BRUNO APOLINÁRIO WOLLINGER
CLAUDIO MANUEL ANDRADE DA SILVA
MARCELO VICTOR CARDOSO SOUSA
PAULO VINÍCIUS DE SOUZA MAVALLI

RIPE: Aplicação web para análise de maturidade do processo de análise de risco

São Caetano do Sul/São Paulo
2020

BRUNO APOLINÁRIO WOLLINGER
CLAUDIO MANUEL ANDRADE DA SILVA
MARCELO VICTOR CARDOSO SOUSA
PAULO VINICIUS DE SOUZA MAVALLI

RIPE: Aplicação web para análise de maturidade do processo de análise de risco

Trabalho de conclusão de curso apresentado à faculdade de tecnologia de São Caetano do Sul, sob a orientação da professora Me. Edna Mataruco Duarte, como requisito parcial para a obtenção do diploma de graduação no curso de Tecnólogo em Segurança da Informação.

São Caetano do Sul/São Paulo
2020

RESUMO

APOLINÁRIO, Bruno. ANDRADE, Claudio Manuel. CARDOSO, Marcelo Victor. MAVALLI, Paulo Vinicius. RIPE: Aplicação web para análise de maturidade do processo de análise de risco. 62 f. Trabalho de Graduação – Faculdade de Tecnologia de São Caetano do Sul, 2020.

Nos últimos tempos a Tecnologia da Informação (TI) assumiu um papel fundamental deixando de exercer uma função de prestação de suporte e tornando-se essencial na estratégia dos negócios das organizações. Neste contexto, passou-se a exigir a qualidade dos serviços fornecidos e a segurança nos processos relacionados a integridade desse conjunto de processos, além de controles que contribuam para agregar valor ao negócio. Atualmente o *framework* COBIT tem grande aceitação por parte dos gestores de TI das organizações, por fornecer um vocabulário comum e controles que poderão contribuir com os processos de TI de uma organização. Dentre as estratégias apresentadas pelo COBIT há o nível de maturidade. Estes níveis servem para avaliar o estado atual de uma área ou de um processo específico, com base em um conjunto de critérios. Diante disto, o objetivo deste trabalho de conclusão de curso é desenvolver uma aplicação capaz de promover o diagnóstico do nível de maturidade de uma Gestão de Análise de Risco de uma organização. A pesquisa realizada é de natureza qualitativa e utiliza-se de uma estratégia documental, análise das normas ISO/IEC 27001, ISO/IEC 27005 e do manual de boas práticas COBIT, que são necessários para determinar os requisitos para a conformidade da ferramenta construída. A partir dos testes e validações realizados durante o desenvolvimento deste trabalho, pode-se afirmar que a ferramenta "RIPE" possui plenas condições de informar o nível de maturidade e possíveis ações para otimizar um processo tão relevante no contexto de segurança de uma organização como a análise de risco.

PALAVRAS-CHAVE: COBIT 5.0; ANÁLISE DE RISCO; ISO/IEC 27001; ISO/IEC 27005.

ABSTRACT

APOLINÁRIO, Bruno. ANDRADE, Claudio Manuel. CARDOSO, Marcelo Victor. MAVALLI, Paulo Vinicius. RIPE: Web application for maturity analysis of the risk analysis process. 62 p. Graduation Work - Faculty of Technology of São Caetano do Sul, 2020.

In recent times, Information Technology (IT) has taken on a fundamental role, ceasing to exercise a function of providing support and making it essential in the business strategy of organizations. In this context, it started to demand the quality of the services used and the security in the processes related to the integrity of this set of processes, in addition to controls that contribute to add value to the business. Nowadays, the COBIT framework accepts most of the IT managers of organizations, providing a common vocabulary and controls that can contribute to an organization's IT processes. Among the strategies applied by COBIT, there is the maturity level. These levels are useful for assessing the current state of an area or a specific process, based on a set of requirements. Therefore, the objective of this course conclusion work is to develop an application capable of promoting the diagnosis of an organization's Risk Analysis maturity level. A research carried out is of a qualitative nature and uses a documentary strategy, analysis of the ISO / IEC 27001, ISO / IEC 27005 standards and COBIT manual of good practices, which are used to determine the requirements for use in the form used. From the tests and validations performed during the development of this work, it can be registered that the "RIPE" tool has indicators of maturity level conditions and possible actions to optimize a process as relevant in the context of an organization's security as the analysis risk.

KEY WORDS: COBIT 5.0; RISK ANALYSIS; ISO / IEC 27001; ISO / IEC 27005.

LISTA DE FIGURAS

FIGURA 1 – COBIT 5: Categories 21
FIGURA 2 – COBIT 5 Process Capability Model ……..... 22
FIGURA 3 – Processo de gestão de riscos de segurança da informação 34
FIGURA 4 – A atividade de tratamento do risco 35
FIGURA 5 – Modelo cliente-servidor 39
FIGURA 6 – Modelo de avaliação RIPE..... 42
FIGURA 7 – Tela de apresentação..... 54
FIGURA 8 – Tela de login..... 55
FIGURA 9 – Tela de exibição do questionário..... 55
FIGURA 10 – Tela de exibição do questionário..... 56

LISTA DE QUADROS

QUADRO 1 – Levantamento de requisitos 38
QUADRO 2 – Níveis de capacidade, atributos de processos e escala de medição... 43
QUADRO 3 – Bloco de perguntas gerais sobre a organização 45
QUADRO 4 – Bloco de perguntas conceituando riscos 45
QUADRO 5 – Bloco de perguntas sobre o processo de análise de riscos 46
QUADRO 6 – Bloco de perguntas sobre priorização dos riscos 47
QUADRO 7 – Bloco de perguntas sobre sistemas de informação 47
QUADRO 8 – Bloco de perguntas sobre segurança da informação 49
QUADRO 9 – Bloco de perguntas sobre segurança da informação 49
QUADRO 10 – Bloco de perguntas sobre a área de gestão da empresa 50
QUADRO 11 – Bloco de perguntas sobre a gestão dos ativos da organização 52
QUADRO 12 – Bloco de perguntas sobre a gestão de continuidade de negócios da empresa..... 52
QUADRO 13 – Bloco de perguntas sobre a gestão de incidentes de segurança da informação..... 53

LISTA DE ABREVIATURAS E SIGLAS

ABNT: Associação Brasileira de Normas Técnicas
COBIT: Control Objectives for Information and related Technology
IEC: International Electrotechnical Commission
ISO: International Organization for Standardization
SGSI: Sistema de Gestão de Segurança da Informação
TI: Tecnologia da Informação

SUMÁRIO

INTRODUÇÃO 9
1 REFERENCIAL TEÓRICO 12
1.1. Capítulo 1: SEGURANÇA DA INFORMAÇÃO.... 12
1.2. Capítulo 2: COBIT 19
1.3. Capítulo 3: NORMAS E PADRÕES DE SEGURANÇA 26
1.4. Capítulo 4: ISO/IEC 27001 27
1.5. Capítulo 5: ISO/IEC 27002 29
1.6. Capítulo 6: ISO/IEC 27005 31
2. RIPE: APLICAÇÃO WEB PARA ANÁLISE DE MATURIDADE DO PROCESSO DE ANÁLISE DE RISCO 37
3. CONCLUSÃO..... 57
4 REFERÊNCIAS BIBLIOGRÁFICAS 58

INTRODUÇÃO

Para o *IT Governance Institute* (2003, p. 10), a governança de tecnologia da informação pode ser definida como:

> Responsabilidade do conselho de diretores e da gerência executiva. Ela é parte integrante da governança corporativa e consiste na liderança, estruturas organizacionais e processos que garantem que a área de TI da organização sustente e estenda as estratégias e objetivos da organização.

No mundo dos negócios a governança bem estruturada é a base para qualquer empreendimento bem sucedido. Para isso, necessário seguir um padrão para obtenção de um melhor controle do que será realizado. Assim, as empresas procuram seguir padrões, normas e boas práticas já consolidadas no mercado (SFALSIN, 2018). A conformidade com normas e boas práticas podem ajudar a gerar melhorias, tais como: melhor relacionamento entre empresa e cliente, entre empresas e domínio, e controle da organização em relação as suas ações.

A tecnologia está cada vez mais enraizada nas organizações. Em uma realidade onde as atividades tornam-se dependentes das tecnologias, a gestão de TI torna-se parte fundamental para o sucesso de todas as outras áreas de um empreendimento.

Nesse contexto, algumas organizações pelo mundo utilizam o *Control Objectives for Information and related Technology* (COBIT), que se trata de um *framework* focado na governança de TI, mantido pela *Information Systems Audit and Control Association* (ISACA), o qual gera, entre outras, certificações de segurança, auditoria, governança e risco. Segundo o ISACA (2012) é possível ter um controle rígido sobre os processos de TI da organização ao ponto de evitar o desperdício de recursos e obter maior objetividade e precisão na realização dos processos operacionais.

Dentre as estratégias apresentadas pelo COBIT, há os níveis de maturidade, os quais servem para avaliar o estado atual de uma área ou de um processo específico, com base em um conjunto de critérios. Diante do exposto, este trabalho de conclusão de curso tem como objetivo geral desenvolver uma aplicação capaz de promover o

diagnóstico do nível de maturidade de uma Gestão de Análise de Risco de uma organização.

No cenário atual observamos diversas instituições que desconhecem ou carecem de conformidade com normas ou boas práticas relacionadas a Análise de Riscos. Em muitos casos a gestão é realizada mesmo que utilizando os conhecimentos básicos de algum funcionário da área de TI. Desta forma, busca mitigar os possíveis riscos que podem acontecer dentro de uma organização como um todo. No entanto, essa atitude, além de deixar a empresa muito vulnerável a ataques, é restrita ao que o funcionário considera que é importante manter seguro, podendo deixar muitas áreas da empresa sem a devida proteção.

A importância de uma eficiente execução da análise de risco é enorme dentro de uma organização, pois evidencia os processos importantes que precisam de proteção e cuidado para mitigar o máximo os riscos envolvidos nos ativos relacionados ao processo. Sabendo quais ativos são mais críticos para o funcionamento da empresa, se torna mais fácil e eficaz o planejamento para conseguir desenvolver e implementar um melhor controle e segurança.

Diante deste cenário, a hipótese apresentada nesse trabalho de conclusão de curso é que o desenvolvimento de uma ferramenta para analisar o nível de maturidade do processo de Análise de Risco poderá ser capaz de gerar melhorias contínuas e relatórios para sua manutenção em uma organização. A ferramenta poderá contribuir com empresas de médio e pequeno porte a se adequar e assegurar que a gestão de análise de riscos está em conformidade com a norma ISO/IEC 27005, além de evidenciar melhorias e otimização de todo o processo.

Há diversas empresas que não estão em conformidade com normas que auxiliam, padronizam e aplicam métodos de boas práticas no âmbito de governança de TI.

Este projeto tem como direcionamento principal o processo de análise de riscos, e visa empresas que carecem de conformidade e segurança, algo que é de extrema importância para qualquer organização. A ferramenta também pode ser utilizada por qualquer pessoa que busca contribuir com uma cultura organizacional voltada para segurança da informação, como plano de fundo a norma ISO/IEC 27001,

base da segurança da informação, a norma ISO/IEC 27005, referência na gestão de risco em tecnologia da informação e o COBIT, framework conhecido por expor a maturidade dos processos de TI nas organizações.

Diante disso, a pesquisa que será realizada é de natureza qualitativa e utiliza-se de uma estratégia documental, análise das normas ISO/IEC 27001, ISO/IEC 27005 e do manual de boas práticas COBIT, que são necessários para determinar os requisitos para a conformidade da ferramenta a ser construída, mostrando sua importância dentro da organização de acordo as normas, fornecendo o nível de maturidade baseado no *framework* COBIT e quais os pontos de controle e recomendações para otimização desse processo e alertando a organização com as possíveis vulnerabilidades e deficiências existentes na gestão da análise de riscos.

