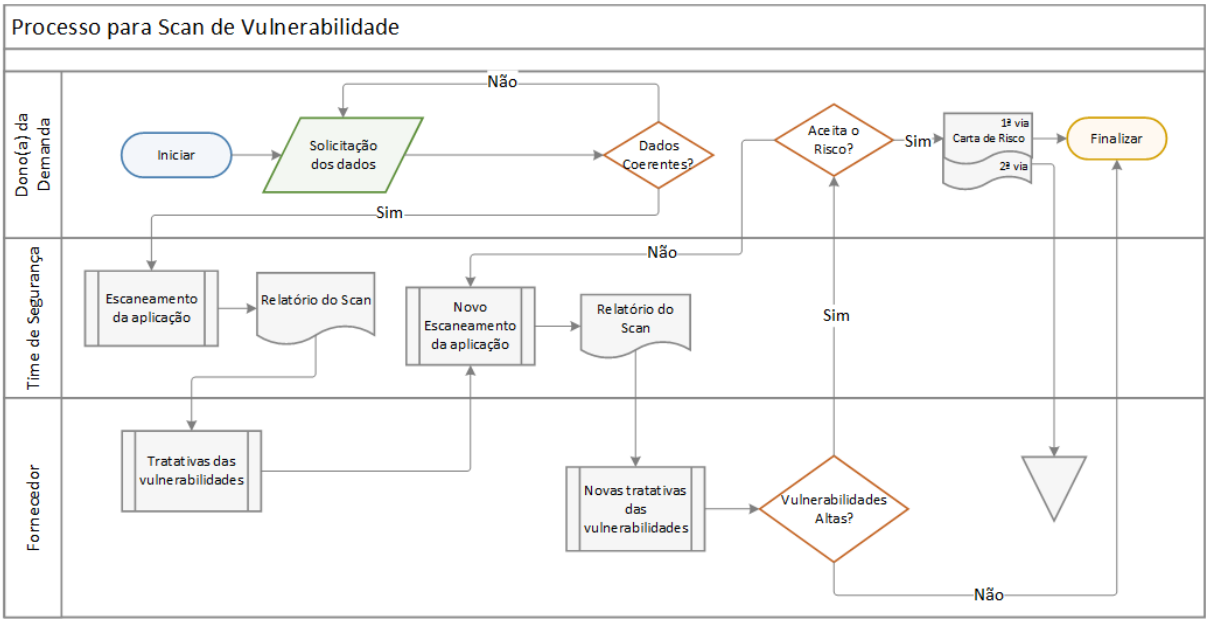
Fonte: Elaboração própria

3.1.2 *Scan* de vulnerabilidades

O procedimento *Scan* rastreia e identifica vulnerabilidades existentes na aplicação e sua infraestrutura. O fornecedor deverá corrigir essas vulnerabilidades, que serão confirmadas através de um novo *Scan*, o procedimento continua até que as vulnerabilidades sejam corrigidas e/ou mitigadas ou até que se assuma o risco ou se rejeite o serviço.

O fluxograma para o *Scan* de vulnerabilidades é mais complexo em relação ao BSLD. O dono da demanda mais uma vez inicia o procedimento solicitando dados aos fornecedores, caso essas informações sejam coerentes, inicia-se a varredura e indicação de tratativas das vulnerabilidades apontadas no relatório do escaneamento e o processo continua até que as fraquezas sejam mitigadas ou o risco seja aceito. Caso as informações fornecidas não estejam de acordo com o solicitado é feita uma nova solicitação até que estejam em conformidade e o processo possa iniciar.

Figura 6 – Fluxograma do processo *Scan* de vulnerabilidades



Fonte: Elaboração própria

O sistema de proteção contra o risco analisado neste estudo utiliza o escaneamento de vulnerabilidades oferecido pela empresa *Qualys*. A metodologia de varredura (*QualysGuard*) concentra-se principalmente nas diferentes etapas seguidas por um invasor em um ataque, utilizando as mesmas técnicas de descoberta e coleta de informações que serão usadas por um invasor. O mecanismo de varredura é composto por diferentes módulos que lidam com tarefas específicas e encadeamentos inteligentes para evitar a execução de verificações de vulnerabilidade sem sentido. Ele apenas

executa a detecção de vulnerabilidade com base em serviços que foram descobertos e identificados corretamente (QUALYS, 2020).

A primeira etapa é verificar se o *host* a ser verificado está ativo e em execução para evitar perda de tempo com a verificação de um *host* inativo ou inacessível. Se o *Scan*receber pelo menos uma resposta do *host* remoto, ele continuará a varredura. Dessa forma, vulnerabilidades de todas as varreduras selecionadas são consolidadas em um relatório para que se possa ver sua evolução (QUALYS, 2020).

A categorização das vulnerabilidades é feita através de um sistema de cores e criticidade, como ilustra a figura a seguir.

Figura 7 – Vulnerabilidades por nível de severidade

Severity	Level	Description
HIGH	High	Indicates that at least one threat was detected with a severity 5 or 4 (confirmed or potential).
MED	Medium	Indicates that at least one threat was detected with a severity 3 (confirmed or potential).
LOW	Low	Indicates that at least one threat was detected with a severity 2 or 1 (confirmed or potential).
INFO	Info	Indicates that only information gathered QIDs were detected.
SAFE	Safe	Indicates that the scan finished and no threats were detected.

Fonte: Qualys (2020)

Vulnerabilidades de nível 4 e 5 (Vermelhas) são falhas de *design*, erros de programação ou configurações incorretas que tornam os produtos suscetíveis a ataques maliciosos. Dependendo do nível de risco de segurança, a exploração bem-sucedida de uma vulnerabilidade pode variar desde a divulgação de informações até o comprometimento total ou parcial do aplicativo podendo, ainda, fazer com que o aplicativo seja usado para lançar ataques contra os usuários do site. Para esse nível de risco é necessário que os problemas sejam resolvidos antes do aplicativo entrar em produção na empresa, caso seja aprovado pelo procedimento de gestão de risco.

Vulnerabilidades de nível 3 ou potenciais (Alaranjadas) indicam que o mecanismo de varredura observou uma fraqueza ou erro que é comumente usado para atacar um aplicativo, sem que se possa confirmar se essa fraqueza ou erro poderia ser explorado. Com vulnerabilidades de nível 2, 1, e 0 (Amarelas), conteúdos sensíveis podem ser detectados com base em padrões conhecidos (números de cartão de crédito, números de previdência social) ou padrões personalizados (*strings*, expressões regulares), dependendo da opção de perfil usada. Os invasores podem obter acesso a conteúdo confidencial que pode resultar em uso indevido ou outras explorações.

