UNIVERSIDADE FEDERAL DO PAMPA

MARIANA POMPEO FREITAS

PROPOSTA DE UM MODELO PARA AUXÍLIO NA GESTÃO DE RISCOS DA INFORMAÇÃO - INTEGRANDO MÉTODOS E NORMAS

Bagé
2021

MARIANA POMPEO FREITAS

PROPOSTA DE UM MODELO PARA AUXÍLIO NA GESTÃO DE RISCOS DA INFORMAÇÃO - INTEGRANDO MÉTODOS E NORMAS

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Engenharia de Computação como requisito parcial para a obtenção do grau de Bacharel em Engenharia de Computação.

Orientador: Érico Marcelo Hoff do Amaral

Bagé
2021

Ficha catalográfica elaborada automaticamente com os dados fornecidos pelo(a) autor(a) através do Módulo de Biblioteca do Sistema GURI (Gestão Unificada de Recursos Institucionais).

F866p Freitas, Mariana Pompeo

Proposta de um Modelo para Auxílio na Gestão de Riscos da Informação - Integrando Métodos e Normas / Mariana Pompeo Freitas.

129 f.: il.

Orientador: Érico Marcelo Hoff do Amaral

Trabalho de Conclusão de Curso (Graduação) - Universidade Federal do Pampa, Engenharia de Computação, 2021.

1. Segurança da informação. 2. Gerenciamento de riscos. 3. Governança de TI. 4. Normas e padrões. I. Título.

SERVIÇO PÚBLICO FEDERAL

MINISTÉRIO DA EDUCAÇÃO

Universidade Federal do Pampa

MARIANA POMPEO FREITAS

PROPOSTA DE UM MODELO PARA AUXÍLIO NA GESTÃO DE RISCOS DA INFORMAÇÃO - INTEGRANDO MÉTODOS E NORMAS

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia de Computação da Universidade Federal do Pampa, como requisito parcial para obtenção do Título de Bacharel em Engenharia de Computação.

Trabalho de Conclusão de Curso defendido e aprovado em: 2 de outubro de 2021.

Banca examinadora:

_____

Prof. Dr. Érico Marcelo Hoff do Amaral

Orientador

Unipampa

_____

Prof. Dr. Carlos Michel Betemps

Unipampa

Prof. Dr. Leonardo Bidese de Pinho

Unipampa

Assinado eletronicamente por **CARLOS MICHEL BETEMPS**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 21/09/2022, às 17:00, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

Assinado eletronicamente por **LEONARDO BIDESE DE PINHO**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 21/09/2022, às 20:33, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

Assinado eletronicamente por **ERICO MARCELO HOFF DO AMARAL**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 21/09/2022, às 21:10, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

A autenticidade deste documento pode ser conferida no site https://sei.unipampa.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0932243** e o código CRC **C475DFF0**.

Referência: Processo nº 23100.017451/2021-96 SEI nº 0932243

Dedico este trabalho ao meu avô Fernando da Costa Pompeo (*in memoriam*), a pessoa mais extraordinária que conheci.

AGRADECIMENTO

Agradeço em primeiro lugar a mim mesma, por nunca ter desistido, mesmo com tantos obstáculos pelo caminho. Reconheço no entanto, que sozinho ninguém chega a lugar algum. Durante essa longa e difícil trajetória contei com o apoio de várias pessoas e a elas agradeço por estarem na minha vida, ou por terem em algum momento, cruzado meu caminho.

Obrigada ao meu avô Fernando (*in memoriam*) pelo orgulho, amor e apoio demonstrado em vida;

A minha mãe, minha maior heroína e inspiração;

Aos demais familiares por sempre terem me apoiado, por nunca terem questionado, quando nem eu tinha tantas certezas sobre minha capacidade;

Ao Micael pelo apoio;

As minhas amigas de infância pelo apoio e amizade;

Aos motoristas da empresa Anversa que enquanto puderam, através de suas caronas (e ainda hoje através do seu trabalho), me forneceram segurança para ir trabalhar;

Aos meus colegas de trabalho da Agência FGTAS/SINE Candiota por toda a compreensão;

Aos amigos que conheci em Bagé, meu agradecimento super especial pelo apoio, pela amizade, pelos longos dias compartilhados de estudos. Obrigada por tudo isso e, por terem tantas vezes tornado meus dias mais leves e divertidos;

Ao meu professor orientador por ter sido aquela pessoa que durante toda a minha graduação me incentivou, agradeço por todo o ensinamento repassado, pelas oportunidades dadas no grupo de pesquisa e pelo apoio necessário e demonstrado durante a execução deste trabalho;

Ao professor Gerson por sua colaboração nesse trabalho;

A esta universidade e a todos os professores dedicados, aos quais sem nominar terão os meus eternos agradecimentos;

A todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigada.

“Cada sonho que você deixa para trás é um pedaço do seu futuro que deixa de existir.”
— Steve Jobs

RESUMO

A informação é considerada um ativo valioso para as empresas, e está sujeita a diversos tipos de ameaças. Objetivando a preservação da confidencialidade, integridade e disponibilidade, a segurança da informação protege os ativos relacionados a informação ou dados da organização. Para assegurar esta proteção e evitar incidentes é necessário adotar práticas de gerenciamento de riscos, que garantem a continuidade do negócio, minimiza o risco e maximiza o retorno sobre o investimento. No entanto, as normas e padrões existentes para a gestão de riscos sugerem práticas não muito claras, o que dificulta sua implantação nas empresas. Como uma maneira de identificar, de forma simplificada, as ameaças que possam colocar em risco os ativos da organização, este trabalho propôs o estudo e criação de um modelo para análise de potenciais riscos baseada em normas e padrões de referência internacional. Este trabalho possui resultados, dentre os quais citam- se: criação e validação de um novo modelo de análise de riscos e a automatização deste, nominado ARION, hospedado em um servidor do Grupo de Pesquisa de Segurança da Informação da Universidade Federal do Pampa. O software pode ser acessado através do endereço: https://arion.gsi.seg.br/. O ARION passou por testes e obteve boa aceitação entre os usuários.

Palavras-chave: Segurança da informação. gerenciamento de riscos. governança de TI. normas e padrões.

ABSTRACT

Information is considered a valuable asset for companies, and is subject to different types of threats. Aiming at preserving confidentiality, integrity and availability, information security protects the organization's information or data assets. To ensure this protection and avoid incidents, it is necessary to adopt risk management practices that ensure business continuity, minimize risk and maximize return on investment. However, existing norms and standards for risk management suggest practices that are not very clear, which makes their implementation in companies difficult. As a way to identify, in a simplified way, the threats that may put the organization's assets at risk, this work proposed the study and creation of a model for the analysis of potential risks based on norms and international reference standards. This work has results, including: creation and validation of a new risk analysis model and its automation, named ARION, hosted on a server of the Information Security Research Group of the Federal University of Pampa. The software can be accessed through the address: https://arion.gsi.seg.br/. ARION has passed tests and gained good acceptance among users.

Keywords: *Information security, risk management, IT governance, standards and standards*.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
COBIT	Control Objectives for Information and related Technology
COVID-19	Corona Virus Disease
CVM	Comissão de Valores Mobiliáros
IEC	International Electrotechnical Commission ISO – International Organization of Standardization Engineers
NBR	Norma Brasileira NIST – National Institute of Standards and Technology
SGSI	Sistema de Gestão de Segurança da Informação
TI	Tecnologia da Informação
USP	Universidade de São Paulo

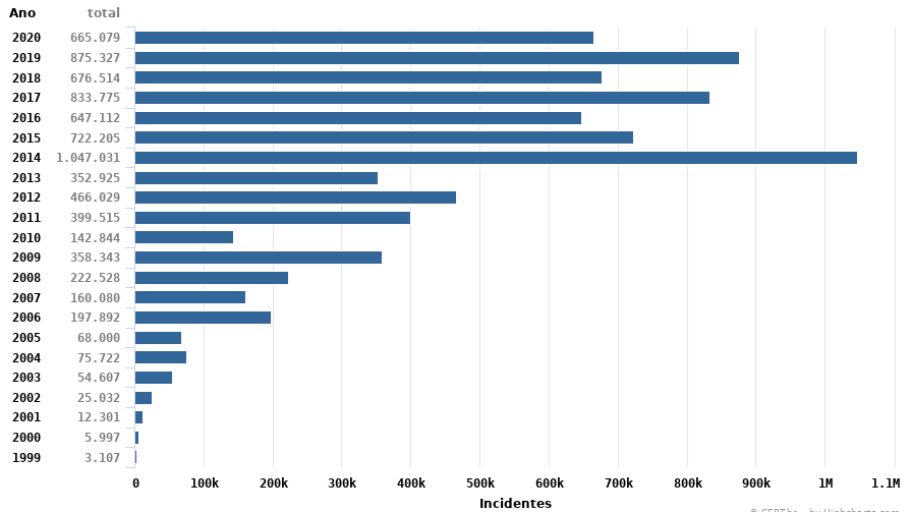
SUMÁRIO

1 INTRODUÇÃO

Atualmente a utilização da Internet e dos recursos tecnológicos vem fazendo parte da rotina das pessoas, especialmente nos últimos dois anos em função da pandemia da COVID-19. Estudos divulgados pela USP (2021), mostraram que nesse tempo, as empresas migraram 41% de sua força de trabalho para o *home-office*, esse número é ainda mais expressivo em empresas pequenas (52% dos funcionários atuaram de forma *home-office*). O mesmo estudo revelou que cerca de 36% das empresas pretendem continuar mantendo essa prática no período após a pandemia.

Neto e Araújo (2019) já tinham afirmado que as organizações estavam passando por uma mudança, em que antigos "colaboradores" que recebiam as informações de forma passiva, estavam dando lugar a "usuários" (elementos ativos), que interagem com os processos e procedimentos organizacionais e com os sistemas de informação. Este caminho requer o uso de gestão de ativos de informação, que está se tornando cada vez mais importante para as empresas. Com a transição de parte dos processos de negócios para o digital, muitas empresas enfrentam novos riscos e ameaças. O CERT (2021) divulgou que somente em 2020 mais de 665 mil incidentes de segurança da informação foram reportados, tais dados podem ser visualizados na figura 1.

Figura 1 – Total de Incidentes por ano reportados ao CERT



(Fonte: CERT, 2021).

Apesar de 2020, em comparação com os anos anteriores, 2020 ter registrado menos ocorrências de incidentes, o Grupo MZ (2021) divulgou que através de dados coletados pelo sistema de busca do site da Comissão de Valores Mobiliários (CVM), o

órgão regulador financeiro do país, as notificações referentes a ataques cibernéticos contra empresas brasileiras cresceram 220% no primeiro semestre deste ano em comparação com o mesmo período de 2020.

Um incidente de segurança pode impactar direta e negativamente as receitas de uma corporação, a confiança dos clientes, o relacionamento com parceiros e fornecedores e, pode impedir, direta ou indiretamente, a organização de cumprir sua missão e de gerar algum lucro. Para enfrentar essas ameaças, Mayer e Lemes (2009) sugerem que as empresas devam adotar atividades proativas, identificando suas vulnerabilidades, bem como os impactos de um incidente de segurança da informação na organização, evitando prejuízos. Isto pode ser obtido através do gerenciamento de riscos. No entanto, a aplicação das abordagens existentes para a gestão de riscos sugere práticas não muito claras. A própria ABNT (2011) informa que a norma não possui uma metodologia específica, e que cabe à organização selecionar seu próprio método para o processo de avaliação de riscos, o que dificulta sua implantação.

Diante desse cenário, este trabalho propôs um estudo e criação de um modelo para análise de potenciais riscos, objetivando fornecer uma maneira de auxiliar o usuário a identificar de forma simplificada os ativos de informação, realizar a análise de risco e verificar aqueles que devem ser minimizados.

1.1 Problema de Pesquisa

É possível implementar uma solução que auxilie na avaliação e gestão de riscos e que possa ser aplicado à organização como um todo, a uma área específica, ou a aspectos particulares de um controle?

1.2 Objetivos

Este trabalho propôs implementar e validar um modelo para avaliação de potenciais riscos e vulnerabilidades encontradas em ativos de informação em instituições públicas e privadas, a fim de garantir o cumprimento dos princípios básicos da segurança da informação. Desta forma, haverá a possibilidade de membros da organização avaliarem os riscos e, posteriormente tomarem medidas para minimizá-los, evitando possíveis incidentes.

1.2.1 Objetivos Específicos

De forma mais detalhada, cabe destacar os seguintes objetivos:

- Realizar um estudo sobre as normas da família ISO/IEC 27000;
- Estudar e definir quais normas serão utilizadas no desenvolvimento do trabalho;
- Realizar um estudo sobre propostas e soluções já disponíveis na área de gestão de riscos de segurança da informação;
- Realizar um estudo sobre modelos de governança disponíveis;
- Com base no estudo realizado, propor e validar um modelo para auxílio na gestão de riscos;
- Realizar a modelagem de software;
- Definir a linguagem de programação e ferramentas a serem utilizadas;
- Implementar o modelo criado e documentar a solução proposta;
- Realizar testes e validar o sistema;
- Analisar e discutir os resultados;

1.3 Organização do trabalho

O restante deste trabalho está organizado conforme segue. O capítulo 2 expõe os conceitos gerais e revisão de literatura. O capítulo 3 apresenta a metodologia adotada para o desenvolvimento deste trabalho. O capítulo 4 aborda o modelo criado e sua validação e detalha a automatização e testes deste. No capítulo 5 têm-se as considerações finais e, algumas sugestões de trabalhos futuros.

2 CONCEITOS GERAIS E REVISÃO DE LITERATURA

A medida que a infraestrutura de informação empresarial se torna mais complexa e conectada, a quantidade de riscos aos ativos de uma empresa aumenta. Assim, como explicado por Bhattacharjee et al. (2012), o processo de identificação, análise e mitigação dos riscos de Segurança da Informação tem assumido um papel importante. Com objetivo de melhor elucidar esse tema, este capítulo realiza uma revisão literária dos principais conceitos que abrangem a Gestão da Segurança da Informação (seção 2.1), a Gestão de Riscos (seção 2.2), Governança de TI (seção 2.3). Além disso, a fim de verificar o estado da arte relacionado ao assunto deste trabalho, na seção 2.4 são apresentadas algumas Tecnologias aplicadas em Gestão, e por último, a seção 2.5 apresenta os Trabalhos Correlatos.

2.1 Gestão de Segurança da Informação

De acordo com a ABNT (2013b), a segurança da informação é a proteção da informação quanto a vários tipos de ameaças, garantindo a continuidade do negócio, minimizando o risco e maximizando o retorno sobre o investimento.

Para tanto, de acordo com Manoel (2014), é necessário atender aos seguintes requisitos lógicos:

• Confidencialidade: assegurar que a informação só será acessível por pessoas autorizadas;

• Integridade: garantia de que as informações se manterão em seu estado original, sem alterações;

• Disponibilidade: a informação deve estar disponível para os usuários sempre que necessário;

• Autenticidade: garantia da identidade de quem está enviando ou recebendo a informação e de que a mensagem não tenha sido alterada durante o envio e recebimento;

• Legalidade: a informação deve estar em conformidade com restrições estabelecidas em normas, leis e contratos.

O não cumprimento desses requisitos pode levar a ocorrência de um incidente. Como bem explicado por Rosemann (2002), o comprometimento do sistema de informações por problemas de segurança pode causar grandes prejuízos ou levar a organização à falência. Dessa forma, a segurança da informação deve ser preocupação

de todos que integram a empresa e sua cadeia de valor.

Segundo Cruz (2012), um Sistema de Gestão de Segurança da Informação (SGSI), fornece um modelo para melhoria da proteção dos ativos de informação, e visa alcançar os objetivos propostos por uma organização baseado numa correta avaliação e gestão de riscos. Em se tratando de Gestão de Segurança da Informação, o padrão de normas *International Organization for Standardization* (ISO) é um referencial internacionalmente aceito. Dentre elas, citam-se:

• ISO/IEC 27000 – ISO/IEC (2014): fornece uma visão geral de um sistema de gestão de segurança e propõe o vocabulário padrão.

• ISO/IEC 27001 - ABNT (2013a): especifica os requisitos para estabelecer, implementar, manter e melhorar um sistema de gestão da segurança da informação. Inclui ainda requisitos para a avaliação e tratamento de riscos de segurança da informação.

• ISO/IEC 27005 - ABNT (2011): fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo aos requisitos de um SGSI, de acordo com a ISO/IEC 27001 (ABNT NBR ISO/IEC, 2011).

• ISO/IEC 27035 – Publication (2011): especifica os requisitos para estabelecer, implementar, manter e melhorar um sistema de gestão de incidentes.

O processo de gestão, descrito nestas normas ISO, fornecem instruções para a construção de metodologias para gestão de segurança. Mas, conforme Konzen, Manzoni e Nunes (2012), especificamente, a NBR 27005, da ABNT (2011), voltada para gestão de riscos, informa o que a organização deve fazer, mas não detalha como executar as atividades, o que dificulta a sua implementação por partes das organizações. A documentação oficial da ABNT (2011), esclarece que não há um método específico para gestão de riscos de segurança da informação, e que cabe a própria organização definir sua abordagem de implementação de gestão de riscos.

Objetivando uma melhor compreensão da gestão de segurança, se faz necessário conhecer definição de alguns conceitos, tais como ameaça, ativos de informação, evento, impacto, incidente de segurança, risco e vulnerabilidade os quais serão descritos a seguir.

Tabela 1 – Conceitos básicos sobre segurança da informação

	Significado
Ameaça	De acordo com a ISO/IEC (2014) é a causa potencial de um incidente, que poderá resultar em danos para um sistema ou organização.
Ativos de Informação	Explanado pela ABNT (2005) como tudo o que tem valor para o negócio da organização e que portanto, requer proteção especial. Podem ser considerados ativos de informação, de acordo com Prado e Souza (2014) : documentos em papel, softwares, hardwares, instalações, pessoas e serviços.
Evento	Explicado pela ISO/IEC (2014) como sendo uma ocorrência ou mudança de um determinado conjunto de circunstâncias.
Impacto	ABNT (2011) informa que está relacionado a medida do sucesso do incidente. Sêmola (2014) explica que se trata da abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio.
Incidente de Segurança	ISO/IEC (2014) define como um ou mais eventos indesejados ou inesperados, com possibilidade de ocorrer comprometimento das operações ou processos de negócios, ameaçando a segurança da informação.
Risco	O risco pode ser entendido, conforme HB (2004), como sendo a chance de alguma coisa acontecer, com possibilidade de produzir um impacto sobre os objetivos. Podem ser classificados em naturais, de acordo com Dantas (2011): aqueles que têm origem a partir de fenômenos da natureza; involuntários: resultado de ações não intencionais; e intencionais geradas a partir de ações planejadas para causarem danos, têm sua origem no ser humano. Considerando a área de tecnologia da informação, Junior (2008) explica que o risco pode ser definido como o impacto negativo ocasionado pela exploração de uma vulnerabilidade. Complementando, ISO/IEC (2014) sugere que pode ser expresso em termos de uma combinação entre consequência e probabilidade.
Vulnerabilidade	A vulnerabilidade pode ser entendida como uma fragilidade de um ativo ou conjunto de ativos que pode vir a ser explorada por uma ou mais ameaças causando um incidente, essa definição foi dada por ISO/IEC (2014).

Fonte: (próprio autor, 2021)

A fim de orientar sobre a aplicação da SGSI nas organizações, a NBR ISO/IEC 27002 da ABNT (2013) define um código de prática que pode ser utilizada na gestão de segurança da informação e orienta sobre os elementos que devem ser considerados. De acordo com a norma, a própria organização deve definir escopos e limites do SGSI levando em conta as características do negócio, sua localização, ativos e tecnologias disponíveis. Em complemento ao que diz a NBR ISO/IEC 27002, a norma NBR ISO/IEC 27001 da ABNT (2013a) provê um modelo para estabelecer, implementar,

operar, monitorar, analisar, manter e melhorar um Sistema de Gestão de Segurança da Informação. São descritas orientações considerando o Modelo PDCA (*Plan, Do, Check, Act*). Este modelo e sua relação com a SGSI está ilustrado na figura 2.

Figura 2 – Modelo do PDCA aplicado aos processos do SGSI.

Fonte: Fontes (2012)

A figura 2, como explicado por Fontes (2012), apresenta o relacionamento do Modelo PDCA com as etapas do SGSI, indicando que o Estabelecimento do SGSI está na etapa de Planejamento (Plan); a manutenção e a melhoria do SGSI encontram-se na fase de Elaboração (Act); o Monitoramento e a Análise do SGSI estão por sua vez na etapa de Verificação (Check) e a Implementação e Operação do SGSI estão na fase do Agir (Do).

2.2 Gestão de Riscos

O gerenciamento de riscos, conforme Sêmola (2014) compreende atividades coordenadas a fim de dirigir e controlar a organização em relação aos riscos. O objetivo da gestão de riscos é fornecer um instrumento para tomada de decisão com base em uma sólida compreensão dos riscos e o possível impacto sobre o alcance dos objetivos. Uma organização pode obter essa compreensão realizando a utilização eficiente de uma estrutura padronizada ou framework de risco que tem uma série de etapas bem definidas. Para Soula (2013), a gestão eficaz de risco ajuda a melhorar o desempenho da empresa contribuindo para:

• Diminuir o número de eventos inesperados;

• Melhorar o fornecimento do serviço;

• Gerenciar mudanças de forma mais eficaz;

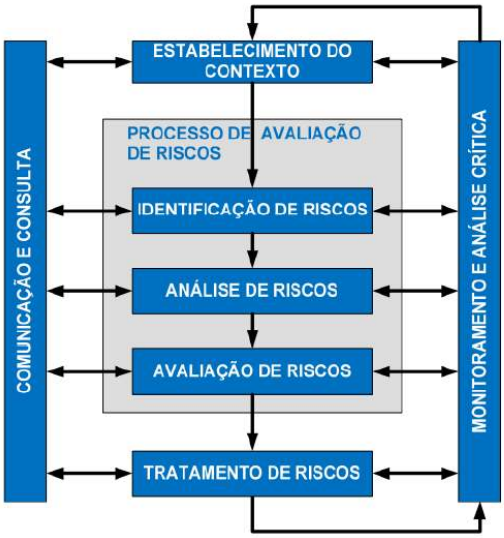
• Melhor utilização dos recursos; e

• Melhor gerenciamento em todos os níveis, visto que possibilita uma melhor tomada de decisões.

O processo de gestão de riscos de segurança da informação sugerido pela norma NBR ISO/IEC 27005 da ABNT (2011) consiste em seis etapas, conforme mostrado na figura 3:

1. Definição do contexto: constitui-se de todas as informações sobre a organização relevantes para a gestão de riscos de segurança da informação.
2. Processo de avaliação de riscos: Espera-se que os riscos sejam devidamente identificados, quantificados ou descritos qualitativamente, priorizados em função dos critérios de avaliação determinada pela organização.
3. Tratamento do risco: Selecionam-se controles para modificar, reter, evitar ou compartilhar os riscos e define-se o plano de tratamento do risco.
4. Aceitação do risco: Depois de analisar o plano de tratamento de risco, podem existir riscos residuais. A aceitação do risco se dá quando os gestores optam formalmente por aceitar esses riscos.
5. Comunicação e consulta do risco: Há o compartilhamento e/ou troca das informações sobre riscos entre as partes interessadas.
6. Monitoramento e análise crítica de riscos: Os riscos e seus fatores (valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidade de ocorrência) devem ser monitorados e analisados criticamente, para identificar, o mais rapidamente possível, eventuais mudanças no contexto da organização.

Figura 3 – Processo de gestão de riscos de segurança da informação



Fonte: ABNT (2011))

Este trabalho foca na fase do macroprocesso de avaliação de riscos, que inclui identificação dos ativos e dos riscos associados, os impactos e as medidas necessárias para minimizar o nível de risco obtido, considerando os diferentes processos e ativos que uma organização pode possuir.

A análise de risco está preocupada com o recolhimento de informações sobre exposição ao risco para que a organização possa tomar decisões apropriadas e gerenciar informações de forma adequada. A análise de risco envolve, de acordo com Soula (2013): a identificação e avaliação do nível dos riscos calculados considerando os valores avaliados dos ativos e os níveis de ameaças e vulnerabilidades desses ativos. Como explicado por Bezerra (2013), em um SGSI, a definição do contexto, o processo de avaliação de riscos, o desenvolvimento do plano de tratamento do risco e a aceitação do risco fazem parte da fase “planejar” do ciclo de melhoria contínua PDCA (Planejar, Executar, Verificar, Agir). A fase “executar” do SGSI, se refere às ações e controles necessários para reduzir os riscos a um nível aceitável e são implementados de acordo com o plano de tratamento do risco. Na fase “verificar”, os gestores determinam a necessidade de revisão da avaliação e tratamento do risco. Na fase “agir”, as ações necessárias são executadas, incluindo a reaplicação do processo de gestão de riscos de segurança da informação. A tabela 2 mostra as principais atividades da Gestão de Risco.

Tabela 2 – Principais atividades da Gestão de Risco

Processo do SGSI	Processo de Gestão de Risco
Planejar(P)	Definição do contexto; avaliação de riscos (risk assessment); definição do plano de tratamento do risco; aceitação do risco.
Executar(D)	Implementação do plano de tratamento do risco.
Verificar(C)	Monitoramento contínuo e análise crítica de riscos.
Agir(A)	Manter e melhorar o processo de gestão de riscos de segurança da informação.

Fonte: ABNT (2011).

A gestão de riscos pode ocorrer em diferentes níveis e pode ser aplicada à organização como um todo ou a setores desta. Cada setor pode conter processos de negócios que se necessário, são decompostos em ativos, tais como hardware, redes e software. FACTI (2015) explica que o gerenciamento de riscos, considerando esses níveis detalhados, permite estabelecer medidas de proteção específicas. A figura 4 mostra os três níveis para a gestão de riscos: 1º nível – gestão de aspectos gerais da organização; 2º nível – gestão voltada para os processos de negócios; 3º nível – gestão específica para cada ativo de informação.

Figura 4 – Níveis de atuação da Gestão de Riscos

Fonte: FACTI (2015)

2.3 Governança de TI

Para ABNT (2009), a Governança de TI avalia e direciona o uso da TI de tal forma que dê suporte à organização e monitore seu uso para realizar planos. O principal

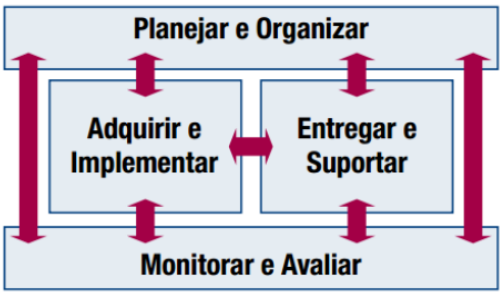
objetivo é o alinhamento da TI aos requisitos do negócio. Para Weill e Ross (2006), a governança de TI pode ser definida como a especificação dos direitos decisórios e do framework de responsabilidades para estimular comportamentos desejáveis na utilização de TI. A governança de TI, objetiva, segundo Fagundes (2012), o retorno dos investimentos realizados no melhoramento da infra-estrutura e dos sistemas de informação, e é constituída por uma estrutura de relações e processos que adicionam valor ao negócio através de um gerenciamento balanceado de riscos. Conforme Fernandes e Abreu (2012), a implantação da Governança de TI pode ser alcançada utilizando-se modelos de melhores práticas para TI. Um destes é o COBIT *(Control Objectives for Information and related Technology)*, que provê um framework referência, a versão 4.1 utilizado neste trabalho é subdividido em quatro domínios:

1. Planejar e Organizar;
2. Adquirir e Implementar;
3. Entregar e dar Suporte;
4. Monitorar e Avaliar;

e 34 processos, conforme ilustrado na figura 5 em linha com as áreas responsáveis por planejar, construir, executar e monitorar, que provê assim, uma visão total da área de TI. Esses domínios mapeiam as tradicionais áreas de responsabilidade de TI de planejamento, construção, processamento e monitoramento.

O domínio de Planejamento e Organização é composto, entre outros, pelo processo de avaliação e gerenciamento de riscos.

Figura 5 – Níveis de atuação da Gestão de Riscos



Fonte: Institute (2007)

A tabela 3 mostra o alinhamento do processo P09 do COBIT 4.1 com a NBR ISO/IEC 27005.

Tabela 3 – Alinhamento do processo P09 do COBIT 4.1 com a NBR ISO/IEC 27005

COBIT 4.1	ISO/IEC 27005:2011
PO9.1 Alinhamento da gestão de riscos de TI e de Negócio: Estabelecer uma estrutura de gestão de riscos de TI alinhada com a estrutura de gestão de riscos da organização (corporação).	Cabe à organização definir sua abordagem ao processo de gestão de riscos, levando em conta, por exemplo, o escopo do seu SGSI, o contexto da gestão de riscos e o seu setor de atividade econômica.
PO9.2 Estabelecimento do Contexto de Risco Estabelecer o contexto ao qual a estrutura de avaliação de risco é aplicada para assegurar resultados esperados. Isso inclui a definição dos contextos interno e externo de cada avaliação de risco, o objetivo da avaliação e os critérios pelos quais os riscos são avaliados.	7.1 Convém que o contexto externo e interno para gestão de riscos de segurança da informação seja estabelecido, o que envolve a definição dos critérios básicos necessários para a gestão de riscos de segurança da informação, a definição do escopo e dos limites e o estabelecimento de uma organização apropriada para operar a gestão de riscos de segurança da informação.
PO9.3 Identificação de Eventos Identificar eventos (importante ameaça real que explora significativas vulnerabilidades) com potencial impacto negativo nos objetivos ou nas operações da organização, incluindo aspectos de negócios, regulamentação, aspectos jurídicos, tecnologia, parcerias de negócio, recursos humanos e operacionais. Determinar a natureza do impacto e manter esta informação. Registrar e manter um histórico dos riscos relevantes.	
PO9.4 Avaliação de Risco: Avaliar regularmente a probabilidade e o impacto de todos os riscos identificados, utilizando métodos qualitativos e quantitativos. A probabilidade e o impacto associado ao risco inerente e residual devem ser determinados individualmente, por categoria e com base no portfólio da organização	8.1 Convém que os riscos sejam identificados, quantificados ou descritos qualitativamente, priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização.