Assim, este trabalho está estruturado em 06 capítulos, começando com a introdução que apresenta o objetivo, justificativa, metodologia e hipótese. Em seguida, O Capítulo 1, que trata da importância da informação para as empresas assim como uma breve estruturação do cenário de segurança da informação atual. O Capítulo 2 aborda os objetivos do *framework* COBIT, assim como a sua importância para a maturidade nos processos que conduzem a operação de uma organização e apresenta a diferença entre a versão 4.1 para a versão 5, utilizada neste trabalho. O Capítulo 3 estabelece o fundamento de norma, seus objetivos e benefícios de sua implantação. O Capítulo 4 introduz brevemente uma visão sobre a ISO/IEC 27001 a respeito dos Sistemas de Gestão de Segurança da Informação e exemplifica sua abordagem no intuito de estabelecer, implementar, operar, monitorar e analisar a segurança da informação dentro de uma empresa. O Capítulo 5 discorre sobre a ISO/IEC 27002 quanto às práticas de controle de segurança da informação e sua função de guiar as operações da organização. O Capítulo 6 aborda a ISO/IEC 27005 sobre a gestão de risco da segurança da informação e sobre as prioridades na proteção de ativos.

1.1. SEGURANÇA DA INFORMAÇÃO

Segundo o conceito exposto por Ramos (2014), a informação hoje tem enorme relevância para a tomada de decisão e, portanto, para qualquer ato de gestão. Atualmente, o volume de informação sofre um crescimento exponencial. Não há limitações de acesso para a grande massa de dados, a informação torna-se cada vez mais acessível. Uma consequência desta realidade é a exigência de organizar essa mesma quantidade de dados gerados. Além de prover proteção a dados sigilosos, a fim de limitar acesso e assegurar integridade.

Tamanha a sua importância, atualmente a informação tornou-se um pilar determinante para a sobrevivência e maturidade de uma organização. “A informação é um ativo da organização, talvez o mais precioso, um bem que deve ser tão protegido quanto os bens físicos, tendo em vista sua importância para a própria existência da organização” (MANOEL, 2014, p.3).

De acordo com Nonata (2008, p.2):

> Informação compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano. Trata-se de tudo aquilo que permite a aquisição de conhecimento. Nesse sentido, a informação digital é um dos principais, senão o mais importante, produto da era atual. Ela pode ser manipulada e visualizada de diversas maneiras. Assim, à medida que a informação digital circula pelos mais variados ambientes, percorrendo diversos fluxos de trabalho, ela pode ser armazenada para os mais variados fins, possibilitando-a ser lida, modificada ou até mesmo apagada.

Para ISO/IEC 17799 (2005), proteger a informação na perspectiva de Segurança da Informação compreende os aspectos de:

a) **Confidencialidade**: propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;
b) **Integridade:** propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação,

incluindo controle de mudanças e garantia do seu ciclo de vida (Corrente, intermediária e permanente)[1];

c) **Disponibilidade:** propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação;

d) **Autenticidade:** propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.

Ainda, conforme definição na norma ISO/IEC 17799 (2005), a segurança da informação é a forma encontrada pelas organizações para proteger os seus dados, através de regras e controles rígidos, estabelecidos, implementados e monitorados constantemente. A norma inicialmente foi elaborada em 11 seções, a fim de definir e categorizar a segurança da informação, em:

a) Política de Segurança da Informação;
b) Organizando a Segurança da Informação;
c) Gestão de Ativos;
d) Segurança em Recursos Humanos;
e) Segurança Física e do Ambiente;
f) Gestão das Operações e Comunicações;
g) Controle de Acesso;
h) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
i) Gestão de Incidentes de Segurança da Informação;
j) Gestão da Continuidade do Negócio;
k) Conformidade.

O trabalho de conclusão aqui proposto, visa intermediar a gestão de riscos de uma organização com base em segurança da informação, conceitos e definições de normas relacionadas a análise de risco e governança de TI.

[1] Corrente: se refere a fase em que a informação está ligada aos objetivos imediatos para que foi coletada; Intermediária: informação originária da informação corrente que não é acessada com a mesma frequência do que a corrente; Permanente: informação que não é mais utilizada e é armazenada de acordo com requisitos legais.

Segundo Guedes (2016, p.51) ao englobar a gestão da segurança da informação, a gestão de riscos tem como principais desafios:

a) Proteger um dos principais ativos da organização;
b) Implementar e gerir controles que tenham como foco principal os objetivos do negócio;
c) Reputação da empresa ou marca;
d) Promover ações corretivas e preventivas de forma eficiente;
e) Garantir o cumprimento de regulamentações;
f) Definir os processos de gestão da Segurança da Informação.

Entre as vantagens de investir na gestão de riscos voltada para a segurança da informação estão a priorização das ações de acordo com a necessidade e os objetivos da empresa, assim como a utilização de métricas e indicadores de resultados.

Segundo a ISO/IEC 27002 (2013), o ativo “é qualquer coisa que tenha valor para a organização”. A Gestão de Ativos, portanto, significa proteger e manter os ativos da organização. Os ativos ainda devem ser classificados conforme o nível de proteção recomendado para cada um deles, e seguir regras documentadas, que definem qual o tipo de uso é permitido. Dessa forma, é necessária uma proteção adequada para o mesmo. A informação pode existir em diversas formas, entretanto, em qualquer que seja a forma de apresentação ou o meio através do qual é compartilhada ou armazenada, é de suma importância que ela esteja sempre segura.

Considerar informação como um ativo não explica o sentido da palavra informação, apenas exalta um de seus atributos. Ainda falta uma definição para o termo informação. A palavra informação é derivativa da palavra informar, a qual vem do latim *“informare”* (FERREIRA, 1996), que significa dar forma, criar, apresentar, colocar em ordem. Observa-se que ao buscar o conceito de informação em sua origem latina, o dicionário da língua portuguesa estabelece a funcionalidade do termo.

Oliveira (2001) afirma que a informação é um recurso vital para a empresa e integra, quando devidamente estruturada, os diversos subsistemas e, portanto, as

funções das várias unidades organizacionais da empresa. No dicionário online *priberam*[2], informação consiste no ato ou efeito de informar, e também em forma de notícia, seja ela dada ou recebida.

Desta forma, as organizações precisam saber como usar a informação e tirar o melhor proveito dela para se colocarem em posição competitiva, acompanhando os novos tempos, mudando suas características gerenciais e estratégicas e com elas todo o seu capital intelectual. A informação deve ser tratada como qualquer outro produto que esteja disponível para consumo. Ela deve ser desejada, para ser necessária. Para ser necessária, deve ser útil. E como tudo que é útil, precisa ser protegida.

A proteção está associada a segurança. O termo segurança apresenta diversidades em seu significado, sendo objeto dos mais variados estudos. Em Dicionário da Língua Portuguesa, a palavra segurança é definida com os seguintes significados:

> 1) Ato ou efeito de segurar; 2) Estado, qualidade ou condição de seguro; 3) Condição daquele ou daquilo em que se pode confiar; 4)Certeza, firmeza, convicção; 5) Confiança em si mesmo, auto confiança; 6) Caução, garantia, seguro; 7) Protesto, afirmação; 8)Prenhes das fêmeas dos quadrúpedes; 9) Pessoa encarregada da segurança pessoal de alguém ou de empresa, guarda-costas. (FERREIRA, 1996, p. 1563)

Entende-se que a informação é todo o dado que possui valor para a pessoa ou organização, sendo assim ela é um bem e deve ser protegida, portanto, subentende-se que a informação é um importante patrimônio, sendo o ponto crucial para sobrevivência das organizações. Por consequência, informação pode ser entendida como qualquer coisa que tenha valor para a organização. Este conceito associado ao que foi desenvolvido por Siqueira (2005), a partir da teoria de Shannon e Waever (1975), leva ao entendimento da informação como estrutura de um sistema. Vale lembrar que Fernandes (2008) considera que sistema pode ser definido como:

> Um conjunto de partes inter-relacionadas formando um todo, que exibe várias propriedades estruturais e processuais (comportamentais) que persistem ao longo de um tempo. O ambiente de um sistema é tudo com o qual o sistema interage, e também pode ser chamado de seu universo (FERNANDES, 2008, p.6).

[2] Definição extraída do dicionário contemporâneo *priberam*. https://dicionario.priberam.org/informação. Acessado em 05/06/2020.

De acordo com Promon (2005, p.6),

> Engana-se quem pensa que as ameaças à segurança da informação estão relacionadas apenas com os sistemas e redes corporativas, conforme comentado até agora, numa área tipicamente denotada por segurança lógica ou digital. O conceito de segurança da informação vai muito além; pressupõe a identificação das diversas vulnerabilidades e a gestão dos riscos associados aos diversos ativos da informação de uma corporação, independentemente de sua forma ou meio em que são compartilhados ou armazenados, digital ou impresso. O objetivo da segurança é garantir a confidencialidade, a integridade e a disponibilidade desses ativos de informação de uma corporação.

E ainda segundo Promon (2005, p.6),

> As fronteiras da segurança da informação vão muito além da segurança lógica. Permeiam também a segurança física, que tem por objetivo prevenir acesso não autorizado, dano e interferência às informações, equipamentos e instalações físicas da organização. O campo da segurança física inclui a utilização de dispositivos que interagem com o mundo físico, em contraste e complementação aos dispositivos lógicos. Alguns exemplos desses dispositivos incluem câmeras de vídeo, catracas, sensores de presença, leitores de cartão de identificação.

Segundo ISO/IEC 27005, para segurança da informação são válidos os conceitos de informação sob enfoque pragmático, semântico e sintático. Pode-se afirmar que a segurança da informação tem alcance holístico quanto ao conceito de seu objeto de estudo. Em síntese, para a segurança da informação, o entendimento sobre informação pode receber contribuições das ciências exatas, das ciências sociais e das ciências humanas.

Sêmola (2003, p.43) define segurança da informação como sendo “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

Beal (2005) entende como segurança da informação o “processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade”. Porém, segurança da informação não pode ser encarada como “guardar em um cofre todas as informações disponíveis”, mas sim elaborar uma boa política de proteção evitando riscos e vulnerabilidade.

Filho (2008) afirma que a segurança da informação compreende um conjunto de medidas que visam proteger e preservar informações e os sistemas de informações, assegurando-lhes integridade, disponibilidade, não repúdio, autenticidade e confidencialidade. Esses elementos constituem os cinco pilares da segurança da informação e, portanto, são essenciais para assegurar a integridade e confiabilidade em sistemas de informações.

Tais pilares, juntamente com mecanismos de proteção, objetivam prover suporte à restauração de sistemas informações, adicionando-lhes capacidades de detecção, reação e proteção. O autor ainda afirma que os componentes criptográficos da segurança da informação tratam da confidencialidade, integridade, não repúdio e autenticidade. Ressalta ainda que o uso desses pilares é feito em conformidade com as necessidades específicas de cada organização.

Assim, o uso desses pilares pode ser determinado pela suscetibilidade das informações ou sistemas de informações, pelo nível de ameaças ou por quaisquer outras decisões de gestão de riscos. É importante se perceber que esses pilares são essenciais no mundo atual, onde se tem ambientes de natureza pública e privada conectados a nível global. Dessa forma, torna-se necessário dispor de uma estratégia, levando em conta os pilares acima mencionados, a fim de compor uma arquitetura de segurança que venha consolidar os objetivos dos cinco pilares. Neste contexto, as organizações e, mais amplamente, os países incluem em suas metas:

a) Forte uso de criptografia;
b) Incentivo à educação em questões de segurança;
c) Disponibilidade de tecnologia da informação com suporte à segurança;
d) Infraestrutura de gestão de segurança;
e) Disponibilidade de mecanismos de monitoramento de ataques, capacidade de alerta e ações coordenadas.