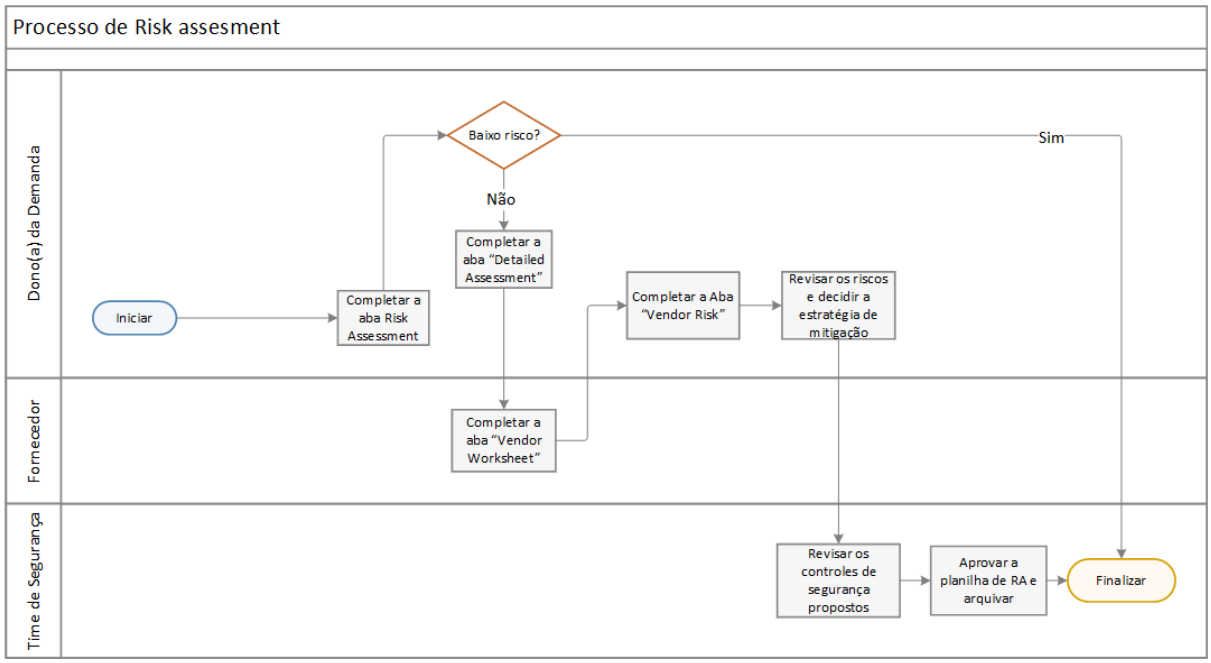
Informações agregadas (Azuis), por sua vez, são as informações coletadas que incluem informações visíveis sobre a plataforma, o código ou a arquitetura do

aplicativo da *web*. Também pode incluir informações sobre os usuários do aplicativo da *web*.

3.1.3 *Risk assessment*

A etapa *Risk assessment* se assemelha à etapa BSLD, em que é necessário apresentar uma série de informações acerca da aplicação a fim de determinar o nível de risco. A diferença é que quem deve fornecer as questões é o dono do ativo em quase todos os componentes. Além disso, traz também possíveis controles mitigatórios para serem implementados na aplicação. Essa avaliação é composta por 6 questionários com diferentes atribuições e objetivos, são eles: avaliação inicial de risco, avaliação detalhada de risco, riscos do fornecedor, planilha do fornecedor e resultados da avaliação de risco. Todas essas etapas são inter-relacionadas, isto é, o nível identificado na avaliação inicial vai influenciar a avaliação detalhada e assim por diante. As planilhas riscos do fornecedor e planilha do fornecedor representam a importância da cooperação entre o avaliador e o fornecedor do serviço.

Figura 8 – Fluxograma do processo *Risk Assessment*



Fonte: Elaboração própria

O fluxograma para o procedimento de *Risk assessment* ressalta que todo o processo é iniciado pelo dono da demanda. Embora também seja composta por questionário, ocorre de maneira mais extensa e detalhada. São submetidas as informações e determinado um nível de risco, caso identifique-se baixo risco no início do processo,

este é finalizado sem mais complicações, caso contrário mais informações e análises serão necessárias.

Na planilha "avaliação de riscos inicial" (Figura 15), a nova demanda é cadastrada e informações como que tipo de dados é processado, armazenado ou transferido; criticidade operacional, ou seja, o impacto para o negócio em caso de paralisação; quais as perdas no caso de a confidencialidade, disponibilidade ou integridade da aplicação estiver seriamente comprometida. Dessa avaliação inicial é determinado um nível de risco. O dono do ativo deve seguir para próxima etapa em que a avaliação de risco é detalhada baseando-se no nível de risco identificado na avaliação inicial. Nesta segunda planilha, questões mais especificas de segurança são respondidas. Seguindo para terceira planilha temos uma estrutura de perguntas que serão enviadas ao fornecedor, isto é, um questionário enviado e respondido pelo fornecedor com base na avaliação de riscos das etapas anteriores. A planilha do fornecedor é organizada em seções, cada uma delas projetada para ajudá-lo a avaliar os riscos, como mostra a figura 17. O gestor deve revisar as respostas do fornecedor, usando essas respostas para fazer sua própria avaliação da probabilidade de ocorrência de um evento de risco. Depois de concluída essas etapas, é obtido um resultado da avaliação de risco, mostrado na planilha *Risk Assessment output* (disponível nas Figuras A1 - A4 na seção de anexos).

A partir desse estudo é possível identificar vulnerabilidades e riscos envolvidos em um processo de oferta de serviços digitais em um processo de gerenciamento real. Busca-se com esse estudo identificar possíveis itens frequentes e assim agregar ao estudo de segurança digital.

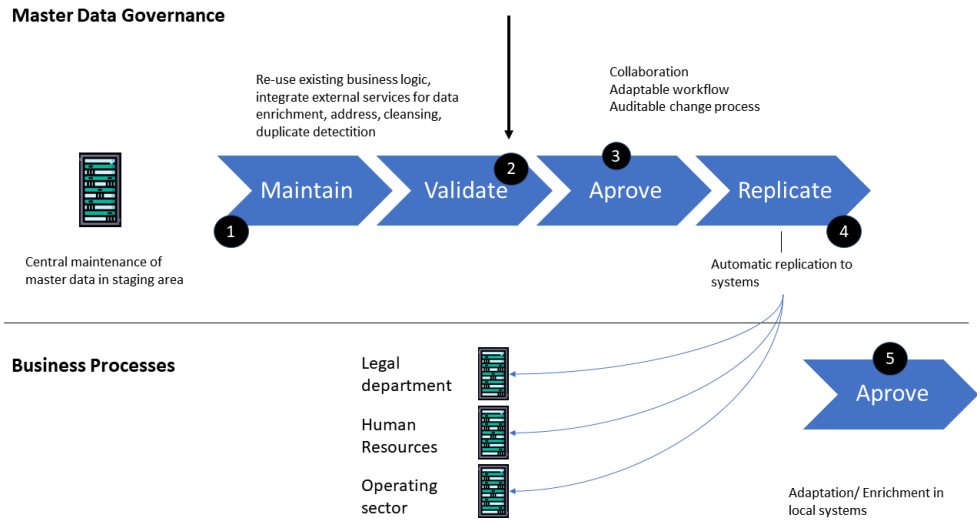
4 Resultados

A análise de riscos abordada neste trabalho consiste em identificar, descrever e documentar os riscos e suas possíveis causas. Além disso, a identificação é conduzida em relação aos ativos detectados, encontrando ameaças e entendendo como elas podem levar a incidentes (e, portanto, riscos) explorando vulnerabilidades (REFSDAL; SOLHAUG; STØLEN, 2015). Neste capítulo, esses componentes identificadores serão investigados a partir dos três instrumentos elencados no capítulo 3: BSLD, *Scan* de Vulnerabilidades e *Risk Assessment*.

4.1 Sistema analisado

Nas próximas seções serão analisados os resultados da aplicação dos procedimentos BSLD, *Risk* e *Scan* a um sistema oferecido por um fornecedor já consolidado na empresa. Esse sistema adicional propõe controlar a governança de dados usando solicitações para controlar a criação e mudança de informações sobre fornecedores. Dessa forma, novos dados só serão transferidos para o sistema após aprovação, sendo que até lá os novos dados são armazenados de forma temporária. Portanto, a qualidade no armazenamento de dados seria aprimorada por meio de um processo de controle estruturado que evitaria registros duplicados. Além disso, o fluxo de trabalho mantém os usuários informados sobre atualizações ou alterações nos dados cadastrais dos fornecedores.

Figura 9 – Processo de um sistema candidato a inserção na empresa.



Fonte: Questionário BSLD.