PO9.5 Resposta ao Risco Desenvolver e manter um processo de respostas a riscos para assegurar que controles com uma adequada relação custo-benefício mitiguem a exposição aos riscos de forma contínua. O processo de resposta ao risco deve identificar estratégias de risco, tais como evitar, reduzir, compartilhar ou aceitar o risco, determinar responsabilidades, e considerar os níveis de tolerância definidos.	9.1 Convém que controles para modificar, reter, evitar ou compartilhar os riscos sejam selecionados e o plano de tratamento do risco seja definido.
PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco Priorizar e planejar as atividades de controle em todos os níveis da organização para implementar as respostas aos riscos identificadas como necessárias, incluindo a identificação de custos, benefícios e responsabilidade pela execução. Obter aprovações para ações recomendadas e aceitação de quaisquer riscos residuais e assegurar que as ações aprovadas sejam assumidas pelos donos dos processos afetados. Monitorar a execução dos planos e reportar qualquer desvio para a Alta Direção.	12.1 Convém que os riscos e seus fatores (isto é, valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidade de ocorrência) sejam monitorados e analisados criticamente, afim de identificar, o mais rapidamente possível, eventuais mudanças no contexto da organização e de manter uma visão geral dos riscos.

Fonte:(Fonte: próprio autor, 2021).

Diante do exposto na tabela 3, em que pôde-se verificar o alinhamento entre um dos processos do COBIT com algumas das regras da NBR ISO/IEC 27005, é plausível afirmar que existe a possibilidade de se criar um modelo de gestão de riscos que atenda a ambos.

2.4 Tecnologias Aplicadas em Gestão de Riscos

Objetivando obter maior conhecimento sobre o estado da arte do assunto relacionado a este trabalho – Gestão de Riscos – foi realizada uma pesquisa bibliográfica sobre softwares relacionados a este assunto disponíveis no mercado. Para realizar esta pesquisa foram lidos diversos artigos e trabalhos oriundos de repositórios relevantes como IEEE, ACM, Periódicos da Capes, Repositórios de Universidades a fim de encontrar possíveis softwares propostos na área. Além disso, foram feitas buscas em

sites específicos, usando para isto palavras chaves relacionadas ao assunto, a fim de verificar resultados de softwares desenvolvidos por empresas. Foram encontrados alguns (detalhados adiante), a maioria são softwares proprietários, que para serem utilizados devem ser comprados, a única que pode ser adquirida de forma gratuita é a ferramenta da Microsoft. Segue abaixo a descrição dos programas encontrados.

• BART: Clavis (2021) descreve o software como sendo reconhecido pelo Ministério da Defesa como Produto de Defesa, o programa permite o gerenciamento de vulnerabilidades e mensura o real impacto e a probabilidade de exploração de uma vulnerabilidade.

• QuantiRisk: Modulo (2021) explicita que se trata de um software para gestão de riscos cibernéticos, este permite a sua mensuração de forma quantitativa. A solução é baseada em normas e padrões como ISO 31000, 27001, FAIR – *Factor Analysis of Information Risk* e a recente versão dos controles do CIS.

• *Microsoft Security Assessment Tool*: Microsoft (2021) esclarece que o programa propõe questões e, conforme as respostas, oferece recomendações baseadas em padrões como ISO 17799 e NIST-800.x. A ferramenta pode ser baixada gratuitamente através do site oficial do projeto. No entanto, a última atualização ocorreu em 2012 e não é compatível com sistemas operacionais populares, tais como Windows 8, 10 e Linux.

2.5 Trabalhos Correlatos

Nesta seção serão apresentados três trabalhos correlatos, relacionados ao tema de pesquisa descrito neste projeto, a fim de identificar o estado da arte nesta área de estudo. O documento "Metodologia de Gestão de Riscos de Segurança da Informação - Desenvolvimento de metodologia e ferramenta de software público de arquitetura aberta para gestão de riscos de segurança da informação na Administração Pública Federal" publicado pela FACTI (2015), apresenta a Metodologia de Gestão de Riscos de Segurança da Informação do SISP (MGR-SISP). Este visa descrever métodos para padronizar e sistematizar a gestão de riscos de segurança da informação na Administração Pública Federal (APF) e objetivou atingir níveis satisfatórios de segurança da informação, bem como racionalizar os investimentos na área de segurança da informação. A metodologia proposta visou uma plataforma integradora de iniciativas do governo com o intuito de aprimorar a segurança da informação na APF. As informações necessárias para a realização dos processos da metodologia proposta foram obtidas por meio de

questionários. O questionário focou em Itens de Controle e admitiu para cada questão a resposta da classificação de grau de implementação do Item de Controle entre zero e cinco (grau variando de: “controles não adotados”, passando por: “controles executados e documentados”, até “controles analisados e aprimorados”). Para cada item de controle foi classificado o Grau de Implementação (GI), que variou entre 0 e 5. Depois de respondidos os questionários para todas as unidades, e abordando todos os ativos, foi possível apurar para cada unidade, uma lista de ativos primários e respectivos valores de criticidade para cada um dos atributos, além de valores totais. Este trabalho correlato é voltado para um órgão em específico, diferente do que é proposto nesse projeto, que deve ser genérico e servir de apoio para qualquer tipo de empresa.

Palko et al. (2020) explicam que desenvolveram um algoritmo de identificação e avaliação de ameaças à segurança da informação e um método de avaliação de risco utilizando inteligência artificial e redes neurais. Os autores afirmam que o módulo de software desenvolvido por eles para avaliar segurança da informação pode ser usado por qualquer organização, independentemente de seu porte, propriedade ou ramo de atividade. No entanto, não foram encontradas informações de acesso a esse software.

O trabalho *Methodology for Dynamic Analysis and Risk Management on ISO27001* de Santos-Olmo et al. (2016) apresenta uma nova metodologia, denominada MARISMA, que visa a realização de uma análise de risco simplificada e dinâmica, válida para todas as empresas. Apesar de ser uma proposta interessante, não foram encontradas uma implementação disponível desta metodologia, ao contrário do modelo desse trabalho que possui uma solução online.

3 METODOLOGIA

A Metodologia pode ser considerada, de acordo com Barros e Lehfeld (2007), como um estudo de técnicas específicas para abordar determinados problemas, utilizando para isso conhecimentos prévios, não buscando soluções, mas fazendo a escolha de formas de achá-las, integrando o conhecimento dos métodos existentes nas diferentes disciplinas científicas ou filosóficas. Este trabalho teve como foco realizar uma pesquisa sobre a segurança da informação, gestão de riscos, incidentes, normas de segurança, modelos de governança e demais assuntos relacionados. Após, construiu-se um modelo para análise de risco, validou-se o modelo, implementou-se, testou-se e analisou-se os resultados. Na sequência segue a proposta de metodologia adotada neste trabalho.

3.1 Caracterização da Pesquisa

De acordo com os tipos de pesquisa descritos por Gil (2010), esse trabalho se classificou como exploratório, visto que propõe maior entendimento sobre o tema em estudo e, a implementação de um recurso de software que auxilie na resolução dos problemas encontrados. Além disso, de acordo com a taxonomia de Vergara (2006), esta pesquisa se classificou como de natureza aplicada, já que objetivava identificar uma situação-problema e buscar, dentre as possíveis soluções, uma que fosse a mais adequada para o contexto; não havia objetivo de criar novos conhecimentos, somente aplicar conhecimentos já existentes a uma situação problema. Quanto à metodologia, se enquadrou no método hipotético-dedutivo, pois a partir da hipótese proposta de um recurso para avaliação da segurança de informação partiu-se para a sua implementação e, posteriormente, para a análise dos resultados alcançados. Quanto aos procedimentos técnicos, este trabalho adotou os tipos bibliográfica, documental e experimental.

3.2 Procedimento Metodológico

Este trabalho foi dividido em três fases distintas, cada uma com um conjunto peculiar de ações, como é apresentado na figura 6.

Figura 6 – Passos adotados na metodologia

(Fonte: Próprio autor, 2021)

A Fase Decisória consistiu em seis passos: Os três primeiros basearam-se na definição do tema e um estudo teórico sobre o estado da arte em relação ao problema de pesquisa, com o intuito de construir uma base de conhecimento necessária para a gestão de riscos. Para atingir esse objetivo, a fase inicial deste projeto teve como foco o levantamento de um referencial bibliográfico sobre o tema em artigos de congressos da área de estudo, revistas, livros e bibliotecas digitais de relevância no meio, como a IEEE, ACM, Periódicos da Capes, Repositórios de Universidades entre outros. O quarto passo consistiu no estudo e definição das normas. Após, partiu-se para o estudo de incidentes de TI e estudo e definição de modelo de governança a ser utilizado no desenvolvimento desde trabalho. A partir da segunda Fase – Construtiva – foi proposto um modelo para avaliação e gestão de riscos. O segundo passo desta fase foi a validação do modelo e, logo após, partiu-se para levantamento e análise de requisitos, o desenvolvimento de um projeto de software para automatização desse modelo e a implementação. Após, foram realizados testes a fim de saber se os resultados fornecidos estavam de acordo com o esperado. Ao final desta fase, tem-se a escrita dos resultados. A Fase Redacional acompanhou simultaneamente todas as demais fases, objetivando a descrição detalhada de todos os passos, desde a fase inicial até a final deste projeto.

4 DESENVOLVIMENTO DA FERRAMENTA ARION

Este capítulo tem como objetivo apresentar a solução proposta após os estudos realizados. Foi possível observar que os maiores problemas relacionados a Gestão de Riscos de segurança da informação estão no fato de que as normas e padrões internacionais recomendadas para tal ação não possuem regras claras de como implantá-las, o que dificulta a adoção das boas práticas de segurança da informação através do gerenciamento de riscos. Sabendo-se disso, apresenta-se na seção 4.1 o modelo proposto neste trabalho, posteriormente nos demais capítulos são apresentados a modelagem, a implementação e os testes de software, bem como são discutidos os resultados obtidos.

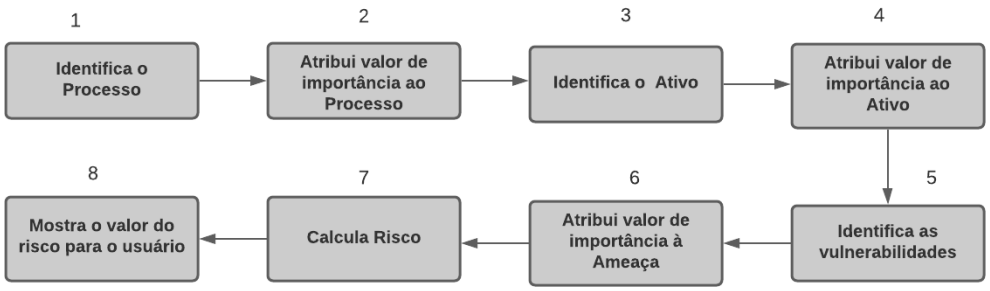
4.1 Modelo Proposto

O modelo criado foi resultado de uma pesquisa bibliográfica sobre o assunto. Como resultado desta pesquisa tem-se a proposição de um modelo e a automatização deste, capaz de auxiliar o usuário na gestão de riscos. Para um melhor entendimento, o modelo será descrito detalhadamente a seguir.

4.1.1 Funcionamento do Modelo

A NBR ISO/IEC 27005 (ABNT, 2011) propõe os seguintes passos para a identificação dos riscos: 1) identificar os ativos; 2) identificar as ameaças a esses ativos; 3) identificar as vulnerabilidades que podem ser exploradas pelas ameaças; 4) identificar os impactos que possam ser causados aos ativos. Sabendo disso, foi construído o modelo ilustrado na figura 7 que consiste em 8 passos.

Figura 7 – Funcionamento do modelo



(Fonte: Próprio autor, 2021)

O modelo funciona da seguinte forma:

1. Identifica os Processos; 2. Atribui o valor de importância com base em uma escala de 3 pontos, conforme tabela 4;

Tabela 4 – Nota e Descrição de importância de processo

Nota	**Descrição da nota**
1	Pouco Importante (alterações no processo não impedem o cumprimento da missão da organização);
2	Importante (alterações podem afetar de forma significativa o cumprimento da missão da organização);
3	Muito Importante (sua interrupção torna impossível o cumprimento da missão da organização);

Fonte: (próprio autor, 2021)

3. Identifica os ativos;

4. Atribui o valor de importância com base em uma escala de 3 pontos, conforme tabela 5.

Tabela 5 – Nota e Descrição de importância do ativo

Nota	**Descrição da nota**
1	Pouco Importante (ativo pode ser substituído/recriado com facilidade);
2	Importante (ativo pode ser substituído/recriado com dificuldade);
3	Muito Importante (ativo não pode ser substituído);

Fonte: (próprio autor, 2021)

Esse tipo de valoração dos ativos (por substituição/recriação) é um dos tipos sugeridos pela norma NBR ISO/IEC 27005 (ABNT, 2011).

5. Identifica as vulnerabilidades;

6. Atribui o valor de importância do impacto com base em uma escala de 5 pontos (tabela 6), conforme sugerido por Dantas (2011);

Tabela 6 – Nota e Descrição de valor de importância do impacto

Nota	**Descrição da nota**
1	Insignificante (nenhum prejuízo na imagem, perdas financeiras irrelevantes, sem impactos sobre os negócios);
2	Menor (pequenos efeitos e facilmente reparados, solução imediata local, perdas financeiras médias);
3	Moderado (efeitos sobre algumas atividades de negócios, possui solução com ajuda externa, perdas financeiras moderadas);
4	Maior (grandes abalos na imagem. interrupção temporária da atividade de negócio, ajuda externa para tratamento, perdas financeiras elevadas);
5	Catastrófico (morte, interrupção total das atividades, solução externa, danos de difícil reparação, perdas financeiras elevadas);

Fonte: (próprio autor, 2021)

De acordo com a norma NBR ISO/IEC 27005 (ABNT, 2011), o impacto que venha a ser causado por um incidente deve ser considerado na avaliação de riscos, a forma como é tratado neste modelo (valor financeiro e consequências resultantes de violações da segurança da informação) são algumas das formas sugeridas pela norma.

7. Calcula risco;

8. Apresenta o índice de risco para o usuário;

Para o cálculo do Risco foram propostas algumas equações, explicadas a seguir.

$$\text{Probabilidade de um incidente acontecer (probabilidade de uma ameaça ser explorada)} = \sum(\text{Agravo e Desagravo}) \quad (1)$$

Para cada ativo há uma lista de ameaças, para cada uma destas há outra lista de possíveis vulnerabilidades (que se exploradas podem provocar o incidente descrito na ameaça), a tabela 7 apresenta um exemplo do que foi explicado, utilizando o ativo hardware, descrevendo uma ameaça (“Furto de mídias ou documentos”) e 3

vulnerabilidades. Se existir a vulnerabilidade então soma-se 1 (Agravo), se não, soma-se 0 (Desagravo). Ao final têm-se o somatório, que retornará à probabilidade de um determinando incidente ocorrer com um ativo em específico.

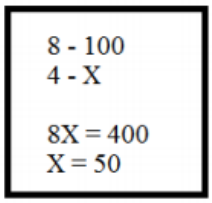
Tabela 7 – Exemplo de Ameaça e Vulnerabilidades para um Ativo

Ativo	**Ameaça**	**Vulnerarbilidade**
Hardware	Furto de Mídias ou Documentos	1. Empresa não possui armazenamento de hardware protegidos; 2. Mídias que possuem informações sensíveis não são guardadas de forma segura; 3. Empresa não controla as cópias realizadas no local

Fonte: (próprio autor, 2021)

Utilizando o exemplo da tabela 7, se um determinado usuário identificasse 1 das 3 vulnerabilidades, então o somatório seria 1 (1 +0 + 0). Considerando os diferentes incidentes possíveis e o número não fixo de vulnerabilidades que podem ser exploradas, se fez necessário encontrar uma maneira de colocar todos os valores possíveis de serem encontrados nessa equação em uma mesma escala. Para atingir esse propósito, faz-se uma regra de 3 considerando o número total de vulnerabilidades e aquelas marcadas pelo usuário. Por exemplo, se para o ativo hardware, em uma determinada ameaça têm-se 8 vulnerabilidades no total (100%), e, o usuário identificou 4 destas, então obtêm-se o valor 50, correspondente a porcentagem 50%, conforme ilustrado na figura 8.

Figura 8 – Exemplo de Conversão.



(Fonte: Próprio autor, 2021)

Após, relaciona-se esse valor com a tabela 8 para enfim obter o resultado numérico final da probabilidade de o incidente ocorrer, o que será usado na equação 2.

Tabela 8 – Escala adotada como resultado na equação 1

Resultado Somatório	**Resultado final a ser utilizado nas demais equações**
0 - 20	1
21 - 41	2
42 - 62	3
63 - 84	4
85 - 100	5

Fonte: (próprio autor, 2021)

$$\begin{aligned} &Risco\ de\ incidente\ para\ um\ ativo \\ &\quad = (probabilidade\ do\ incidente\ acontecer) \\ &\quad * (valor\ de\ importância\ da\ ameaça) \\ &\quad * (valor\ de\ importância\ do\ processo) \\ &\quad * (valor\ de\ importância\ do\ ativo) \end{aligned} \tag{2}$$

A equação 2 determina o risco final de ocorrer um determinado incidente, levando em consideração o valor de importância do impacto da ameaça, do processo e do ativo. Multiplica-se todos esses valores, e têm-se um resultado numérico de risco.

As equações 1 e 2 são aplicadas para cada ativo e para cada ameaça. Objetivando determinar um único valor de risco total para o ativo, optou-se por comparar os índices de riscos calculados a partir das Equações 1 e 2 na análise e fornecer ao usuário como risco final do ativo o maior valor encontrado. Essa escolha teve como embasamento os testes realizados na validação do modelo, fornecer uma média, por exemplo, retornava muitas vezes um valor de risco baixo ou médio, o que poderia dar ao usuário uma falsa ideia de bom nível de segurança. Por exemplo: Um usuário ao efetuar a análise do risco de um ativo hardware encontrou os seguintes valores:

- Risco de ocorrer incidente 1: 8
- Risco de ocorrer incidente 2: 16
- Risco de ocorrer incidente 3: 8
- Risco de ocorrer incidente 4: 60
- Risco de ocorrer incidente 5: 4
- Risco de ocorrer incidente 6: 80

O valor do risco médio retornado para o ativo hardware será 80. Se fosse realizado uma média aritmética por exemplo, o valor seria 30.

Além de um valor quantitativo que se refere àqueles expressos em escala de razão,

Alencar e Schmitz (2006) explicam que os riscos podem assumir um valor qualitativo, tal classificação é recomendada, pois substitui os valores numéricos do risco quantitativo (muitas vezes difíceis de compreender) por rótulos como "Alto", "Médio"e "Baixo", mais simples de serem compreendidos.

Neste trabalho para classificação de riscos quantitativos será adotado a escala *Likert*. Os valores quantitativos e qualitativos correspondentes, adotados neste trabalho, podem ser visualizados na tabela 9.

Tabela 9 – Nota e Descrição de Risco

Classificação Qualitativa	Classificação Quantitativa
Risco Muito Baixo	0 – 25
Risco Baixo	26 – 40
Risco Moderado	41 – 60
Risco Alto	61 – 100
Risco Muito Alto	Acima de 100

Fonte: (próprio autor, 2021)

As classificações, bem como os intervalos quantitativos para cada risco qualitativo descritos na tabela 9 foram obtidos por método de tentativa e erro e foram validados. No próximo subcapítulo será descrito como se deu esse processo de validação.

4.1.2 Validação do Modelo

Para avaliar de forma preliminar o modelo proposto, foram realizados testes. Estes são constituídos de três passos, detalhados a seguir:

1. Foram elencadas cinco empresas reais para testar o modelo;
2. Os profissionais das empresas responderam ao questionário (Apêndice B);
3. Foi realizada a análise de risco considerando as respostas fornecidas no questionário.

O resultado final está na tabela 10. Profissionais de diversas empresas com diferentes ramos de atuação (financeiro, comércio, indústria, educação, órgão/instituição pública e prestação de serviços) responderam aos questionários.

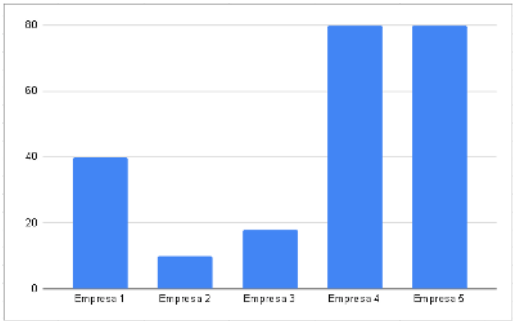
Tabela 10 – Resultado dos Testes do Modelo criado

Empresa	**Ativo Hardware**	**Ativo Software**	**Ativo Redes**
Empresa 1 (Pública Federal)	40	100	60
Empresa 2 (Privada)	10	8	4
Empresa 3 (Privada)	18	18	16
Empresa 4 (Pública Estadual)	80	120	60
Empresa 5 (Privado)	80	64	48

Fonte: (próprio autor, 2021)

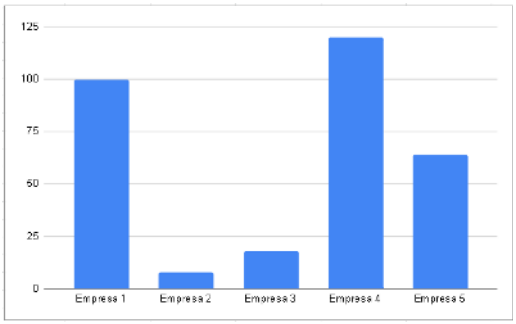
Os questionários utilizados no passo 2 para identificação de vulnerabilidades e ameaças foram baseadas na norma NBR ISO/IEC 27005 (ABNT, 2011). Para cada resposta dada pelo usuário, era verificado se aquilo que o modelo retornava era aceitável considerando a quantidade de vulnerabilidades encontradas e os valores atribuídos aos ativos e ameaças. Os valores de risco obtidos entre as 5 empresas, por ativo, pode ser visualizados graficamente nas figuras 9 à 11.

Figura 9 – Valores obtidos para o Ativo Hardware



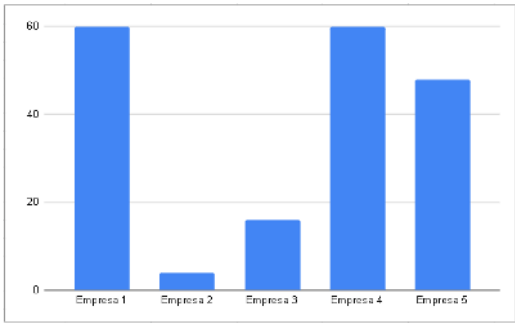
Fonte: próprio autor, 2021)

Figura 10 – Valores obtidos para o Ativo Software



Fonte: próprio autor, 2021)

Figura 11 – Valores obtidos para o Ativo Redes



Fonte: próprio autor, 2021)

Considerando que os resultados de risco encontrados no modelo criado corresponderam àqueles que eram esperados, pode-se concluir que o modelo foi validado com sucesso. Assim, parte-se para a próxima fase: a automatização, que começa a ser descrita na próxima seção.

4.2 Modelagem do ARION

Adotando as boas práticas de engenharia de software, que de acordo com Pressman (2011), visa proporcionar um produto confiável e que funcione de maneira eficiente, antes da implementação do projeto em si, fez-se a modelagem. Pressman (2011) explica que a modelagem permite compreender o que será realmente construído. Do ponto de vista de software, os modelos devem cumprir seus objetivos em diferentes níveis de abstração, considerando o ponto de vista do cliente e um nível mais técnico.

Para o planejamento de um sistema automatizado de cálculo de risco, que vise contribuir para melhorar o nível de segurança de informação de empresas/organizações, foram levantados os requisitos descritos nas tabelas 11 e 12. Os detalhes de descrição, entradas e saídas esperadas, os processos e prioridades de cada um dos requisitos estão detalhados no Apêndice A deste trabalho.

Tabela 11 – Requisitos Funcionais

RF01	Cadastro de Usuário
RF02	Cadastro de Empresa
RF03	Cadastro de Processo
RF04	Cadastro de Ativo
RF05	Login de Usuário
RF06	Editar Usuário
RF07	Editar Empresa
RF08	Excluir Usuário
RF09	Excluir Processo
RF10	Excluir Empresa
RF11	Realizar Análise
RF12	Acessar Relatórios
RF13	Excluir Relatórios

Fonte: (próprio autor, 2021)

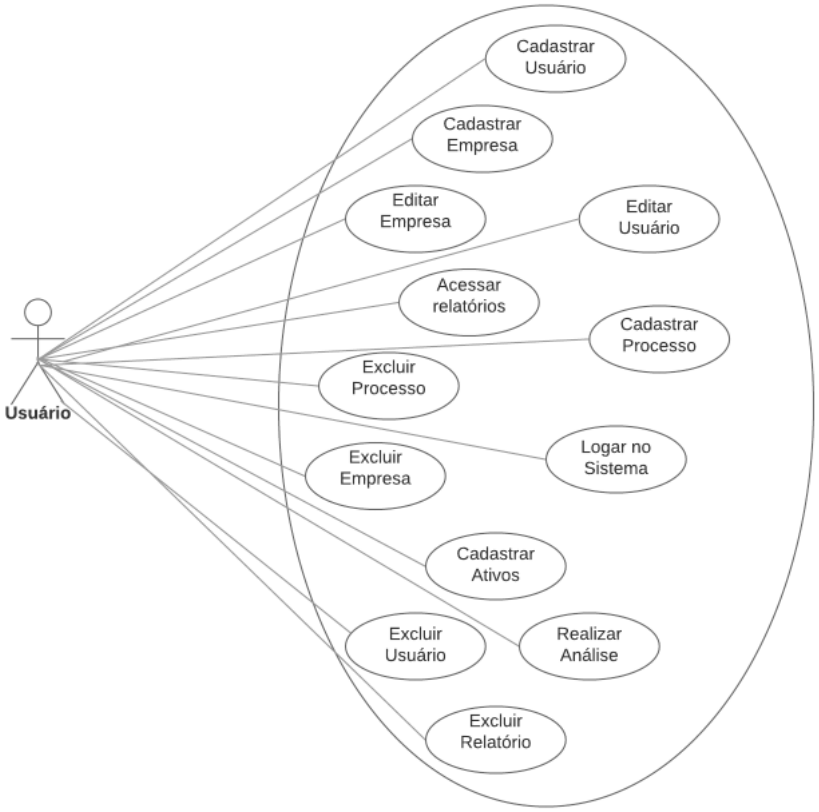
Tabela 12 – Requisitos Não Funcionais

NF001	Linguagem de Programação e Ambiente de Programação
NF002	Usabilidade

Fonte: (próprio autor, 2021)

Após, elaborou-se os Diagramas UML que, conforme ensinado por Sommerville (2019), permitem modelar sistemas de software: de Casos de Uso (figura 12), que permite visualizar quais funcionalidades devem estar disponíveis ao usuário; o Diagrama de Classes Conceitual (figura 13) que, de acordo com Departamento de Sistemas e Computação - DSC (2021), permite obter uma perspectiva destinada ao cliente, o Diagrama de Sequências (figura 14) que, conforme Sommerville (2019), modelam as interações entre os componentes do sistema e, por fim, o Diagrama Entidade-Relacionamento (E-R), explicado por Silberschatz, Korth e Sudarshan (2006), como uma forma de expressar graficamente a estrutura lógica de um banco de dados.

Figura 12 – Casos de uso de Usuário



Fonte: próprio autor, 2021.

Cenários:

Cadastrar Usuário

Tabela 13 – Caso de Uso: Cadastrar Usuário

Descrição	Este caso de uso tem por objetivo cadastrar o Usuário
Ator	Usuário

Fonte: (próprio autor, 2021)

Cenário Principal:

1. O sistema exibe as informações necessárias para realizar o cadastro do Usuário:

• Nome;

• E-mail;

• CPF;

• Senha;

• Cargo;

2. O usuário preenche as informações;

3. O sistema cadastra o usuário;

Cenário Alternativo:

1. Usuário já cadastrado: Se já existir um cadastro, será retornado uma mensagem de erro. A comparação de existência de cadastro será realizada através do E-mail informado.

Tabela 14 – Caso de Uso: Editar Usuário

Descrição	Este caso de uso tem por objetivo editar dados de cadastro de Usuário
Ator	Usuário

Fonte: (próprio autor, 2021)

Cenário Principal:

1. O sistema exibe as informações cadastradas pelo Usuário:

• Nome;

• E-mail;

• CPF;

• Senha;

• Cargo;

2. O usuário altera as informações que desejar;

3. O sistema salva as informações;

Cenário Alternativo:

Não há

Tabela 15 – Caso de Uso: Excluir Usuário

Descrição	Este caso de uso tem por objetivo excluir todos os dados do Usuário
Ator	Usuário

Fonte: (próprio autor, 2021)

Cenário Principal:

1. O sistema exibe mensagem perguntando ao Usuário se realmente deseja executar essa ação e informa que esta não pode ser desfeita.
2. O usuário exclui sua conta;
3. O sistema confirma a exclusão de conta.

Cenário Alternativo:

Não há.

Cadastrar Empresa

Tabela 16 – Caso de Uso - Cadastrar Empresa

Descrição	Este caso de uso tem por objetivo cadastrar a Empresa
Ator	Usuário

Fonte: (próprio autor, 2021)

Cenário Principal:

1. O sistema exibe as informações necessárias:
• Nome Fantasia da Empresa;
• CNPJ ou CEI;
• Endereço;
• Cidade;
2. O usuário preenche as informações;
3. O sistema cadastra a empresa.

Cenário Alternativo:

Não há.

Editar Empresa

Tabela 17 – Caso de Uso - Editar Empresa

Descrição	Este caso de uso tem por objetivo editar dados de Empresa
Ator	Usuário

Fonte: (próprio autor, 2021)

Cenário Principal:

1. O sistema exibe as informações cadastradas da empresa:

• Nome Fantasia da Empresa;

• CNPJ ou CEI;

• Endereço;

• Cidade;

2. O usuário altera as informações que desejar;

3. O sistema salva as informações.

Cenário Alternativo:

Não há.

Excluir Empresa

Tabela 18 – Caso de Uso - Excluir Empresa

Descrição	Este caso de uso tem por objetivo excluir dados de Empresa
Ator	Usuário

Fonte: (próprio autor, 2021)

Cenário Principal:

1. O sistema exibe as empresas cadastradas;

2. O usuário seleciona a empresas que deseja excluir;

3. O sistema confirma a exclusão da empresa.

Cenário Alternativo:

Não há.