Segurança possui sentido mais amplo do que defesa. O caráter da segurança é abrangente, enquanto o da defesa é específico. A defesa contém em si mesma a sua finalidade, enquanto a segurança é disperso e necessita de um foco para se tornar eficiente. A norma ISO/IEC 27002 define a segurança da informação como a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre investimentos e as oportunidades de negócio.

A concepção de segurança adotada pela ISO/IEC 27002 pode ser entendida como um ato de proteção para defender a informação que está em um ambiente de perigo, risco ou incerteza. Para obter segurança é necessária a implementação de controles. Os controles devem ser selecionados e implementados para assegurar que

os riscos sejam reduzidos a um nível aceitável pela organização. Nesse ponto, há exigência de que seja realizada uma análise de custo benefício, pois os custos para implementação de controles não podem superar o valor da informação que se pretender proteger com tal controle.

A ISO/IEC 27002 define controle da seguinte forma:

> Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica de gestão ou legal. Controle é também usado como um sinônimo para proteção ou contra medida.

Tal definição de controle mostra que controlar é ação determinante na garantia da segurança da informação. Relacionando o conceito descrito pela norma com o conceito de informação abaixo:

> A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado. As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por códigos maliciosos, *"hackers"* e ataques de *"denial of service"* estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados. (ABNT, 2007, p. ix).

Considerando os dois conceitos e exaltando a necessidade de controle e a importância da informação dentro de uma organização, é evidente a relevância e notoriedade que devemos ter com toda a área de segurança da informação.

A partir das informações apresentadas, pode-se entender que a segurança da informação possui seus princípios básicos, assim sendo a confidencialidade, integridade e disponibilidade das informações. De acordo com todos os aspectos citados, os benefícios apresentados no trabalho consistem em reduzir os riscos de ataques que possam comprometer os princípios básicos, como por exemplo: dano físico, eventos naturais, falhas técnicas, ações não autorizadas, comprometimento de funções, fraudes, erros, sabotagens, roubo de informações e diversos outros problemas.

Por fim, pode-se afirmar que segurança é um instrumento de suma importância para proteção das pessoas e organizações contra ameaças às informações que a elas pertençam ou que estejam sob sua incumbência.

Estabelecido o cenário de segurança da informação em que as empresas se encontram é preciso fornece guias e abordagens para que a transição em direção a conformidade seja alcançada, como vemos nos próximos capítulos com *frameworks* e normas relacionadas à segurança da informação.

1.2. COBIT

COBIT, na prática, significa uma estrutura capaz de fornecer governança de TI. Essa estrutura foi criada pela ISACA e tem como principal objetivo gerar valor para a empresa e para os seus processos. Ainda, funciona por meio da aplicação de diversas práticas de controle da informação, que vão desde o planejamento até o monitoramento de resultados. Assim, de modo geral o COBIT começa por estabelecer as melhores práticas de governança de TI e que estejam em consonância com os objetivos da empresa (ISACA, 2012).

A primeira e segunda edição do *framework* COBIT foram publicadas respectivamente em 1996 e 1998 e possuíam foco em objetivos de controle para auditoria, porém, com visão de boas práticas, pois não servia como certificação. Em 2000 a terceira edição é publicada com foco na gestão de TI devido ao acréscimo de orientações para aplicar esta gestão. Finalmente em 2005 a quarta edição e, em 2007, a atualização 4.1, implementa processos de governança e conformidade, além de remover alguns processos de garantia. Em 2012 temos a publicação da versão atual, COBIT 5 que engloba a versão 4.1 juntamente com o *framework* Val IT 2.0, que foca em princípios chave para o gerenciamento e investimento em habilitadores de TI para a geração de valor ao negócio mais *frameworks* de risco de TI. (ISACA, 2012)

O COBIT 5 tem 5 pilares principais para a governança e gestão de TI das organizações, são eles:

a) Reunir as necessidades dos *stakeholders*;

b) Cobrir a empresa do início ao fim;

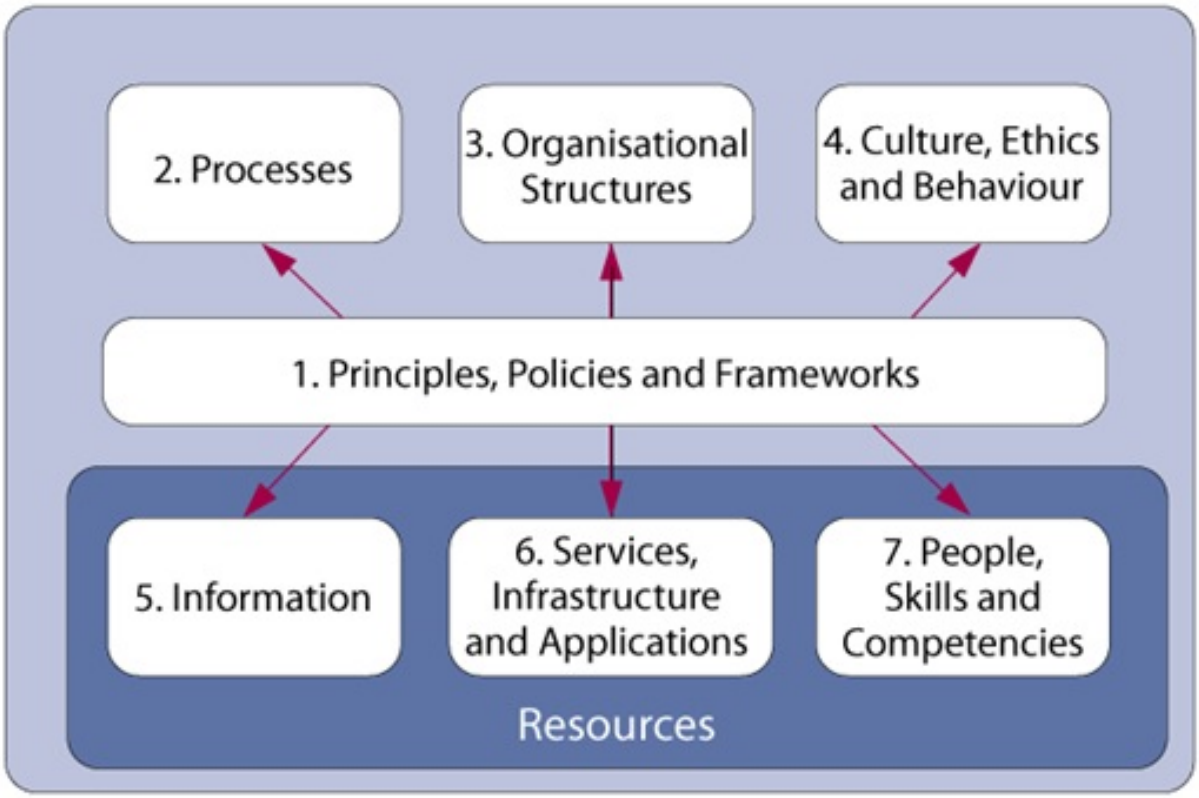
c) Aplicar um *framework* homogêneo e integrado;
d) Aplicar uma abordagem holística;
e) Separar a governança da gestão.

Além disso, utiliza 7 categorias de facilitadores:

a) Princípios, políticas e quadros são os veículos para traduzir o comportamento desejado em orientações práticas para o dia-a-dia de gestão;
b) Os processos descrevem um conjunto organizado de práticas e atividades para atingir certos objetivos e produzir um conjunto de saídas para atingir as metas de TI;
c) As estruturas organizacionais são as principais entidades de tomada de decisão em uma empresa;
d) A cultura, a ética e o comportamento dos indivíduos e da empresa são muitas vezes subestimados como fator de sucesso em atividades de governança e gestão;
e) A informação é necessária para manter a organização funcionando e bem governada, mas no nível operacional, a informação é muitas vezes a chave do produto da própria empresa;
f) Os Serviços, a infraestrutura e as aplicações fornecem as empresas os recursos necessários para o processamento de informação;
g) Pessoas, habilidades e competências são necessárias para que as atividades sejam executadas com sucesso assim como as decisões e ações corretivas.

Como podemos observar na Figura 1, O COBIT está dividido em sete categorias distintas:

Figura 1 - COBIT 5: Categorias

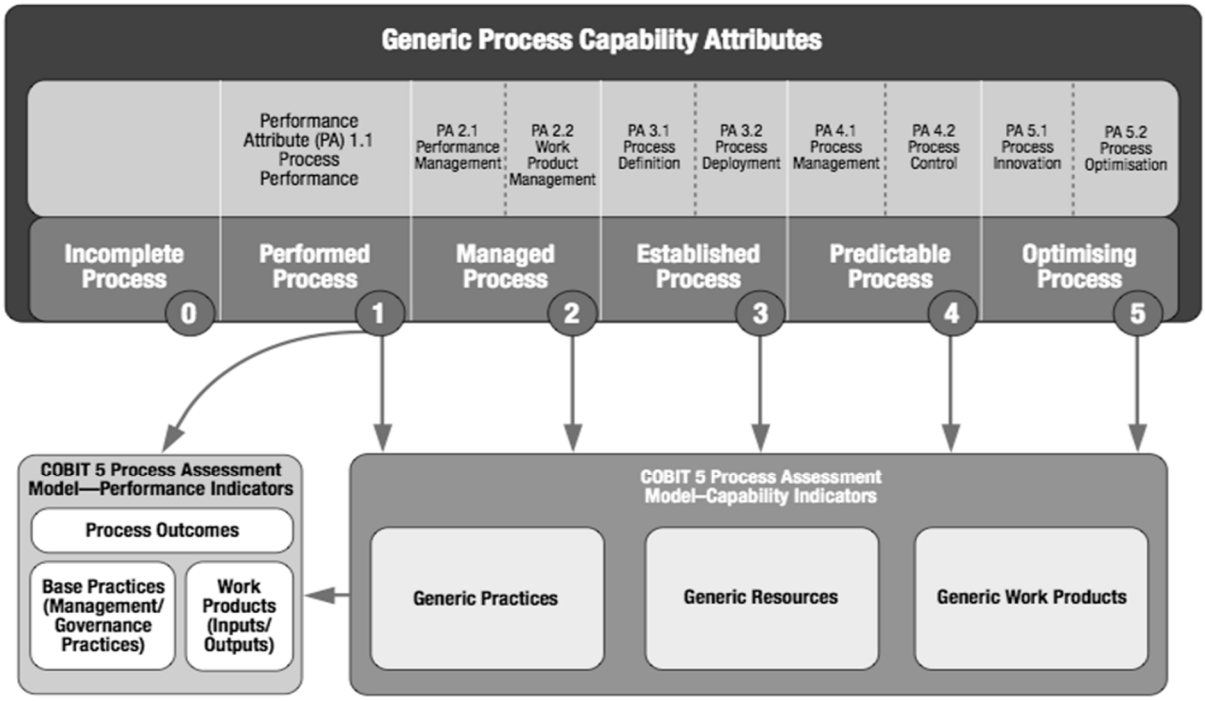


Fonte: ISACA (2012, p. 29).

O modelo de referência do COBIT 5 passou a dividir as práticas e atividades da TI entre a governança e gestão, sendo avaliar, medir e monitorar para a governança e planejar, construir, executar e monitorar para a gestão.

A principal diferença da versão 4.1, no que tange ao modelo de maturidade, com relação a versão 5, é a atribuição da importância aos processos. Ainda, a tarefa do novo Modelo de Capacidade de Processo do COBIT 5 é a mesma do Modelo de Maturidade da versão 4.1, mas a estrutura do *framework* foi modificada. Como visto na Figura 2, o número de níveis para avaliar um processo é o mesmo (seis), embora o nome, o significado e, principalmente, os atributos para avaliar um processo sejam diferentes. De acordo com Dourado (2012) as duas estruturas podem parecer semelhantes, mas existem diferenças de escopo e intenções.

Figura 2 - COBIT 5 Process Capability Model



Fonte: ISACA (2012, p.44).