A Figura 7 demonstra o processo de funcionamento do sistema que consiste em manter, validar, aprovar possíveis mudanças de dados, evitar duplicações e adaptar os dados aos sistemas de outros tipos. Os objetivos propostos são, portanto, melhorar a qualidade dos dados por meio de regras de validação, integridade e consistência; consolidar e harmonizar o sistema de governança de dados; aumentar a assertividade para evitar "retrabalho", diminuindo, assim, custos de manutenção.

4.2 Aplicação do BSLD

O ponto de partida no procedimento BSLD consiste nos impactos mencionados na tabela 3. No caso de uma falha que impossibilite o funcionamento do sistema, o responsável pelo preenchimento do questionário, ou seja, o dono da demanda, considerou que os danos seriam mínimos, representando uma perda financeira de menos de 1000 unidades monetárias, tal como demostra a figura 10.

Figura 10 – Impacto da ausência do serviço candidato em caso de falha.

Fonte: Questionário BSLD.

Um ponto importante em segurança é a possibilidade de acesso à aplicação, já que se trata de um conjunto de dados de fornecedores. O sistema estará disponível para os funcionários da empresa contratante que têm a responsabilidade pela criação e/ou alteração de dados mestres de fornecedores, isto é, o gerente de linha. O gerente de linha precisará fornecer informações importantes no formulário de solicitação do usuário.

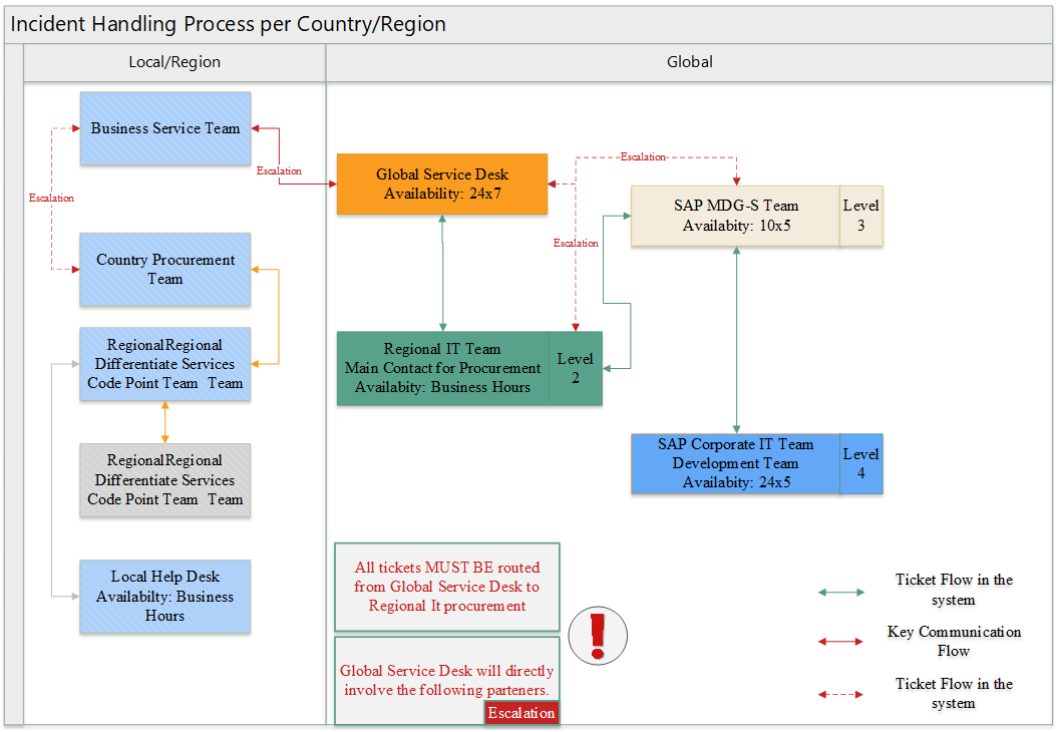
A divisão de responsabilidades fornecida no questionário define, portanto, que os componentes que compõem o serviço serão: melhorias; resolução de incidentes e defeitos; manutenção do sistema e monitoramento de desempenho; segurança e acesso; administração de IDs de usuários novos e obsoletos e atualização da estrutura organizacional, entre outros. A empresa contratante também deve ter responsabilidades, entre elas a definição do nível de autorização e aprovação de novos IDs de

usuário e identificação de IDs de usuário obsoletos, além de identificar mudanças na estrutura organizacional e propriedade e manutenção dos dados no sistema por meio de processos atualizados. Além dessas responsabilidades, é ideal que o contratante solicite e aprove redefinições de senha, teste de novos desenvolvimentos, melhorias, correções de incidentes.

Observou-se que a segurança e manutenção da aplicação é de responsabilidade mútua do servidor e do contratante. Ambos responsáveis pela atenção aos acessos e melhorias contínuas do aplicativo. A sensibilidade ao acesso de dados confidenciais também é observada pelo direcionamento de responsabilidades, em que a empresa que deve inserir a aplicação deve estar atenta ao controle de acesso e sua própria estrutura organizacional, para que novos acessos e responsáveis estejam constantemente atualizados.

Outra informação necessária ressaltada na seção metodológica é a disponibilidade do fornecedor. O serviço em estudo propõe disponibilidade de 24 horas por dia, 5 dias por semana (de segunda a sexta-feira; durante os fins de semana, a disponibilidade é restrita devido à janela de manutenção necessária). Essa informação é importante no caso de um incidente ou falha importante. Nesse caso, o fornecedor pleiteante propõe o processo de tratamento de incidentes por país/região demonstrado na Figura 11.

Figura 11 – Tratamento de incidentes por região.



Fonte: Questionário BSLD.

Outro ponto discutido na descrição do procedimento BSLD refere-se ao plano de recuperação. Viu-se que, em caso de ocorrência de incidentes, é necessário que existam pontos e estratégias de recuperação e *backup*. O ponto de recuperação é o ponto anterior ao desastre, até o qual a recuperação de dados pode ser realizada de acordo com a arquitetura atual e os arranjos de *backup*. Com isso, o fornecedor declarou que o *backup* será feito todos os dias à meia-noite e a recuperação pontual é possível aplicando os arquivos específicos (cujo *backup* é feito a cada 15 minutos) para atualizar o sistema até certo ponto do tempo para minimizar a perda de dados. Com essa estratégia de *backup*, não se espera que o sistema sofra perda de dados no caso de perda de energia ou falha de uma unidade de disco.

O tempo de recuperação, por sua vez, isto é, o período entre uma interrupção não planejada das operações comerciais e a retomada dos negócios proposto é de no máximo 12 horas.

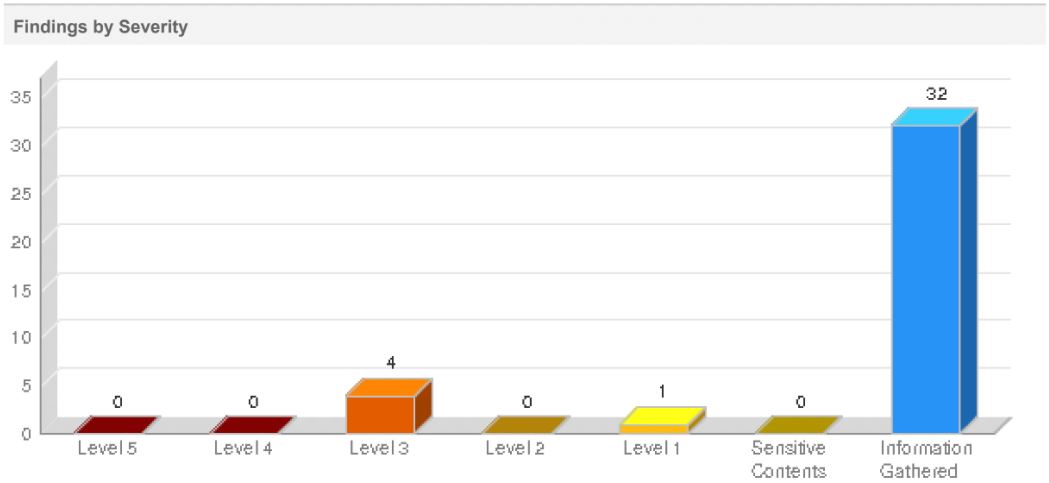
No caso do sistema proposto, o processo de negócios será suportado até que o plano de recuperação seja executado no caso de um desastre. Para manter a continuidade, os usuários e a equipe de suporte devem implementar soluções provisórias para os problemas sempre que possível, conforme sugerido pelo fornecedor. As regiões/países que executam o sistema revertem para as atualizações mestre do fornecedor no sistema, quando possível. No entanto, cada região precisa documentar seu plano de continuidade de negócios específico.