Cadastrar Processo

Tabela 19 – Caso de Uso - Cadastrar Processo

Descrição	Este caso de uso tem por objetivo cadastrar o Processo
Ator	Usuário

Fonte: (próprio autor, 2021)

Cenário Principal:

1. Sistema exibe uma lista das empresas cadastradas pelo usuário;
2. Usuário seleciona a empresa para cadastrar processo;
3. O sistema exibe as informações necessárias:
• Descrição do Processo
• Valor de Importância do Processo;
4. O usuário preenche as informações;
5. O sistema confirma o cadastro do processo;

Cenário Alternativo:

Não há.

Excluir Processo

Tabela 20 – Caso de Uso - Excluir Processo

Descrição	Este caso de uso tem por objetivo excluir dados de Processo
Ator	Usuário

Fonte: (próprio autor, 2021)

Cenário Principal:

1. Sistema exibe uma lista de processos cadastrados pelo usuário;
2. Usuário seleciona o processo para ser excluído;
3. O sistema confirma a exclusão do processo;

Cenário Alternativo:

Não há.

Cadastrar Ativo

Cenário Principal:

1. Sistema exibe uma lista das empresas cadastradas pelo usuário;
2. Usuário seleciona a empresa;

Tabela 21 – Caso de Uso - Cadastrar Ativo

Descrição	Este caso de uso tem por objetivo cadastrar o Ativo
Ator	Usuário

Fonte: (próprio autor, 2021)

3. O sistema exibe a lista de processos correspondentes a empresa selecionada;

4. O usuário seleciona o processo;

5. O sistema exibe as informações para cadastrar o ativo:

• Descrição do Ativo;

• Tipo do Ativo;

• Valor de Importância do Ativo;

Cenário Alternativo:

Não há.

Logar no Sistema

Tabela 22 – Caso de Uso - Logar no Sistema

Descrição	Este caso de uso tem por objetivo logar o usuário no sistema
Ator	Usuário

Fonte: (próprio autor, 2021)

Cenário Principal:

1. Sistema exibe as informações necessárias para logar:

2. Usuário insere as informações corretas (cadastradas no Banco);

3. Sistema loga e vai para outra página.

Cenário Alternativo:

1. Usuário insere informações diferentes daquelas salvas no Banco: Se o usuário digitar o email e/ou senha diferente(s) do que foi salvo na hora do Cadastro, o sistema redirecionará à página inicial do sistema.

Realizar a análise de risco

Cenário Principal:

1. Sistema exibe uma lista das empresas cadastradas pelo usuário;

Tabela 23 – Caso de Uso - Realizar Análise

Descrição	Este caso de uso tem por objetivo realizar a análise de risco
Ator	Usuário

Fonte: (próprio autor, 2021)

2. Usuário seleciona a empresa;
3. Sistema exibe uma lista de processos cadastrasdos para a empresa selecionada;
4. Usuário seleciona o processo;
5. Sistema exibe uma lista de ativos cadastrados para aquele processo;
6. Usuário seleciona o ativo;
7. Sistema exibe o check-list;
8. Usuário preenche o check-list;
9. Sistema exibe uma tela com o valor de risco quantitativo para o ativo.
10. Usuário pode salvar relatório da análise em pdf.

Cenário Alternativo:

Não há, a análise só pode ser realizada depois de todos os passos descritos serem concluídos.

Acessar e Baixar relatórios

Tabela 24 – Caso de Uso: Acessar e baixar relatórios

Descrição	Este caso de uso tem por objetivo acessar e baixar relatórios das análises de riscos
Ator	Usuário

Fonte: (próprio autor, 2021)

Cenário Principal:

1. Sistema exibe uma lista de relatórios salvos pelo usuário;
2. Usuário escolhe qual relatório baixar;
3. Sistema baixa o relatório escolhido;

Cenário Alternativo:

Não há.

Excluir relatórios

Tabela 25 – Caso de Uso: Excluir relatórios

Descrição	Este caso de uso tem por objetivo excluir relatórios das análises de riscos
Ator	Usuário

Fonte: (próprio autor, 2021)

Cenário Principal:

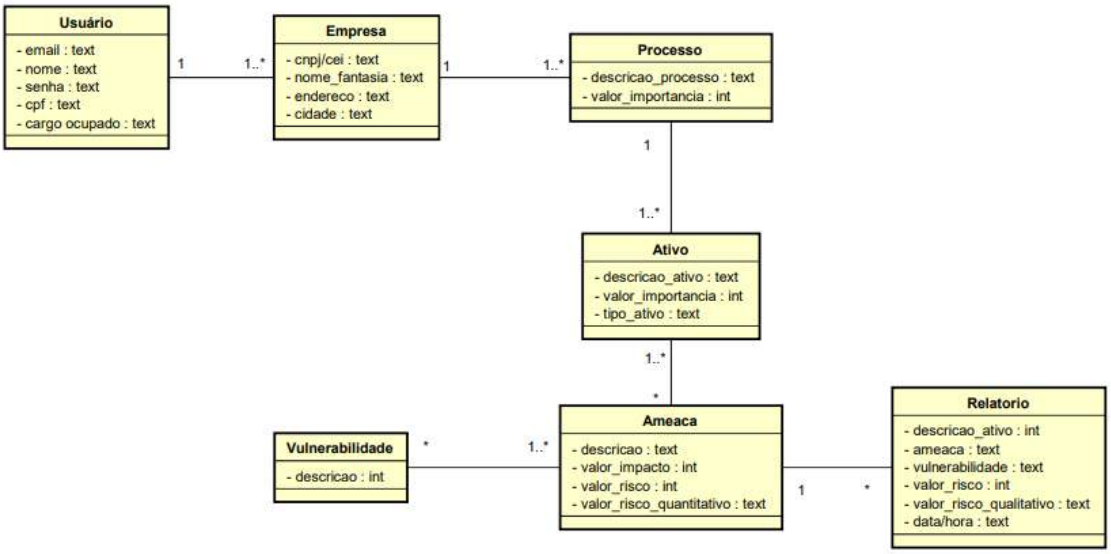
1. Sistema exibe uma lista de relatórios salvos pelo usuário;
2. Usuário escolhe qual relatório deseja excluir;
3. Sistema exclui relatório;

Cenário Alternativo:

Não há.

Após a elaboração dos casos de uso, criou-se o diagrama de classes conceitual, esta é formada por conceitos (classes de abstração) e associações (relacionamentos).

Figura 13 – Diagrama de Classe Conceitual

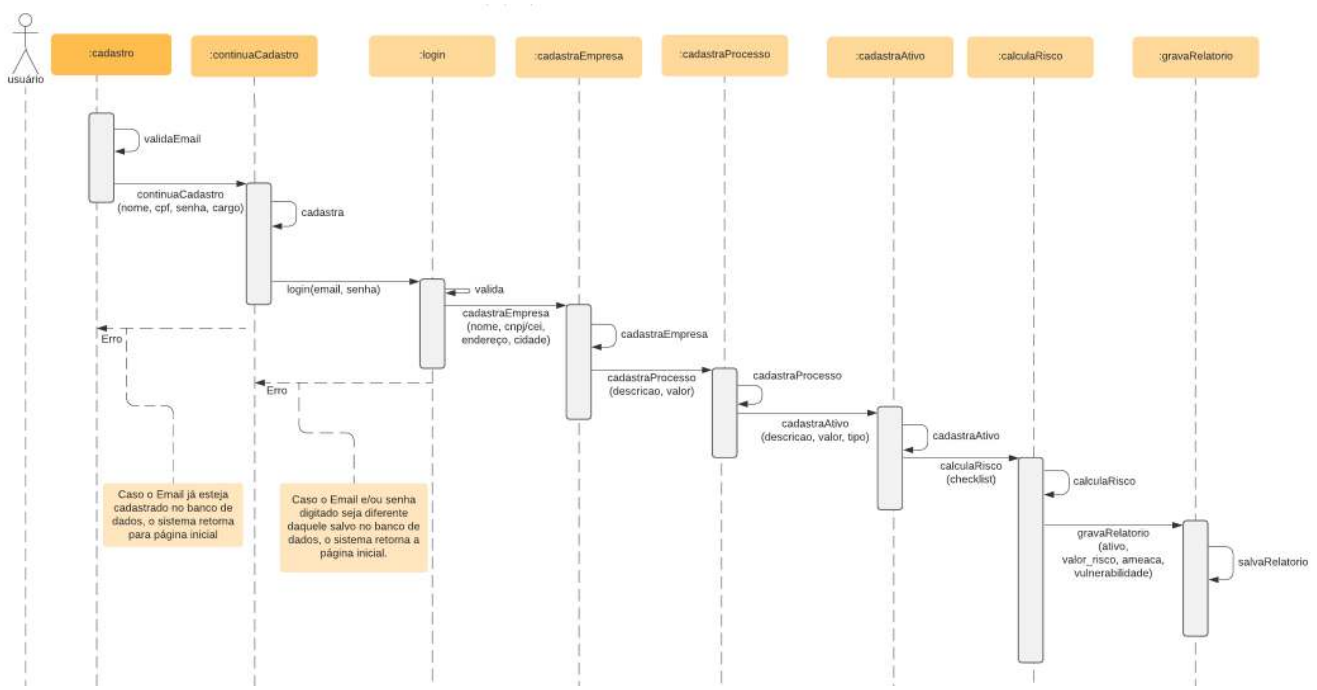


Fonte: próprio autor, 2021.

O diagrama demonstrado na figura 13 foi construído considerando os passos necessários para a realização de análise de risco. Pode-se observar, através das relações, que o usuário deve cadastrar pelo menos 1 empresa, esta deve possuir pelo menos 1 processo, que deve contar com pelo menos 1 ativo, que poderá ser analisado. Após realizar esses passos, um relatório pode ser salvo.

O funcionamento do programa, considerando que o usuário ainda não possui cadastro, pode ser melhor entendido com diagrama de sequências ilustrado na figura 14.

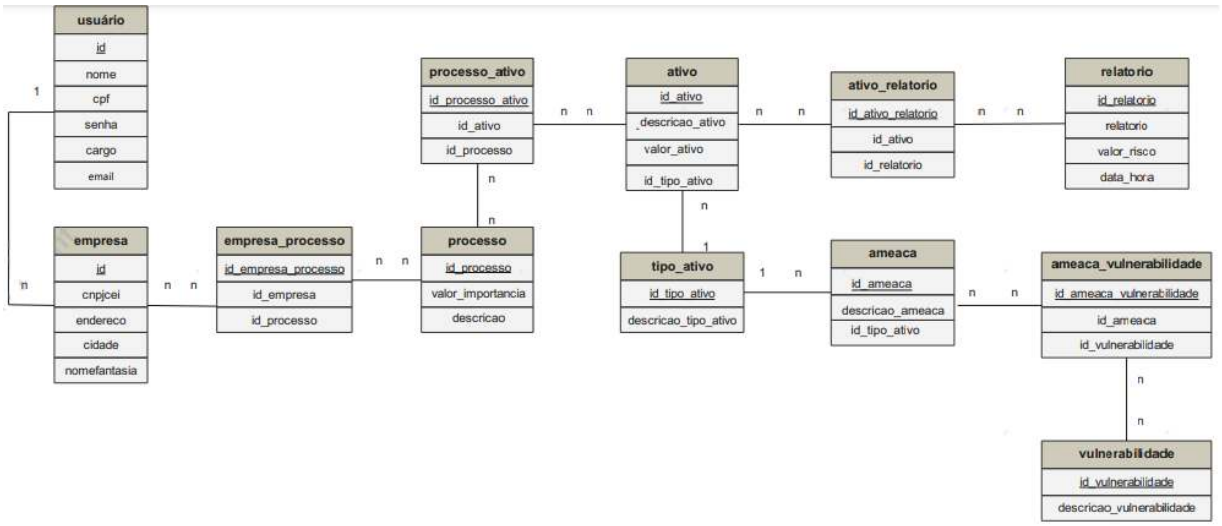
Figura 14 – Diagrama de Sequências



Fonte: próprio autor, 2021.

Inicialmente o usuário deve realizar seu cadastro, após, deve realizar o cadastro da organização. Assim que essa etapa for concluída, o usuário pode começar a realizar a análise de risco (cadastrando processo, ativo e preenchendo o cheklist).
Posteriormente, pela necessidade do uso de Banco de Dados, elaborou-se o diagrama ER (figura 15).

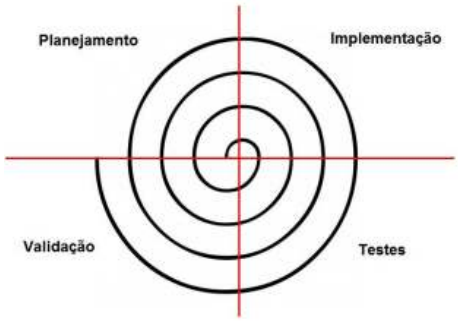
Figura 15 – Diagrama ER



Fonte: próprio autor, 2021.

Ao término da modelagem do sistema, definiu-se a metodologia para a implementação. A escolhida foi a espiral. Cada ciclo desse modelo possui quatro atividades principais: planejamento, implementação, testes e validação, as quais podem ser ciclicamente repetidas, como é mostrado na figura 16.

Figura 16 – Modelo Espiral



Fonte: próprio autor, 2021.

Essa metodologia foi escolhida pelo fato de a ideia ser a de implementar uma funcionalidade por vez, planejando, implementando e testando e ir evoluindo com versões cada vez mais completas, com mais funcionalidades.
Nos próximos subcapítulos serão descritas as ferramentas utilizadas para o desenvolvimento do ARION, bem como serão demostrados alguns códigos de algumas das funcionalidades do software.

4.3 Aparato Tecnológico

A fim de implementar a ferramenta ARION, estudou-se um conjunto de aparato tecnológico (figura 17). A utilização destes visa facilitar a construção do software.

Figura 17 – Aparato Tecnológico Estudado

Fonte: próprio autor, 2021.

Como resultado do estudo: elencou-se como linguagem de implementação do *Back-End* o PHP devido ao conjunto de funcionalidades: suporte à maioria dos servidores web, incluindo o Apache, utilizado neste trabalho; possibilidade de geração de arquivos PDF, importante para a criação de relatórios previstos neste trabalho; suporte a uma ampla variedade de banco de dados; implementação simples de páginas web que fazem consultas no Banco de Dados, interessante funcionalidade, visto que o software deste projeto deve executar várias consultas no Banco de Dados. Além disso, PHP (2021) informa de que se trata de uma linguagem de programação de ampla utilização e que pode ser integrada dentro do código. Como complemento, Bento (2014), explica que essa linguagem possibilita o pré-processamento de páginas HTML (é possível alterar o conteúdo de uma página, antes de enviá-la para o navegador) e permite capturar entradas de dados do usuário. Além do PHP, se necessário será utilizado o JavaScript, pois conforme Mozilla (2021), permite programar o comportamento de uma página web a partir de uma ocorrência de um evento. Tais funcionalidades são importantes para o funcionamento do software proposto.

Em relação ao Banco de Dados, será utilizado o de MySQL (2021), escolhido por ser uma base de dados em código aberto e ser o mais popular do mundo.

Para o *Front-End* optou-se pelo framework Bootstrap por possuir uma grande quantidade de materiais com instruções, de fácil acesso e, como descrito por Bootstrap (2021), ser *open-source*, fácil de manusear, permitir projetar sites responsivos e ser o kit de ferramentas de front-end de código aberto mais popular do mundo.

A IDE (Ambiente de Desenvolvimento Integrado) escolhida foi o Sublime Text.

A fim de descrever a implementação, no próximo subcapítulo serão detalhadas como se deu a programação de algumas funcionalidades.

4.4 Programação do ARION

Foram implementadas as seguintes funcionalidades:

- Cadastro, edição e exclusão de usuário;
- Login de usuário;
- Cadastro, edição e exclusão de empresa;
- Cadastro e exclusão de processo;
- Cadastro de ativos;
- Cálculo do Risco;
- Gravação de Relatório em PDF;
- Demais implementações em html (dicas de segurança, manual de software);

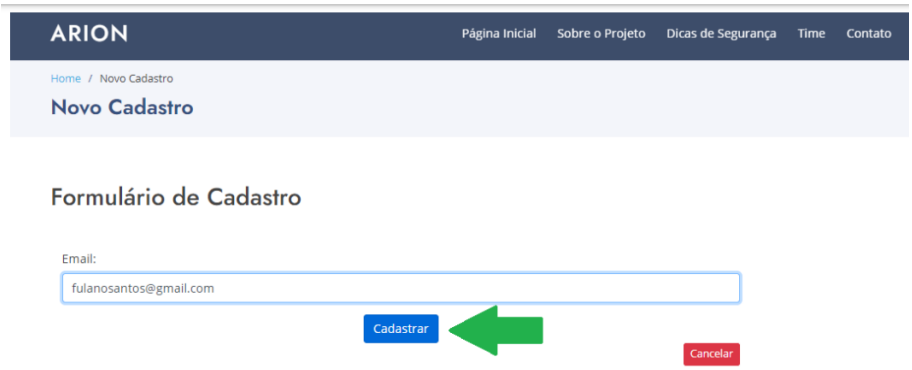
Para cada funcionalidade do programa, foi desenvolvida uma página .html ou .php. Todas as páginas contam com implementações para *front-end*, para esta foi utilizado um template gratuito e construído para o Bootstrap, nominado Arsha, do Bootstrapmade (2021).

Com relação ao *back-end*, alguns dos códigos foram desenvolvidos da seguinte forma:

- Cadastro: Ao usar o programa pela primeira vez, o usuário deverá efetuar seu cadastro.

A página construída (figura 18) é um formulário que recolhe a informação de email digitado e envia para outra página (validaEmail.php), conforme mostrado na figura 19.

Figura 18 – Página de Cadastro de Usuário - Inserção de Email



Fonte: Próprio autor, 2021.

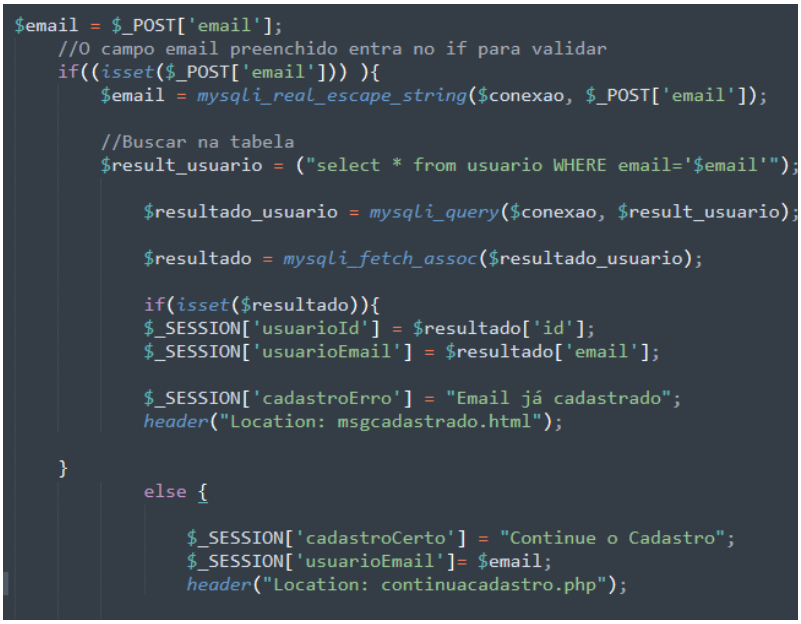
Figura 19 – Código de Cadastro de Usuário

```
<h2>Formulário de Cadastro</h2>
<p>Cadastro de Usuário</p>
  <form action="validaEmail.php" method="post" style="margin-top: 20px">
  <!-- O atributo action define o local (uma URL) em que os dados recolhidos do formulário devem ser
  enviados - então aqui pego o email do usuário e envio para a página validaEmail -->
  <div class="form-group">
    <label class="control-label col-sm-2" for="nome">Email:</label>
    <div class="col-sm-10">
      <input type="email" class="form-control" id="email" placeholder="Enter email" name="email">
      <input type="hidden" id="email" value = email>
    </div>
  </div>

  <div class="form-group">
    <div class="col-sm-offset-2 col-sm-10">
      <div style="text-align: center">
      <button type="submit" id="botao" class="btn btn-primary botao">Cadastrar</button> </div>

      <div style="text-align: right;">
      <a href="index.html" role="button" class="btn btn-sm btn-danger">Cancelar</a></div>
    </div>
```

Fonte: próprio autor, 2021.

O atributo *action* define o local (uma URL) em que os dados recolhidos do formulário (nesse caso, o email) devem ser enviados. A marca <INPUT> com o atributo type="hidden"permite definir dados que são passados a próxima página, neste caso, o email digitado. A página validaEmail.php recebe o email digitado na página anterior e realiza uma consulta no Banco de Dados, conforme mostrado na figura 20.

Figura 20 – Código de validação de email

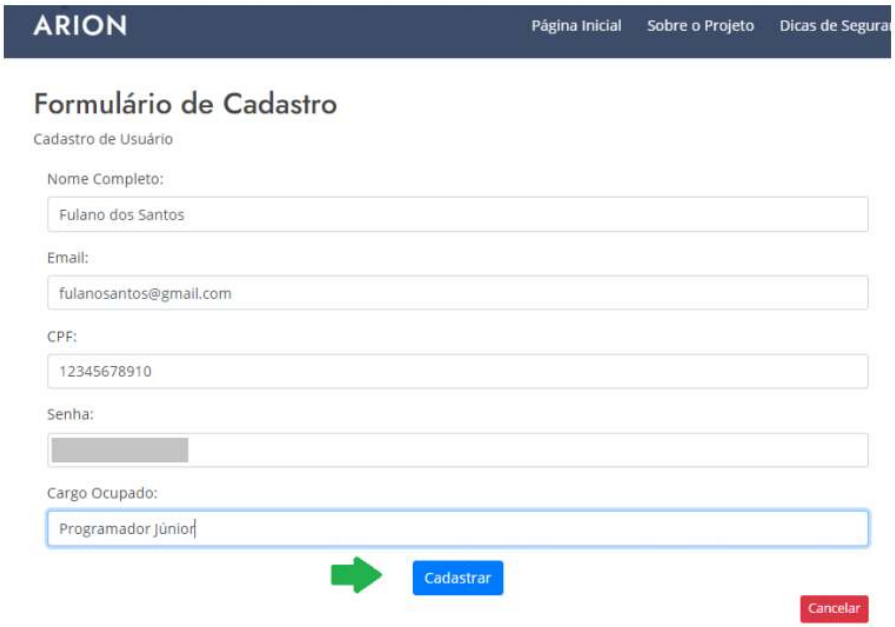


```php
$email = $_POST['email'];
    //O campo email preenchido entra no if para validar
    if((isset($_POST['email'])) ){
        $email = mysqli_real_escape_string($conexao, $_POST['email']);

        //Buscar na tabela
        $result_usuario = ("select * from usuario WHERE email='$email'");

            $resultado_usuario = mysqli_query($conexao, $result_usuario);

            $resultado = mysqli_fetch_assoc($resultado_usuario);

            if(isset($resultado)){
            $_SESSION['usuarioId'] = $resultado['id'];
            $_SESSION['usuarioEmail'] = $resultado['email'];

            $_SESSION['cadastroErro'] = "Email já cadastrado";
            header("Location: msgcadastrado.html");

    }
            else {

                $_SESSION['cadastroCerto'] = "Continue o Cadastro";
                $_SESSION['usuarioEmail']= $email;
                header("Location: continuacadastro.php");
```

Fonte: próprio autor, 2021.

Caso o email digitado seja encontrado no Banco de Dados, então o usuário é redirecionado à msgcadastrado.html, nesta página é mostrada uma mensagem de que aquele email já está cadastrado e orienta o usuário a voltar para página inicial e realizar login ou tentar recuperar senha. Caso o email não seja encontrado no Banco de Dados, o usuário é redirecionado à página continuaCadastro.php (figura 21), nesta, mais informações são requeridas: nome, cpf, senha e cargo ocupado, e salvos no Banco de Dados.

Figura 21 – Página de Cadastro de Usuário - Continuação do cadastro

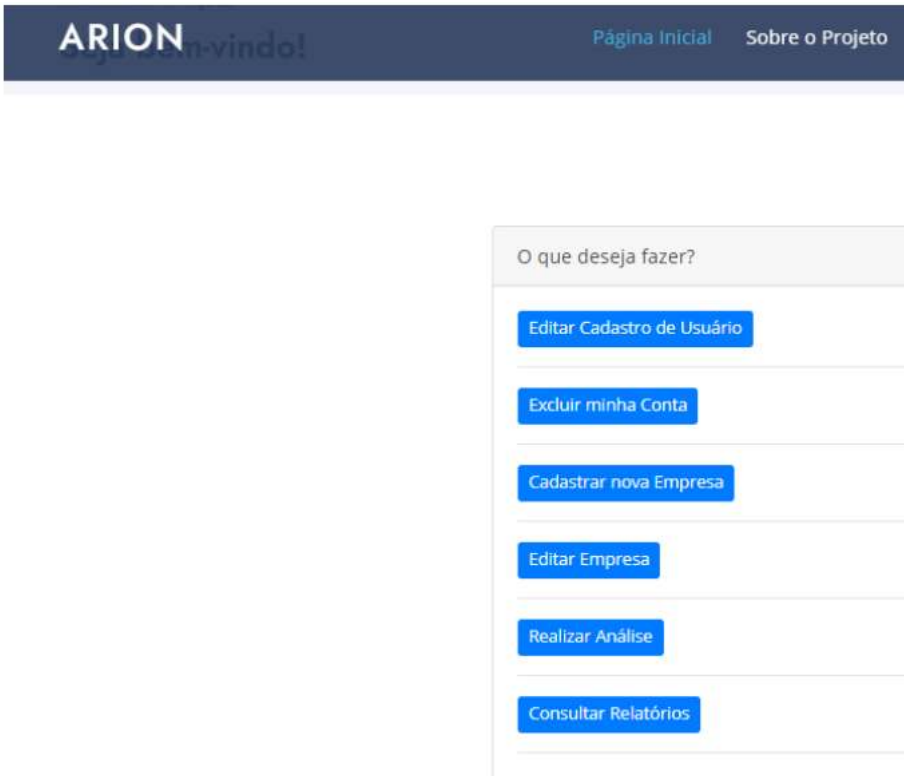


Fonte: Próprio autor, 2021.

Após cadastrado, o usuário pode efetuar login.

- Login: Se trata de um formulário que recebe as informações de email e senha e envia essas informações para outra página: valida.php, nesta as informações são recebidas e é efetuada uma consulta no Banco de Dados que verifica se os dados estão cadastrados. Caso não sejam encontrados as informações de email e senha no Banco de Dados, o usuário é redirecionado à página inicial do projeto (index.html). Caso as informções sejam encontradas, o usuário é redirecionado à página de Menu de Ações (figura 22), a qual se trata de um conjunto de funcionaliadades oferecidas pelo ARION.

Figura 22 – Página de Menu de Ações disponíveis



Fonte: Próprio autor, 2021.

Figura 23 – Código de Menu de Ações

```
<div class="span3">
    <a href="usuario_editar_1.php" role="button" class="btn btn-sm btn-primary">Editar Cadastro de
    Usuário </a> <hr/>
    <a href="confirmaexclusao.php" role="button" class="btn btn-sm btn-primary">Excluir minha Conta
    </a> <hr/>
     <a href="cadastroempresa.php" role="button" class="btn btn-sm btn-primary">Cadastrar nova
     Empresa</a> <hr/>
     <a href="empresa_lista3.php" role="button" class="btn btn-sm btn-primary"> Editar Empresa</a> <
     hr/>
     <a href="empresa_lista2.php" role="button" class="btn btn-sm btn-primary">Realizar Análise</a>
<hr/>
     <a href="mostrarRelatorio.php" role="button" class="btn btn-sm btn-primary">Consultar
     Relatórios</a> <hr/>
```

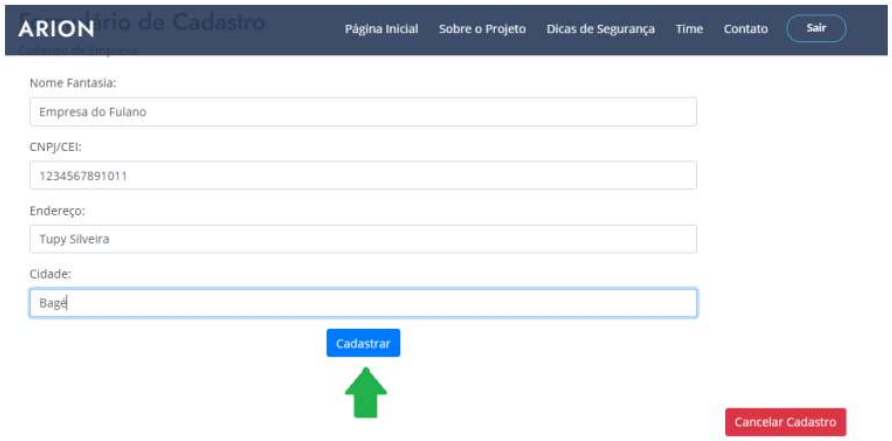
Fonte: próprio autor, 2021.

O usuário, ao clicar em um dos botões, será redirecionado à pagina correspondente ao link.

- Cadastrar Empresa: Assim como o cadastro de usuário (explicado anteriormente), a página de cadastro de empresa (cadastroempresa.php) se trata de um formulário que recebe informações referentes a empresa (CNPJ/CEI, Nome Fantasia, Endereço e Cidade) e envia para a página empresa_insert, esta recebe as informações e cadastra no Banco de Dados. Esta página como visualizada pelo usuário, pode ser vista na

figura 24.

Figura 24 – Página de Cadastro de empresa



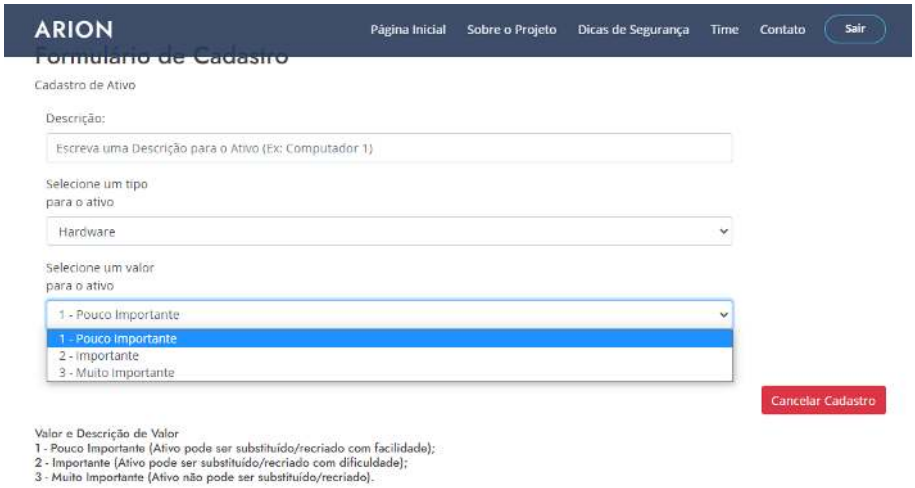
Fonte: Próprio autor, 2021.