A diferença de intenções entre os níveis está ligada ao foco significativo na realização dos propósitos dos processos de TI e a uma avaliação mais formal trazida pela nova estrutura. Além disso, de acordo com (ISACA, 2012), na prática, a pontuação que uma empresa pode atingir com o COBIT 4.1*: Maturity Model*, geralmente é maior ou igual à pontuação alcançável com o COBIT 5: *Process Capability Model*. Isso ficará mais claro após a explicação dos seis níveis de avaliação dos processos de TI no COBIT 5. A tarefa de avaliação no COBIT 5 é baseada na ISO/IEC 15504, destacando o forte alinhamento dessa estrutura com as melhores práticas e padrões geralmente aceitos.

1.2.1. MODELO DE CAPACIDADE DOS PROCESSOS

De acordo com (ISACA, 2012), os seis níveis do Modelo de Capacidade do Processo COBIT 5 são:

a) **Nível 0:** Processo incompleto. O processo não é colocado ou não pode alcançar seu objetivo. Nesse nível, o processo não tem objetivo a ser alcançado. Por esse motivo, este nível não possui atributo;
b) **Nível 1:** Processo realizado. O processo está em vigor e atinge seu próprio objetivo. Este nível possui apenas "Desempenho do Processo" como atributo do processo;
c) **Nível 2:** Processo gerenciado. O processo é implementado após uma série de atividades, como planejamento, monitoramento e ajuste de atividades. Os resultados são estabelecidos, controlados e mantidos. Este nível tem "Gerenciamento de desempenho" e "Gerenciamento de produtos de trabalho" como atributos do processo;
d) **Nível 3:** Processo estabelecido. O nível anterior agora é implementado após um processo definido que permite a obtenção dos resultados do processo. Este nível tem "Definição de Processo" e "Implantação de Processo" como atributos do processo;
e) **Nível 4:** Processo previsível. Esse nível implementa processos dentro de um limite definido que permite a obtenção dos resultados dos processos. Este nível tem "Gerenciamento de processos" e "Controle de processo" como atributos;
f) **Nível 5:** processo de otimização. Esse nível implementa processos da maneira que possibilita alcançar objetivos de negócios relevantes, atuais e projetados. Este nível tem "Inovação de processo" e "Otimização de processo" como atributos do processo.

No COBIT 5, para atingir um determinado nível de capacidade, o nível anterior deve ser completamente alcançado. Cumprindo todas as validações necessárias, sem exceção (ISACA, 2012). Há uma grande lacuna entre "Nível 0: processo incompleto" e "Nível 1: processo executado". De fato, alcançar o primeiro nível significa que um processo realiza sua tarefa em grande parte. Assim, de acordo com (ISACA, 2012) “Nesse esquema de avaliação, atingir um nível de capacidade 1, mesmo na escala de 5, já é uma conquista importante para uma empresa”.

Além disso, de acordo com (ISACA, 2012), “No Modelo de Maturidade do COBIT 4.1, um processo pode atingir um nível 1 ou 2 sem atingir plenamente todos

os objetivos do processo". Isso difere do Modelo de Capacidade do Processo do COBIT 5, onde haveria uma pontuação mais baixa do nível 0 ou nível 1. Isso explica por que, no modelo de maturidade do COBIT 4.1(ISACA,2007), o mesmo processo não atinge um resultado menor em comparação com as avaliações realizadas pelo modelo de capacidade de processo do COBIT 5, mas atinge o mesmo ou, pelo menos, um resultado maior.

Como mostra a Figura 2, o *Process Capability Model* baseia sua metodologia de avaliação em seis níveis. Exceto pelo primeiro nível (Nível 0) em que o objetivo do processo não é atingido, em todos os outros níveis, há pelo menos um atributo. Portanto, para atingir um nível, um processo de TI precisa atingir totalmente os atributos relacionados, baseados em indicadores.

Em particular, o Nível 1 deve ajustar indicadores de capacidade e indicadores de desempenho, que verificam os resultados do processo, o alinhamento com as melhores práticas e os recursos utilizados. Isso ocorre porque, para atingir o Nível 1, o objetivo do processo deve ser alcançado. Nos níveis mais altos, os indicadores de desempenho não estão envolvidos, porque ir além do Nível 1 significa que eles foram totalmente alcançados. Assim, no processo de avaliação, do terceiro nível (Nível 2) ao último nível de maturidade (Nível 5), apenas os indicadores de capacidade estão sempre envolvidos. Eles são necessários para avaliar o nível de capacidade de um processo de TI. De fato, o objetivo dos indicadores de capacidade é avaliar a capacidade dos processos para atingir objetivos específicos (ISACA, 2012).

1.2.2. Princípios fundamentais

Lançado em 2012, o *COBIT 5* foi construído e integrado com base em 20 anos de desenvolvimento neste campo de atuação. Desde os seus primórdios, centrado na comunidade de auditoria de TI, o COBIT se tornou um *framework* de Governança e Gerenciamento de TI mais abrangente, compreensivo e aceito, baseado em cinco princípios fundamentais:

a) Satisfazer necessidades das partes interessadas: Este princípio implica que o COBIT fornece todos os processos e habilitadores necessários para suportar a

criação de valor através do uso da TI. Este princípio está intimamente alinhado com o conceito de longa data chamado alinhamento estratégico. A convicção de que um componente núcleo da governança de TI é atingir o alinhamento estratégico entre TI e o resto da organização é um elemento crítico do COBIT;

b) Cobrir a organização de ponta a ponta: Este princípio considera que o COBIT cobre todas as funções e processos de uma organização. O COBIT não foca somente na função de TI, mas trata a informação e tecnologias relacionadas como ativos que precisam ser tratados como qualquer outro ativo da organização;

c) Aplicar um framework integrado e único: Este princípio descreve o alinhamento em alto nível do COBIT com outros padrões e frameworks relevantes, servindo como um framework abrangente para a Governança Empresarial de TI. A ISACA alinhou o COBIT com outros frameworks, como COSO, ITIL, PMBOK, TOGAF, PRINCE2, etc;

d) Possibilitar uma visão holística: Este princípio explica que a implementação eficaz e eficiente da Governança Empresarial de TI requer uma visão holística, levando em consideração vários componentes interativos – como processos, estruturas e pessoas. Este desafio de implementação está relacionado ao que é descrito em literaturas de gerenciamento estratégico como uma necessidade para um sistema organizacional, como a forma que uma empresa coloca as pessoas para trabalharem juntas a favor do negócio;

e) Separar Governança do Gerenciamento: Este último princípio consiste na distinção entre a governança e o gerenciamento. Esta distinção alinha-se com a norma ISO/IEC38500. No COBIT é declarado que os processos de governança de TI e de gerenciamento de TI referem-se a diferentes tipos de atividades.

Os processos de governança são organizados conforme o modelo *Evaluate, Direct and Monitor* (EDM), proposto na ISO/IEC 38500. Os processos de gerenciamento de TI asseguram que os objetivos da empresa sejam atingidos por meio da avaliação das necessidades das partes interessadas, definindo a direção

através da priorização e tomada de decisão, e monitorando o desempenho, a conformidade e o progresso com relação aos planos (ISACA, 2012).

Embora as boas práticas de um *framework* como o COBIT5 consigam estabelecer maturidade nos processos de uma empresa que estejam ligados ou não a geração de valor, muitas vezes é necessário recorrer a normas que devido aos seus requisitos obrigatórios tornam a empresa melhor alinhada com o mercado como veremos nos próximos capítulos.

1.3. NORMAS E PADRÕES DE SEGURANÇA

Antes de iniciar o estudo das normas e da ferramenta, cabe elucidar alguns conceitos sobre cada um desses elementos. Norma é aquilo que se estabelece como medida para a realização de uma atividade. Uma norma tem como propósito definir regras e instrumentos de controle para assegurar a conformidade de um processo ou serviço (FAGUNDES, 2013).

Conforme definido pela Associação Brasileira de Normas Técnicas (ABNT), os objetivos da normalização são:

> Comunicação: proporcionar meios mais eficientes na troca de informação entre o fabricante e o cliente, melhorando a confiabilidade das relações comerciais e de serviços; Segurança: proteger a vida humana e a saúde; Proteção do consumidor: prover a sociedade de mecanismos eficazes para aferir qualidade dos produtos; Eliminação de barreiras técnicas e comerciais: evitar a existência de regulamentos conflitantes sobre produtos e serviços em diferentes países, facilitando assim o intercâmbio comercial (ABNT, 2020).

As ferramentas são instrumentos que facilitam a aplicação de determinada metodologia. Neste caso, foi elaborada uma página *web* para a geração de relatórios, com objetivo de mostrar o nível de conformidade do processo de análise de riscos de uma corporação utilizando os níveis do modelo de maturidade do COBIT5 (2012).

Na próxima seção será abordado, superficialmente, o ciclo de normas relacionadas a família ISO/IEC 27000 - Gestão da Segurança da Informação para fundamentar o contexto, porém, será dada maior ênfase as normas que estejam relacionadas diretamente com o tema central da ferramenta que será desenvolvida, no caso, Análise de Risco.

Utilizamos também o modelo descrito na norma ISO/IEC 15504 que define os requisitos para o Método de Avaliação de Processos e tem como objetivo determinar o nível de capacidade dos processos de uma organização.

Desta forma, foi conceituado pontos específicos de cada norma, a fim de fundamentar e contextualizar todo o processo de análise de risco e sua importância dentro da gestão da segurança da informação.

1.4. ISO/IEC 27001

A ISO/IEC 27001 é uma norma de vigência internacional, cujo objetivo é determinar as diretrizes necessárias para uma gestão de segurança da informação nas organizações, sejam elas especializadas nesse tipo de serviço, sejam aquelas que tenham um setor interno dedicado à proteção dos dados. Sua última versão foi publicada em 2013.

As normas são aplicáveis em qualquer tipo de organização: com ou sem fins lucrativos, privada ou pública, de qualquer porte. Sua elaboração é realizada pelos mais importantes especialistas da área no mundo, determinando as principais diretrizes sobre o assunto, disponibilizando uma certificação muito bem conceituada sobre a norma ISO/IEC 27001, que ocorre por meio da avaliação realizada por um órgão certificador independente, previamente autorizado pela ISO.

Seu objetivo principal é proteger a integridade dos dados, bem como a confidencialidade e a disponibilidade deles dentro do ambiente organizacional. Isso ocorre por meio de uma análise de problemas em potencial (avaliações de risco) e ações que possam prevenir ou minimizar esses problemas (mitigação e tratamento de risco). Além disso, deve-se também avaliar a importância de cada risco de forma a focar nos mais importantes.