Nota-se que o fornecedor possui uma proposta bem definida de aplicação ajustável às regiões ou países em que se instalou o sistema. Embora obrigatória, não foi fornecida, no entanto, uma matriz RACI de responsabilidades. Isso pode ter ocorrido por diversos motivos, entre eles a falta de conhecimento técnico por parte dos responsáveis pela documentação das informações. Dessa forma, cabe ao gestor de riscos avaliar o nível de conformidade das informações e então decidir pela inserção do sistema ou reavaliação dos dados informados aceitando ou não os riscos, tendo em vista a lacuna da proposta em relação ao seu sistema de responsabilidades formalizado.

4.3 Aplicação do *Scan* de vulnerabilidades

A seguir serão apresentados os resultados de um primeiro *Scan* de vulnerabilidades para o aplicativo candidato a ser inserido entre os fornecedores de serviços da empresa em estudo.

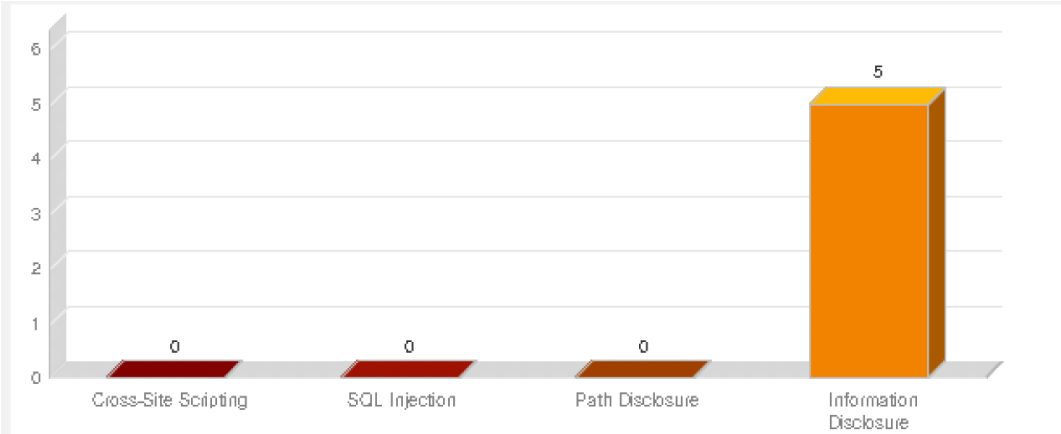
Figura 12 – 1º *Scan* de vulnerabilidades



Nota: Vermelhas (nível 4 e 5), Alaranjadas (nível 3), Amarelas (nível 20,1 e 0), Azuis (Informações).
Fonte: *Scan* de vulnerabilidades.

Nota-se, na figura 1, a existência de 5 vulnerabilidades com risco médio na aplicação. Abaixo podemos verificar as fraquezas por grupo. Todas as vulnerabilidades na primeira varredura da aplicação estavam concentradas em revelação de informação (*Information Disclosure*).

Figura 13 – 1º *Scan* - Categorias de Vulnerabilidades



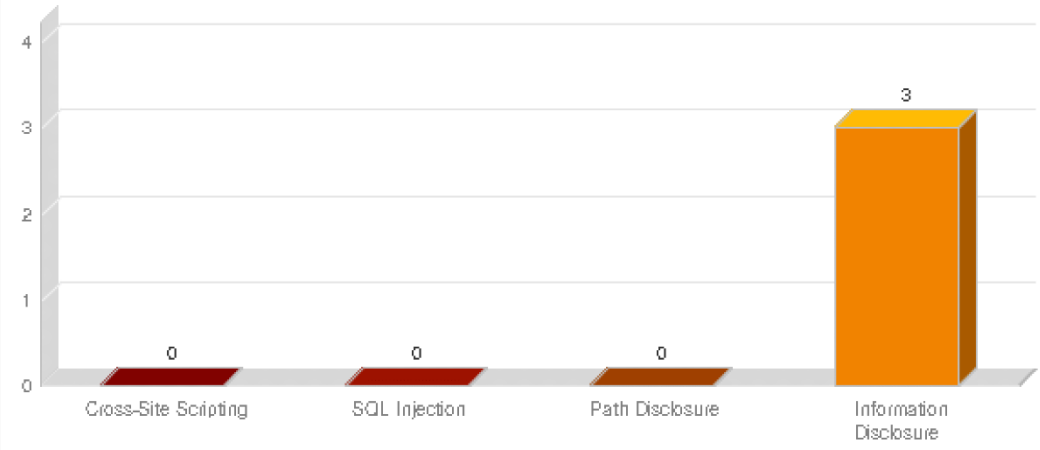
Fonte: *Scan* de vulnerabilidades.

Em se tratando de vulnerabilidades do tipo *Information Disclosure*, o TLS (*Transport Layer Security*) é capaz de usar uma infinidade de cifras (algoritmos) para criar os pares de chaves públicas e privadas, enfraquecendo a segurança. Um invasor pode explorar falhas criptográficas para conduzir ataques do tipo *man-in-the-middle* ou para descriptografar comunicações. Por exemplo, um invasor pode ler comunicações seguras ou modificar mensagens de forma mal-intencionada. O próprio *Scan* fornece as

soluções indicadas para fraquezas como as supracitadas, nesse caso, desativar o uso de protocolos já usados em favor de outros criptograficamente mais fortes

Dentro do diagnóstico da varredura estão aqueles níveis de criticidade mencionados na Tabela 2. Aquelas vulnerabilidades identificadas como críticas ou altas deverão ser resolvidas antes que a aplicação entre em uso, enquanto aquelas médias e baixas poderão ser resolvidas com mais parcimônia, devendo existir um plano de correção, com prazos de implantação, baseado em aplicações de *patch* e/ou novas versões da aplicação. As vulnerabilidades classificadas como informativas, são para conhecimento do desenvolvedor e suas correções elegíveis. A correção foi evidenciada após um novo teste de vulnerabilidade quando o desenvolvedor sinalizar que a aplicação está apta para novo teste. A figura a seguir demonstra o resultado de um 6º *Scan*, isto é, após correções e adaptações, a aplicação é submetida novamente aos testes de vulnerabilidades.