- Cadastrar Processo e Cadastrar Ativo: O usuário insere as informações (Descrição e Valor de importância do Processo e Descrição, Valor de importância e Tipo para o Ativo) que são repassadas para outra página, e, esta salva no Banco de Dados. A principal diferença com relação ao cadastro de Empresa é que para cadastro de Processo e Ativo há um campo de "nota de importância"com opções pré-definidas. Nas figuras 25 e 26 é possível visualizar essas opções.

Figura 25 – Página de Cadastro de processo

Fonte: Próprio autor, 2021.

Figura 26 – Página de Cadastro de ativo



Fonte: Próprio autor, 2021.

No código de Cadastro de Ativo (cadastroativo.php), há o campo "Tipo de Ativo"com opções pré-definidas (Hardware, Software, Redes, Recursos Humanos, Local ou Instalações e Organização), estas opções estão definidas no Banco de Dados. Para apresentá-las, primeiramente realiza-se uma consulta no Banco de Dados.

Depois de o usuário ter cadastrado a Empresa, o Processo e o Ativo, pode-se realizar a Análise de Risco. Antes de continuar detalhando a implementação das funcionalidades do ARION, se faz necessário retomar algumas definições, a fim de facilitar o entendimento da implementação do Cálculo de Risco:

- Ameaça - definido pela ISO/IEC (2014) é a causa potencial de um, aquilo que poderá resultar em danos para um sistema ou organização;
- Impacto - a ABNT (2011) informa que está relacionado a medida do sucesso do incidente;
- Vulnerabilidade - pode ser entendida, de acordo com a ISO/IEC (2014) como uma fragilidade de um ativo ou conjunto de ativos que pode vir a ser explorada por uma ou mais ameaças causando um incidente.

Após retomar a definição dos conceitos acima, pode-se continuar a descrição da programação do ARION.

- Cálculo de Risco: a página que calcula o risco é a "ameacas.php". Nesta, conforme mostrado na figura 27, faz-se, uma consulta no Banco de Dados para verificar os valores de Processo e Ativo que serão utilizados no cálculo de Risco.

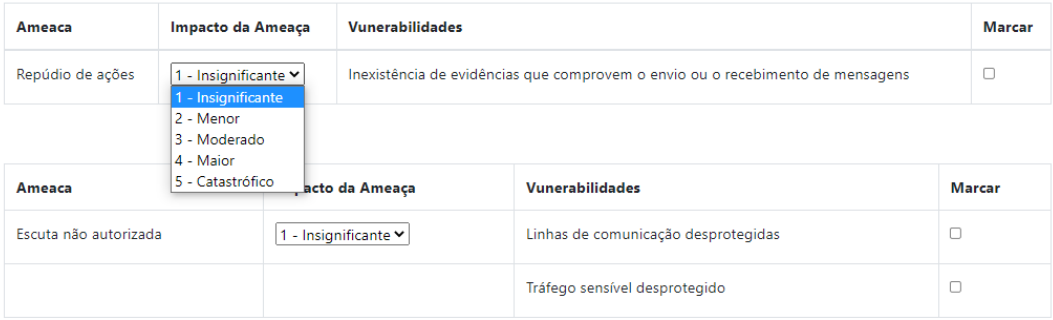
Figura 27 – Código de Análise de Risco - Consulta no Banco para buscar valores de Processo e Ativo

```php
<?php
        session_start();
        include('conexao.php');

        $id_tipo_ativo= $_POST['id_tipo_ativo'] ;
        $id_processo= $_POST['id_processo'] ;
        $id_ativo= $_POST['id_ativo'] ;
        $id= $_POST['id'] ;
        //echo $id_tipo_ativo .' - '. $id_processo . ' - ' . $id_ativo  ;

        //pega valor do processo
        $sql_peso_processo= "select valor_processo from processo where id_processo=$id_processo";
        $busca_valor_processo = mysqli_query($conexao,$sql_peso_processo);
        $result = mysqli_fetch_array($busca_valor_processo);
        $valor_processo = $result[0];

        //pega valor do ativo
        $sql_valor_ativo= "select valor_ativo, descricao_ativo from ativo where id_ativo=$id_ativo";
        $busca_valor_ativo = mysqli_query($conexao,$sql_valor_ativo);
        $result = mysqli_fetch_array($busca_valor_ativo);
        $valor_ativo = $result[0];
        $descricao_ativo = $result[1];
?>
```

Fonte: próprio autor, 2021.

Para criar as tabelas com ameaças, valor de impacto, vulnerabilidades e possibilidade de marcar estas, conforme mostrado na figura 28, foi utilizado a classe table (nativa do Bootstrap).

Figura 28 – Página de Análise de Risco

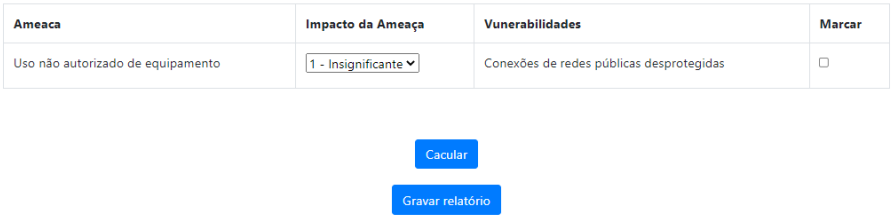


Fonte: próprio autor, 2021.

Para exibir as informações de "Vulnerabilidades", conforme mostrado na figura 28, é realizado uma consulta no Banco de Dados, visto que já estão lá definidas, o resultado desta consulta é exibido na terceira coluna, e para cada vulnerabilidade gera-se uma caixa de checagem, através do elemento "checkbox"que permitirá ao usuário "selecionar"a vulnerabilidade que estiver presente no ativo.

Ao final desta página (ameacas.php), conforme mostrado na figura 29, há as seguintes opções de ações (através de botões) para o usuário: "Calcula Risco", que calcula e exibe o risco do ativo e "Salva Relatório", que guarda um relatório da análise realizada no Banco de Dados.

Figura 29 – Botões mostrados ao final da página ameacas.php



Fonte: próprio autor, 2021.

Quando o usuário clica em "Calcula Risco", é chamado a função calcula(), esta é responsável por fazer o cálculo do risco e mostrar o resultado ao usuário, a implementação pode ser visto nas figuras 30 e 31.

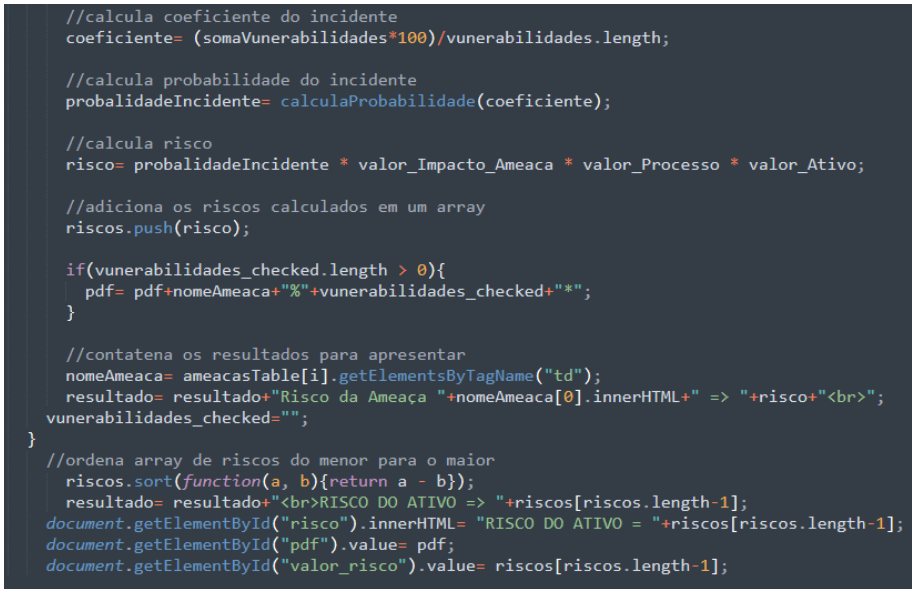
Figura 30 – Código de Análise de Risco - Função calcula()

```
function calcula() {
  //variaveis
    var valor_Processo=<?php print $valor_processo; ?>;
    var valor_Ativo=<?php print $valor_ativo; ?>;
    var riscos=[];
    var resultado="";//usado somente para dar o resultado
    var vunerabilidades_checked="";
    var pdf="";

    console.log( document.getElementById("descricao_ativo").value );

    //Pega todas as tables, pois cada table representa uma ameaca
    var ameacasTable= document.getElementsByTagName("table");
    //percorre as ameacas
    for(let i = 0; i < ameacasTable.length; i++){
      somaVunerabilidades=0;
      //pega o valor do impacto da ameaca
        objSelectImpacto= ameacasTable[i].getElementsByTagName("select");

        valor_Impacto_Ameaca= objSelectImpacto[0].value;

    //nome da ameaca
        nomeAmeaca= (ameacasTable[i].getElementsByTagName("td"))[0].innerHTML;

        //percorre vunerabilidades e soma
        vunerabilidades= ameacasTable[i].getElementsByTagName("input");

        for(let x = 0; x < vunerabilidades.length; x++){
          if(vunerabilidades[x].checked){
              somaVunerabilidades= somaVunerabilidades +1;
              vunerabilidades_checked= vunerabilidades_checked+vunerabilidades[x].value+"%";
           }
        }
```

Fonte: próprio autor, 2021.

A função calcula() foi implementada em JavaScript. De forma geral, a parte do código demonstrada na figura 30 mostra que é feito uma leitura de todas as ameaças e os valores de impactos selecionados pelo usuário e soma-se as vulnerabilidades marcadas, guardando o resultado na variável somaVulnerabilidades. A figura 31 apresenta a implementação das equações para o cálculo do Risco.

Figura 31 – Código de Análise de Risco - Função calcula() - Continuação



```
    //calcula coeficiente do incidente
    coeficiente= (somaVunerabilidades*100)/vunerabilidades.length;

    //calcula probabilidade do incidente
    probalidadeIncidente= calculaProbabilidade(coeficiente);

    //calcula risco
    risco= probalidadeIncidente * valor_Impacto_Ameaca * valor_Processo * valor_Ativo;

    //adiciona os riscos calculados em um array
    riscos.push(risco);

    if(vunerabilidades_checked.length > 0){
      pdf= pdf+nomeAmeaca+"%"+vunerabilidades_checked+"*";
    }

    //contatena os resultados para apresentar
    nomeAmeaca= ameacasTable[i].getElementsByTagName("td");
    resultado= resultado+"Risco da Ameaça "+nomeAmeaca[0].innerHTML+" => "+risco+"<br>";
  vunerabilidades_checked="";
}
  //ordena array de riscos do menor para o maior
    riscos.sort(function(a, b){return a - b});
    resultado= resultado+"<br>RISCO DO ATIVO => "+riscos[riscos.length-1];
  document.getElementById("risco").innerHTML= "RISCO DO ATIVO = "+riscos[riscos.length-1];
  document.getElementById("pdf").value= pdf;
  document.getElementById("valor_risco").value= riscos[riscos.length-1];
```

Fonte: próprio autor, 2021.

Na equação:

$$coeficiente = (somaVunerabilidades \times 100)/vunerabilidades.length; \quad (3)$$

a variável "coeficiente" guarda a porcentagem de quantidade de vulnerabilidades encontradas para uma determinada ameaça. É o resultado armazenado em somaVulnerabilidades multiplicado por 100 e dividido pela quantidade de vulnerabilidades correspondentes à ameaça.

Considerando o exemplo fornecido na tabela 7, supondo que o usuário identifique 2 das 3 vulnerabilidades ali presentes, então: somaVulnerabilidades = 2; coeficiente = 67 (resultado de (2*100)/3), significa que foram identificadas 67% das vulnerabilidades possíveis.

Após, têm-se no código a equação:

$$probalidadeIncidente = calculaProbabilidade(coeficiente); \quad (4)$$

que chama a função calculaProbabilidade passando como parâmetro o resultado obtido anteriormente. Esse cálculo serve para fazer a conversão, descrita na tabela 8. A implementação da função pode ser vista na figura 32.

Figura 32 – Código de Análise de Risco - Função calculaProbabilidade

```
<script>
//recebe um coeficiente de vunerabilidade para uma determinada ameaca
//retorna 0 caso o valor de entrada nao esteja dentro da faixa de 0 a 100
function calculaProbabilidade(coeficiente){
  if(coeficiente >=0 && coeficiente <=20){ return 1}

    if(coeficiente >=21 && coeficiente <=41){ return 2}

    if(coeficiente >=42 && coeficiente <=62){ return 3}

    if(coeficiente >=63 && coeficiente <=84){ return 4}

    if(coeficiente >=85 && coeficiente <=100){ return 5}
```

Fonte: próprio autor, 2021.

Finalmente, no código demonstrado na Figura 31, têm-se a equação:

$$risco = probalidadeIncidente \times valor\_Impacto\_Ameaca \times valor\_Processo \times valor\_Ativo; \quad (5)$$

que calcula o valor de risco.

Após calcular o risco para cada ameaça, ordena-se os resultados em ordem crescente, e mostra-se ao usuário, como risco do ativo, o último (de maior valor).

- Gravar Relatório: Para gerar os relatórios das análises em formato PDF, conforme a figura 33, foi utilizado a biblioteca FPDF.

Figura 33 – Código de Gerar Relatório em PDF

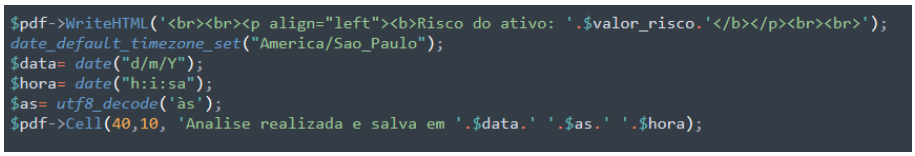
```
$pdf=new PDF_HTML();
$pdf->AddPage();
$pdf->SetFont('Arial');
//nome do ativo
$pdf->WriteHTML('<p align="center"><b>ATIVO: '.$descricao_ativo.'</b></p>');

$ameacas= explode("*",$conteudo);

for ($x = 0; $x < count($ameacas); $x++){
    $ameaca_vunerabilidades= explode("%",$ameacas[$x]);
    for ($y = 0; $y < (count($ameaca_vunerabilidades)-1); $y++){
        if($y==0){
            $pdf->WriteHTML('<br><p align="left"><b>Ameaça: </b>'. $ameaca_vunerabilidades[$y].'</p>');
            $pdf->WriteHTML('<br><p align="left"><b>            Vunerabilidade(s) existente(s): </b></p>');

        }else{
            $pdf->WriteHTML('<br><p align="left">                              -'.$ameaca_vunerabilidades[$y].'
                </p>');

        }
```

Fonte: próprio autor, 2021.

Primeiro, criou-se um objeto FPDF ($pdf = new FPDF();), inseriu-se a página ($pdf->AddPage();), aplicou-se a formatação (tipo de fonte 'Arial') e definiu-se o conteúdo a ser exibido no relatório: as ameaças e vulnerabilidades marcadas como

existentes durante o preenchimento do checklist, o valor de risco do ativo e a data e hora em que o relatório foi salvo. A variável $conteúdo vem no seguinte formato: ameaca1%vulnerabilidade1%vulnerabilidade2*ameaca2%vulnerabilidade1%vulnerabilidade2. No primeiro "explode", usa-se o * para separar o conjunto ameaças-vulnerabilidades. Depois, no outro "explode", usando % separa-se as vulnerabilidades.

Figura 34 – Código de Gerar Relatório - Data e Hora

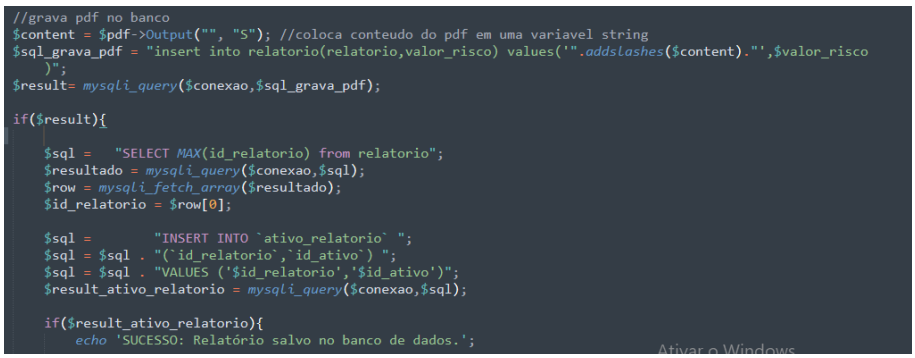


```
$pdf->WriteHTML('<br><br><p align="left"><b>Risco do ativo: '.$valor_risco.'</b></p><br><br>');
date_default_timezone_set("America/Sao_Paulo");
$data= date("d/m/Y");
$hora= date("h:i:sa");
$as= utf8_decode('às');
$pdf->Cell(40,10, 'Analise realizada e salva em '.$data.' '.$as.' '.$hora);
```

Fonte: próprio autor, 2021.

Após, implementou-se o código para salvar o relatório no Banco de Dados (figura 35).

Figura 35 – Código de Gerar Relatório - Salvando Relatório no Banco de Dados



```
//grava pdf no banco
$content = $pdf->Output("", "S"); //coloca conteudo do pdf em uma variavel string
$sql_grava_pdf = "insert into relatorio(relatorio,valor_risco) values('".addslashes($content)."',$valor_risco
    )";
$result= mysqli_query($conexao,$sql_grava_pdf);

if($result){

    $sql =   "SELECT MAX(id_relatorio) from relatorio";
    $resultado = mysqli_query($conexao,$sql);
    $row = mysqli_fetch_array($resultado);
    $id_relatorio = $row[0];

    $sql =        "INSERT INTO `ativo_relatorio` ";
    $sql = $sql . "(`id_relatorio`,`id_ativo`) ";
    $sql = $sql . "VALUES ('$id_relatorio','$id_ativo')";
    $result_ativo_relatorio = mysqli_query($conexao,$sql);

    if($result_ativo_relatorio){
        echo 'SUCESSO: Relatório salvo no banco de dados.';
```

Fonte: próprio autor, 2021.

Primeiro, insere-se o relatório na tabela "relatório". Após, é necessário inserir na tabela "ativo_relatório". Para isto, precisa-se primeiro do *id* do relatório fornecido pelo Banco de Dados, então, faz-se a operação SELECT MAX que ordena os id_relatório e pega o último (o mais atual) para inserir esse id na tabela ativo_relatorio.

- Acessar e Baixar Relatórios: Primeiro criou-se uma página que exibe todos os relatórios do usuário (figura 36).

Figura 36 – Tela que mostra Relatórios aos Usuários

Fonte: próprio autor, 2021.

Na implementação desta página, realizou-se uma consulta no Banco de Dados. O resultado (Nome Fantasia da Empresa, Descrição do Processo, Descrição do Ativo, Tipo de Ativo, Valor de Risco, Data/Hora) foi organizado e colocado nas colunas a serem exibidas ao usuário.

As duas últimas colunas - Relatório e Excluir Relatório - possuem um botão, que se selecionados, vão Baixar o Relatório em PDF ou excluir o relatório respectivamente. Isso é possível porque o *form action* da página é uma outra que executa essas funcionalidades, no caso a baixarRelatorio.php. Esta recebe o id do relatório selecionado tanto para baixar (id_relatorio_baixar) quanto para excluir (id_relatorio_excluir), conforme mostrado na figura 37.

Figura 37 – Código Baixar ou Excluir Relatório

```php
$id_relatorio_baixar= $_POST['id_relatorio_baixar'];
$id_relatorio_excluir= $_POST['id_relatorio_excluir'];

if($id_relatorio_baixar != ""){
  $sql = "select * from relatorio where id_relatorio =".$id_relatorio_baixar;
  $result = mysqli_query($conexao,$sql);
    $rs = mysqli_fetch_assoc($result);
    $content = $rs['relatorio'];

    header('Content-Type: application/pdf');
    header("Content-Length: ".strlen($content));
    header('Content-Disposition: attachment; filename=relatorio.pdf');
    //echo 'PARAMETRO= '.$q;
    print $content;
}

if($id_relatorio_excluir != ""){
  $sql = "DELETE FROM ativo_relatorio WHERE id_relatorio =".$id_relatorio_excluir;
    $result_ativo_relatorio = mysqli_query($conexao,$sql);

    $sql = "DELETE FROM relatorio WHERE id_relatorio =".$id_relatorio_excluir;
    $result_relatorio = mysqli_query($conexao,$sql);

    header("Location: mostrarRelatorio.php");
}
```

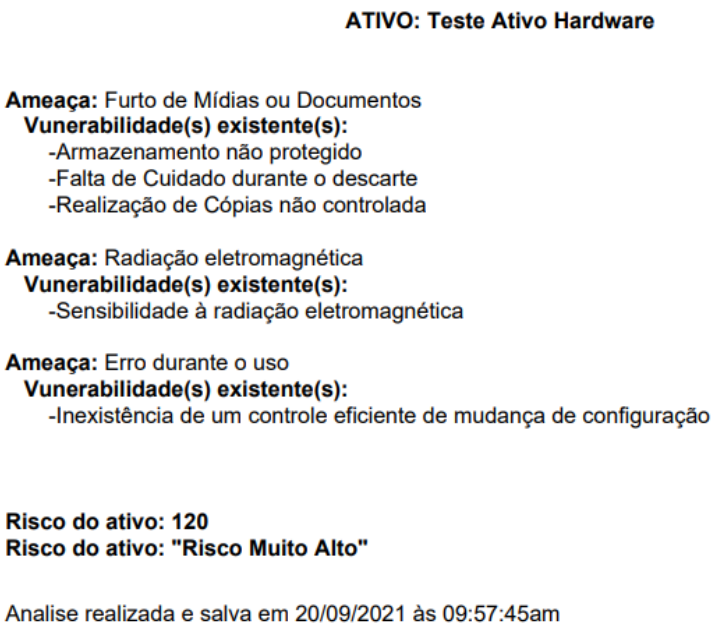
Fonte: próprio autor, 2021.

Caso o usuário clique em Baixar Relatório, então um javascript é chamado e seta a variável id_baixar_relatório com o id do relatório a ser baixado e a variável

id_excluir_relatório fica em branco e vice-versa. A página baixarRelatorio.php verifica quais das operações deve fazer através da variável setada. A figura 37 mostra a implementação das funcionalidades.

Caso a variável setada seja a id_baixar_relatório, faz-se uma consulta no Banco de Dados para encontrar o relatório com o id correspondente ao selecionado pelo usuário para baixar, após, para que seja possível baixar o relatório, guarda-se o conteúdo do relatório na variável $content, diz-se para o browser, através de cabeçalhos que há um conteúdo do tipo PDF, o tamanho do arquivo e o nome e "imprime"esse conteúdo, no caso o browser faz o donwload. A figura 38 exibe um relatório que é baixado pelo usuário.

Figura 38 – Relatório



Fonte: próprio autor, 2021.

Percebe-se que o relatório possui as informações de "Descrição do Ativo"analisado, as Ameaças e Vulnerabilidades correspondentes identificadas (que devem ser preferencialmente extintas), os Valores de Risco (quantitativo e qualitativo) e Data e Hora em que o relatório foi salvo.

Caso a variável setada seja id_excluir_relatório, então executa-se o comando DELETE no relatório com o id correspondente no Banco de Dados. A função header("Location: mostrarRelatorio.php"); força um reload na página, assim atualiza-se e o usuário consegue visualizar a página sem o relatório, que foi excluído.

Foi implementada na página que mostra os Relatórios (mostrarRelatorios.php)

a função sortTable, essa permite ao usuário ordenar a exibição dos resultados na Tela em forma crescente ou decrescente. Sugere-se que o usuário sempre opte por ordenar os riscos em forma decrescente, assim, ele consegue visualizar primeiro (no topo da exibição) o ativo com o maior valor de risco e que necessita, portanto, de medidas mais urgentes para minimizá-lo. Mas, caso queira, o usuário pode ordenar (crescente ou decrescente) pela Empresa, Processo, Ativo, Tipo de Ativo, Data/Hora.

- Excluir Empresa: Na exclusão da empresa, além dos dados da empresa em si (CNPJ/CEI, Nome Fantasia, Endereço e Cidade), também é necessário excluir dados vinculados a esta empresa, tais como os processos, os ativos e os relatórios de análise, para não haver inconsistência no Banco de Dados, ou seja, para não haverem dados relacionados a uma empresa que não existe.

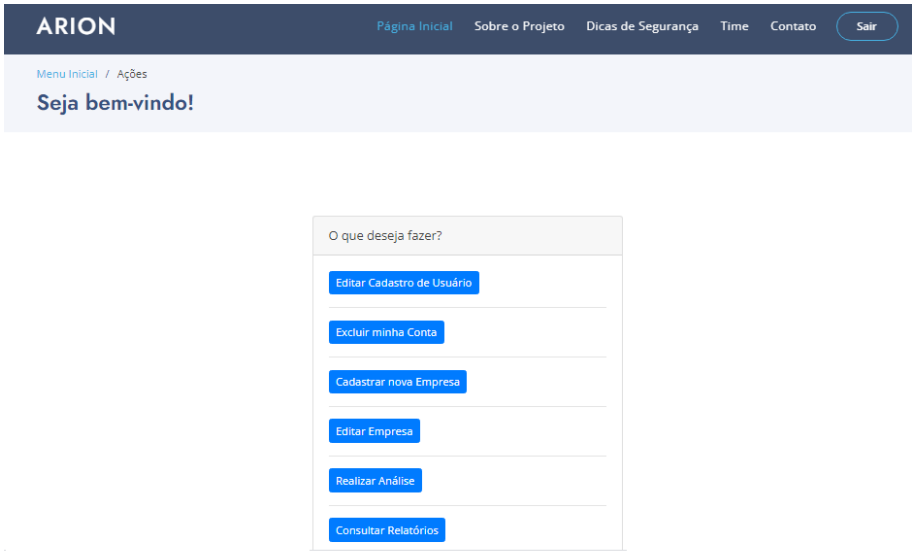
  Para implementar a funcionalidade "Excluir", foi necessário fazer consultas no banco de dados relacionados aos relatórios, aos ativos, aos processos e a empresa em si. Em cada consulta foi utilizado o comando DELETE.

- Editar Empresa: Para editar empresa há um formuário em uma página (empresa_editar.php que recolhe os dados alterados pelo usuário e envia a outra página (empresa_update.php), responsável por atualizar as informações no Banco de Dados.

Considerando que o software desenvolvido deve auxiliar na análise de riscos, e que deve estar online a fim de facilitar o acesso por empresas, nomeou-se a ferramenta como "ARION", esse nome surgiu da abreviação de "Análise de Riscos Online".

As figuras 39 à mostram as telas da ferramenta criada, considerando o seguinte cenário: um usuário, que já realizou seu cadastro e efetuou login, deseja cadastrar uma empresa e realizar uma análise de riscos de um determinado ativo.

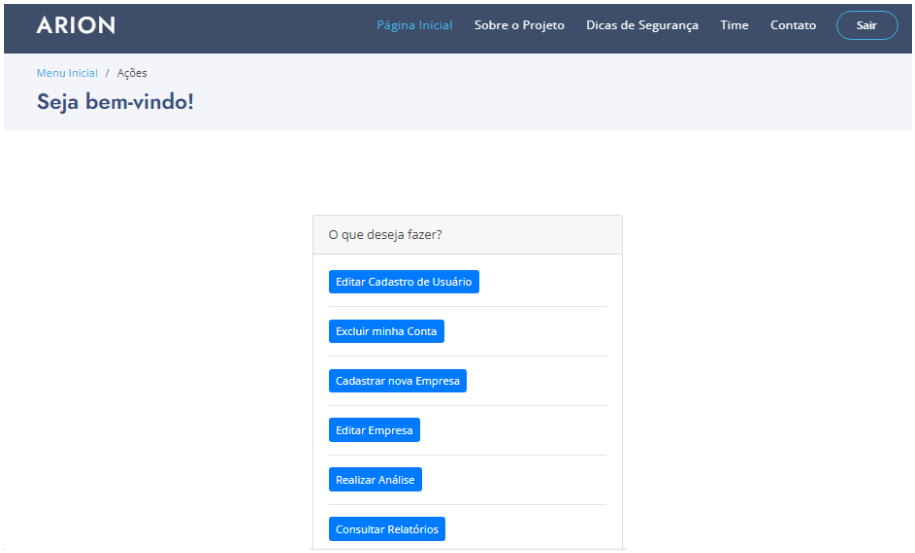
Figura 39 – Tela de menu principal mostrada após o usuário efetuar login



Fonte: próprio autor, 2021

Após efetuar login, aparecerá uma tela com um menu de opções do ARION disponíveis ao usuário, para realizar uma análise, supondo que não haja uma empresa cadastrada, o profissional deve clicar em "Cadastrar nova Empresa" ou em "Realizar Análise"após, conforme mostrado na figura 40 será exibido um formulário a ser preenchido com os dados necessários para o cadastro da empresa.