Assim, seu principal fundamento é realizar uma gestão de riscos eficaz, de forma a diagnosticá-los e minimizá-los no ambiente interno. Isso é feito por meio de políticas, procedimentos e implementações técnicas preestabelecidas pela norma. Embora a avaliação e o tratamento de riscos sejam etapas de trabalho complexas,

muito frequentemente ele é mistificado desnecessariamente. Podemos definir 6 métodos a fim de otimizá-los, utilizando como base a norma ISO/IEC 27001 (2005)**:**

a) Metodologia de análise de risco: Esta é a principal etapa. Definição de regras sobre como será realizada a gestão de riscos de forma abrangente e para que seja aplicada a toda a organização. O maior problema com a gestão de riscos acontece pela necessidade de unificar diferentes partes da organização, onde todas precisam respeitá-la. Assim define-se que uma avaliação de riscos pode ser qualitativa ou quantitativa, quaisquer que sejam as escalas para uma avaliação qualitativa, qual será o nível aceitável de risco, etc;
b) Implementação da avaliação de riscos: Uma vez definidas as regras auxiliaram na identificação de quais problemas em potencial poderão acontecer à empresa – deve-se listar todos os ativos, depois ameaças e vulnerabilidades relacionadas a estes ativos, avaliar o impacto e a probabilidade para cada combinação de ativos/ameaças/vulnerabilidades e finalmente calcular o nível de risco;
c) Implementação do tratamento de riscos: De forma geral nem todos os riscos têm origens comuns – devemos focar nos mais importantes, os assim chamados “riscos inaceitáveis”;
d) Relatório de avaliação de riscos do SGSI: Documentar todos os passos e ações tomadas. Não apenas para os auditores, mas para uma futura checagem de resultados;
e) Declaração de Aplicabilidade: Desenvolver um documento definindo qual o perfil de segurança da organização – baseando-se nos resultados do tratamento de riscos, listando os controles implementados, o porquê e como foram implementados. Este documento é também muito importante porque o auditor de certificação que irá se orientar para os processos de uma auditoria;
f) Plano de Tratamento de Risco: Transformando toda a teoria em prática. Este é o propósito do Plano de Tratamento de Risco – é de extrema importância definir o responsável pela implementação de cada controle, em que espaço de tempo, com qual orçamento, etc;

Com este documento pronto e de forma detalhada, é crucial obter a aprovação da direção da organização, por envolver uma quantidade considerável de tempo, esforço e dinheiro, dedicados para implementar todos os controles planejados até aqui. A definição desses métodos de forma sistemática e detalhada está presente na norma ISO/IEC 27001, que utilizamos como base para toda a nossa ferramenta. Contudo, sabemos que somente essa norma não expõe a profundidade necessária dentro do tema de segurança da informação, bem como não enfatiza o processo de análise de risco. Sendo assim, definimos e estudamos as normas ISO/IEC 27002 e ISO/IEC 27005, como será descrito nas próximas seções.

1.5. ISO/IEC 27002

A ISO/IEC 27002 é um código de práticas para a gestão de segurança da informação. Esta norma pode ser vista como um prelúdio para o desenvolvimento de diretrizes e princípios gerais sobre metas geralmente aceitas para a gestão da segurança da informação.

A gestão da segurança da informação necessita de um planejamento adequado ao negócio da organização. Deve ser elaborado um plano estratégico de segurança que atenda a toda a organização. O plano deve identificar o cenário da organização aonde a segurança da informação deverá atuar. Segundo Fontes (2000) não existe solução certa ou errada, mas sim há solução que é mais adequada a cada organização. Independentemente de como você rotule o seu planejamento de segurança, não deixe de fazê-lo. Como qualquer outro planejamento, ele é o rumo a ser seguido com os objetivos definidos.

A gestão da segurança deve abranger todos os aspectos do trabalho diário: a avaliação do ambiente organizacional, a valoração do risco e a análise de incidentes de segurança. Todos os processos de gestão da segurança se baseiem no plano estratégico da organização. O plano apresenta os princípios e diretrizes que norteiam a organização no cumprimento de sua missão.

De acordo com a norma ISO/IEC 27002:2008, existem 11(onze) seções de controle de segurança da informação, os quais são dispostos abaixo com seus respectivos objetivos:

a) Política de segurança da informação: Prover uma orientação e apoio a direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes;
b) Organização da segurança da informação: Gerenciar a segurança da informação dentro da organização;
c) Gestão de ativos: Alcançar e manter a proteção adequada dos ativos da organização;
d) Segurança em recursos humanos: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de furto ou roubo, fraude ou mal uso de recursos;
e) Segurança física e do ambiente: Prevenir o acesso físico não autorizado, danos e interferência com as instalações e informações da organização;
f) Gerenciamento das operações e comunicações: Garantir a operação segura e correta dos recursos de processamento da informação;
g) Controle de acesso: Controlar o acesso à informação com base nos requisitos de negócio e segurança da informação;
h) Aquisição, desenvolvimento e manutenção de sistemas de informação: Garantir que segurança é parte integrante de sistemas de informação;
i) Gestão de incidentes de segurança da informação: Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil;
j) Gestão de continuidade de negócio: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se forem o caso;

k) Conformidade: Evitar violações de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação.

Embora o conteúdo da política de segurança possa variar de acordo com o tipo da instituição, ela deverá abranger, sempre que cabível, os controles apontados. Segundo a ISO/IEC 27002, a ordem dos controles não significa o seu grau de importância. Dependendo das circunstâncias, todas as seções podem ser importantes. Portanto, convém que cada organização que utilize esta norma identifique quais são os itens aplicáveis, quão importantes eles são e a sua aplicação para os processos específicos do negócio.

1.6. ISO/IEC 27005

O risco é entendido como alguma coisa que cria possibilidades ou produz danos. No que se refere à segurança, os riscos são entendidos como circunstâncias que geram ou agregam a potencialidade de perdas e danos. É possível calculá-lo por meio da probabilidade de um evento acontecer e causar perdas.

Várias definições são encontradas para definir o risco, no entanto, a definição adotada neste trabalho é o que foi estabelecido pela norma ISO/IEC *Guide 73:2002*, que o define como “a combinação da probabilidade de um evento e suas consequências.”

Também é importante evidenciar a definição de risco de segurança da informação e seus componentes, segundo a ISO/IEC 27005:

> Riscos de segurança da informação é a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira prejudicando a organização. (ABNT, 2008, p.1)

Existem 4 (quatro) elementos que são primordiais para o processo de gestão de riscos, a partir do conceito citado é possível compreendê-los. De acordo com a ISO/IEC 27002:

> 1) Ativo: Qualquer coisa que tenha valor para a organização [...]
> 2) Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização [...]

> 3) Vulnerabilidade: Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças [...]
> 4) Proteção - É a forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal (ABNT NBR ISO/IEC 27002, 2005, p. 1, 3).

A norma ISO/IEC 27005 convém que a gestão de riscos de segurança da informação possa contribuir para:

- Identificação de riscos;
- Análise/avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência;
- Comunicação e entendimento da probabilidade e das consequências destes riscos;
- Estabelecimento da ordem prioritária para tratamento do risco;
- Priorização das ações para reduzir a ocorrência dos riscos;
- Envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e mantidas informadas sobrea situação da gestão de riscos;
- Eficácia do monitoramento do tratamento do risco;
- Monitoramento e a análise crítica regular de riscos e do processo de gestão dos mesmos;
- Coleta de informações de forma a melhorar a abordagem da gestão de riscos;
- Treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los. (ABNT, 2011).

Riscos de segurança da informação são as possibilidades de uma ameaça explorar vulnerabilidades dos ativos, comprometendo a confidencialidade, integridade e disponibilidade das informações de uma organização (ABNT NBR ISO/IEC 27005, 2008). Já Oliveira (2006) classifica os riscos como sendo uma oportunidade, uma incerteza ou uma ameaça. Esta última como sendo de maior preocupação, pois está atrelada à ocorrência de efeitos negativos como, por exemplo, perda financeira, fraude, roubo, comprometimento da imagem, infração legal, indisponibilidade de serviços, dentre outros (VASILE; STUPARU; DANIASA, 2010).

Gerenciar os riscos é um dos principais processos da gestão da segurança da informação, pois visam à identificação, avaliação e priorização de riscos, seguido pela aplicação coordenada e econômica dos recursos para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos, reduzindo o risco a um nível aceitável.

Devido à importância do processo de gestão de riscos para as organizações, algumas normas internacionais foram criadas com o intuito de nortear os conceitos e práticas de gestão de riscos. Dentre estas normas, pode-se citar a ISO/IEC 27005, que discute tecnologia da informação, técnicas de segurança e gestão de riscos de segurança da informação. A utilização de normas de segurança da informação garante que a organização está seguindo as diretrizes dos processos de gestão da segurança da informação e possibilita com que a organização seja reconhecida pela utilização de boas práticas em gestão da segurança da informação.

A norma internacional ISO/IEC 27005 é parte da série de normas da ISO/IEC 27000, a qual é uma série bem estabelecida de normas de gestão de segurança da informação e é aceita em todo o mundo. O âmbito de aplicação destas normas pode ser na organização como um todo, ou em partes, como os processos de um departamento, uma aplicação de TI ou uma infraestrutura de TI (BECKERS *et al*, 2011). Esta norma internacional fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI).

A ISO/IEC 27005 define o processo de gestão de risco como atividades coordenadas para dirigir e controlar o risco de uma organização (LUND; SOLHAUG; STØLEN, 2010).

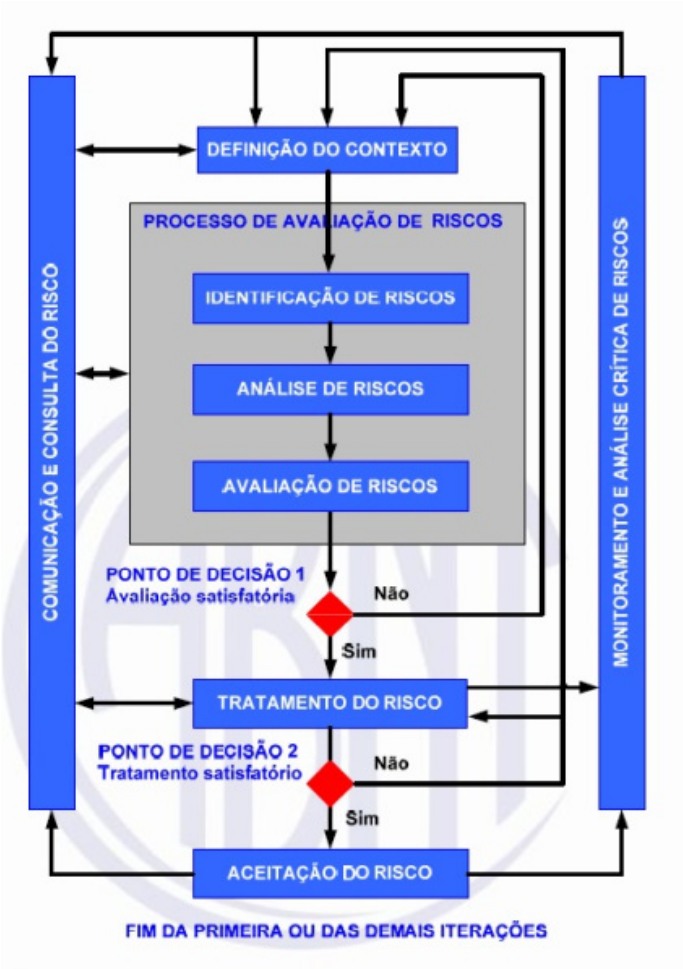
Neste contexto, o processo de gestão de riscos é definido por oito atividades, como pode ser observado na Figura 3 para cada atividade da norma são propostas diretrizes para implementação que serão brevemente descritas a seguir (ABNT NBR ISO/IEC 27005, 2008).

1.6.1. O PROCESSO DE GESTÃO DE RISCOS

O procedimento e atividades da gestão de risco de segurança da informação (GRSI) está descrito na norma ISO/IEC 27005. As atividades do processo se iniciam com a atividade de definição do contexto, seguidas de análise/avaliação de riscos, tratamento do risco, aceitação do risco, comunicação do risco, por final o

monitoramento e análise crítica de riscos. A ligação entre as atividades do processo de GRSI é observada na figura 3.