Figura 14 – 6º *Scan* - Categorias de Vulnerabilidades



Fonte: *Scan* de vulnerabilidades

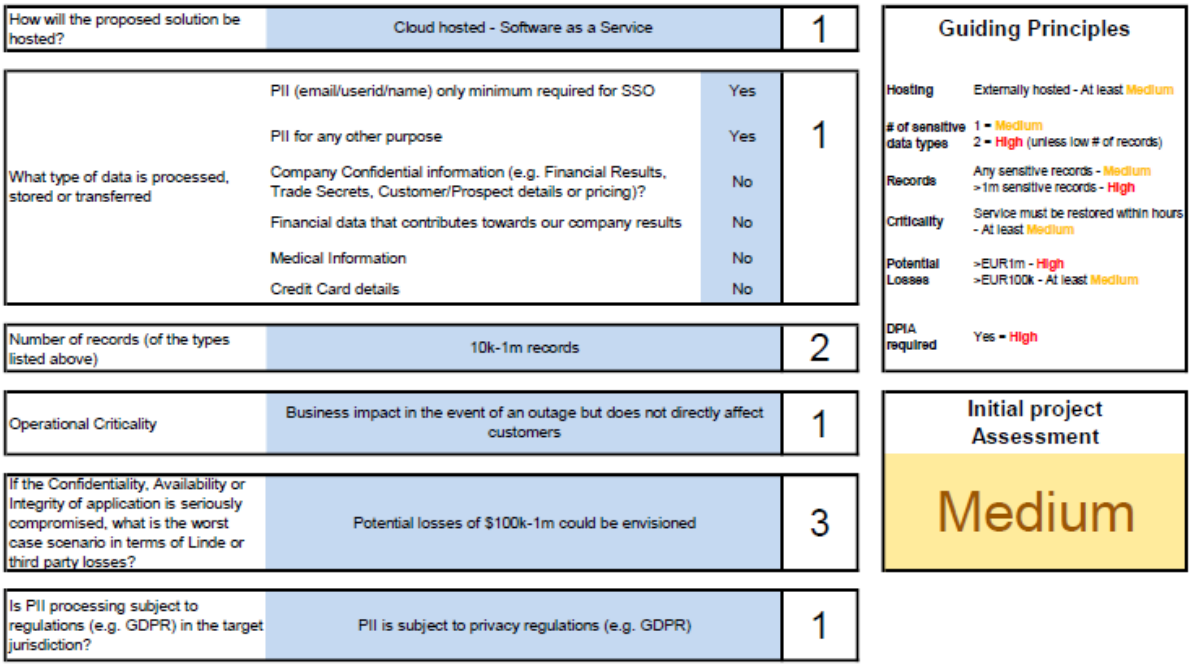
Percebemos através da figura acima que ainda persistem vulnerabilidades do tipo *Information Disclosure*. Dessa forma, o processo deve prosseguir até que o gestor decida descartar a aplicação ou assumir os riscos apresentados.

4.4 Aplicação da avaliação de riscos - *Risk assessment*

A aplicação do procedimento *Risk Assessment* inicia-se com as informações da planilha de avaliação inicial. Dessa forma, na Figura 15 temos as informações sobre os tipos de dados (Que tipo de dados são processados, armazenados ou transformados - *what type of data is processed, stored or transformed?*). Como observamos a demanda não necessita de informações mais delicadas do que dados cadastrais básicos como e-mail. A criticidade operacional (*Operational criticality*) é semelhante ao questionário BSLD ao

solicitar que seja determinado um grau de impacto. No caso do procedimento desta seção, o impacto para o negócio em caso de paralisação é de grau 1 ou médio. Já o impacto financeiro é alto (100 mil unidades monetárias), o que deve determinar uma análise mais aprofundada de segurança. Ao fim do relatório é determinado o grau de risco inicial do serviço, neste caso específico foi determinado risco de nível médio.

Figura 15 – Avaliação inicial de riscos



Fonte: Documentos procedimento *Risk assessment*

Um ponto determinante para as próximas etapas é o tipo de *host* em que o sistema está baseado. Na figura 15 foi informado um *Cloud Hosted - Software as a service (SaaS)*, isto é, o sistema é hospedado na nuvem, o que possibilita um nível de escala maior do que a hospedagem tradicional, na própria empresa. Sendo assim, esse modelo de hospedagem é baseado no compartilhamento de recursos, o que não exige servidores locais para lidar com os dados. Por esse motivo, esse tipo de hospedagem vai gerar uma série de perguntas de segurança que serão respondidas nas próximas etapas do procedimento, como mostra a figura a seguir.

Figura 16 – Avaliação detalhada de riscos

Detailed Risk Assessment

Your project has been identified as Medium risk, therefore you are now required to complete a detailed risk assessment. To do so, please answer each question below and then press the button Run Detailed Risk Assessment

	You have already informed that:	
1	Who will host the intended solution	Cloud hosted - Software as a Service
3	Will the intended solution store or process personal information subject to regulations?	Yes
4	Will the intended solution store or process data that could be considered competitively sensitive (e.g. Financial Results, Trade Secrets, Customer/Prospect details or pricing)?	No
5	Will the intended solution store or process medical or patient information?	No
6	Will the intended solution be used for calculation or reporting of company financial results?	No
7	Will the intended solution store credit card details or process credit card payments?	No

	Please confirm the following additional details:	
2	If PII (covered by privacy regulations) is being processed or stored, where?	PII held at third-party location
8	Will the intended solution form part of a time critical operational process?	No
9	Will the intended solution be interfaced in any way to existing systems?	Yes - file-based automatic interface
10	Will the intended solution include a logon process which will identify and authenticate users?	Yes - combination of SSO and own process
11	Will the intended solution be accessible from outside the network?	Yes, over the internet using any device
12	Will the intended solution be developed specifically for or purchased off the shelf?	Off the shelf
13	Who will be the users of the intended service?	employees and/or third parties (e.g. agents/partners)

A etapa subsequente será de análise de novas perguntas técnicas respondidas ainda pelo dono da demanda, ou seja, o gestor. Na figura 16 temos o questionário referente ao serviço em análise, baseado no nível de risco determinado na avaliação inicial, médio.

A avaliação segue para comunicação entre o dono da demanda e o fornecedor. Nessas etapas, um questionário é enviado e respondido pelo fornecedor e avaliado novamente pelo dono da demanda, que deve determinar a probabilidade dos riscos e a aceitabilidade ou não. Na figura 17 temos esse procedimento estruturado em 9 seções de perguntas. Entre elas, informações de gestão de dados, um risco de impacto significativo, embora com baixa probabilidade (*highly unlikely)*. A decisão de aceitar o risco ou tomar outras medias é feita na coluna *Project Approach*, ou abordagem do projeto. O único risco aceito refere-se ao *backgroud* do fornecedor (V1), referente ao risco de parada nas trocas do fornecedor, com impacto operacional. Todos as outras seções exigem a implementação de controles padronizados (*implement std control*). No caso da gestão de dados, é sugerido um aumento da capacidade de *backup* do sistema.