Figura 40 – Tela de cadastro de empresa

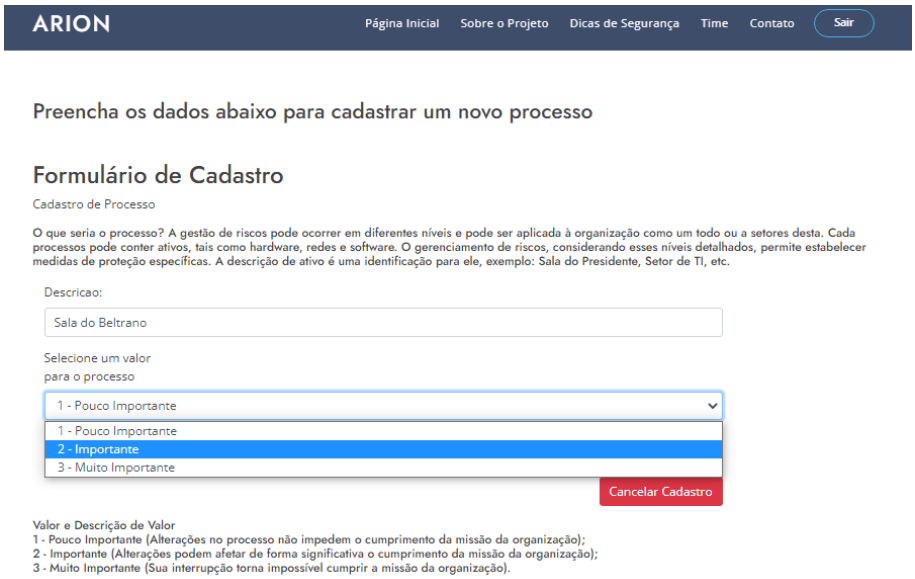


Fonte: próprio autor, 2021

Após, o usuário deverá cadastrar um processo referente à empresa, conforme

mostrado na figura 41, será exibido um formulário a ser preenchido com os dados necessários para o cadastro.

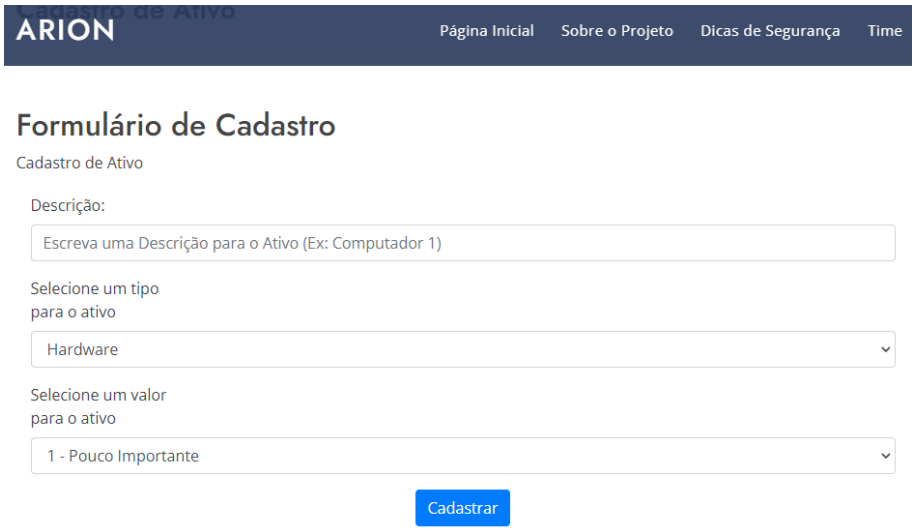
Figura 41 – Tela de cadastro de processo



Fonte: próprio autor, 2021

Após, o usuário deverá cadastrar um ativo referente ao processo, conforme mostrado na figura 42, será exibido um formulário a ser preenchido com os dados necessários para o cadastro.

Figura 42 – Tela de cadastro de ativo

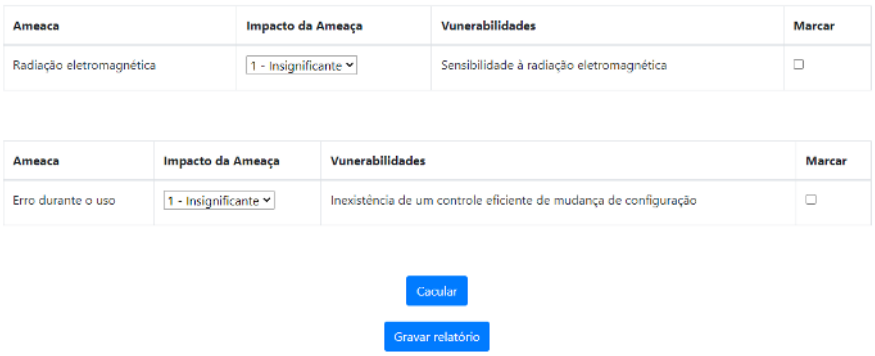


Fonte: próprio autor, 2021

Após, o usuário poderá realizar a análise de risco do ativo cadastrado. Para isto,

deverá preencher o check-list (figura 43), identificando as vulnerabilidades e definindo um valor de impacto para a ameaça.

Figura 43 – Tela de realização de análise de risco



Fonte: próprio autor, 2021

Na página demonstrada na figura 43, o usuário poderá calcular o risco, clicando em "Calcular", esta opção não salva os valores obtidos no Banco de Dados. Ao clicar em "Gravar relatório", os valores de riscos poderão ser acessados no relatório, posteriormente.

Os códigos implementados nesse projeto estão disponíveis em: "https://github.com/marianapompeo/ARION_2021".

Na próxima seção serão apresentados os testes realizados durante a implementação do Sistema, visando validar as funcionalidades oferecidas pelo mesmo.

4.5 Testes de Software do ARION

Pressman (2011) explica que testes são importantes por se tratar de um processo pelo qual se experimenta o software, a fim de encontrar e corrigir erros. Durante a implementação desse projeto, foram elaboradaos e realizados casos de testes para verificar se as funcionalidades estavam se comportando de forma esperada. Será abordado sobre esses testes e os resultados obtidos a seguir.

4.5.1 Casos de Testes

Para cada um dos Casos de Teste foram determinados objetivo, os passos necessários para atingir o objetivo proposto e os critérios de êxito, esses estão descritos detalhadamente nas tabelas 26 à 37.

Tabela 26 – Casos de Teste - Cadastrar Usuário

Caso Nº	CT001 - Cadastrar Usuário
Objetivo do Teste	Verificar se o usuário consegue se cadastrar no sistema.
Passos	1. Usuário acessa a página; 2. Usuário escolhe a opção Novo Cadastro; 3. Sistema mostra as informações necessárias; 4. Usuário insere as informações.
Critêrios de Êxito	O usuário deve conseguir se cadastrar. As informações devem ser cadastradas no Banco de Dados. Caso o usuário já esteja cadastrado, uma mensagem de erro deve ser retornada. A verificação é feita através do e-mail.

Fonte: (próprio autor, 2021)

Tabela 27 – Casos de Teste - Cadastrar Empresa

Caso Nº	CT002 - Cadastrar Empresa
Objetivo do Teste	Verificar se o usuário consegue cadastrar a empresa.
Passos	1. Usuário acessa a página; 2. Usuário loga; 3. Usuário escolhe a opção Cadastrar nova Empresa; 4. Sistema mostra as informações necessárias; 5. Usuário insere as informações;
Critêrios de Êxito	O usuário deve conseguir cadastrar a empresa. Os dados devem ser salvos no Banco de Dados.

Fonte: (próprio autor, 2021)

Tabela 28 – Casos de Teste - Cadastrar Processo

Caso Nº	CT003 - Cadastrar Processo
Objetivo do Teste	Verificar se o usuário consegue cadastrar processo.
Passos	1. Usuário acessa a página; 2. Usuário loga; 3. Usuário escolher a opção Realizar Análise; 4. Usuário seleciona a empresa; 5. Usuário escolhe cadastrar o processo; 6. Sistema mostra as informações necessárias; 7. Usuário insere as informações;
Critêrios de Êxito	O usuário deve conseguir cadastrar o processo. Os dados devem ser salvos no Banco de Dados.

Fonte: (próprio autor, 2021)

Tabela 29 – Casos de Teste - Cadastrar Ativo

Caso Nº	CT004 - Cadastrar Ativo
Objetivo do Teste	Verificar se o usuário consegue cadastrar ativo.
Passos	1. Usuário acessa a página; 2. Usuário loga; 3. Usuário seleciona a empresa; 4. Usuário seleciona o processo; 5. Usuário seleciona Cadastrar Ativo; 6. Sistema mostra as informações necessárias; 7. Usuário insere as informações;
Critêrios de Êxito	O usuário deve conseguir cadastrar o ativo. Os dados devem ser salvos no Banco de Dados.

Fonte: (próprio autor, 2021)

Tabela 30 – Casos de Teste - Editar Cadastro de Usuário

Caso Nº	CT005 - Editar Cadastro de Usuário
Objetivo do Teste	Verificar se o usuário consegue editar suas informações de cadastro.
Passos	1. Usuário acessa a página; 2. Usuário loga; 3. Usuário escolhe a opção Editar Cadastro de Usuário; 4. Sistema mostra as informações cadastradas; 5. Usuário altera as informações que deseja.
Critêrios de Êxito	O usuário deve conseguir alterar as informações desejadas. As informações devem ser atualizadas no Banco de Dados.

Fonte: (próprio autor, 2021)

Tabela 31 – Casos de Teste - Editar Cadastro de Empresa

Caso Nº	CT006 - Editar Cadastro de Empresa
Objetivo do Teste	Verificar se o usuário consegue editar as informações de cadastro de Empresa.
Passos	1. Usuário acessa a página; 2. Usuário loga; 3. Usuário escolhe a opção Editar Empresa; 4. Sistema mostra as empresas cadastradas; 5. Usuário seleciona a empresa que deseja editar; 6. Sistema mostra as informações cadastradas da empresa; 7. Usuário altera as informações que deseja.
Critêrios de Êxito	O usuário deve conseguir alterar as informações desejadas.As informações devem ser atualizadas no Banco de Dados.

Fonte: (próprio autor, 2021)

Tabela 32 – Casos de Teste - Excluir Processo

Caso Nº	CT007 - Excluir Processo
Objetivo do Teste	Verificar se o usuário consegue excluir todas as informações de determinado Processo.
Passos	1. Usuário acessa a página; 2. Usuário loga; 3. Usuário escolhe a opção Editar Empresa; 4. Sistema mostra as empresas cadastradas; 5. Usuário seleciona a empresa; 6. Sistema mostra os processos cadastrados; 7. Usuário escolhe e exclui o processo.
Critêrios de Êxito	O usuário deve conseguir excluir todos os dados referentes ao processo selecionado. As informações devem ser deletadas no Banco de Dados.

Fonte: (próprio autor, 2021)

Tabela 33 – Casos de Teste - Excluir Empresa

Caso Nº	CT008 - Excluir Empresa
Objetivo do Teste	Verificar se o usuário consegue excluir todas as informações de determinada Empresa.
Passos	1. Usuário acessa a página; 2. Usuário loga; 3. Usuário escolhe a opção Editar Empresa; 4. Sistema mostra as empresas cadastradas; 5. Usuário seleciona e exclui a empresa desejada;
Critêrios de Êxito	O usuário deve conseguir excluir todos os dados referentes à empresa selecionada. As informações devem ser deletadas no Banco de Dados.

Fonte: (próprio autor, 2021)

Tabela 34 – Casos de Teste - Logar no Sistema

Caso Nº	CT009 - Logar no Sistema
Objetivo do Teste	Verificar se o usuário consegue logar no sistema utilizando o e-mail se senha cadastrados.
Passos	1. Usuário acessa a página; 2. Usuário escolhe a opção Login; 3. Sistema mostra as informações necessárias; 4. Usuário insere as informações corretas.
Critêrios de Êxito	O usuário deve conseguir logar no sistema, se inserir e-mail e senha corretos. Caso insira e-mail e/ou senha incorretos, não deve conseguir logar e sistema deve redirecionar à página inicial

Fonte: (próprio autor, 2021)

Tabela 35 – Casos de Teste - Acessar e Baixar Relatórios

Caso Nº	CT010 - Acessar e Baixar Relatórios
Objetivo do Teste	Verificar se o usuário consegue acessar e baixar relatórios.
Passos	1. Usuário acessa a página; 2. Usuário loga; 3. Usuário escolhe a opção Consultar Relatórios; 4. Sistema mostra os relatórios disponíveis; 5. Usuário escolhe um relatório para baixar e clica em Baixar Relatório; 6. Sistema efetua download do relatório selecionado.
Critêrios de Êxito	O usuário deve acessar e baixar os relatórios que deseja em formato PDF. Os Relatórios devem abrir de forma correta.

Fonte: (próprio autor, 2021)

Tabela 36 – Casos de Teste - Realizar Análise de Risco e Salvar Relatório

Caso Nº	CT011 - Realizar Análise de Risco e Salvar Relatório.
Objetivo do Teste	Verificar se o usuário consegue obter o valor de risco para determinado ativo e deve conseguir salvar Relatório da Análise.
Passos	1. Usuário acessa a página; 2. Usuário loga; 3. Usuário escolhe a opção Realizar Análise de Risco; 4. Sistema mostra as empresas cadastradas; 5. Usuário escolhe uma empresa; 6. Sistema mostra os processos cadastrados; 7. Usuário escolhe um processo; 8. Sistema mostra os ativos cadastrados; 9. Usuário escolhe o ativo; 10. Sistema exibe o check-list; 11. Usuário preenche o check-list e clica em Calcular; 12. Sistema mostra o valor de risco para o ativo; 13. Usuário escolhe Salvar Relatório.
Critêrios de Êxito	O usuário deve conseguir visualizar o valor de risco para determinado ativo e deve conseguir salvar relatório. As informações de relatório devem ser salvas no Banco de Dados.

Fonte: (próprio autor, 2021)

Tabela 37 – Casos de Teste - Excluir Relatório

Caso Nº	CT012 - Excluir Relatório
Objetivo do Teste	Verificar se o usuário consegue excluir relatório.
Passos	1.Usuário acessa a página; 2. Usuário loga; 3. Usuário escolhe a opção Consultar Relatórios; 4. Sistema mostra os relatórios disponíveis; 5. Usuário escolhe um relatório para excluir e clica em Excluir Relatório; 6. Sistema exclui relatório.
Critêrios de Êxito	O usuário deve conseguir excluir todos os dados referentes ao relatório selecionado.As informações devem ser deletadas no Banco de Dados.

Fonte: (próprio autor, 2021)

Todos os critérios de êxitos de cada caso de teste detalhados nas tabelas 26 à 37. foram atingidos.

Após, disponibilizou-se o ARION em um servidor do Grupo de Pesquisa de Segurança da Informação da Universidade Federal do Pampa, com o endereço: https://arion.gsi.seg.br/ e iniciou-se a fase de Experimentação do Software, descrito na próxima subseção.

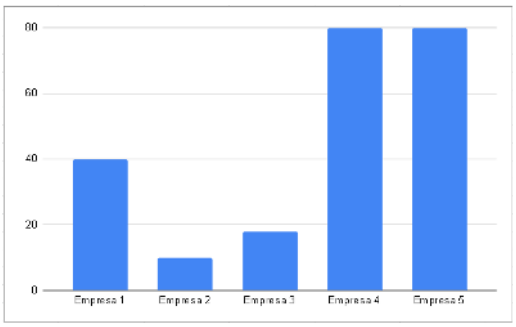
4.5.2 Experimentação do Software

Esta etapa de experimentação do software foi dividida em duas fases distintas, detalhadas a seguir.

Fase 1 - Utilizando respostas fornecidas na validação do modelo

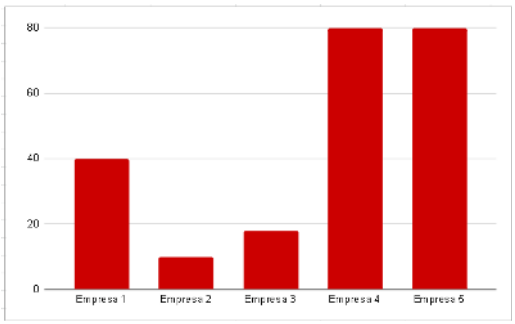
Na subseção 4.1.2 deste trabalho, explicou-se que, para a validação do modelo, profissionais de diversas empresas com diferentes ramos de atuação responderam a questionários e, que foi realizada uma análise de risco considerando as respostas fornecidas. A fim de verificar se o ARION retornaria os mesmos valores de risco que aqueles obtidos na fase de validação do modelo, criou-se no sistema - usuários e empresas fictícios - e aplicou-se os valores de importância de processo, ativo e impacto da ameaça, bem como selecionou-se as vulnerabilidades identificadas nos questionários. Os valores de riscos para os ativos Hardware, Software e Redes para as 5 empresas foram exatamente iguais aos obtidos na validação. Tal fato pode ser verificado nas figuras 44 à 49, que trazem o resultado obtidos na Validação do modelo e do ARION.

Figura 44 – Valores de Risco par o Ativo Hardware - Validação



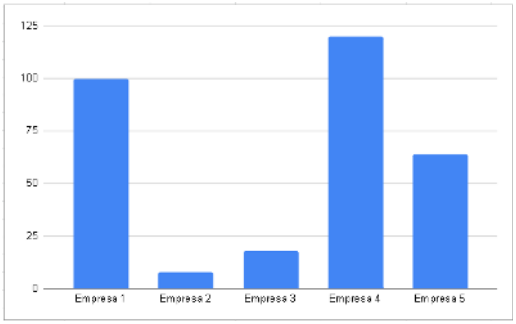
Fonte: próprio autor, 2021)

Figura 45 – Valores de Risco para o Ativo Hardware - ARION



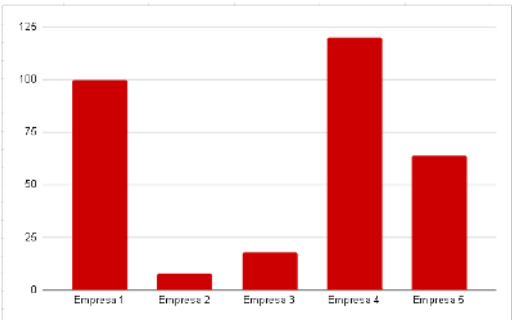
Fonte: próprio autor, 2021)

Figura 46 – Valores de Risco par o Ativo Software - Validação



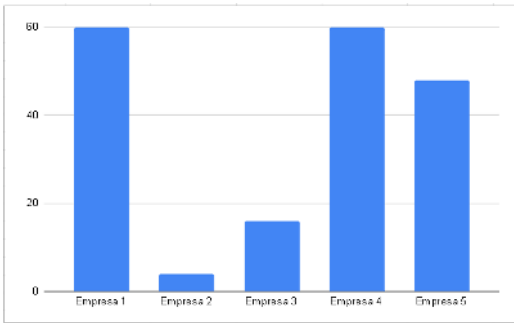
Fonte: próprio autor, 2021)

Figura 47 – Valores de Risco para o Ativo Software - ARION



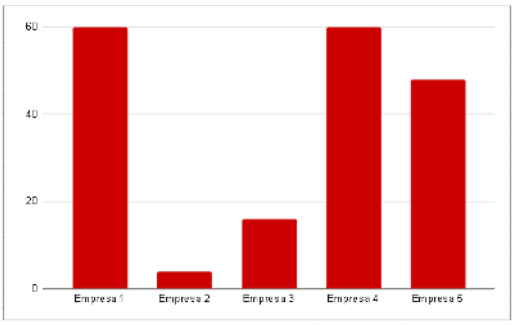
Fonte: próprio autor, 2021)

Figura 48 – Valores de Risco para o Ativo Redes - Validação



Fonte: próprio autor, 2021)

Figura 49 – Valores de Risco para o Ativo Redes - ARION



Fonte: próprio autor, 2021)

Desta forma, pode-se afirmar que o ARION corresponde ao modelo criado e validado anteriormente.

A partir disso, planejou-se uma nova rodada de testes – a Fase 2.

Fase 2:

Nesta fase, foi enviado o endereço do ARION à algumas empresas e outros possíveis interessados na área de segurança da informação.
Foi solicitado que executassem as seguintes atividades:

- Todos os passos necessários até a realização de Análise de Risco;
- Acessassem os Relatórios;
- Respondessem a um Questionário;

Foram contatadas entre 10 à 20 empresas. Dessas, 6 realizaram a análise de risco e salvaram o relatório. Cada uma cadastrou um processo e um ativo correspondente. Os ativos cadastrados e analisados por essas empresas são de diferentes tipos.

Os resultados de análise de riscos obtidos por essas empresas podem ser visualizadas na tabela 38.

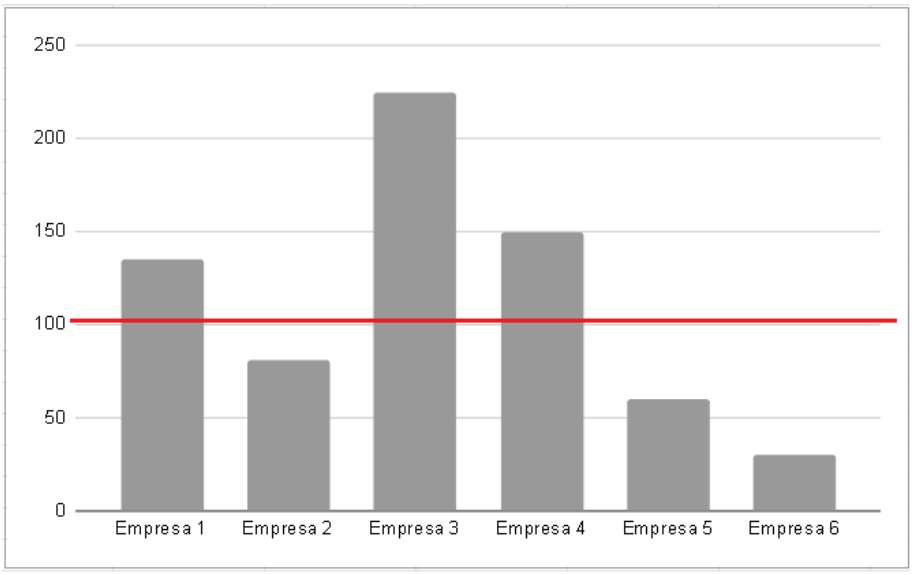
Tabela 38 – Resultado de Risco obtido pelas empresas

Empresa	**Valor de Risco**
1	135
2	81
3	225
4	150
5	60
6	30

Fonte: (próprio autor, 2021)

A figura 50 permite visualizar os resultados graficamente. A linha vermelha indica o início de valores correspondentes à "Risco Muito Alto".

Figura 50 – Resultado de Risco obtido pelas empresas



Fonte: próprio autor, 2021.

Observando os valores de risco, na tabela 38 e na figura 50, verifica-se que 50% das empresas obtiveram valores correspondentes a "Risco Muito Alto"(Acima de 100). Uma maneira de começar a diminuir esse risco é o profissional acessar o ARION e baixar o relatório, que constarão todas as vulnerabilidades presentes na empresa e que devem, preferencialmente, serem extintas.

A última atividade solicitada às organizações que testaram o ARION - responder o questionário - tinha como objetivo desse obter um *feedback* sobre o programa.

Foram elaboradas questões que abordavam a usabilidade de software, baseadas em Pressman (2011) que afirma que estes, voltados para WebApp, avaliam o grau com o qual os usuários podem interagir efetivamente com o software e determina o grau com o qual a interface da WebApp facilita a vida do usuário. Além dessas, foram elaboradas questões para traçar o perfil dos usuários. As perguntas estão descritas na tabela 39:

Tabela 39 – Perguntas do Questionário

1. Interatividade — Os mecanismos de interação (por exemplo, menus e botões) são fáceis de entender e usar?
2. Layout — Os mecanismos de navegação e conteúdo são colocados de maneira que permita ao usuário encontrá-los rapidamente?
3. Clareza — O texto do ARION é bem escrito e fácil de ser entendido?
4. Estética — O layout, a cor, o tipo de letra e características relacionadas facilitam o uso? Você se sentiu "confortável" com a aparência e comportamento do ARION?
5. Características da tela — O ARION otimiza o uso do tamanho da tela e da resolução?
6. Sensibilidade ao tempo — Características importantes, funções e conteúdo podem ser usados ou acessados no tempo correto?
7. A empresa/organização em que você atua é:
8. Qual a sua Escolaridade?
9. Você possui alguma formação ou cursos específicos na área de TI?
10. Antes de usar o software pela primeira vez: você acessou e leu o manual?
11. O manual ajudou de forma efetiva a entender como utilizar todas as funcionalidades do programa?
12. Você achou que a resposta (nível de risco) fornecido pelo ARION corresponde a realidade da empresa?
13. Você indicaria o uso do ARION para outras empresas?
14. O ARION atendeu às suas expectativas (considerando a proposta de ser um software voltado para análise de risco)?
15. Quais foram suas maiores dificuldades no uso do ARION?
16. Caso possua sugestões de como melhorar o software, escreva, por favor!

Fonte: (próprio autor, 2021)

A seguir serão mostradas e discutidas as respostas obtidas. Observa-se que 8 empresas responderam ao questionário. Anteriormente foi dito que 6 empresas realizaram a análise de risco. A diferença pode ser explicada pelo fato de que para calcular o risco não era obrigatório salvar o relatório, passo necessário para salvar os resultados no Banco

de Dados, o que permitiria posterior visualização dos resultados. Provavelmente duas, das oito empresas apenas clicaram em "Calcular o Risco".

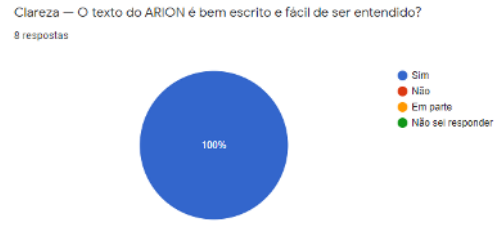
Figura 51 – Respostas obtidas para a questão 1

Fonte: próprio autor, 2021)

Figura 52 – Respostas obtidas para a questão 2

Fonte: próprio autor, 2021)

Figura 53 – Respostas obtidas para a questão 3

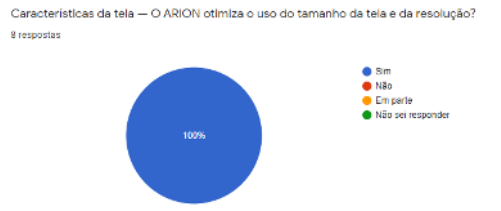


Fonte: próprio autor, 2021)

Figura 54 – Respostas obtidas para a questão 4

Fonte: próprio autor, 2021)

Figura 55 – Respostas obtidas para a questão 5



Fonte: próprio autor, 2021)

Figura 56 – Respostas obtidas para a questão 6

Fonte: próprio autor, 2021)

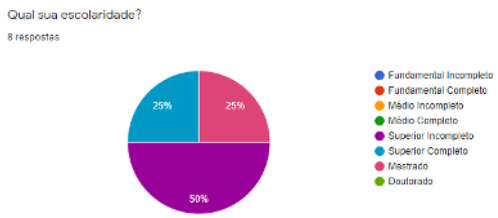
As questões 1 à 6 foram baseadas em Pressman (2011). As respostas favoráveis permitem considerar que o ARION foi aprovado no quesito usabilidade. Ou seja, possui características que facilitam o uso do software pelo usuário.

Figura 57 – Respostas obtidas para a questão 7

(Fonte: Próprio autor, 2021)

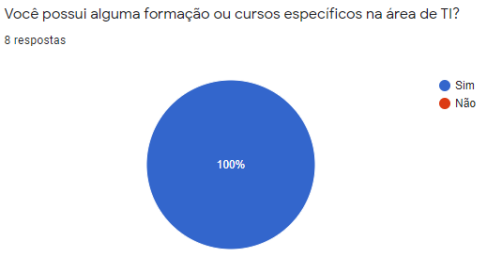
Percebeu-se que usuários de todos os tipos de empresas testaram o software, o que torna as respostas fornecidas ainda mais relevantes para o projeto, visto que a ideia era que o ARION pudesse ser usado por qualquer tipo de organização.

Figura 58 – Respostas obtidas para a questão 8



Fonte: próprio autor, 2021)

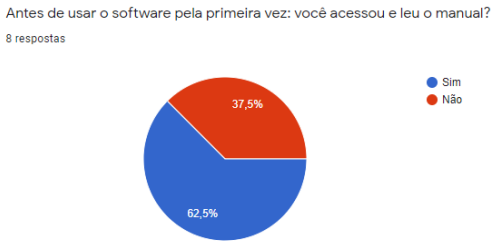
Figura 59 – Respostas obtidas para a questão 9



Fonte: próprio autor, 2021)

Considerando que o projeto deste trabalho deve resultar em um software e, que todos os usuários afirmaram possuir conhecimento na área de Tecnologia da Informação (TI): as respostas deste questionário, principalmente referentes às melhorias que possam ser feitas, se tornam mais relevantes.

Figura 60 – Respostas obtidas para a questão 10



Fonte: próprio autor, 2021)

Figura 61 – Respostas obtidas para a questão 11

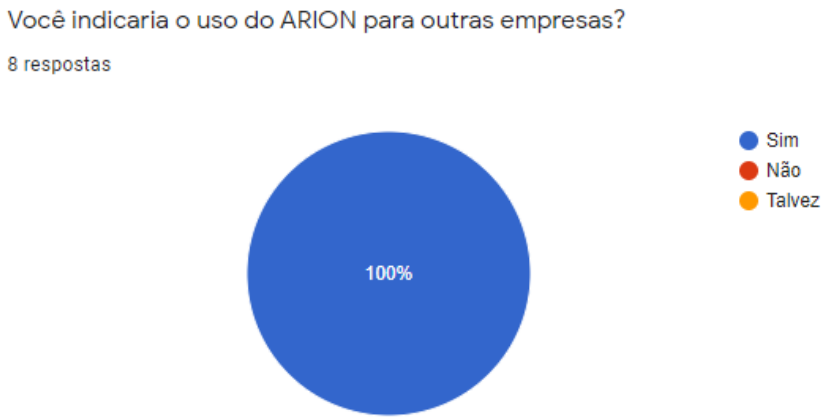
Fonte: próprio autor, 2021)

Observando as respostas obtidas, em que a maioria afirmou ter lido o manual e que este auxiliou a utilizar as funcionalidades do ARION, poderia ser sugerido que os usuários só conseguiram utilizar a ferramenta através do manual. No entanto, as respostas obtidas nas questões 1 à 6 que abordam a usabilidade respalda a possibilidade de que mesmo que não houvesse um manual disponível, o ARION poderia ser facilmente utilizado.

Figura 62 – Respostas obtidas para a questão 12

(Fonte: Próprio autor, 2021)

Figura 63 – Respostas obtidas para a questão 13



(Fonte: Próprio autor, 2021)

Figura 64 – Respostas obtidas para a questão 14

(Fonte: Próprio autor, 2021)

Sabendo-se que todos os usuários que responderam ao questionário possuem algum nível de conhecimento na área de TI, e que estes (100%) afirmaram concordar com o risco fornecido pelo ARION, pode-se pressupor que a ferramenta desenvolvida retorna valores condizentes com a realidade.