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



Fonte: ABNT NBR ISO/IEC 27005 (2011)

A definição do contexto designa o alvo cujo a gestão de risco vai proceder. Como entrada, a atividade recebe todas as informações relevantes sobre a organização para a definição do contexto da gestão de riscos de segurança da informação. E gera como saída:

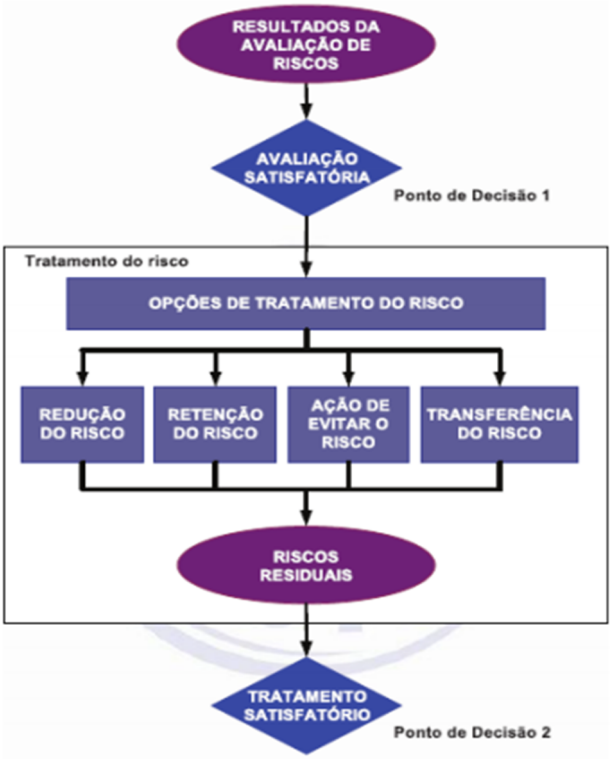
a) Especificação dos critérios básicos, critérios esses que se dividem em critérios para avaliação de riscos, critérios de impacto e critérios para aceitação do risco;
b) O escopo e os limites do processo de GRSI;

c) A organização responsável pelo processo.

A análise/avaliação de riscos tem o papel de identificar, quantificar ou descrever qualitativamente os riscos, priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização. Esta atividade recebe como entrada os critérios básicos, o escopo e os limites, e a organização do processo de GRSI que se está definindo. Como saída é gerada uma lista de riscos avaliados, ordenados por prioridade de acordo com os critérios de avaliação de riscos.

O tratamento do risco convém em controles para reduzir, reter, evitar ou transferi-los, para que os mesmos sejam selecionados e o plano de tratamento do risco seja definido. Como entrada a atividade recebe uma lista de riscos ordenados por prioridade (de acordo com os critérios de avaliação de riscos) e associados aos cenários de incidentes que os provocam. Na saída é gerado um plano de tratamento do risco e os riscos residuais, sujeitos à decisão de aceitação por parte dos gestores da organização. A Figura 4 mostra a atividade de tratamento do risco.

Figura 4 – A atividade de tratamento do risco



Fonte: ABNT NBR ISO/IEC 27005 (2011)

A atividade de aceitação do risco de segurança da informação convém que a decisão de aceitar os riscos seja realizada e formalmente registrada, juntamente com a responsabilidade pela decisão. Como entrada recebe o plano de tratamento do risco e a análise/avaliação do risco residual sujeito à decisão dos gestores da organização relativa à aceitação do mesmo. Como saída é gerado uma lista de riscos aceitos, incluindo uma justificativa para aqueles que não satisfaçam os critérios normais para aceitação do risco.

Na Comunicação do risco de segurança da informação, as informações sobre os riscos são trocadas e/ou compartilhadas entre o tomador de decisão e as outras partes interessadas. Tem como entrada todas as informações sobre os riscos obtidas através das atividades de gestão de riscos (como visto na Figura 4). E como saída o entendimento contínuo do procedimento de GRSI da organização e dos resultados obtidos.

A última atividade, Monitoramento e análise crítica de riscos de segurança da informação, do processo de GRSI convém que todos os riscos e seus fatores (isto é, valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidade de ocorrência) sejam monitorados e analisados criticamente, a fim de se identificar, o mais rapidamente possível, eventuais mudanças no contexto da organização e de se manter uma visão geral dos riscos. Recebe como entrada todas as informações sobre os riscos obtidas através das atividades de gestão de riscos (ver Figura 4 acima). E tem como saída um alinhamento contínuo da gestão de riscos com os objetivos de negócios da organização e com os critérios para a aceitação do risco. No final do processo de GRSI, o mesmo tem que ser continuamente monitorado, analisado criticamente e melhorado, quando necessário e apropriado.

Uma vez apresentado referencial teórico composto por Segurança da Informação, COBIT e Normas e Padrões de Segurança, bem como ter apresentado o processo de Análise de Risco, no próximo capítulo será apresentada a ferramenta produto deste trabalho de conclusão de curso.

2. RIPE: APLICAÇÃO WEB PARA ANÁLISE DE MATURIDADE DO PROCESSO DE ANÁLISE DE RISCO

Este capítulo apresenta a análise realizada para desenvolvimento da ferramenta, alguns diagramas e imagens que exemplificam a utilização do sistema proposto. São apresentados também o procedimento de desenvolvimento do site, as telas e funcionalidades que representam o principal objetivo da aplicação: a análise da maturidade do processo de análise de risco de uma organização e eventualmente a apresentação de possíveis ações para otimizá-lo.

2.1. DESENVOLVIMENTO DO APLICATIVO WEB

Este trabalho tem como produto uma aplicação web. A seguir serão apresentadas as definições de requisitos, o projeto de sistema, a implementação e a descrição completa da ferramenta.

2.1.1. DEFINIÇÃO DE REQUISITOS

Os requisitos de um sistema, segundo SOMMERVILLE (2007), são descrições dos serviços fornecidos pelo sistema e as suas restrições operacionais. Os requisitos refletem as necessidades dos clientes de um sistema que ajuda a resolver algum problema, por exemplo, controlar um dispositivo, enviar um pedido ou encontrar informações.

Frequentemente, as especificações de requisitos de software são criadas sem que haja real entendimento das necessidades e problemas da organização. Por meio das técnicas de modelagem de processo de negócio, é possível compreender melhor o ambiente no qual o sistema a ser construído irá funcionar, o que possibilita identificar requisitos correspondentes às reais necessidades do negócio (BAKER, 2001). O trabalho aqui descrito apresentará a modelagem de requisitos usando a notação *Unified Modeling Language* (UML).

A forma utilizada para levantar os requisitos foi a entrevista, que fazem parte da maioria dos processos de engenharia de requisitos. Foram formuladas questões para os usuários sobre os recursos que eles usam e o sistema a ser desenvolvido. Os requisitos são derivados das respostas dessas questões. Entrevista é uma das técnicas tradicionais mais simples de utilizar e que produz bons resultados na fase inicial de obtenção de dados.

Na Quadro 1 é apresentado todos os requisitos levantados após as várias entrevistas com os usuários:

Quadro 1: Levantamento de requisitos.

Requisitos	Descrição
1- Autenticação	O Sistema deve oferecer na página inicial um formulário de login.
2- Permissão	1. Usuários devem ser divididos entre clientes registrados e usuários comuns.
3- Módulo Cliente Registrado	1. Cadastro do cliente 2. Cadastro da empresa 3. Solicitar um orçamento para um futuro acompanhamento e implementação do produto proposto 4. Acesso ao questionário de forma integral 5. Acesso ao relatório que expõe o resultado superficial através do questionário 6. Listar todos os relatórios existentes para o cadastro 7. Listar possíveis melhorias evidenciadas nos relatórios 8. Enviar requisição de acompanhamento, através de e-mail 9. Enviar os relatórios para o e-mail cadastrado 10. Atualizar dados cadastrais xi. Fazer logout no sistema.
4-Módulo Usuário comum	1. Acessar a tela inicial, que irá exibir uma descrição breve do produto disponível 2. Acessar cadastros de clientes 3. Acesso à um formulário default, sem a possibilidade de interação. 4. Enviar mensagem direta para a nossa empresa.
5- Segurança	1. Páginas terão que conter restrição de acesso; 2. Somente clientes registrados tem acesso a todo conteúdo disponível.

Fonte: Autoria Nossa

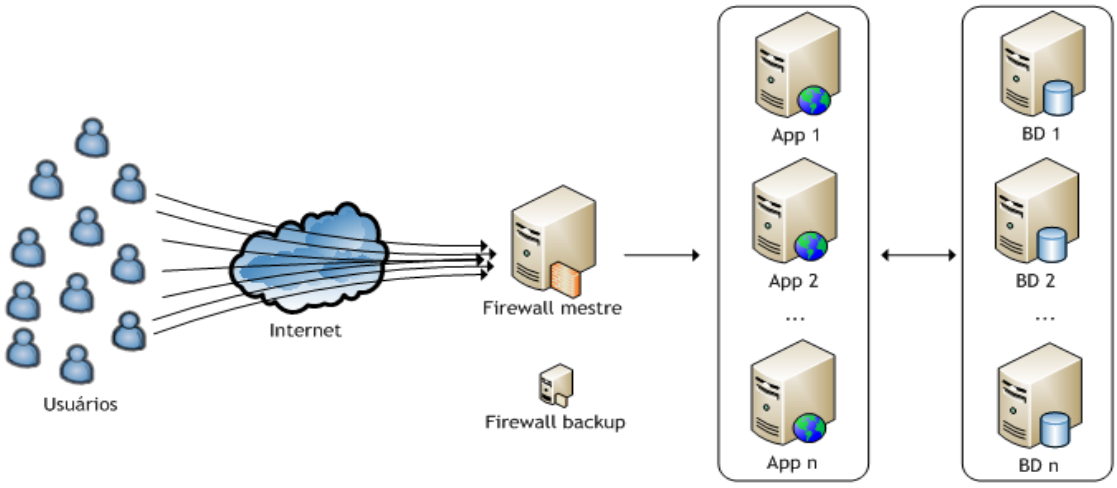
2.1.2. MODELO CLIENTE-SERVIDOR

O conceito de cliente-servidor segundo RENAUD (1994, p.3), cliente-servidor é um conceito lógico, mais precisamente um paradigma, ou modelo para interação entre processos de software em execução concorrente.

Geralmente o modelo cliente-servidor faz uso de protocolos de comunicação simples do tipo requisição/resposta. A fim de obter um serviço, um cliente envia uma requisição ao servidor. Este, por sua vez, executa as operações associadas ao serviço e envia uma resposta ao cliente, contendo dados ou um código de erro, caso o serviço não possa ser executado.

Existem vários tipos de servidores, como por exemplo, servidor de arquivos, servidor DHCP, que fornecem IPs para máquinas na rede, servidor DNS, que resolvem nome de domínio em endereço IP. O servidor Web, hospeda uma ou mais páginas na internet para que sejam acessadas pelos clientes, dentre vários outros. Neste trabalho será usado o servidor web como forma de hospedar o sistema desenvolvido para que ele seja acessado de qualquer lugar tanto na rede interna, quanto externa, e é conhecido como plataforma cliente-servidor. A Figura 5 apresenta a estrutura básica do modelo cliente-servidor:

Figura 5: Modelo cliente-servidor



Fonte: Sommerville (2007).

Pela Figura 5, é possível observar como os clientes através da internet conseguem enviar requisições para um servidor web, na figura representada pelos servidores das aplicações (App n).

2.2. PROJETOS DE SISTEMAS E SOFTWARE

Um projeto de software é a descrição da estrutura de software a ser implementada, dos dados que são partes do sistema, das interfaces entre os componentes do sistema e dos algoritmos usados. Os projetistas não chegam ao projeto final imediatamente, mas desenvolvem o projeto iterativamente por meio de várias versões (SOMMERVILLE, 2007).

2.2.1. IDENTIFICAÇÃO DAS FERRAMENTAS

A proposta é implementar uma aplicação web, que estará disponível para qualquer dispositivo conectado à internet. Sendo apresentado e executado através de quaisquer navegadores como Internet Explorer, Mozilla Firefox, Google Chrome etc. Sendo assim, as tecnologias escolhidas para o desenvolvimento da aplicação foram:

a) Linguagem de marcação de Hipertexto: HTML;
b) Linguagem de Scripting: *JavaScript*;
c) Ajax (*Asynchronous JavaScript* and XML);
d) CSS (*Cascading Style Sheets*);
e) Utilizaremos Angular 6 como framework e plataforma da aplicação;
f) Linguagem de programação principal: ASP.NET Core;
g) Banco de dados: MySQL.

2.2.2. DESCRIÇÃO DA APLICAÇÃO

RIPE, o nome da nossa aplicação, é uma palavra da língua inglesa, com tradução literal: “maduro ou madura”, levando em consideração a principal função de disponibilizar um “*ripening process*”, ou processo de amadurecimento.