Figura 17 – Riscos avaliados entre fornecedor e gestor

Risk ID	Risk	Probability	Impact	Project Approach	Details
V1	**Supplier Background** There is a risk that the supplier stops trading with the impact that Operational Processes are impacted	1 - Highly unlikely	3 - Managable impact	Accept Risk	If discontinues to work with we would not have a system and hence would be difficult to proof that trainings are done. As this is highly unlikely the risk is accepted
V2	**Data Management** There is a risk that data is indequately managed by the vendor with the impact that information is lost and cannot be recovered	1 - Highly unlikely	4 - Significant impact	Implement std control	As uses AWS it is highly unlikely that data is lost and cannot be recovered. As part of the standard controls their backup capability should be assessed.
V3	**Encryption** There is a risk that the cloud service provider's computing environment is inadequately secured by the cloud provider with an impact that proprietary information is disclosed to unauthorised individuals	1 - Highly unlikely	4 - Significant impact	Implement std control	As is one of the biggest vendors in the market using AWS it is highly unlikely that this is not properly secured. This shall be audited via regular audits and possible feedbaxck regarding pen testing.
V5	**Regulatory Compliance** There is a risk that a solution will be implemented that is not compliant with regulations with an impact of fines and/or operational impact	3 - Possible	4 - Significant impact	Implement std control	As the implementation of features sits within the area of responsibility we can implememt e.g. non GDPR compliant logic - this has to be prevented by standard internal controls and regular audits.
V6	**Baseline Security** There is a risk that the application has been developed by a supplier with inadequate consideration to IT Security topics with the impact that our data is processed in an insecure manner	1 - Highly unlikely	4 - Significant impact	Implement std control	As is one of the biggest vendors in the market it is highly unlikely that this is not properly secured. This shall be audited via regular security and SCO2 audits.
V7	**IAM & People Management** There is a risk that access to the system will be inadequately controlled with the impact that unauthorised persons are given access to the system	1 - Highly unlikely	4 - Significant impact	Implement std control	As is one of the biggest vendors in the market it is highly unlikely that this is not properly secured. This shall be audited via regular security and SCO2 audits.
V8	**Cyber Security Management** There is a risk that the cloud service provider's computing environment is inadequately secured by the cloud provider with the impact that proprietary information is disclosed to unauthorised persons	1 - Highly unlikely	4 - Significant impact	Implement std control	As is one of the biggest vendors in the market using AWS it is highly unlikely that this is not properly secured. This shall be audited via regular audits and possible feedbaxck regarding pen testing.
V9	**Fourth Party Risk** There is a risk that the cloud service provider's computing environment is inadequately secured by the cloud provider with the impact that proprietary information is disclosed to unauthorised persons	1 - Highly unlikely	4 - Significant impact	Implement std control	As is one of the biggest vendors in the market using AWS it is highly unlikely that this is not properly secured. This shall be audited via regular audits and possible feedbaxck regarding pen testing.
V11	IT Baseline security Controls There is a risk that the cloud service provider's computing environment is inadequately secured by the cloud provider with the impact that proprietary information is disclosed to unauthorised individuals OR the system is rendered unusable for a period of time	1 - Highly unlikely	4 - Significant impact	Implement std control	As is one of the biggest vendors in the market using AWS it is highly unlikely that this is not properly secured. This shall be audited via regular audits and possible feedbaxck regarding pen testing.

Fonte: Documentos procedimento *Risk assessment*

Por fim, os resultados da avaliação trazem um apanhado geral em que se deve avaliar quais riscos são relevantes para o seu projeto. No caso da análise da demanda em questão alguns desses riscos estão dispostos no Quadro 4.

Quadro 4 - Principais riscos na avaliação final

Risco	Mitigação de controle	Responsável	Situação
Controle inadequado de acesso ao sistema	- Questionamento ao fornecedor - Gerenciamento de pessoal	Dono da demanda	Implementar controle
Os dados são gerenciados de maneira inadequada pelo fornecedor	- Questionamentos ao fornecedor - Abordagens de gerenciamento de dados	Dono da demanda	Implementar controle
Terceiros mal-intencionados podem ter acesso ao sistema	- Criptografia de dados em trânsito	Proprietário do aplicativo	Implementar controle
O diretório ativo não está suficientemente seguro	- Senhas fortes - Identificação de vulnerabilidades - Controle de privilégios de acesso.	Chefe de departamento	Controle implementado

Fonte: Elaboração própria.

O primeiro risco mostrado na tabela acima é o controle inadequado do acesso ao sistema, causando o acesso de pessoas não autorizadas. Na descrição do problema temos que o fornecedor foi solicitado a responder as perguntas de segurança o implementador revisou as respostas e atualizou os riscos relacionados e os controles de mitigação propostos. Quanto ao controle de mitigação, questionamentos ao fornecedor a respeito do problema e o gerenciamento de pessoal são algumas atitudes propostas na análise. Nota-se que este controle ainda está pendente de implementação, enquanto as correções no diretório já estão completas. Novamente, dados gerenciados de maneira inadequada pelo fornecedor podem causar perda irrecuperável de dados. Nesses casos é importante a revisão de segurança junto ao fornecedor e aprimoramento dos procedimentos de gestão de dados.

4.5 Discussão

O processo de identificação de riscos descrito acima é um sistema consolidado na empresa em estudo. São utilizados diversos procedimentos indicados por organizações internacionais e na literatura especializada em *cybersecurity*. No entanto, como foi possível verificar, o processo é extenso e exaustivo. Gestores despreparados muitas vezes se deparam com o desafio de lidar com as diversas questões técnicas colocadas na fase de *Risk assessment*, que consiste, em sua maioria, na responsabilidade do dono do ativo. Esses desafios se estendem a todas as fases do sistema, como, por exemplo, no fornecimento de uma matriz RACI na fase BSLD. Como vimos, o responsável pelo preenchimento não forneceu uma estrutura formalizada da estrutura de responsabilidades.

Em se tratando de continuidade de avaliação, o sistema não é necessariamente contínuo. Após ser aprovado pelo procedimento apresentado, o fornecedor passa por verificações de vulnerabilidades extraordinárias, apenas em casos específicos. Essa, por si só, é uma vulnerabilidade do processo, tendo em vista a nomenclatura apresentada pela NIST em segurança digital, que constitui um processo contínuo dividido em fases. Além disso, muitas vezes os gestores, que possuem autonomia para tomar decisões de aceitar o risco, escolhem receber a aplicações com vulnerabilidades não tratadas, aumentando o risco de vazamento de dados, e/ou prejuízos para a companhia. O *tradeoff* preço e segurança também pode influenciar na decisão final do gestor.

Alguns riscos apresentados na fase final do *Risk assessment* podem ser aceitos mediante apresentação de Controles de Serviços e Organizações 2 (SOC 2 ou *Service and Organization Controls* 2) por parte dos fornecedores. Esses controles são uma auditoria de procedimentos em organizações de tecnologia da informação. Em resumo, é um padrão internacional para relatórios sobre sistemas de gerenciamento de riscos de

cibersegurança. Essa pode ser uma ferramenta de proteção que parte, principalmente, dos fornecedores.

Em se tratando de comunicação fornecedor e empresa, foi possível observar que é uma parte sensível da gestão de riscos. Quanto maior a qualidade dessa comunicação, maiores as chances de aplicação de procedimentos de forma otimizada. Portanto, procedimentos que visem melhorar a sociabilidade entre as partes devem ser priorizados pelas empresas. Com visto no capítulo 2, questionários são úteis no processo de análise de riscos, mas também é necessário um aprimoramento através de encontros e *brainstormings*.

É importante ressaltar que um procedimento padronizado é de suma importância dentro de uma organização preocupada com a segurança digital e a proteção de dados. A constante mudança nas relações empresariais com os serviços digitais e a atenção a novas ferramentas disponíveis, bem como as atualizações das organizações especializadas são de extrema necessidade na era digital, tendo em vista o surgimento constante de novas ameaças e, portanto, riscos. O cuidado deve garantir não só a proteção das informações de clientes e fornecedores, mas a redução de custos e retrabalho.

5 Considerações Finais

O objetivo deste trabalho foi definir um procedimento de análise de *cyber-risks* que compõe um processo de gestão de risco e descrever a aplicação do mesmo em uma empresa de grande porte. Entre as etapas apresentadas no capítulo 2, a identificação foi a fase escolhida como objeto de estudo, em que estão incluídas ferramentas de gerenciamento de ativos, *risk assessment* governança, ambiente de negócios e estratégia de gestão de risco.

Os resultados descrevem três ferramentas principais no processo de Gerenciamento de Segurança da Informação (GSI) adotado pela empresa. A avaliação é feita utilizando-se de documentos descritivos e procedimentos de análise de risco, cujos componentes desse processo são: BSLD , *Risk Assessment* e *Scan* de Vulnerabilidades.