O resultado obtido com a questão 13, em que TODOS (100%) afirmaram que indicariam o uso do ARION para outras empresas corrobora com o que foi pressuposto anteriormente.

As questões 15 e 16 eram dissertativas e não obrigatórias. Objetivavam permitir ao usuário escrever sobre suas dificuldades e opiniar sobre possíveis melhorias.

A questão 15 abordava sobre as dificuldades encontradas ao utilizar o ARION. Ao

analisar as respostas, percebeu-se que:

- 80% afirmaram não terem tido dificuldades;
- 20% alegaram ter dificuldades em entender o que é um ativo e o que é um processo.

Diante desse cenário, procurou-se fazer algumas melhorias no software a fim de minimizar as dificuldades citadas. Na página de cadastro de processo foi inserido um breve texto explicando sobre o que é um processo. Na página de cadastro de ativo foi inserido um exemplo de ativo para tornar mais fácil o entendimento do que seria um ativo. Ressalta-se no entanto, que há explicações bem detalhadas de processos, ativos e tipos de ativos no manual.

A questão 16 foi elaborada para permitir o recebimento de sugestões dos usuários. Foram recebidas algumas em relação ao design de algumas telas e botões, sobre especificar mais as questões do *checklist* e possibilidade de visualizar um histórico de evolução ou involução do risco. Algumas sugestões, por questão de tempo ficaram como trabalhos futuros, outras foram atendidas, sendo criada uma versão 2 do ARION.

Na seção 4.2 nominada "Modelagem do ARION" definiu-se como metodologia de implementação a Espiral, que possui as atividades de: planejamento, implementação, testes e validação, as quais podem ser ciclicamente repetidas. O uso efetivo dessa metodologia pode ser observada durante todo o desenvolvimento do software, onde cada funcionalidade do ARION era planejada, implementada e testada gerando dessa forma, um programa cada vez mais completo. A adoção do modelo Espiral também pode ser observada depois da fase de testes com empresas reais, quando o ARION estava disponível de forma online. Ao verificar as respostas obtidas pelos usuários no questionário, fez-se um planejamento de melhorias que poderiam ser realizadas, como por exemplo formas de amenizar as dificuldades citadas pelos usuários em entender o que é um processo e um ativo e colocar o design de algumas telas e botões dentro do padrão do ARION. Essas, foram implementadas e testadas e após foi disponibilizado a versão 2 (atual).

Considerando a extensão desse trabalho, fez-se necessário uma última seção para discutir rapidamente tudo o que foi apresentado até o momento.

4.6 Discussão

Para desenvolver este projeto, considerando o problema de pesquisa apresentado, definiu-se os objetivos e fez-se uma revisão literária, a fim de verificar o estado da arte relacionado ao assunto do trabalho. Após, baseado em normas e padrões internacionalmente aceitos, criou-se e validou-se um modelo para análise de riscos. Posteriormente, para o planejamento da automatização do modelo, foram levantados os requisitos e elaboradas as demais modelagens. Após, definiu-se a metodologia de implementação e o aparato tecnológico a ser utilizado no desenvolvimento do ARION. Em seguida, iniciou-se a programação e, durante toda essa fase, as funcionalidades foram testadas respeitando os casos de testes estabelecidos. Ao ser concluído, o ARION foi disponibilizado em um servidor do Grupo de Pesquisa de Segurança da Informação da Unipampa e se tornou acessível ao mundo através do endereço: https://arion.gsi.seg.br/ . Assim, pode-se afirmar que a resposta para o problema de pesquisa deste trabalho: "É possível implementar uma solução que auxilie na avaliação e gestão de riscos e que possa ser aplicado à organização como um todo, a uma área específica, ou a aspectos particulares de um controle?" é SIM, foi possível implementar uma solução visando a avaliação de riscos. O ARION retorna ao usuário o valor de risco qualitativo e quantitativo por ativo de cada processo da empresa.

Com o objetivo de verificar a usabilidade e possibilitar aos usuários sugerirem melhorias para o ARION, realizou-se estudos sobre possíveis testes que poderiam ser feitos. Elaborou-se os testes. 8 empresas responderam ao questionário e os resultados demonstraram que de forma geral, o ARION atingiu seu objetivo de permitir uma análise de riscos, visto que todas as empresas concordaram com o valor de risco retornado pelo sistema e pode-se afirmar também que o ARION teve boa aceitação, pois todos concordaram que o software possui mecanismos de navegação e interatividade e layout amigáveis. As dificuldades citadas por uma das empresas: "Dificuldade em entender o que é um ativo e um processo" foi amenizada colocando nas próprias páginas de cadastro de ativo e processo conceitos e exemplos a fim de facilitar o entendimento. Ressalta-se que a definição de processo e ativo foram inseridos no manual desde sua criação. No entanto, nem todos os usuários lêem o manual, fato comprovado no proprio questionário em que uma parcela pequena das empresas admitiram não terem lido o manual. Algumas das sugestões dadas pelos usuários foram atendidas, outras por questão de tempo ficaram como atividades de trabalhos futuros.

Sabe-se que o ARION pode melhorar. Mas por hora, pode-se dizer que hoje, qualquer pessoa tem acesso a uma ferramenta de análise de riscos de forma gratuita e baseada em normas e padrões de referência e aceitação internacional.

5 CONSIDERAÇÕES FINAIS

Neste trabalho foi exposto a importância de se manter seguros os ativos de informação, e que isto é possível através do gerenciamento de riscos. Além disso, é abordado um problema caracterizado pela dificuldade em se implantar as normas e padrões internacionais relacionadas a gestão de riscos. Sabendo disso, a proposta para esse problema foi a construção de um modelo para o cálculo de riscos simplificado e que permitisse a qualquer pessoa executar uma análise de risco.

Após estudos sobre as tecnologias disponíveis e das normas da família ISO/IEC e modelos de governança, o modelo foi criado, validado e automatizado, através do ARION. Esta se encontra disponível, de forma online e de fácil acesso.

O modelo tem grande relevância, por apresentar os valores de riscos quantitativamente e qualitativamente, de forma simples e clara para o usuário, e mostra através dos relatórios, as vulnerabilidades encontradas e que devem ser preferencialmente extintas, trazendo dessa forma, benefícios para a organização. Para o desenvolvimento deste trabalho se colocou em prática conceitos aprendidos durante todo o curso.

Constatou-se que melhorias podem ser realizadas. No entanto, os resultados obtidos permitem afirmar que os objetivos propostos foram cumpridos, ou seja, o projeto de criação, validação e implementação do modelo de análise de risco foram realizados e obtiveram êxito.

Como trabalhos futuros, a fim de aperfeiçoar a ferramenta ARION, sugere-se implementar as seguintes funcionalidades:

1. Implementar a possibilidade de Recuperar Senha: necessário caso o usuário possua cadastro e esqueça a senha para efetuar login no ARION;
2. Acesso por níveis, ao ARION (administrador e usuário, por exemplo): essa funcionalidade atenderia de forma mais específica o princípio da confidencialidade da segurança da informação, pois somente pessoas autorizadas poderiam realizar a análise de riscos;
3. Realizar um estudo mais aprofundado de Usabilidade a fim de melhorar e ampliar o check-list: as questões presentes no ARION foram baseadas na norma ISO/IEC 27005 mas, outras questões abrangendo outras ameaças e vulnerabilidades já catalogadas complementando as que já estão cadastradas na ferramenta tornaria o ARION ainda mais completo;
4. Implementar possibilidade de visualizar a evolução do risco, através de gráficos, por

exemplo: atendendo a uma das sugestões recebidas pelos usuários que participaram dos testes da ferramenta - uma forma de visualização de evolução ou involução do risco faciliataria o entendimento do profissional dos resultados de risco no decorrer de um determinado tempo;

5. Adequar o ARION à Lei Geral de Proteção de Dados (LGPD): apesar do ARION permitir a exclusão de todos os dados inseridos pelo usuário, o que é previsto na LGPD, não foi realizado por questões de tempo, um estudo específico para que a ferramenta se enquadre em todos os aspectos da lei.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 27002: Tecnologia da Informação – Técnicas de segurança – Código de Prática para controles de segurança da informação**. Rio de Janeiro/RJ, 2005. Norma Técnica.

ABNT. **NBR ISO/IEC 38500: Tecnologia da Informação – Governança corporativa de tecnologia da informação**. Rio de Janeiro/RJ, 2009. Norma Técnica.

ABNT. **Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação**. Rio de Janeiro/RJ, 2011. Norma Técnica.

ABNT. **NBR ISO/IEC 27001: Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos**. Rio de Janeiro/RJ, 2013. Norma Técnica.

ABNT. **NBR ISO/IEC 27002: Tecnologia da Informação – Técnicas de segurança – Código de Práticas para controles de segurança da informação**. Rio de Janeiro/RJ, 2013. Norma Técnica.

ALENCAR, A. J.; SCHMITZ, E. A. **Análise de Risco em Gerência de Projetos**. São Paulo, SP: Brasport, 2006.

BARROS, A. J. da S.; LEHFELD, N. A. de S. **Fundamentos de metodologia científica**. 3. ed. São Paulo, SP: Pearson Universidades, 2007. ISBN 9788576051565.

BEZERRA, E. K. **Gestão de Riscos de TI - NBR 27005**. Rio de Janeiro, RJ: Escola Superior de Redes, 2013. ISBN 9788563630322.

BHATTACHARJEE, J. et al. Two-phase quantitative methodology for enterprise information security risk analysis. **ACM**, 2012.

Bootstrapmade. **Arsha - Free Corporate Bootstrap HTML Template**. 2021. Disponível em: bootstrapmade.com.

CERT. **Estatísticas dos Incidentes Reportados ao CERT.br**. 2021. Disponível em: https://www.cert.br/stats/incidentes/.

Clavis. **BART - Baselines, Análises de Riscos, Testes de Segurança**. 2021. Disponível em: https://clavis.com.br/solucoes/bart-gerenciamento-de-vulnerabilidade-baselines-analises-de-risco-testes-de

CRUZ, J. M. de M. **Segurança da Informação: a Norma ISO/IEC 27000 e ISO/IEC 27001**. Dissertação (Mestrado) — Faculdade de Engenharia da Universidade do Porto, Porto, 2012.

DANTAS, M. L. **Segurança da Informação: Uma Abordagem Focada em Gestão de Riscos**. [S.l.]: Livro Rápido, 2011. ISBN 97885406004781.

Departamento de Sistemas e Computação - DSC. **Diagrama de Classes - Um diagrama de três faces**. 2021. Disponível em: http://www.dsc.ufcg.edu.br/ jacques/cursos/map/html/uml/diagramas/classes/classes1.htm.

FACTI. **Metodologia de Gestão de Riscos de Segurança da Informação**. Campinas, SP, 2015. Relatório RM2.

FAGUNDES, E. M. **COBIT - Um kit de ferramentas para excelência na gestão de TI**. Campinas, SP, 2012. Relatorio RM2.

FERNANDES, A. A.; ABREU, V. F. de. **Implantando a Governança de TI - da Estratégia à Gestão dos Processos e Serviços**. 3. ed. Rio de Janeiro, RJ: Brasport, 2012. ISBN 9788574525334.

FONTES, E. **Políticas e Normas para a Segurança da Informação - Como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações**. [S.l.]: Brasport, 2012. ISBN 9788574525150.

GIL, A. C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo, SP: Atlas, 2010. ISBN 9788597012613.

Grupo MZ. **Ataques Cibernéticos no 1S21**. 2021. Disponível em: https://blog.mzgroup.com/pt-br/ataques-ciberneticos-no-1s21/.

HB. **HB 231:2004 Information Security Risk Management Guidelines**. Sidney/Wellington, Australia/New Zealand, 2004.

INSTITUTE, I. G. **COBIT 4.1**. Rolling Meadows, USA, 2007. Modelo de Governança.

ISO/IEC. **INTERNATIONAL STANDARD ISO/IEC 27000 – Information technology – Security techiques – Information security management systems – Overview and vocabulary**. [S.l.], 2014. Norma Técnica.

JUNIOR, A. G.

Metodologias de Gerenciamento de riscos em Sistemas de Tecnologias da Informação e Comunicação - abordagem prática para conscientização e implantação nas organizações — Universidade Federal do Rio Grande do Sul, 2008. Trabalho de Conclusão de Curso.

KONZEN, M. P.; MANZONI, L.; NUNES, R. C. Gestão de riscos de segurança da informação baseada na norma iso/iec 27005 usando padrões de segurança. In: **Anais Eletrônicos do IX Simpósio de Excelência em Gestão de Tecnologia**. [S.l.: s.n.], 2012. Disponível em: <http://www.aedb.br/seget/arquivos/artigos12/57616827.pdf> Acesso em: julho de 2021.

MANOEL, S. da S. **Governança de Segurança da Informação**. Rio de Janeiro, RJ: Brasport, 2014.

MAYER, J.; LEMES, L. A model to assess the maturity level of the risk management process in information security. **IEEE**, 2009.

Microsoft. **Ferramenta de Avaliação do Microsoft Security 4.0**. 2021. Disponível em: https://www.microsoft.com/pt-BR/download/details.aspx?id=12273.

Modulo. **QuantiRisk**. 2021. Disponível em: https://www.modulo.com.br/quantrisk/.

Mozilla. **Sobre JavaScript**. 2021. Disponível em: https://developer.mozilla.org/pt-BR/docs/Web/JavaScript/About_JavaScript.

MySQL. **MySQL**. 2021. Disponível em: https://www.mysql.com/.

NETO, P. T. M.; ARAúJO, W. J. **Segurança da Informação - Uma visão sistêmica para implantação em organizações**. João Pessoa, PB: Editora UFB, 2019. ISBN 9788523714734.

PALKO, D. et al. Model of information security critical incident risk assessment. **IEEE**, 2020.

PHP. **PHP: O que o PHP pode fazer?** 2021. Disponível em: https:https://www.php.net/manual/pt_BR/intro-whatcando.php.

PRADO, E. P. V.; SOUZA, C. A. de. **Fundamentos de sistemas de informação**. Rio de Janeiro: Elsevier, 2014. ISBN 9788535274356.

PRESSMAN, R. S. **Engenharia de Software - Uma Abordagem Profissional**. 7. ed. [S.l.]: Bookman, 2011. ISBN 9788580550443.

PUBLICATION, B. S. **Information technology — Security techniques — Information security incident management**. [S.l.], 2011. Norma Técnica.

ROSEMANN, D.

Software para avaliação da segurança da informação de uma empresa conforme a norma NBR ISO/IEC 17799 — Universidade Regional de Blumenau, 2002. Trabalho de Conclusão de Curso.

SANTOS-OLMO, A. et al. Methodology for dynamic analysis and risk management on iso27001. **IEEE**, 2016.

SÊMOLA, M. **Gestão da Segurança da Informação – Uma Visão Executiva**. 2. ed. [S.l.]: Elsevier, 2014. ISBN 9788535271782.

SILBERSCHATZ, A.; KORTH, H. F.; SUDARSHAN, S. **Sistema de Banco de Dados**. 5. ed. São Paulo, SP: Elsevier, 2006. ISBN 8535211078.

SOMMERVILLE, I. **Engenharia de Software**. 10. ed. São Paulo, SP: Pearson Universidades, 2019. ISBN 9788543024974.

SOULA, J. M. F. **ISO/IEC 20000 - Gerenciamento de Serviços de Tecnologia de Informação**. 1. ed. [S.l.]: Brasport, 2013. ISBN 9788574525518.

USP. **Pesquisa Gestão de Pessoas na Crise COVID-19: Relatório Final**. 2021. Disponível em: jornal.usp.br.

VERGARA, S. C. **Projetos e relatórios de pesquisa em administração**. São Paulo, SP: Atlas, 2006.

WEILL, P.; ROSS, J. W. **Governança de TI - Tecnologia da Informação**. 1. ed. Harvard: M Books, 2006. ISBN 8589384780.

APÊNDICE A – DOCUMENTO DE REQUISITOS

[adaptado de Sommerville (2007) e Pressman Maxim (2016)]

1. Introdução

Este documento especifica os requisitos do sistema, fornecendo as informações necessárias para o projeto e implementação, bem como para a realização dos testes e homologação do sistema.

Visão geral do documento Além desta seção introdutória, as seções seguintes estão organizadas como descrito abaixo.

Seção 2 – Descrição geral do sistema: apresenta uma visão geral do sistema, caracterizando qual é o seu escopo e descrevendo seus usuários.

Seção 3 – Requisitos funcionais: relacionam a maneira de como o sistema deve operar, onde se especificam as entradas e saídas do sistema.

Seção 4 – Requisitos não funcionais: especifica todos os requisitos não funcionais do sistema, divididos em requisitos de usabilidade, confiabilidade, desempenho, segurança, distribuição, adequação a padrões e requisitos de hardware e software.

Convenções, termos e abreviações.

Identificação dos requisitos Por convenção, a referência a requisitos é feita através do nome da subseção onde eles estão descritos, seguidos do identificador do requisito, de acordo com a especificação a seguir: [nome da subseção. Identificador do requisito]. Prioridades dos requisitos Para estabelecer a prioridade dos requisitos, nas seções 3 e 4, foram adotadas as denominações “essencial”, “importante” e “desejável”. Essencial é o requisito sem o qual o sistema não entra em funcionamento. Requisitos essenciais são requisitos imprescindíveis, que têm que ser implementados impreterivelmente. Importante é o requisito sem o qual o sistema entra em funcionamento, mas de forma não satisfatória. Requisitos importantes devem ser implementados, mas, se não forem, o sistema poderá ser implantado e usado mesmo assim. Desejável é o requisito que não compromete as funcionalidades básicas do sistema, isto é, o sistema pode funcionar de forma satisfatória sem ele. Requisitos desejáveis podem ser deixados para versões posteriores do sistema, caso não haja tempo hábil para implementá-los na versão que está sendo especificada.

2. Descrição geral do sistema

Abrangência do sistema

O sistema é um modelo automatizado para o cálculo do risco, e, visa contribuir para melhorar o nível de segurança de informação de empresas/organizações.

3. Requisitos Funcionais

Requisito 1: [RF01] Cadastro de Usuário

•Descrição: Permitir o cadastro de usuários interessados em realizar análise de risco.

•Entradas: Nome, E-mail, Senha, CPF, Cargo;

•Processo: O cadastro será incluído no sistema.

•Saída: Se o cadastro for bem-sucedido deverá existir uma confirmação, caso contrário, apresentar uma mensagem de erro.

Prioridade:

X	Essencial		Importante		Desejável

Requisito 2: [RF02] Cadastro de Empresa

•Descrição: Permitir aos usuários o cadastro da empresa.

•Entradas: Nome Fantasia, CNPJ ou CEI, Endereço, Cidade;

•Processo: O cadastro será incluído no sistema.

•Saída: Se o cadastro for bem-sucedido deverá existir uma confirmação, caso contrário, apresentar uma mensagem de erro.

Prioridade:

X	Essencial		Importante		Desejável

Requisito 3: [RF03] Cadastro de Processo

•Descrição: Permitir aos usuários o cadastro de processos referente a alguma empresa já cadastrada.

•Entradas: Descrição, Valor de importância;

•Processo: O cadastro será incluído no sistema.

•Saída: Se o cadastro for bem-sucedido deverá existir uma confirmação, caso contrário, apresentar uma mensagem de erro.

Prioridade:

X	Essencial		Importante		Desejável

Requisito 4: [RF04] Cadastro de Ativos

•Descrição: Permitir aos usuários o cadastro de ativos referentes a algum processo já cadastrado.

•Entradas: Descrição, Valor de importância, Tipo;

•Processo: O cadastro será incluído no sistema.

•Saída: Se o cadastro for bem-sucedido deverá existir uma confirmação, caso contrário, apresentar uma mensagem de erro.

Prioridade:

X	Essencial		Importante		Desejável

Requisito 5: [RF05] Login de Usuário

•Descrição: Permitir que somente usuários cadastrados consigam efetuar login e tenham acesso as funcionalidades do programa;

•Entradas: Email, Senha;

•Processo: O sistema irá buscar informações no banco de dados;

•Saída: Se a busca obtiver resultados, o programa abrirá página com funcionalidades, caso contrário, volta para a página inicial.

Prioridade:

X	Essencial		Importante		Desejável

Requisito 6: [RF06] Editar Usuário

•Descrição: Permitir aos usuários que alterem dados referentes ao seu cadastro;

•Entradas: Informações a serem alteradas;

•Processo: O cadastro será alterado no sistema.

•Saída: Se a alteração for bem-sucedida deverá existir uma confirmação, caso contrário, os dados permanecem como antes.

Prioridade:

X	Essencial		Importante		Desejável

Requisito 7: [RF07] Editar Empresa

•Descrição: Permitir aos usuários que alterem dados referentes ao cadastro de empresa;

•Entradas: ;

•Processo: O cadastro será alterado no sistema.

•Saída: Se a alteração for bem-sucedida deverá existir uma confirmação, caso contrário, os dados permanecem como antes.

Prioridade:

X	Essencial		Importante		Desejável

Requisito 8: [RF08] Excluir Usuário

•Descrição: Permitir aos usuários que excluam seu cadastro no sistema e todos os seus dados, bem como de empresas, processos, ativos e relatórios sejam excluídos;

•Entradas: Todos os dados cadastrados pelo usuário;

•Processo: Todos os dados do usuário serão excluídos do banco de dados.

•Saída: Se a exclusão for bem-sucedida deverá existir uma confirmação, caso contrário, os dados permanecem como antes.

Prioridade:

X	Essencial		Importante		Desejável

Requisito 9: [RF09] Excluir Processo

•Descrição: Permitir aos usuários que excluam o cadastro de processo referente a alguma empresa;

•Entradas: Todos os dados referentes ao processo;

•Processo: O cadastro será excluído do banco de dados.

•Saída: Se a exclusão for bem-sucedida deverá existir uma confirmação, caso contrário, os dados permanecem como antes.

Prioridade:

X	Essencial		Importante		Desejável

Requisito 10: [RF10] Excluir Empresa

•Descrição: Permitir aos usuários que excluam o cadastro de alguma empresa referente ao seu cadastro de usuário;

•Entradas: Todos os dados referentes à empresa;

•Processo: O cadastro será excluído do banco de dados.

•Saída: Se a exclusão for bem-sucedida deverá existir uma confirmação, caso contrário, os dados permanecem como antes.

Prioridade:

X	Essencial		Importante		Desejável

Requisito 11: [RF11] Análise de Risco

•Descrição: Permitir aos usuários a identificação de ameaças e vulnerabilidades existentes e o nível de risco;

•Entradas: Valor de importância de Ativo, Processo e de impacto da ameaça e Vulnerabilidades presentes;

•Processo: O cálculo do risco será executado;

•Saída: Valor de Risco.

Prioridade:

X	Essencial		Importante		Desejável

Requisito 12: [RF12] Acessar Relatórios

•Descrição: Permitir aos usuários o acesso à todos os relatórios de análise de risco salvos;

•Entradas: Todos os relatórios salvos pelo usuário;

•Processo: O sistema deve consultar no Banco de Dados todos os relatórios salvos pelo usuário;

•Saída: O sistema deve exibir todos os relatórios salvos pelo usuário e dar possibilidade de baixá-los;

Prioridade:

X	Essencial		Importante		Desejável

Requisito 13: [RF13] Excluir Relatórios

•Descrição: Permitir aos usuários a exclusão de relatório;

•Entradas: Relatório a ser excluído;

•Processo: Sistema deve excluir toodas as informações de relatório a ser excluído;

•Saída: Relatório é excluído.

Prioridade:

X	Essencial		Importante		Desejável

4. Requisitos Não Funcionais

[NF001] Linguagem de Programação e Ambiente de Desenvolvimento

A implementação deste sistema será feita em linguagem de programação PHP e SQL (Back-End) e utilizará o framework Bootstrap (Front-End); O ambiente de desenvolvimento escolhido é a IDE Sublime Text.

Prioridade:

X	Essencial		Importante		Desejável

[NF002] Usabilidade

O sistema terá uma interface amigável e objetiva ao usuário.

Prioridade:

X	Essencial		Importante		Desejável

APÊNDICE B – QUESTIONÁRIO PARA TESTES DE PROTÓTIPO - VALIDAÇÃO DO MODELO

1. Questões relacionadas a Identificação da Empresa:

1.1 Nome Fantasia/Cidade de Localização: _____

1.2 Número de funcionários da Empresa: ___

1.3 Número de processos: ___

2. Questões relacionadas a Identificação de Vulnerabilidades (o respondente deveria marcar àquelas vulnerabilidades encontradas em seu ambiente de trabalho)

2.1 Ativo hardware:

Numere o valor de importância deste ativo: ___

Vulnerabilidade	Possui Vulnerabilidade	Ameaça	Valor da Ameaça
Empresa possui manutenção insuficiente/defeituosa de mídia de armazenamento		Violação das condições de uso do sistema de informação que possibilitam sua manutenção	
Empresa não possui uma rotina de substituição periódica de componentes de hardware		Destruição de Equipamento ou mídia	
Os hardwares da empresa possuem sensibilidade à umidade, poeira e sujeira		Poeira, corrosão, congelamento	
Os hardwares da empresa possuem sensibilidade a variações de voltagem		Interrupção do suprimento de energia	
Os hardwares da empresa possuem sensibilidade a variações de temperatura		Fenômeno meteorológico	
A empresa não possui armazenamento de hardware protegidos		Furto de mídias ou documentos	
Mídias que possuem informações sensíveis não são guardadas e descartadas de forma segura		Furto de mídias ou documentos	
Empresa não controla as cópias realizadas no local		Furto de mídias ou documentos	

2.2 Ativo software:

Numere o valor de importância deste ativo: ___

Vulnerabilidade	Possui Vulnerabilidade	Ameaça	Valor da Ameaça
Não são estabelecidos procedimentos para notificar mau funcionamento do software		Abuso de direitos	
Empresa utiliza software amplamente distribuído		Comprometimento dos dados	
Empresa utiliza programas aplicativos com um conjunto errado de dados (referentes a um outro período)		Comprometimento dos dados	
Empresa utiliza programas com Interface de usuário complicada		Erro durante o uso	
Empresa utiliza software que não possui documentação		Erro durante o uso	
Empresa utiliza software sem mecanismos de autenticação e identificação como, por exemplo, para a autenticação de usuário		Forjamento de direitos	
Não são instalados e/ou atualizados software para detecção e remoção de vírus dos computadores e meios magnéticos		Comprometimento dos dados	
Empresa não adota uma política de gerenciamento de senhas		Forjamento de direitos	
Empresa possui serviços desnecessários que permanecem habilitados		Processamento ilegal de dados	
Empresa não separa os ambientes de desenvolvimento, teste e produção de software		Defeito de software	
Empresa não estabelece critérios de aceitação para novos sistemas		Defeito de software	
Empresa não adota um controle eficaz de mudanças de software		Alteração de software	
Ocorrem download e uso não controlado de software		Alteração de software	
Empresa não possui cópias de segurança (back-up)		Alteração de software	
Não são feitas análises críticas regulares de software que suportam processos críticos do negócio		Defeito de software	

2.3 Vulnerabilidades relacionadas ao ativo redes:

Numere o valor de importância deste ativo: ___

Vulnerabilidade	Possui Vulnerabilidade	Ameaça	Valor da Ameaça
Não é utilizado um conjunto de controles para obter e preservar a segurança nas redes de computadores		Falha de Equipamento	
Não são estabelecidos procedimentos e responsabilidades para gerenciamento de equipamentos remotos		Forjamento de direitos	
A organização possui redes compartilhadas que se estendem além dos limites físicos da organização		Abuso de direitos	
Empresa possui/usa linhas de comunicação desprotegidas		Escutas não autorizadas	
A estrutura de redes possui junções de cabeamento mal feitas		Falha de Equipamento	
Conexões a sistemas remotos de computadores não são autenticados		Forjamento de direitos	
Não são estabelecidos controles para a confidencialidade integridade dos dados que trafegam em rede pública		Abuso de direitos	
Os controles de roteamento não são baseados em fontes confiáveis e mecanismos de checagem de endereço de destino		Abuso de direitos	
Os usuários possuem acesso não somente aos serviços que estão autorizados mas a outros também		Forjamento de direitos	

APÊNDICE C – MANUAL DE UTILIZAÇÃO DO SOFTWARE

ARION
Manual de Utilização do Software

1. Introdução

O que é análise de risco?

Uma técnica de levantamento de informações sobre a empresa que permite verificar a exposição ao risco em que a organização se encontra para que possa tomar decisões apropriadas e gerenciar informações de forma adequada. A análise de risco envolve a identificação e avaliação do nível dos riscos calculados considerando os valores avaliados dos ativos e os níveis de ameaças e vulnerabilidades desses ativos.

Pensando em uma forma simplificada e gratuita de realizar a análise de riscos, é que foi criado o Arion, um projeto baseado em normas de referências internacionais, como por exemplo a família da norma ISO/IEC 27000, em especial a ISO/IEC 27005 e alguns domínios do COBIT.

2. Funcionalidades

- Realização de Análise de Riscos de Informação;
- Edição de algumas informações inseridas;
- Acesso a relatórios de análises já realizadas.

3. Benefícios Esperados

- É uma forma simples e gratuita de realizar uma análise de riscos;
- Antecipa e reduz os efeitos de eventos inesperados;
- Permite o planejamento de respostas e tomada de decisões com base em vulnerabilidades presentes na empresa;
- Projeto implementado com base em normas de referências internacionais.

4. Como Acessar o Sistema

Através do endereço https://arion.gsi.seg.br/

5. Realizar um Novo Cadastro de Usuário

Caso o usuário não possua cadastro no Sistema Arion, deve seguir os passos:

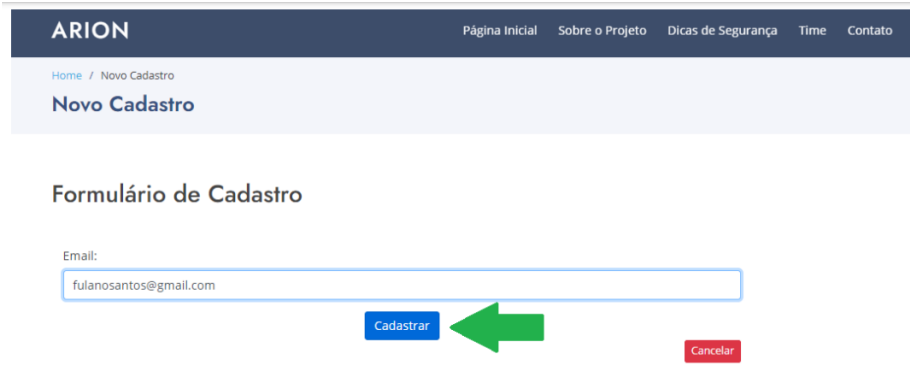
1. Acesse o endereço: https://arion.gsi.seg.br/
2. Na Página Inicial clique em Novo Cadastro, conforme mostrado na Figura 65 :

Figura 65 – Página Inicial com identificação de botão de “Novo Cadastro

Fonte: Próprio autor, 2021.