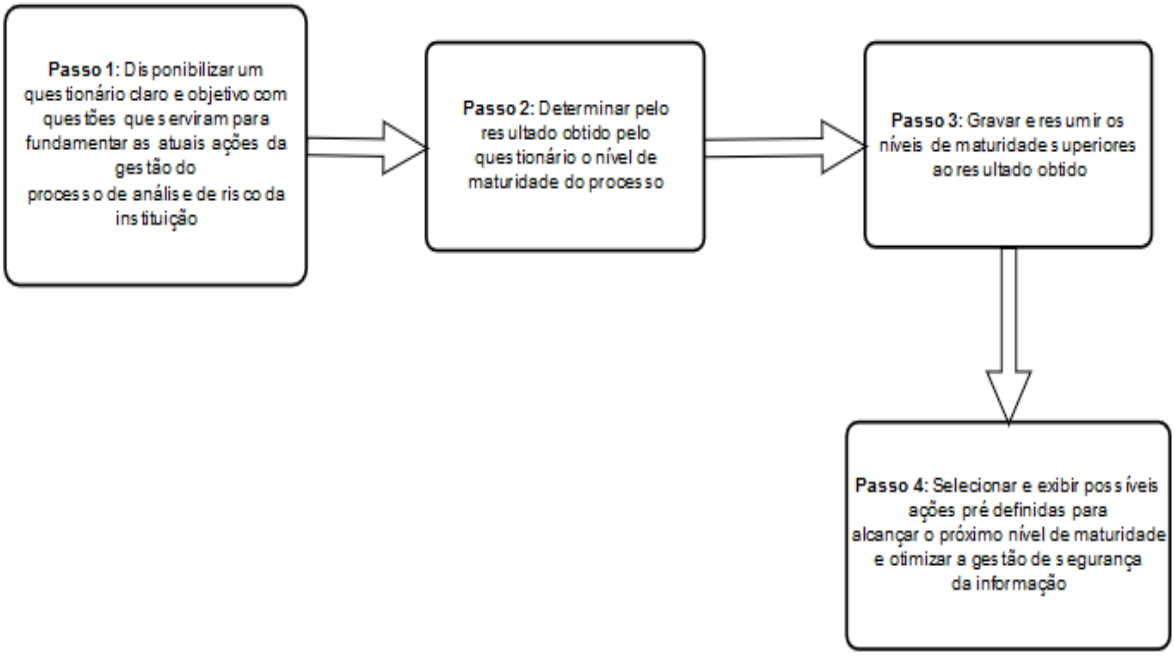
Como descrito anteriormente, seguimos o *framework* COBIT, na versão 5, para definir e estruturar nossa aplicação. O estudo feito envolveu conceitos mais específicos onde relacionamos as boas práticas do COBIT, a segurança da informação e uma série de normas técnicas internacionais, publicadas pela *International Organization of Standardization* (ISO) em conjunto com a *International Electrotechnical Commission* (IEC), que rege os sistemas de gestão da qualidade em conjunto com a *ABNT* - Associação Brasileira de *Normas* Técnicas. Os conceitos aprendidos e descritos até aqui estruturam toda a aplicação RIPE.

2.2.3. FUNCIONALIDADES

A aplicação tem como principal funcionalidade, o questionário, disponibilizado para os usuários da ferramenta, a partir dele é gerado um relatório que exibe o resultado do nível de maturidade de acordo com as respostas obtidas.

Definimos as principais ações da nossa ferramenta e resumimos no modelo apresentado abaixo.

Figura 6: Modelo de avaliação RIPE



Fonte: Autoria Nossa

2.2.4. QUESTIONÁRIO

O questionário foi desenvolvido para compreender os conceitos expostos, com o objetivo de aderir as diretrizes e boas práticas descritas pelo COBIT, respeitando as normas descritas sobre gestão de segurança da informação e evidenciando a definição de risco de segurança da informação e seus componentes.

A avaliação da maturidade é composta por um total de 140 perguntas detalhadas ao final deste tema, que estão agrupadas por tópicos, onde cada tópico se refere a um ponto crucial para a análise de risco, pontos como: áreas específicas da empresa, políticas e documentações utilizadas ou gestões específicas adotadas ou não pela organização. Nas perguntas o cliente/usuário poderá escolher entre as opções SIM (processo ou adequação implantada), NÃO (processo ou adequação não implantada) ou Não se aplica a minha empresa (o tópico não se enquadra no ramo da organização).

Para que seja possível a mensuração do grau de maturidade do COBIT definimos que cada pergunta terá o mesmo peso e cada pergunta represente 0.714%

aproximadamente sobre um total de 140 (cento e quarenta) perguntas, avaliando assim o total atingido de acordo com as respostas de cada usuário

O framework de medição, com os níveis de capacidade, atributos de processo (*Process Atribute* – PA) e sua relação com a escala de medição utilizados são apresentados no quadro 1. A escala utilizada favorece a otimização da avaliação tendo em vista que para se avaliar um nível superior da maturidade, o nível imediatamente anterior deve alcançar a escala de "F" (Completamente alcançado), ou seja, acima de 89%.

Quadro 2: Níveis de capacidade, atributos de processos e escala de medição

	Nível 0 - Incompleto	Nível 1 - Executado	Nível 2 - Gerenciado	Nível 3 - Estabelecido	Nível 4 - Previsível	Nível 5 - Otimizado
	0	1	2	3	4	5
PA 5.2 Otimização						L ou F
PA 5.1 Inovação						L ou F
PA 4.2 Controle					L ou F	F
PA 4.1 Medição					L ou F	
PA 3.2 Desenvolivmento				L ou F	F	F
PA 3.1 Definição				L ou F		
PA 2.2 Gerenciamento dos produtos de Trabalho			L ou F	F	F	F
PA 2.1 Gerenciamento da Execução			L ou F			
PA 1.1 Execução do Processo	N ou P	L ou F	F	F	F	F

Fonte: Autoria Nossa

De acordo com os conceitos descritos na norma ISO/IEC 15504, foi possível definir os níveis de capacidade citados no Quadro 1:

a) **Nível 0: Incompleto –** Processo não existe ou falha em atingir seus objetivos
b) **Nível 1: Executado** – Processo geralmente atinge os objetivos, porém sem padrão de qualidade e sem controle de prazos e custos
c) **Nível 2: Gerenciado** – Processo planejado e acompanhando, e satisfaz requisitos definidos de: qualidade, prazo e custos

d) **Nível 3: Estabelecido** – Processo executado e gerenciado com uma adaptação deum processo padrão definido, eficaz e eficiente.
e) **Nível 4: Previsível** – Processo executado dentro de limites de controle definidos e com medições detalhadas e analisadas.
f) **Nível 5: Otimizado** – Processo melhorado continuamente de forma disciplinada

Cada atributo é medido com base na escala padrão da ISO/IEC 15504 que consiste em:

a) **N (Não alcançado)** – Há pouca ou nenhuma evidência de que os atributos definidos são alcançados no processo avaliado. Considera-se que entre 0 e 15% dos quesitos são atendidos.
b) **P (Parcialmente alcançado)** – Há alguma evidência do cumprimento dos atributos definidos no processo avaliado. Alguns aspectos podem ser imprevisíveis. Considera-se que entre 15% e 50% dos quesitos são atendidos.
c) **L (Amplamente – Largely – alcançado)** – Há evidência de uma abordagem sistemática, com o alcance significativo dos atributos definidos no processo avaliado. Algumas falhas relacionadas aos atributos podem existir. Considera-se que entre 50% e 89% dos quesitos são atendidos.
d) **F (Completamente – Fully – alcançado)** – Há evidência de uma abordagem sistemática completa, assim como o alcance completo dos atributos definidos para o processo avaliado. Não existe falha significante relativa aos atributos. Considera-se que mais de 85% dos quesitos são atendidos.

Como a escala não é clara em relação aos valores limites, admitiu-se para os resultados gerados um padrão para as escalas utilizadas:

$$\mathbf{N \leq 14\% < P \geq 49\% < L \geq 89\% < F \geq 100\%.}$$

Segue a exibição do conteúdo do questionário de forma integral:

Quadro 3: Bloco de perguntas gerais sobre a organização

A Organização	Atualmente a organização:	
	1	Explora adequadamente as ameaças identificadas pela ocorrência de determinados riscos?
	2	Explora adequadamente as oportunidades identificadas pela ocorrência de determinados riscos?
	3	Depende das iniciativas de caráter individual para o sucesso do gerenciamento de riscos?
	4	Não é uma organização "orientada a riscos"?
	5	Tem alta probabilidade de ocorrência de eventos que impactem fortemente e negativamente?
	6	Já está sofrendo algum tipo de prejuízo por não explorar o gerenciamento de risco de forma adequada?

Fonte: Autoria Nossa

Quadro 4: Bloco de perguntas conceituando riscos.

Conceito de Risco para a organização	1	Risco está relacionado com o nível de satisfação e a expectativa do cliente?
	2	Risco está relacionado com o alcance dos objetivos da organização?
	3	O conceito de risco tem mais foco no cliente do que na organização?
	4	Risco é o efeito acumulativo da probabilidade de ocorrências incertas que podem afetar positivamente ou negativamente os objetivos finais da organização?
	5	A organização atualmente avalia o processo de análise de riscos como um fator de extrema importância?
	6	A organização possui um processo exclusivo para análise de riscos?

Fonte: Autoria Nossa

Quadro 5: Bloco de perguntas sobre o processo de análise de riscos

Avaliar e controlar os Riscos de TI	1	Existe uma estrutura de gestão de riscos de TI alinhada com a estrutura de gestão de riscos da organização?
	2	Os contextos internos e externos estão documentados e alinhados? Considerando que a gestão de riscos de TI aborde contextos internos, e a gestão de riscos no geral englobe os contextos externos
	3	Existe o processo para avaliação de risco?
	4	Existe uma documentação para descrever os objetivos das avaliações e os critérios pelos quais os riscos são avaliados?
	5	Há métodos periódicos, cujo o objetivo seja mensurar os possíveis riscos?
	6	São identificados 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?
	7	É avaliado regularmente a probabilidade e o impacto de todos os riscos identificados, utilizando métodos qualitativos e quantitativos?
	8	É mantido um processo de respostas a riscos para assegurar que controles com uma adequada relação custo-benefício mitiguem a exposição aos riscos de forma contínua?
	9	Existe um planejamento e priorização das atividades de controle para implementar as respostas aos riscos identificadas como necessárias?
	10	Esse planejamento inclui a identificação de custos, benefícios e os responsáveis pela execução de controle?
	11	Existe um gerenciamento específico para o acesso ao banco de dados?
	12	Há documentações e políticas para gravação, leitura e alteração de informações internas?
	13	Existe um planejamento e priorização de informações?
	14	Existem cópias de segurança para qualquer tipo de informação?
	15	Existem cópias de segurança para informações essenciais para o funcionamento da organização?

Fonte: Autoria Nossa

Quadro 6: Bloco de perguntas sobre priorização dos riscos.

Priorização de riscos	Existe uma atenção especial aos:	
	1	Riscos do tipo financeiro.
	2	Riscos do tipo estratégico.
	3	Riscos do tipo operacional
	4	Riscos relacionados com desastres.
	5	Riscos relacionados com o ambiente externo
	6	Riscos relacionados com o ambiente interno.

Fonte: Autoria Nossa

Quadro 7: Bloco de perguntas sobre sistemas de informação.

Aquisição, desenvolvimento e manutenção de sistemas de informação	1	Existe um tratamento específico para requisitos de segurança de sistemas de informação?
	2	Existe um processo de análise e especificação dos requisitos de segurança?
	3	Existe alguma ferramenta que acompanhe o processamento correto nas aplicações utilizadas internamente?
	4	Existem parâmetros de validação dos dados de entrada?
	5	Existe algum controle do processamento de dados interno?
	6	Existe alguma método de verificação de integridade de mensagens compartilhadas (Ex: e-mails)?
	7	Existem parâmetros de validação dos dados de saída?
	8	Há algum processo de controles criptográficos? Para uma possível troca de dados.
	9	Existe uma política para o uso de controles criptográficos?
	10	Caso as duas últimas perguntas se apliquem a organização, existem um gerenciamento de chaves utilizadas para criptografia?