O extenso processo de identificação de riscos inclui em seu escopo os componentes apontados pela literatura que caracterizam identificação de risco, sendo estes: identificar, descrever e documentar os riscos e suas possíveis causas. A ferramenta BSLD, com diversos questionamentos dirigidos ao fornecedor potencial, tem como objetivo identificar e documentar possíveis riscos e seus impactos para o dono do ativo. A ferramenta *Scan* é mais operacional, é por si só uma aplicação que consiste em identificar vulnerabilidades e indicar o tratamento adequado conforme níveis de criticidade pré-estabelecidos. A ferramenta *Risk assessment* consiste em um conjunto de questionários dirigidos, principalmente, ao gestor ou dono do ativo, que deve tomar a decisão do risco do projeto para a empresa.

Foi observado no decorrer da descrição do processo estudado que há limitações relacionadas à aplicação das tarefas. Muitas vezes, o procedimento pode não ser adequado quando gestores e fornecedores de deparam com questionamentos desconhecidos. Apesar disso, o processo está consolidado na empresa e tem sido útil na identificação e gestão de riscos, podendo ser aprimorado e expandido conforme a necessidade e a busca por novas diretrizes. Tendo em vista a constante atualização de ferramentas de segurança digital para empresas e fornecedores.

A importância da análise proposta nesse trabalho para empresa em estudo está em analisar um processo de identificação de riscos já estabelecido em suas várias facetas. Embora esse sistema tenha garantido em certo nível a segurança contra riscos, é importante observar as possibilidades de aprimoramento e as vulnerabilidades passiveis de correção.

Destarte, há espaço para novas avaliações de técnicas ainda não exploradas

ou pouco utilizadas. O constante aumento da relação humana com a tecnologia e o aumento de agregação de dados deve exigir uma constante atualização dos procedimentos que tem como objetivo garantir a segurança dos dados e, no caso das organizações, da continuidade do negócio. Portanto, trabalhos futuros podem explorar diversos caminhos. O riscos envolvidos no gerenciamento de dados dentro das organizações, por exemplo, é um tema cada vez mais relevante nos estudos em segurança tecnológica, abrangendo uma infinidade de subtópicos. *Softwares* de análise de riscos também se mostraram como objeto de estudo relevante, dada a crescente oferta de novas opções. Além desses, estratégias de continuidade de negócios diante de incidentes também figuram uma oportunidade de abranger a literatura especializada em *cybersecurity*.

Referências

ALI, A.; WARREN, D.; MATHIASSEN, L. Cloud-based business services innovation: A risk management model. *International Journal of Information Management*, v. 37, n. 6, p. 639–649, 2017.

ALMEIDA, A. B. d. Gestão do risco e da incerteza: conceitos e filosofia subjacente. In: *Realidades e desafios na gestão dos riscos: dialogo entre ciência e utilizadores*. Coimbra: Imprensa da Universidade de Coimbra, 2014. p. 19–29. Disponível em: <https://digitalis.uc.pt/handle/10316.2/35747>.

ASHOOR, A. S.; GORE, S. What is the difference between hackers and intruders. *International Journal of Scientific Engineering Research*, v. 2, n. 7, p. 1–3, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. *ABNT NBR ISO 31000*: Gestão de risco - princípios e diretrizes. Brasil, 2009.

BRASILIANO, A. C. R. *Inteligência em Riscos: gestão integrada em riscos corporativos*. [S.l.]: São Paulo: Sicurezza, 2016.

CHANG, E. S. et al. Managing cyber security vulnerabilities in large networks. *Technical Journal*, v. 4, n. 4, p. 252–272, 1999.

CISA, C. I. S. A. *National Incident Scoring System*. 2021. Acesso: 18-06-2021. Disponível em: <https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System>.

CROSSKNOWLEDGE, B. *Matriz RACI: o que é e como aplicar? Saiba tudo sobre!* 2020. Acesso: 01-07-2021. Disponível em: <https://blog.crossknowledge.com/pt/matriz-raci/>.

CUSTOIAS, G. B.; MENDONÇA, L. B.; CUNHA, D. V. *Estudo sobre solução tecnológica para a mitigação dos riscos cibernéticos no setor financeiro*. 20 p. — Universidade Presbiteriana Mackenzie. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação, São Paulo, 2019.

DELOITTE; IBCG. *Os cinco Pilares do Risco*. 2019. Acesso: 12-05-2021. Disponível em: <https://www2.deloitte.com/br/pt/pages/risk/articles/os-cinco-pilares-dos-riscos-empresariais.html>.

DIKMEN, I.; BIRGONUL, M. T.; ARIKAN, A. E. A critical review of risk management support tools. In: *20th Annual Conference of Association of Researchers in Construction Management (ARCOM)*. [S.l.: s.n.], 2004. p. 1–3.

GALOYAN, A. *Segurança cibernética no âmbito das relações internacionais*. 102 f. Dissertação (Mestrado em Relações Internacionais) — Universidade de Brasília, Brasília, 2019.

HERNÁNDEZ, M.; CARREÑO, M. L.; CASTILLO, L. Methodologies and tools of risk management: Hurricane risk index. *International Journal of Disaster Risk Reduction*, v. 31, p. 926–937, 2018.

HUMAYUN, M. et al. Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, v. 45, n. 4, p. 3171–3189, 2020.

INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION. *ISACA. COBIT 5*: A business framework for the governance and management of enterprice. [S.l.], 2012.

INFOSEC, G. *Implementação do NIST Cybersecurity Framework*. 2021. Acesso: 18-06-2021. Disponível em: <https://www.gat.digital/blog/implementacao-do-nist-cybersecurity-framework/>.

JIAXI, Y.; ANJIA, M.; ZHIZHONG, G. Vulnerability assessment of cyber security in power industry. In: IEEE. *2006 IEEE PES Power Systems Conference and Exposition*. [S.l.], 2006. p. 2200–2205.

LANEVE, G. et al. Space-based information support for prevention and recovery of forest fire emergency in the mediterranean area. In: *34th Symposium Proceedings*. [S.l.: s.n.], 2014.

LIN, Y.; ZHOU, L. The impacts of product design changes on supply chain risk: a case study. *International Journal of Physical Distribution & Logistics Management*, v. 41, n. 2, p. 162–186, 2011.

MEYER, C. B. A case in case study methodology. *Field methods*, v. 13, n. 4, p. 329–352, 2001.

QUALYS. *How does vulnerability scanning work?* . 2020. Acesso: 08-05-2021. Disponível em: <ttps://qualys-secure.force.com/discussions/s/article/000006137>.

REFSDAL, A.; SOLHAUG, B.; STØLEN, K. *Cyber-risk management*. [S.l.]: Springer, 2015.

ROLDÁN-MOLINA, G. et al. A comparison of cybersecurity risk analysis tools. *Procedia Computer Science*, v. 121, p. 568–575, 2017.

TANG, M. et al. Disclosure of cyber security vulnerabilities: time series modelling. *International Journal of Electronic Security and Digital Forensics*, v. 10, n. 3, p. 255–275, 2018.

TAVARES, B. G.; SILVA, C. E. S. da; SOUZA, A. D. de. Practices to improve risk management in agile projects. *International Journal of Software Engineering and Knowledge Engineering*, v. 29, n. 03, p. 381–399, 2019.

ULSCH, M. *Cyber threat!: How to manage the growing risk of cyber attacks*. [S.l.]: Wiley Online Library, 2014.