Ao clicar em “Novo Cadastro” o usuário será redirecionado à página de Cadastro. A primeira informação a ser inserida é o e-mail, conforme mostrado na Figura **??**. Depois de escrever o e-mail, o usuário deve clicar em “Cadastrar”.

Figura 66 – Primeira parte de Cadastro de Usuário



Fonte: Próprio autor, 2021.

Se, ao invés de clicar em "Cadastrar", for clicado no botão “Cancelar” (localizado no canto inferior direito, na cor vermelha), o usuário será redirecionado à página inicial, nenhum dado digitado será salvo. Após clicar em “Cadastrar” têm-se duas situações possíveis:

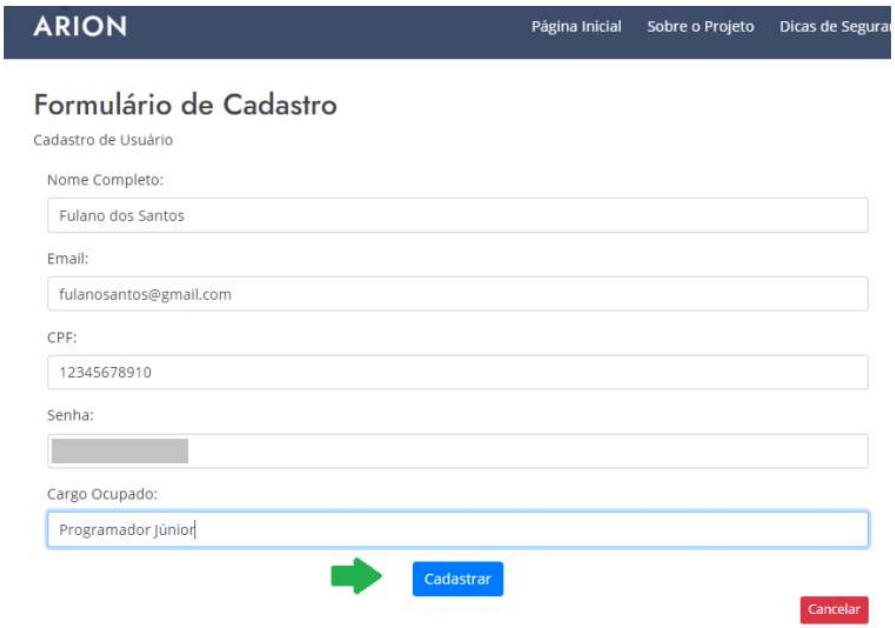
1. o usuário já possui cadastro: caso o email digitado já esteja no Banco de Dados do ARION, o usuário será redirecionado à página inicial. Sugere-se nesse caso, que seja

realizado login.

2. o usuário não possui cadastro: caso o e-mail digitado não esteja no Banco de Dados do ARION, o usuário será redirecionado a próxima página de cadastro, onde mais dados são solicitados.

O usuário deve preencher esses dados, e ao final, clicar em “Cadastrar”, conforme mostrado na Figura 67.

Figura 67 – Continuação do Cadastro de Usuário



Fonte: Próprio autor, 2021.

Se, ao invés de clicar em "Cadastrar", for clicado no botão “Cancelar” (localizado no canto inferior direito, na cor vermelha), o usuário será redirecionado à página inicial, nenhum dado digitado será salvo. Ao clicar em “Cadastrar”, uma mensagem (Figura 68) será exibida. O usuário deve clicar em “Voltar para Página Inicial” e realizar Login.

Figura 68 – Mensagem de Cadastro de Usuário

Fonte: Próprio autor, 2021.

6. Realizar Login

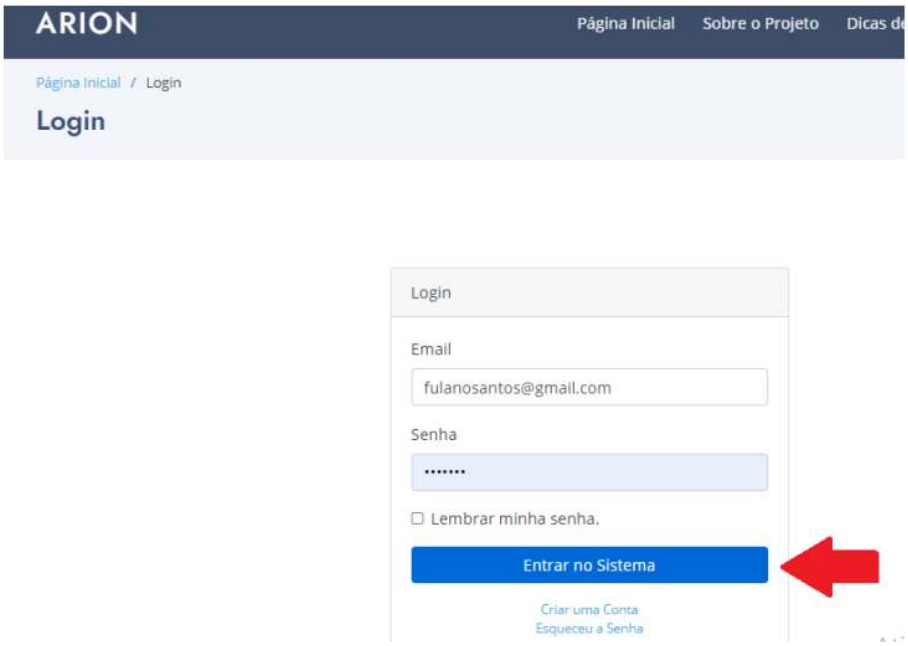
1. Acessar o endereço: arion.gsi.seg.br ;
2. Clicar em “Login”, conforme mostrado na Figura 69.

Figura 69 – Página inicial com sinalização do botão “Login”

Fonte: Próprio autor, 2021.

Ao clicar em “Login”, o usuário será redirecionado à página de login (Figura 70) e deve digitar o e-mail e senha cadastrado, e clicar em “Entrar no Sistema”.

Figura 70 – Página de Login

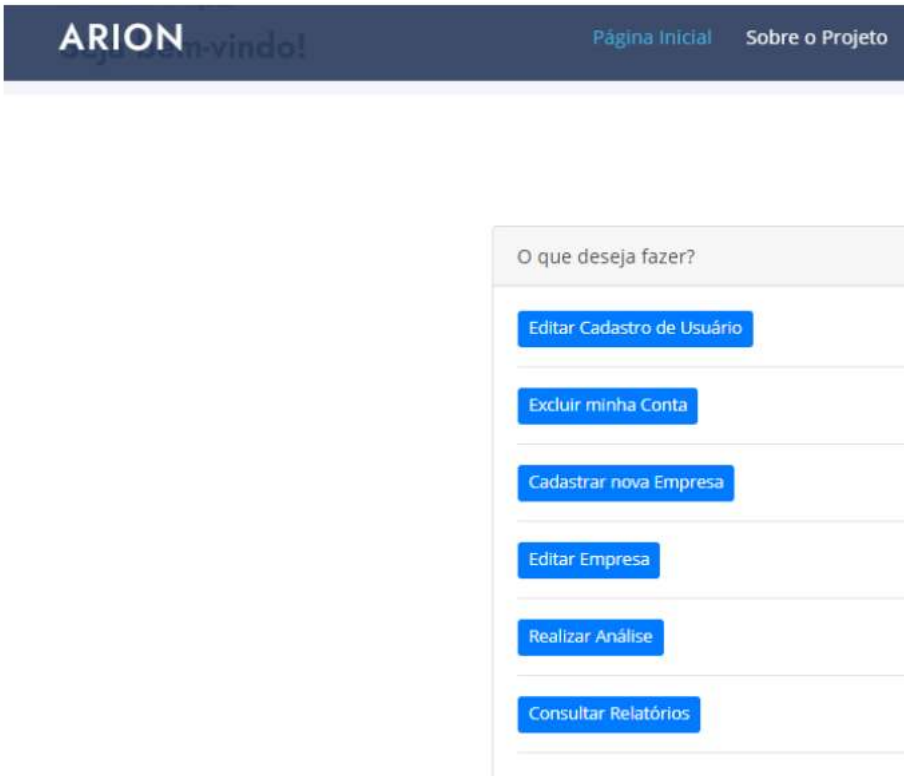


Fonte: Próprio autor, 2021.

Após clicar em “Entrar no Sistema” têm-se duas situações possíveis, considerando que o usuário já fez o Cadastro anteriormente:

1. O usuário digitou e-mail ou senha (ou ambos) errado (diferente do que foi cadastrado): será redirecionado à página inicial, sugere-se fazer nova tentativa de login;
2. O usuário digitou o e-mail e senha corretos (iguais aos que foram cadastrados): o usuário será redirecionado à tela com menu de ações (Figura 71).

Figura 71 – Tela após login - Menu de ações disponíveis



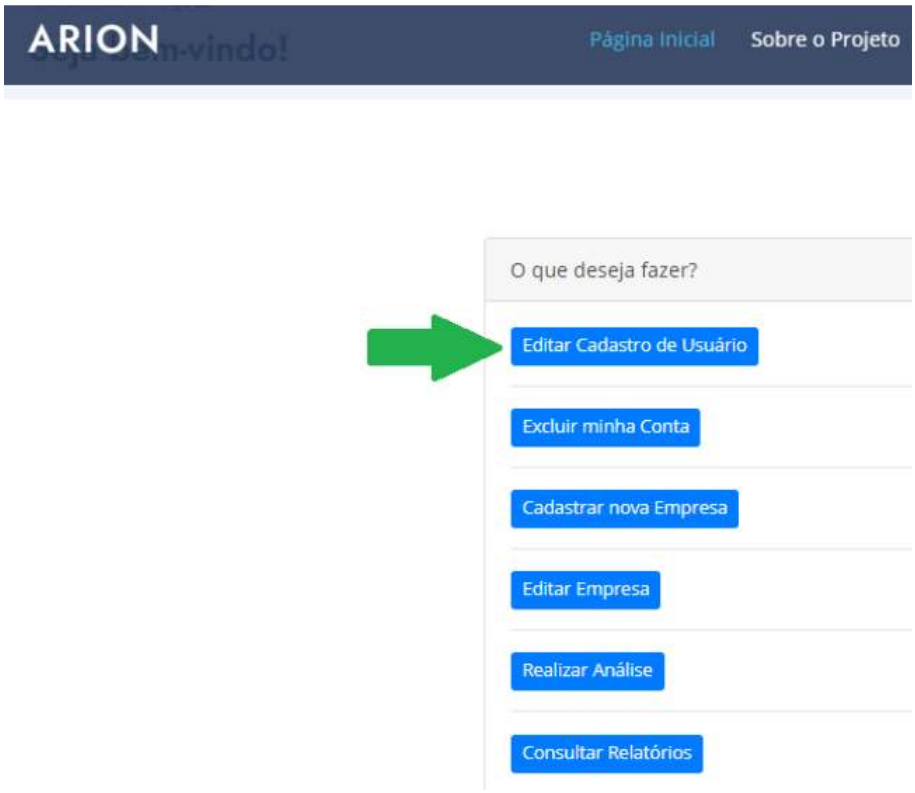
Fonte: Próprio autor, 2021.

7. Editar Cadastro de Usuário

Permite ao usuário alterar dados cadastrados: Nome, Email, CPF, Senha, Cargo. Para executar essa ação, o usuário deve:

1. fazer login, ao inserir email e senha corretos, será redirecionado à tela com opções de ações (Figura 71).
2. clicar em “Editar Cadastro de Usuário” (Figura 72).

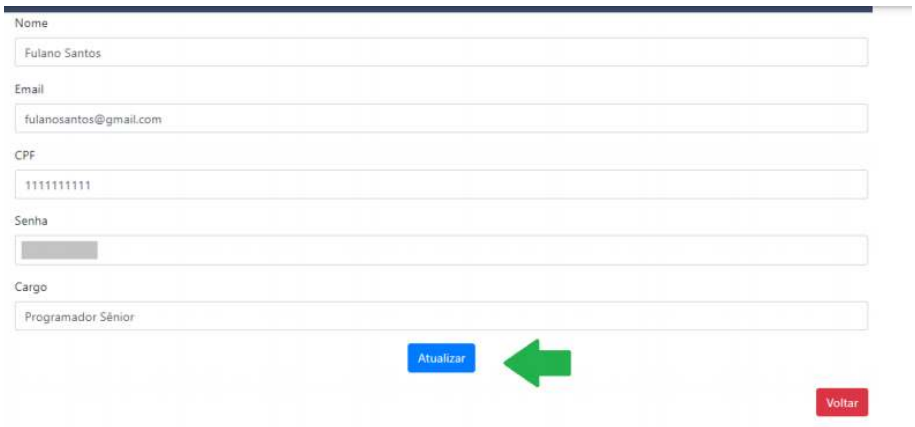
Figura 72 – Tela de menu com sinalização do botão “Editar Cadastro de Usuário”



Fonte: Próprio autor, 2021.

3. Ao clicar em “Editar Cadastro de Usuário”. O usuário será redirecionado à página de Edição de Cadastro, nesta, basta alterar o campo desejado e, posteriormente, clicar em “Atualizar”, conforme mostrado na Figura 73).

Figura 73 – Edição de Cadastro de Usuário



Fonte: Próprio autor, 2021.

Caso seja clicado em “Voltar”, o usuário será redirecionado à tela com opções de ações (Figura 71) e nenhum dado será alterado. Ao clicar em “Atualizar”, uma mensagem será mostrada (Figura 74).

Figura 74 – Mensagem de confirmação de atualização de cadastro de usuário

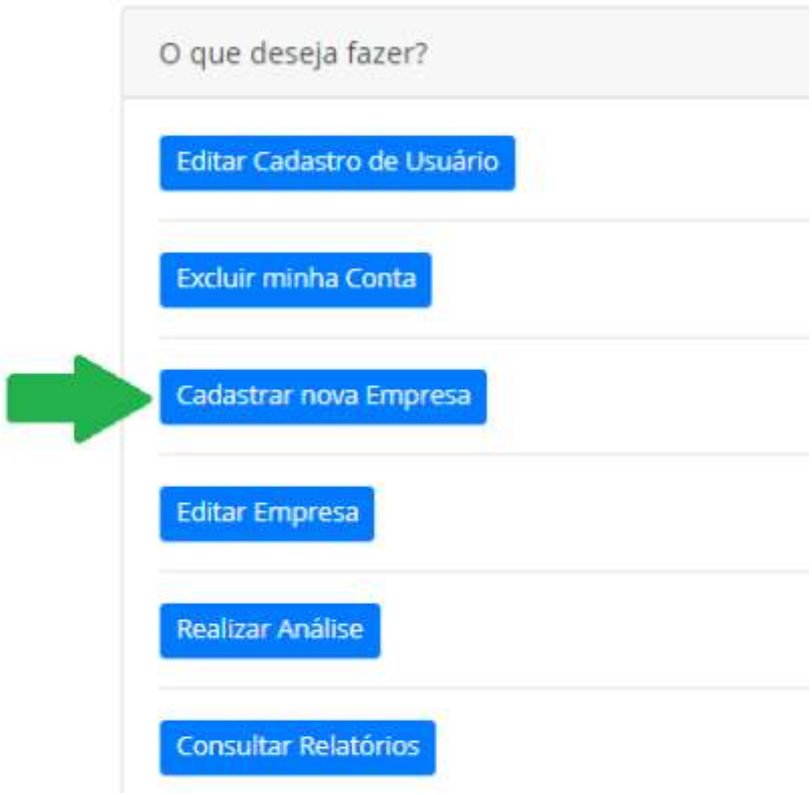
Fonte: Próprio autor, 2021.

8. Cadastrar Empresa

Permite ao usuário cadastrar uma empresa para posterior realização de análise de risco. Para executar essa ação, o usuário deve:

1. fazer login, ao inserir email e senha corretos, será redirecionado à tela com opções de ações (Figura 71);
2. clicar em “Cadastrar nova Empresa” (Figura 75).

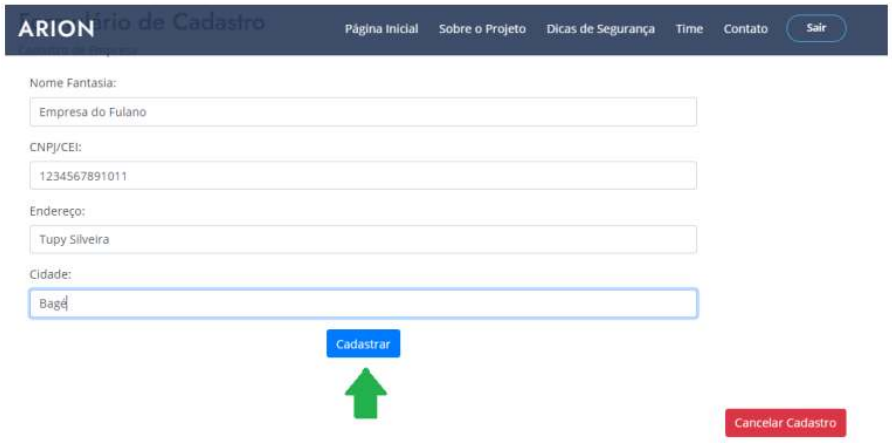
Figura 75 – Tela de menu com sinalização do botão “Cadastrar nova Empresa”



Fonte: Próprio autor, 2021.

Ao clicar em “Cadastrar nova Empresa”, o usuário será redirecionado à página de Cadastro de Empresa e deverá inserir as informações solicitadas, e após, clicar em “Cadastrar”, conforme mostrado na Figura 76.

Figura 76 – Tela de Cadastro de empresa



Fonte: Próprio autor, 2021.

Caso seja clicado em “Cancelar Cadastro”, o usuário será redirecionado à tela com opções de ações (Figura 71) e nenhuma empresa será cadastrada. Ao clicar em “Cadastrar”, uma mensagem será mostrada (Figura 77).

Figura 77 – Mensagem de confirmação de cadastro de empresa

Fonte: Próprio autor, 2021.

Ao clicar em “Voltar”, o usuário será redirecionado à tela de ações (Figura 71).

9. Editar e Excluir Empresa

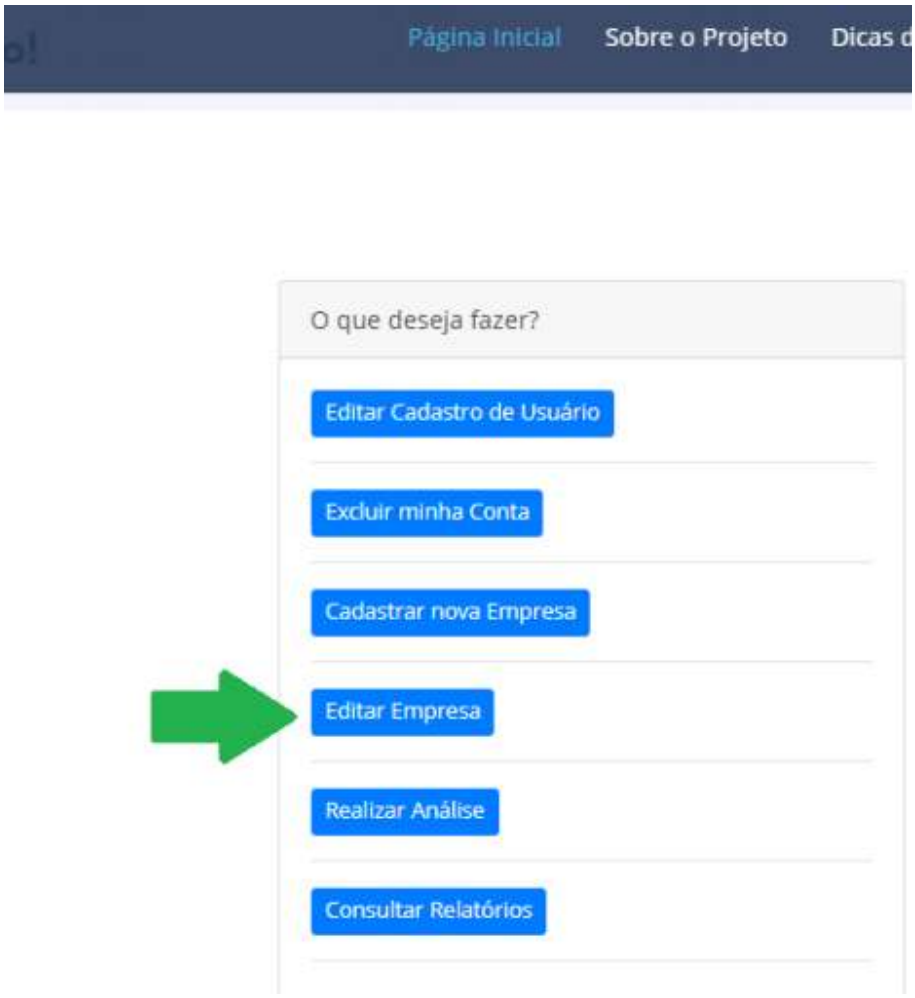
Editar Empresa - Permite ao usuário editar informações (Nome Fantasia, CNPJ/CEI, Endereço, Cidade) referentes a alguma empresa cadastrada por ele. Para executar tal ação o usuário deve:

1. fazer login, ao inserir email e senha corretos, será redirecionado à tela com opções de

ações (Figura 23).

2. clicar em “Editar Empresa” (Figura 78).

Figura 78 – Tela de menu com sinalização do botão “Editar Empresa”



Fonte: Próprio autor, 2021.

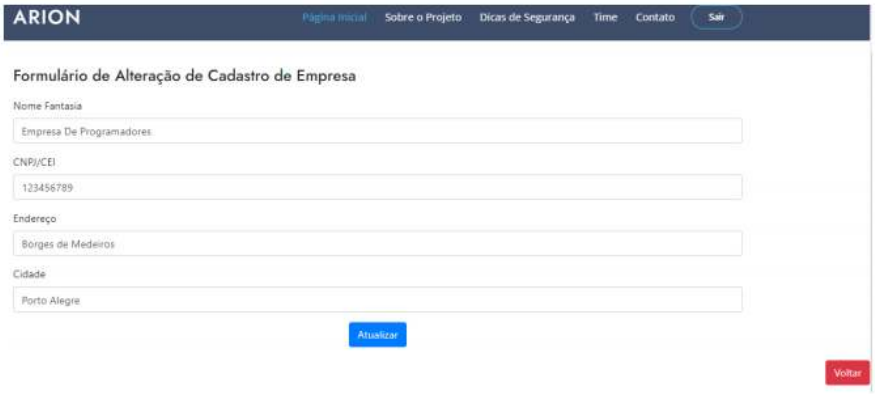
Ao clicar em “Editar Empresa” será exibida uma lista de empresa(s) cadastrada(s) pelo usuário (Figura 79), o usuário deve selecionar a empresa que deseja editar as informações, clicando em “Editar Empresa”.

Figura 79 – Tela de listas de empresas

Fonte: Próprio autor, 2021.

Ao clicar no botão “Editar Empresa” correspondente a empresa a ser editada, o usuário será redirecionado à página de edição (Figura 80), onde poderá alterar os dados que quiser.

Figura 80 – Tela de edição de empresa



Fonte: Próprio autor, 2021.

Basta alterar os campos que desejar e clicar em “Atualizar” e uma mensagem (Figura 81) será exibida. Se o usuário clicar em “Voltar”, será redirecionado a página de lista de empresas (Figura 79) e nenhum dado será alterado.

Figura 81 – Mensagem de confirmação de atualização de dados de Empresa

Fonte: Próprio autor, 2021.

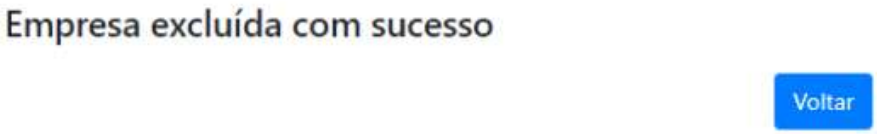
Depois de alterados os dados da empresa e exibida a mensagem, ao clicar em "Voltar", o usuário é redirecionado a página de lista de empresas (Figura 79).

Excluir Empresa - Permite ao usuário que exclua uma empresa de seu cadastro. Para executar tal ação o usuário deve:

1. fazer login, ao inserir email e senha corretos, será redirecionado à tela com opções de ações (Figura 71);
2. clicar em "Editar Empresa" (Figura 78);

Ao clicar em "Editar Empresa" será exibida uma lista de empresa(s) cadastrada(s) pelo usuário (Figura 79), o usuário deve selecionar a empresa que deseja excluir, clicando em "Excluir Empresa". Ao clicar no botão "Excluir Empresa" correspondente a empresa a ser apagada, o usuário será redirecionado à página com uma mensagem de confirmação de exclusão (Figura 82).

Figura 82 – Mensagem de confirmação de exclusão de empresa



Fonte: Próprio autor, 2021.

Depois de excluída a empresa, ao clicar em "Voltar", o usuário é redirecionado à página de lista de empresas (Figura 79).

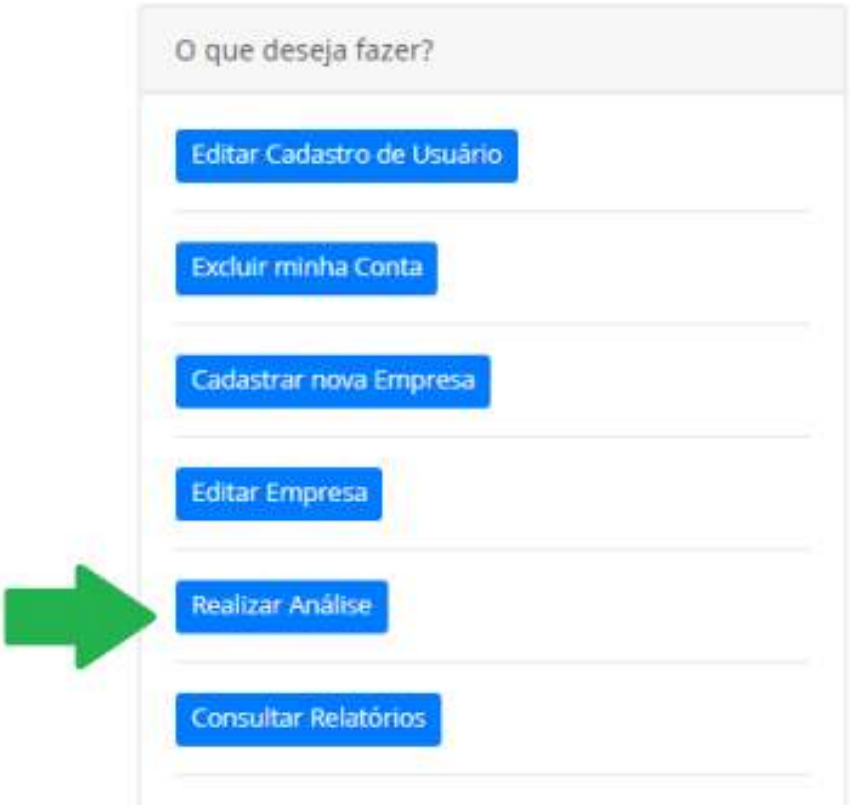
10. Realizar Análise

Permite ao usuário realizar análise de riscos. Para executar tal ação o usuário deve:

1. fazer login, ao inserir email e senha corretos, será redirecionado à tela com opções de

ações (Figura 71);
2. clicar em “Realizar Análise” (Figura 83);

Figura 83 – Tela de menu com sinalização do botão “Realizar Análise”



Fonte: Próprio autor, 2021.

Ao clicar em “Realizar Análise”, o usuário será redirecionado à página de lista de empresas cadastradas (Figura 84) e deve escolher por qual delas deseja realizar a análise.

Figura 84 – Lista de empresas para realização de análise de risco

Fonte: Próprio autor, 2021.

Caso nenhuma empresa esteja cadastrada: haverá a opção de “Cadastrar Nova Empresa”. Caso o usuário clique em voltar, ele será redirecionado à página de opções de ações (Figura 71). Caso o usuário clique em “Selecionar” significa que ele selecionou aquela empresa correspondente para realizar a Análise, e irá para a página de Processos (Figura 85).

Processo pode ser um setor, um processo de um setor, entre outros, depende de como está organizado a empresa, cabe ao usuário definir. O objetivo em implementar dessa forma foi possibilitar a análise em diferentes níveis. O gerenciamento de riscos considerando níveis detalhados permite estabelecer medidas de proteção específicas.

Figura 85 – Lista de Processos

Fonte: Próprio autor, 2021.

Caso não haja nenhum processo cadastrado (como mostrado na Figura acima), o usuário deverá cadastrar um novo, pois a análise de risco só pode ser feita a partir de um processo e ativos relacionados a ele. Ao clicar em “Cadastrar Novo Processo”, o usuário será redirecionado à página de Cadastro de Processo (Figura 86). Ao processo deve ser estabelecido uma Descrição, que é uma identificação e o valor correspondente à ele.

Os valores de processos possíveis e o que siginificam são o seguinte:

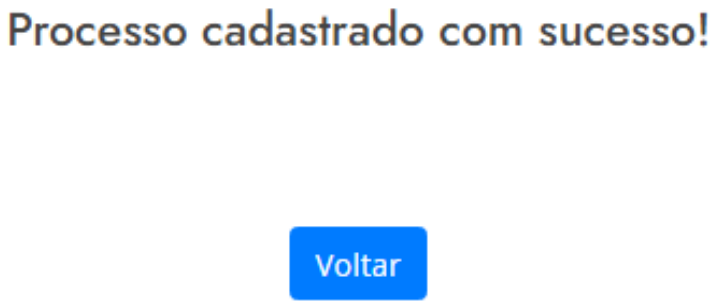
Valor de Importância	Descrição
1 - Pouco Importante	Alterações no processo não impedem o cumprimento da missão da organização.
2 - Importante	Alterações podem afetar de forma significativa o cumprimento da missão da organização.
3 - Muito Importante	Sua interrupção torna impossível cumprir a missão da organização.

Figura 86 – Página de Cadastro de processo

Fonte: Próprio autor, 2021.