Apêndice

Quadro A1 - Resumo do questionário BSLD

Objeto	Descrição
Descrição do serviço	Indica o impacto relativo da perda do aplicativo no Processo de Negócios para cada período de tempo específico.
Monitoramento do serviço	Quais procedimentos de monitoramento e responsáveis pelo atendimento de alertas.
Segurança	Descrição detalhada de como a segurança do aplicativo será mantida.
Arquitetura do Sistema	Diagrama da arquitetura do serviço, incluindo interfaces, entradas, dependências, etc.
Variações geográficas no processo de negócios ou serviço	Relata o funcionamento do serviço em diferentes níveis geográficos.
Principais clientes do serviço	Descrições de funções e grupos-chave que usam o serviço.
Tecnologia da Informação e responsabilidades comerciais	Criação de uma matriz RACI de responsabilidades.
Disponibilidade	A disponibilidade dos serviços de TI.
Processo de gerenciamento de incidentes.	Fornecimento de um diagrama detalhado do processo de ação diante de incidentes.
Prazos de resolução	Documentação do tempo de resolução de incidentes acordado entre as partes.
Continuidade e estratégia de Backup	Definição de um ponto de recuperação anterior ao desastre até o qual a recuperação de dados pode ser realizada de acordo com a arquitetura atual e os arranjos de backup.
Continuidade de negócios Questões legai s	Descrição do processo de negócios ou plano de recuperação em caso de desastre. Contratos e descrição do tratamento de dados.

Fonte: Elaboração própria.

Anexos

Figura A1 – Parte 1 - *Risk assessemt output*

There is a risk that.....	with the impact that....	Mitigating Control	Resp
access to the system will be inadequately controlled	unauthorised persons are given access to the system	Vendor Questions - IAM & People Management	Project Team
the cloud service provider's computing environment is inadequately secured by the cloud provider	proprietary information is disclosed to unauthorised individuals OR the system is rendered unusable for a period of time	Vendor Questions - Encryption	Project Team
		Vendor Questions - Cyber Security Mgmt	Project Team
		Vendor Questions - Fourth Party Risk	Project Team
		Vendor Questions - Baseline Controls	Project Team
the cloud application's configuration settings are inadequately and/or insecurely configured by the project team	proprietary information is disclosed to unauthorised individuals	Secure configuration of Cloud environment	Project Team
	unauthorised business transactions are performed in the system	Logging for data changes	Application Owner
the vendor stops trading	operational processes are impacted	Vendor Questions - Background Questions	Project Team
	data is lost and cannot be recovered	Contractural Clauses to protect	Project Team
data is inadequately managed by the vendor	data is lost and cannot be recovered	Vendor Questions - Data Management Approach	Project Team
solution will be implemented that is not compliant with regulations	fines and /or operational impact	Vendor Questions - Regulatory Compliance	Project Team
baseline controls are not implemented	inadequate security posture and high risk to confidentiality, integrity & availability of information	Confirm vendor's baseline controls are effective	Project Team
personal information will be disclosed to unauthorised third parties	need to inform ICO of a GDPR relavent breach	PII Data at Rest	Application Owner
the automated interface will fail to run	innacurate information or unexpected operation of system	ITGC_14 - Job Scheduling	Project Team
the file will be obtained by unauthorised third party	loss of control of sensitive information and associated business impact	Encryption of data in transit	Application Owner

Figura A2 – Parte 2 - *Risk assessemt output*

active directory is insufficiently secured	unauthorised persons can access the system	Encryption of password hashes	Head of GSO
		Password strength	Head of GSO
		High privilege access	Head of GSO
		Least privilege access	Head of GSO
		Vulnerability identification (servers)	Head of GSO
		Vulnerability identification (resources)	Head of GSO
the SSO functionality is incorrectly configured	the system is accessible to non-authorised employees	Secure implementation of SSO	Project Team
unauthorised users will be granted access to the system	loss of control of sensitive information or processing of unauthorised transactions and associated business impact	Approval of application access	Application Owner
passwords will be stored in a manner that allows them to be accessed by unauthorised parties		Encryption of password hashes	Application Owner
		Password strength	Application Owner
authorised users will retain access to the system even if their job role no longer requires access		Periodic access level check	Application Owner
malicious third parties will gain access to the system	non-availability of the system due to denial of service attack	Web application firewall	Application Owner
	uncontrolled disclosure of sensitive information and associated business impact	PenTesting	Application Owner
		Vulnerability identification	Head of Network Ops
		Encryption of data in transit	Application Owner
		Web Vulnerability ident.	Head of EA Service Del. App
the endpoint device will become infected with malicious code which then infects the system	affecting the confidentiality, integrity or availability of the system	Malware Protection	Project Team
the hosting provider cannot support our required security controls	the application is vulnerable to attack and unauthorised access to data	Vendor Questions - Baseline Security	Project Team
the application security patches are not kept up to date	the application is vulnerable to attack and unauthorised access to data	Timely security patching	Application Owner
that third parties will be able to access records that are not applicable to them	inadvertent disclosure of sensitive information and associated business impact	Specific Testing of Thirdparty/Customer Permissior	Project Team

Figura A3 – Parte 3 - *Risk assessemt output*

Project Task	Project approach
Vendor Review Complete	Implement std control
Vendor Review Complete	Implement std control
Vendor Review Complete	Implement std control
Vendor Review Complete	Implement std control
Vendor Review Complete	Implement std control
Implement Control	Implement std control
Implement Control	Implement std control
Vendor Review Complete	Accept Risk
Implement Control	Implement std control
Vendor Review Complete	Implement std control
Vendor Review Complete	Implement std control
Implement Control	Control already effective
Implement Control	Control already effective
Implement Control	Control already effective
Implement Control	Control already effective
Already implemented	
Already implemented	
Already implemented	
Already implemented	
Already implemented	
Already implemented	
Implement Control	Implement std control
Implement Control	Implement std control
Implement Control	Control already effective
Implement Control	Control already effective
Implement Control	Control already effective
Implement Control	Control already effective
Implement Control	Control already effective
Implement Control	Control already effective
Implement Control	Control already effective
Implement Control	Control already effective

Figura A4 – Parte 4 - *Risk assessemt output*

Details
As is one of the biggest vendors in the market it is highly unlikely that this is not properly secured. This shall be audited via regular security and SCO2 audits.
As is one of the biggest vendors in the market using AWS it is highly unlikely that this is not properly secured. This shall be audited via regular audits and possible feedbaxck rega
As is one of the biggest vendors in the market using AWS it is highly unlikely that this is not properly secured. This shall be audited via regular audits and possible feedbaxck re
As is one of the biggest vendors in the market using AWS it is highly unlikely that this is not properly secured. This shall be audited via regular audits and possible feedbaxck re
As is one of the biggest vendors in the market using AWS it is highly unlikely that this is not properly secured. This shall be audited via regular audits and possible feedbaxck re
Vendors hardening guidelines would be followed
Logging would be enabled for all relevant fields (e.g. assignment of courses, user information)
If discontinues to work with we would not have a system and hence would be difficult to proof that trainings are done. As this is highly unlikely the risk is accepted
Global Procurement to be used
As uses AWS it is highly unlikely that data is lost and cannot be recovered. As part of the standard controls their backup capability should be assessed.
As the implementation of features sits within the area of responsibility we can implememt e.g. non GDPR compliant logic - this has to be prevented by standard internal controls
This has been confirmed as part of SOC2 assessment
Data at Rest implemented
SAPHRON sends to PI/PO that send files to CS where the data is read and not stored. Standard interface monitoring controls in place.
TLS1.2 or higher used by Cornerstone
Internal standard SSO process used
Standard process in place via admins to rerquest access to as admin. As leaner also standard process in place.
FB CS: HTTPS/TLS encryption- All passwords are stored in the database in a hashed format to minimize security liability. Passwords are hashed using PBKDF2 and salted and it
Implemented as per SOC2 report
Implemented as per SOC2 report
Implemented as per SOC2 report
Implemented as per SOC2 report
Implemented as per SOC2 report