Caso seja clicado em “Cancelar Cadastro” o sistema voltará à página anterior (Figura 85) e nenhum processo será cadastrado. Caso o usuário clique em “Cadastrar”, o processo será cadastrado e uma mensagem será exibida (Figura 87).

Figura 87 – Mensagem de confirmação de cadastro de processo



Fonte: Próprio autor, 2021.

Ao clicar em “Voltar” o usuário será redirecionado à página de listas de processos (Figura 88) e poderá iniciar a Análise de Riscos com aqueles já cadastrados.

Figura 88 – Página com lista de processos

Fonte: Próprio autor, 2021.

Para dar continuidade a Análise de Riscos, o usuário deverá selecionar um processo, clicando em “Selecionar Processo”, após será encaminhado à página de ativos (Figura 89). Caso clique em “Voltar”, o sistema voltará para a página de listas de Empresas cadastradas (Figura 84).

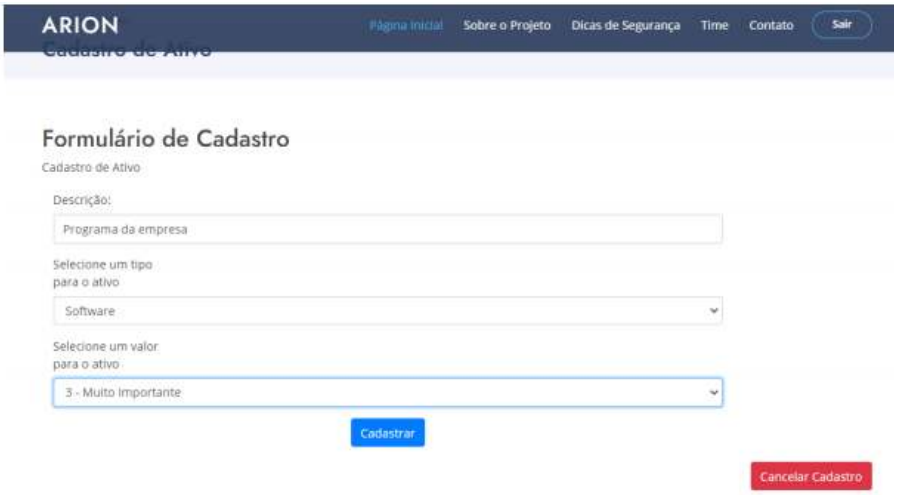
Figura 89 – Lista de ativos

Fonte: Próprio autor, 2021.

A análise de riscos é realizada por ativos, portanto é necessário que hajam ativos

cadastrados. O cadastro é simples, basta clicar em “Cadastrar Ativos” e preencher as informações de descrição (uma identificação para facilitar a identificação do ativo para o usuário), o valor e o tipo (conforme mostrado na Figura abaixo).

Figura 90 – Página de Cadastro de Ativos



Fonte: Próprio autor, 2021.

Os tipos de ativos que podem ser cadastrados (até o presente momento) são:

- Hardware;
- Software;
- Redes;
- Recursos Humanos;
- Local ou Instalações;
- Organização.

Caso tenha dúvidas sobre o que é cada tipo de ativo, consulte a definição ao final do manual.

Os valores de importância de ativos possíveis e suas descrições são as seguintes:

Valor de Importância	Descrição
1 - Pouco Importante	Ativo pode ser substituído/recriado com facilidade
2 - Importante	Ativo pode ser substituído/recriado com dificuldade
3 - Muito Importante	Ativo não pode ser substituído/recriado

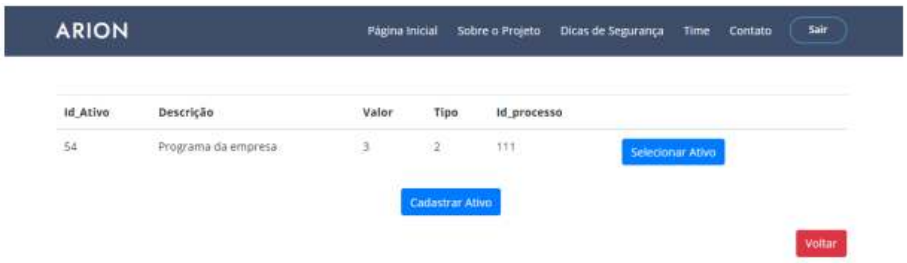
Ao clicar em “Cancelar Cadastro”, o sistema volta para a página anterior. Ao clicar em “Cadastrar”, depois de preencher os campos necessários, o usuário deverá ver uma mensagem (Figura 91).

Figura 91 – Confirmação de cadastro de ativos

Fonte: Próprio autor, 2021.

Após a exibição da mensagem, o usuário deverá clicar em “Voltar” e será redirecionado à página de lista de ativos (Figura 92), onde enfim poderá executar a análise de risco.

Figura 92 – Lista de ativos



Fonte: Próprio autor, 2021.

Para realizar a análise, o usuário deve selecionar um ativo cadastrado e clicar em “Selecionar Ativo”. Após, o sistema redireciona para uma página de check-list (Figura 93).

Figura 93 – Check-list para realização de análise de risco

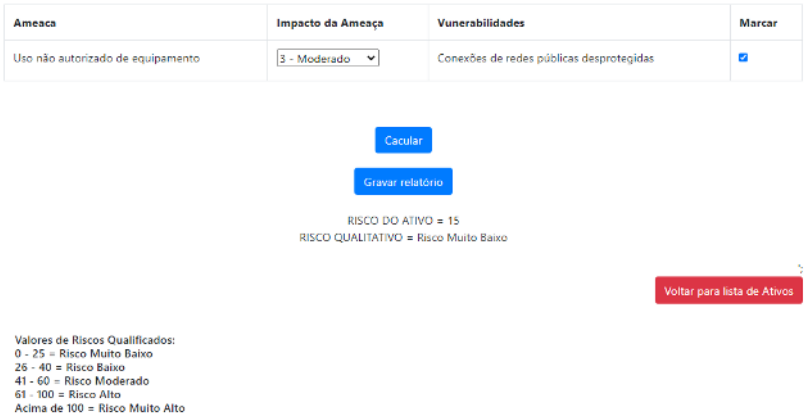
Fonte: Próprio autor, 2021.

O usuário deverá identificar as vulnerabilidades existentes marcando no check-box da coluna “Marcar”, bem como deverá dar uma nota de impacto para cada ameaça considerando o seguinte:

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

Ao final do check-list, depois de marcar as vulnerabilidades existentes e dar nota às ameaças, o usuário deve clicar em “Calcular”, após, verá o valor do risco (Figura 94).

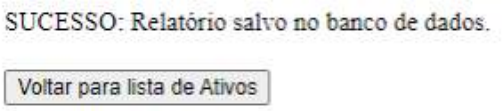
Figura 94 – Executando o cálculo do Risco



Fonte: Próprio autor, 2021.

Caso seja clicado em “Voltar para lista de Ativos” sem antes clicar em “Gravar Relatório”, este não será salvo e o sistema redireciona à página de lista de ativos (Figura 92) . Se for clicado, posteriormente, em “Gravar Relatório”, este será salvo no Banco de Dados e poderá ser consultado posteriormente. Ao clicar em “Gravar Relatório”, uma mensagem será exibida (Figura 95).

Figura 95 – Mensagem de Relatório Salvo



Fonte: Próprio autor, 2021.

Após a exibição da mensagem, ao clicar em “Voltar para a lista de ativos”, o usuário é redirecionado à página de Lista de Ativos (Figura 92).

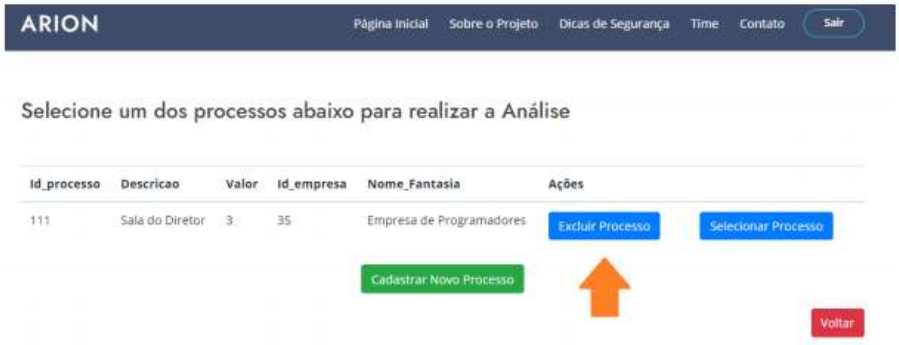
11. Excluir Processo

Permite ao usuário excluir processos de empresas. Para executar tal ação o usuário deve:

1. fazer login, ao inserir email e senha corretos, será redirecionado à tela com opções de ações (Figura 71);
2. clicar em “Realizar Análise” (Figura 83);
3. será exibida uma lista de empresas cadastradas (Figura 84);
4. selecionar a empresa a qual o processo está cadastrado clicando em “Selecionar Empresa”;
5. será exibida uma lista de processos;

6. clicar em “Excluir Processo” conforme apontado na Figura 96

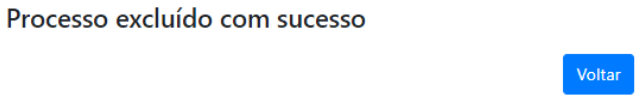
Figura 96 – Lista de Processos



Fonte: Próprio autor, 2021.

Ao clicar em “Voltar”, o usuário será redirecionado à página de lista de empresas (Figura 84). Ao clicar em “Excluir Processo” o usuário deverá ver uma mensagem de confirmação de Exclusão de Processo, como mostrado na Figura 97 .

Figura 97 – Mensagem de confirmação de exclusão de processo



Fonte: Próprio autor, 2021.

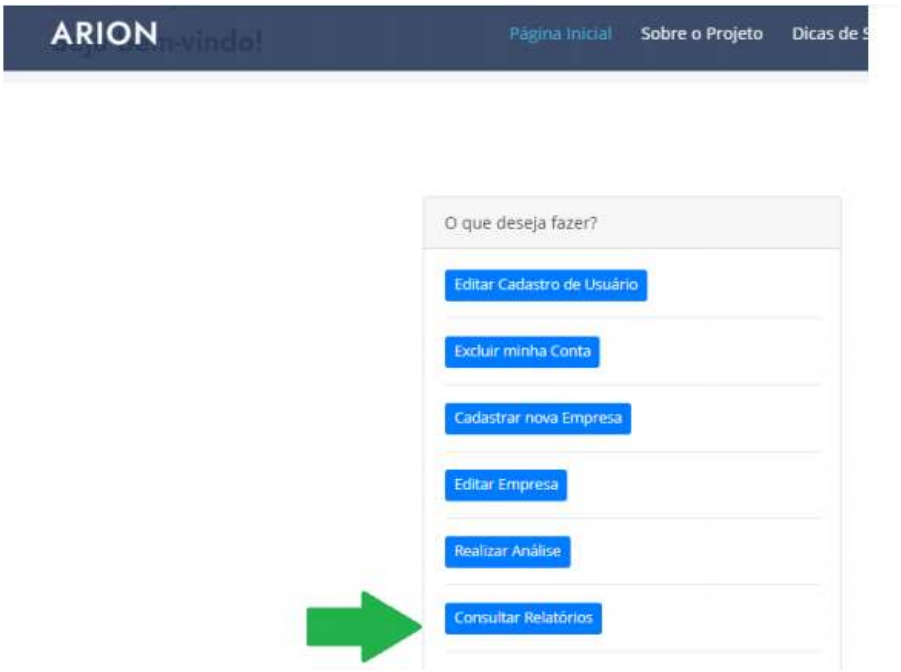
Após, ao clicar em “Voltar”, o usuário será redirecionado à página de lista de processos (Figura 96).

12. Acessar Relatórios

Permite ao usuário consultar os relatórios salvos de análise de riscos. Para executar tal ação o usuário deve:

1. fazer login, ao inserir email e senha corretos, será redirecionado à tela com opções de ações (Figura 71);
2. clicar em “Consultar Relatórios”(Figura 98);

Figura 98 – Tela de menu com sinalização do botão "Consultar Relatórios"



Fonte: Próprio autor, 2021.

Após clicar em “Consultar Relatórios”, o usuário será redirecionado à página de Relatórios (Figura 99). Nesta página, estarão disponíveis todos os relatórios salvos de todas as empresas e processos cadastrados pelo usuário.

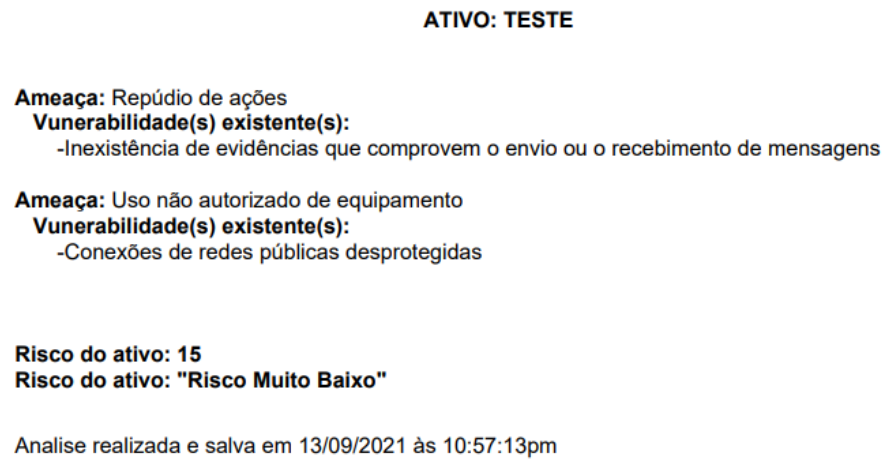
Os relatórios podem ser ordenados em ordem crescente ou decrescente em quaisquer das colunas: Empresa, Processo, Ativo, Tipo de Ativo, Data/hora. Para ordenar basta clicar em uma coluna. Recomenda-se que o usuário deixe ordenado em ordem decrescente considerando a coluna Risco, dessa forma, os primeiros relatórios serão aqueles com o valor de risco mais alto, que requerem uma medidas protetivas, respostas mais urgentes.

Figura 99 – Página de Relatórios

Fonte: Próprio autor, 2021.

Ao clicar em “Baixar Relatório”, será baixado o arquivo em PDF. O arquivo estará no formato demonstrado abaixo:

Figura 100 – Relatório



Fonte: Próprio autor, 2021.

O Relatório é formado pelas seguintes informações:

- Descrição do Ativo;
- Ameaças e suas vulnerabilidades marcadas (através do check box) como existentes;
- Valor Quantitativo do Risco;
- Valor Qualitativo do Risco;
- Data e horário em que o relatório foi salvo.

No relatório aparecem apenas as ameaças em que pelo menos uma vulnerabilidade foi marcada como existente.
O objetivo é que o usuário tenha acesso àquelas vulnerabilidades existentes e tome medidas para que aquelas deixem de existir, o que diminuirá o nível de risco.

13. Trocar e-mail e/ou Senha

Permite ao usuário trocar os dados de acesso ao sistema. Para executar tal ação o usuário deve:
1. Repetir as ações mencionadas em “Editar Cadastro de Usuário” e digitar o novo email e/ou senha.

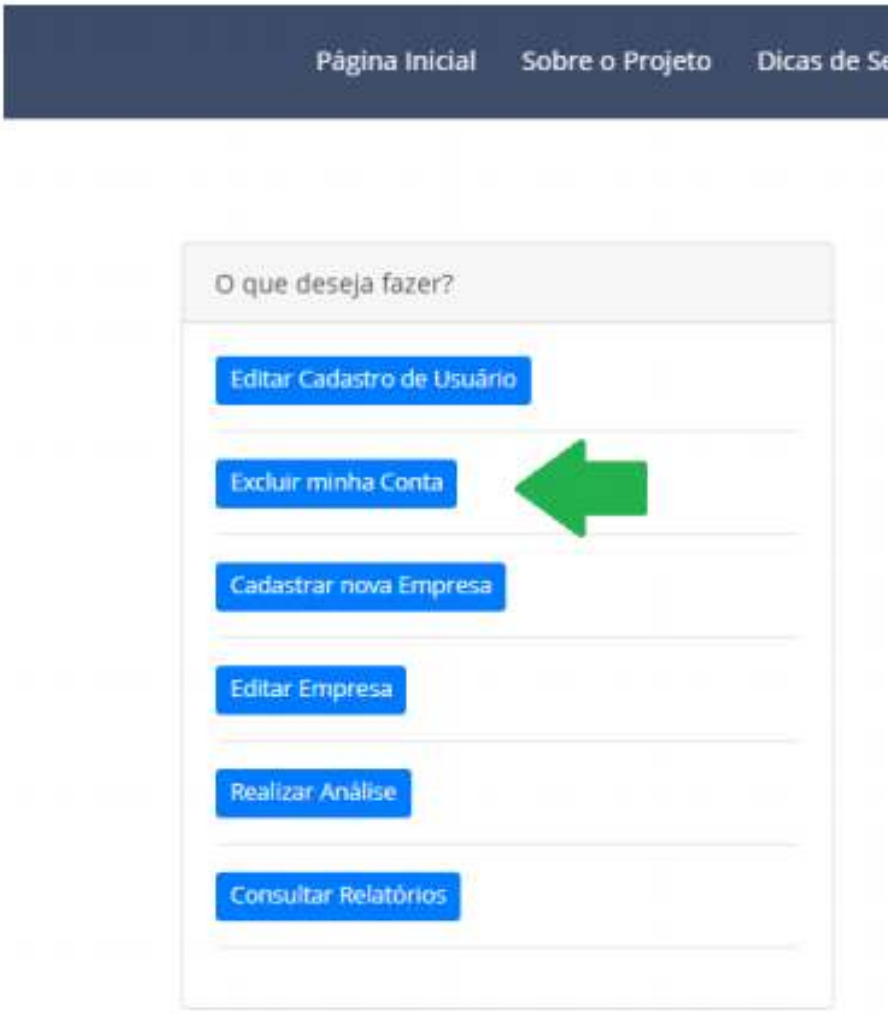
14. Excluir Conta de Usuário

Permite ao usuário excluir sua conta no ARION, essa ação é permanente e irreversível. Todos os dados referentes à dados do usuário, empresas, processos,ativos, relatórios de

análises serão excluídos! Para executar tal ação o usuário deve:

1. fazer login, ao inserir email e senha corretos, será redirecionado à tela com opções de ações (Figura 71);
2. clicar em “Excluir minha Conta” (Figura 101).

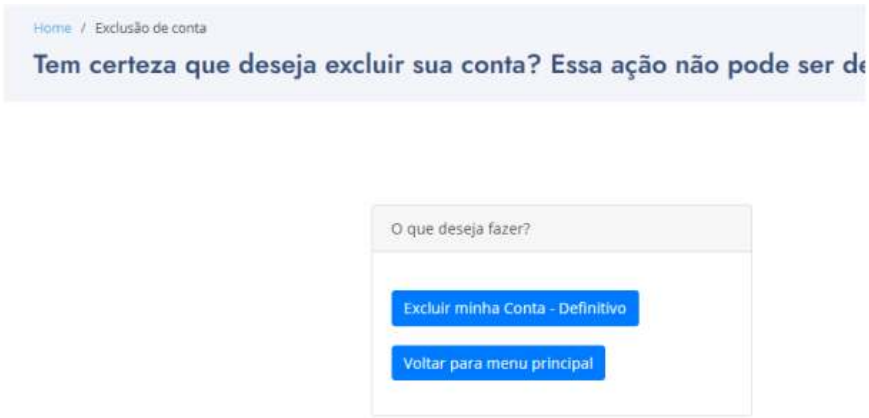
Figura 101 – Tela de menu com sinalização do botão "Excluir minha Conta"



Fonte: Próprio autor, 2021.

Após, será exibida uma mensagem perguntando ao usuário se realmente deseja excluir sua conta (Figura 102).

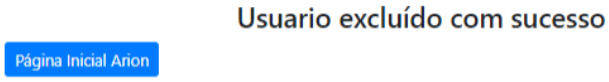
Figura 102 – Tela de Confirmação de Exclusão de Conta



Fonte: Próprio autor, 2021.

Nesta tela, ao clicar em “Voltar para o Menu Principal”, o sistema redireciona à página anterior (Menu de Ações) e nada é excluído. Ao clicar em “Excluir minha Conta - Definitivo”, o ARION exibe uma mensagem de confirmação de exclusão de conta de usuário (Figura 103).

Figura 103 – Mensagem de confirmação de exclusão de conta de usuário



Fonte: Próprio autor, 2021.

Após, a única alternativa no ARION, é clicar em “Página Inicial Arion” e o sistema redireciona à página inicial.

Definição dos tipos de Ativos (retirado da ISO/IEC 27005 de 2011):

Hardware: O tipo hardware compreende os elementos físicos que dão suporte aos processos.

Equipamento de processamento de dados (ativo): Equipamento automático de processamento de dados incluindo os itens necessários para sua operação independente.

Equipamento móvel: Computadores portáteis. Exemplos: laptops, agendas eletrônicas (Personal Digital Assistants - PDAs).

Equipamento fixo: Computadores utilizados nas instalações da organização. Exemplos: servidores, microcomputadores utilizados como estações de trabalho.

Periféricos de processamento: Equipamento conectado a um computador através de uma

porta de comunicação (serial, paralela etc.) para a entrada, o transporte ou a transmissão de dados. Exemplos: impressoras, unidades de disco removível.

Mídia de dados (passiva): Este tipo compreende a mídia para o armazenamento de dados ou funções.

Mídia eletrônica: Uma mídia com informações que pode ser conectada a um computador ou a uma rede de computadores para o armazenamento de dados. Apesar de seu tamanho reduzido, esse tipo de mídia pode conter um grande volume de dados e pode ser utilizada com equipamentos computadorizados comuns. Exemplos: disco flexível, CD ROM, cartucho de “back-up”, unidade de disco removível, cartão de memória, fita.

Outros tipos de mídia: Mídia estática, não-eletrônica, contendo dados. Exemplos: papel, slides, transparências, documentação, fax.

Software: O tipo software compreende todos os programas que contribuem para a operação de um sistema de processamento de dados. Sistema operacional: Este tipo inclui os programas que fornecem as operações básicas de um computador, a partir das quais os outros programas (serviços e aplicações) são executados. Nele encontramos um núcleo ("kernel") e as funções ou serviços básicos. Dependendo de sua arquitetura, um sistema operacional pode ser monolítico ou formado por um "micro-kernel"e um conjunto de serviços do sistema. Os principais elementos de um sistema operacional são os serviços de gerenciamento do equipamento (CPU, memória, disco e interfaces de rede), os de gerenciamento de tarefas ou processos e os serviços de gerenciamento de direitos de usuário.

Software de serviço, manutenção ou administração: Software caracterizado pelo fato de servir como complemento dos serviços do sistema operacional e não estar diretamente a serviço dos usuários ou aplicações (apesar de ser, normalmente, essencial e até mesmo indispensável para a operação do sistema de informação como um todo).

Software de pacote ou de prateleira: Software de pacote ou software-padrão é aquele que é comercializado como um produto completo (e não como um serviço de desenvolvimento específico) com mídia, versão e manutenção. Ele fornece serviços para usuários e aplicações, mas não é personalizado ou específico como, por exemplo, aplicações de negócio o são. Exemplos: software para o gerenciamento de bases de dados, software de mensagens eletrônicas, "groupware"(software de gerenciamento de fluxo de trabalho), software de diretório, servidores web etc.

Aplicações de negócio padronizadas: Este tipo de software comercial é projetado para

dar aos usuários acesso direto a serviços e funções que eles demandam de seus sistemas de informação, em função das áreas em que atuam profissionalmente. Existe uma gama enorme, teoricamente ilimitada, de campos de atuação. Exemplos: software de contabilidade, software para o controle de maquinário, software para administração do relacionamento com clientes, software para gestão de competências dos recursos humanos, software administrativo etc.

Aplicações de negócio específicas: Vários aspectos desse tipo de software (principalmente o suporte, a manutenção e a atualização de versões etc.) são desenvolvidos especificamente para dar aos usuários acesso direto aos serviços e funções que eles demandam de seus sistemas de informação. Existe uma gama enorme, teoricamente ilimitada, de áreas em que esse tipo de software é encontrado. Exemplos: Administração das notas fiscais de clientes para as operadoras de telecomunicação, aplicação para monitoramento em tempo real do lançamento de foguetes.

Rede: O tipo rede compreende os dispositivos de telecomunicação utilizados para interconectar computadores ou quaisquer outros elementos remotos de um sistema de informação.

O meio físico e a infraestrutura: Os equipamentos de comunicação ou de telecomunicação são identificados principalmente pelas suas características físicas e técnicas (ponto-a-ponto, de "broadcast") e pelos protocolos de comunicação utilizados (na camada de enlace de dados ou na camada de rede - níveis 2 e 3 do modelo OSI de 7 camadas). Exemplos: Rede telefônica pública comutada ("Public Switching Telephone Network"ou PSTN), "Ethernet", "GigabitEthernet", Linha digital assimétrica para assinante ("Asymmetric Digital Subscriber Line"ou ADSL), especificações de protocolo para comunicação sem fio (por exemplo, o WiFi 802.11), "Bluetooth", "FireWire".

Pontes ("relays") passivas ou ativas: Este subtipo não compreende os dispositivos que ficam nas extremidades lógicas da conexão (na perspectiva do sistema de informação), mas sim os que são intermediários no processo de comunicação, repassando o tráfego. Pontes são caracterizadas pelos protocolos de comunicação de rede com os quais funcionam. Além da função básica de repasse do tráfego, elas frequentemente são dotadas da capacidade de roteamento e/ou de serviços de filtragem, com o emprego de comutadores de comunicação ("switches") e roteadores com filtros. Com frequência, elas podem ser administradas remotamente e são normalmente capazes de gerar arquivos de auditoria ("logs"). Exemplos: pontes ("bridges"), roteadores, "hubs", comutadores

("switches"), centrais telefônicas automáticas.

Interface de Comunicação: As interfaces de comunicação conectadas às unidades de processamento são, porém, caracterizadas pela mídia e protocolos com os quais funcionam; pelos serviços de filtragem, de auditoria e de alerta instalados, se houver, e por suas funcionalidades; e pela possibilidade e requisitos de administração remota. Exemplos: Serviço Geral de Pacotes por Rádio ("General Packet Radio Service"ou GPRS), adaptador "Ethernet".

Recursos humanos: O tipo recursos humanos compreende todas as classes de pessoas envolvidas com os sistemas de informação.

Tomador de decisão: Tomadores de decisão são aqueles responsáveis pelos ativos primários (informação e processos) e os gestores da organização ou, se for o caso, de um projeto específico. Exemplos: alta direção, líderes de projeto.

Usuários: São recursos humanos que manipulam material sensível no curso de suas atividades e que, portanto, possuem uma responsabilidade especial nesse contexto. Eles podem ter direitos especiais de acesso aos sistemas de informação para desempenhar suas atividades rotineiras. Exemplos: gestores da área de recursos humanos, gerentes financeiros, gestores dos riscos.

Pessoal de produção/manutenção: Estes são os recursos humanos responsáveis pela operação e manutenção dos sistemas de informação. Eles possuem direitos especiais de acesso aos sistemas de informação para desempenhar suas atividades rotineiras. Exemplos: administradores de sistema; administradores de dados; operadores de “backup”, “Help Desk” e de instalação de aplicativos; especialistas em segurança.

Desenvolvedores: São responsáveis pelo desenvolvimento dos sistemas aplicativos da organização. Eles possuem acesso com alto privilégio a uma parte dos sistemas de informação, mas não interferem com os dados de produção. Exemplos: Desenvolvedores de aplicações de negócio.

Instalações físicas: O tipo instalações compreende os lugares onde encontramos o escopo (ou parte dele) e os meios físicos necessários para as operações nele contidas.

Ambiente externo: Compreende as localidades em que as medidas de segurança de uma organização não podem ser aplicadas. Exemplos: os lares das pessoas, as instalações de outra organização, o ambiente externo ao local da organização (áreas urbanas, zonas perigosas).

Edificações: Esse lugar é limitado pelo perímetro externo da organização, isto é por aquilo que fica em contato direto com o exterior. Isso pode ser uma linha de proteção física formada por barreiras ou por mecanismos de vigilância ao redor dos prédios. Exemplos: estabelecimentos, prédios.
Zona: Uma zona é limitada por linhas de proteção física que criam partições dentro das instalações da organização. É obtida por meio da criação de barreiras físicas ao redor das áreas com a infraestrutura de processamento de informações da organização. Exemplos: escritórios, áreas de acesso restrito, zonas de segurança.
Serviços essenciais: Todos os serviços necessários para que os equipamentos da organização possam operar normalmente.
Comunicação: Serviços de telecomunicação e equipamento fornecido por uma operadora. Exemplos: linha telefônica, PABX, redes internas de telefonia.
Serviços de Infraestrutura: Serviços e os meios (alimentação e fiação) necessários para o fornecimento de energia elétrica aos equipamentos de tecnologia da informação e aos seus periféricos. Exemplos: fonte de alimentação de baixa tensão, inversor, central de circuitos elétricos; Fornecimento de água - Saneamento e esgoto. Serviços e os meios (equipamento, controle) para refrigeração e purificação do ar. Exemplos: tubulação de água refrigerada, ar condicionados.

Organização: O tipo organização descreve a estrutura da organização, compreendendo as hierarquias de pessoas voltadas para a execução de uma tarefa e os procedimentos que controlam essas hierarquias.
Autoridades: Essas são as organizações de onde a organização em questão obtém sua autoridade . Elas podem ser legalmente afiliadas ou ter um caráter mais externo. Isso impõe restrições à organização em questão com relação a regulamentos, decisões e ações. Exemplos: corpo administrativo, sede da organização.
A estrutura da organização: Compreende os vários ramos da organização, incluindo suas atividades multidisciplinares, sob controle de sua direção. Exemplos: gestão de recursos humanos, gestão te TI, gestão de compras, gerenciamento de unidade de negócio, serviço de segurança predial, serviço de combate a incêndios, gerenciamento da auditoria.
Organização de projeto ou serviço: Compreende a organização montada para um projeto ou serviço específico. Exemplos: projeto de desenvolvimento de uma nova aplicação, projeto de migração de sistema de informação.
Subcontratados / Fornecedores / Fabricantes: Essas são organizações que fornecem

serviços ou recursos para a organização em questão segundo os termos de um contrato. Exemplos: empresa de gerenciamento de instalações, empresa prestadora de serviços terceirizados, empresas de consultoria.