	11	Atualmente, qual o nível de segurança dos arquivos gerais do sistema interno da empresa?
	12	Há um controle de software operacional?
	13	Existe uma política de proteção de dados internos?
	14	Há um controle de acesso aos códigos-fonte dos programas/ferramentas utilizadas?
	15	Atualmente, em qual nível estaria a segurança adotada para processos de desenvolvimento e suporte?
	16	Existem uma documentação com procedimentos para controle de mudanças, considerando as mudanças dentro do âmbito de tecnologia da informação?
	17	Existe um processo de análise crítica/técnica das aplicações após mudanças?
	18	Existe Restrições sobre mudanças em pacotes de software
	19	Há um controle para evitar/ter ciência de possíveis vazamentos de informações?
	20	Há desenvolvimento terceirizado de software? Ou dependência de um software terceiro?
	21	Há uma gestão específica para vulnerabilidades técnicas?
	22	Há controle de vulnerabilidades técnicas?

Fonte: Autoria Nossa

Quadro 8: Bloco de perguntas sobre segurança da informação.

Organizando a segurança da informação - Parte Interna	1	Atualmente a organização tem uma área ou responsáveis específicos com a segurança da informação?
	2	Existe uma coordenação da segurança da informação?
	3	Existe uma distribuição de responsabilidades para ações de segurança da informação?
	4	Existe algum processo de autorização para os recursos de processamento da informação
	5	Existem termos de confidencialidade?
	6	Há políticas e documentos para especificar o uso de informações privadas?
	7	Há algum contato com técnicos externos especialistas em segurança da informação?
	8	Há uma análise crítica independente da segurança da informação?

Fonte: Autoria Nossa

Quadro 9: Bloco de perguntas sobre segurança da informação.

Organizando a segurança da informação - Parte Externa	1	Há identificação dos riscos relacionados com partes externas?
	2	Há identificações e alinhamento com a segurança da informação, quando existe relação com clientes externos?
	3	Há identificação e alinhamento com a segurança da informação nos acordos com terceiros?
	4	Existe uma política ou algum documento específico para lidar com o acesso a dados por terceiros?
	5	Existe alguma medida preventiva para limitar esse acesso de terceiros?
	6	Há algum método de armazenamento de ações de terceiros dentro da organização (exemplo: logs para rastreio)

	7	Quando há troca de dados sigilosos com terceiros existe um tratamento específico para assegurar a integridade dos dados em trânsito?
	8	A organização toma medidas de segurança específicas para o relacionamento com terceiros?

Fonte: Autoria Nossa

Quadro 10: Bloco de perguntas sobre a área de gestão da empresa.

Gerenciamento **1 e 2** Gestão Operacional **3 a 5** Gestão de mudanças **6 à 11** Gerenciamento de serviços terceirizados **12 à 17** Gestão de capacidade **18 à 20** Gerenciamento da segurança em redes **21 a 41** Gerenciamento e definição de normas de conduta	1	Existe uma área para procedimentos e responsabilidades operacionais?
	2	Existe Documentação dos procedimentos de operação?
	3	Há uma área específica ou que aborde o assunto: gestão de mudanças?
	4	Há segregação de funções?
	5	Existe a separação dos recursos de desenvolvimento, teste e de produção?
	6	Há um gerenciamento de serviços terceirizados?
	7	Existe uma supervisão específica para as entregas de serviços?
	8	Há monitoramento e análise crítica de serviços terceirizados?
	9	Há gerenciamento de mudanças para serviços terceirizados?
	10	Há planejamento e aceitação dos sistemas
	11	existe um gerenciamento de capacidade?
	12	Existe um termo para aceitação de sistemas?
	13	Há proteção contra códigos maliciosos e códigos móveis?
	14	Há controles contra códigos maliciosos?
	15	Há controles contra códigos móveis?
	16	Existem cópias de segurança?
	17	Existem cópias de segurança específicas para informações?
	18	Há gerenciamento da segurança em redes?
	19	Existem controles de redes?
	20	Há termos de segurança dos serviços de rede?
	21	Existem uma definição das normas de conduta?

	22	Há um termo para manuseio de mídias internamente?
	23	Há um gerenciamento de mídias removíveis?
	24	Há uma política para descarte de mídias?
	25	Existem procedimentos para tratamento de informação?
	26	Há termos de segurança e/ou documentação dos sistemas?
	27	Existe algum gerenciamento das normas de conduta?
	28	Existem políticas e procedimentos para troca de informações?
	29	As políticas costumam ser reavaliadas com o passar do tempo?
	30	Há política de segurança para mídias em trânsito, como mensagens eletrônicas?
	31	Existe sistemas específicos que armazene informações de negócios?
	32	A organização utiliza serviços de comércio eletrônico?
	33	A organização costuma atualizar os documentos e políticas de segurança da informação?
	34	A organização trabalha com transações online?
	35	Existem informações publicamente disponíveis?
	36	Há um banco específico para armazenar registros de ações (logs) para diferentes funções que atuem diretamente com informações restritas/secretas?
	37	Existem registros de auditoria
	38	Há monitoramento de uso dos sistemas internos?
	39	Há proteções das informações dos registros (logs)?
	40	Há registros (logs) de administradores e operadores?
	41	Registros (log) de falhas
	42	Há sincronização dos relógios utilizados nos sistemas internos?

Fonte: Autoria Nossa

Quadro 11: Bloco de perguntas sobre a gestão dos ativos da organização

Gestão de ativos	1	Há uma gestão específica que especifique as responsabilidades pelos ativos?
	2	Há um inventário dos ativos?
	3	Existe um proprietário/responsável pelos ativos?
	4	Há um termo de aceite para especifícar o uso aceitável dos ativos?
	5	Existe algum tipo de classificação da informação?
	6	Se houver classificação, há alguma recomendação ou norma específica para esta classificação?
	7	Existem tratamentos da informação de acordo com sua "classe"?
	8	A organização mensura em níveis de sigilo as informações/dados internos?

Fonte: Autoria Nossa

Quadro 12: Bloco de perguntas sobre a gestão de continuidade de negócios da empresa

Gestão da continuidade do negócio	1	Existem alguma medida específica da área de T.I para considerar parâmetros de continuidade do negócio, relativos à segurança da informação?
	2	Existe o processo de continuidade de negócios e análise/avaliação de riscos?
	3	Atualmente a segurança da informação faz parte do processo de gestão da continuidade do negócio?
	4	Há um desenvolvimento e implementação de planos de continuidade relativos à segurança da informação?
	5	Atualmente existe um documento detalhando os planos de continuidade do negócio?
	6	Existem testes periódicos, manutenção e reavaliação dos planos de continuidade do negócio?

Fonte: Autoria Nossa

Quadro 13: Bloco de perguntas sobre a gestão de incidentes de segurança da informação.

Gestão de incidentes de segurança da informação	1	Há notificações sobre fragilidades e eventos de segurança da informação?
	2	Há notificações de eventos de segurança da informação?
	3	Há notificações de fragilidades de segurança da informação?
	4	Há uma gestão de incidentes de segurança da informação?
	5	Existe um termo para fidelizar as responsabilidades e procedimentos dentro do setor de T.I?
	6	Existe um processo de documentação pós-incidente, com objetivo de aprendizado com os incidentes de segurança da informação e melhorias?
	7	Há um processo de coleta de evidências?

Fonte: Autoria Nossa

2.2.5. RELATÓRIO

A partir da avaliação realizada, pode-se extrair algumas informações acerca dos níveis de maturidade atual do processo da análise de riscos da empresa fundamentado pelas boas práticas sugeridas pelo COBIT.

O relatório demonstrará o nível de maturidade do processo através de gráficos, além de descrever alguns fatores que levaram o processo de análise de risco da empresa avaliada estar no nível exibido e quais ações são plausíveis para otimizá-lo com o objetivo de aderir as diretrizes necessárias para uma melhor gestão de segurança da informação.

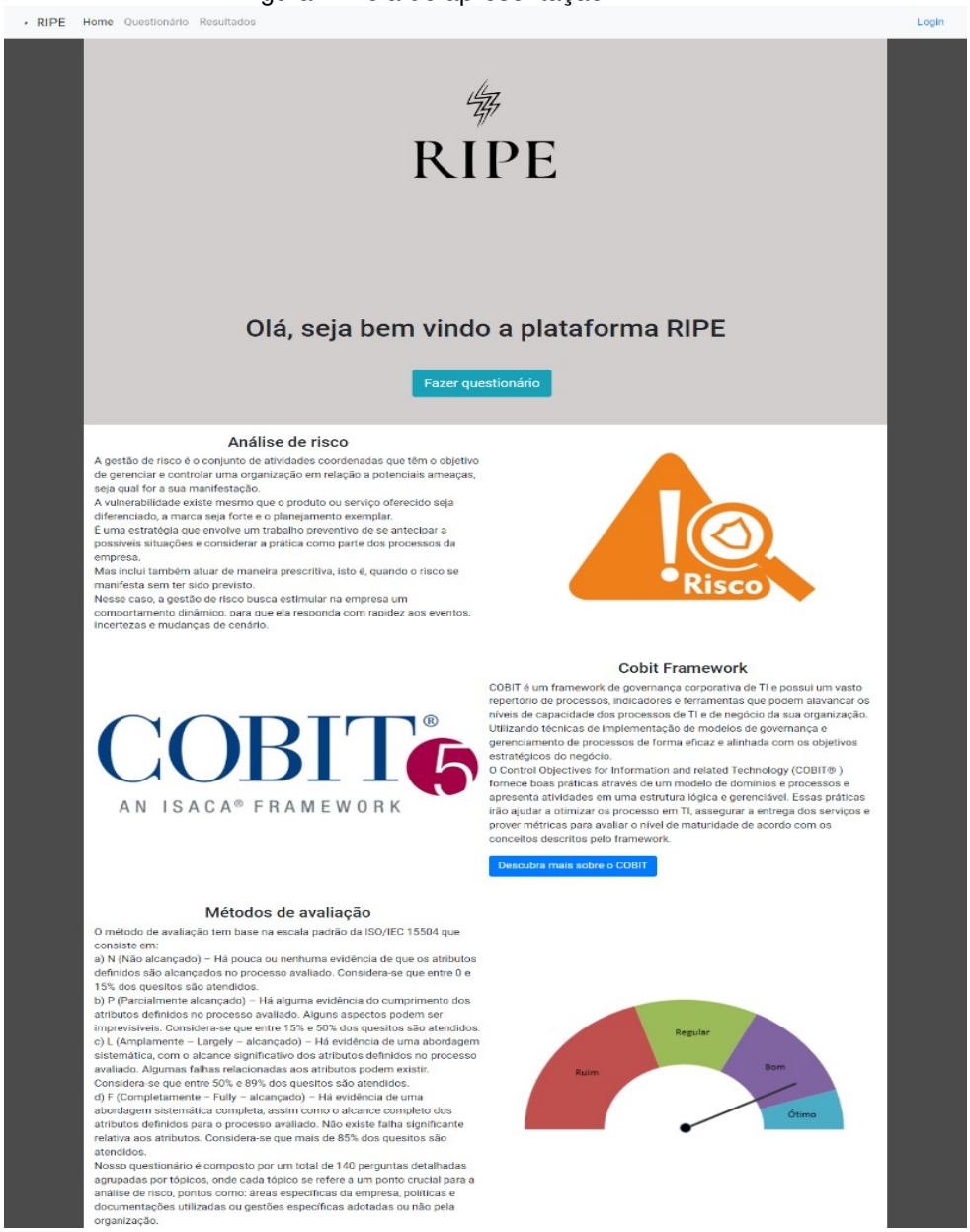
2.2.6. PROTÓTIPO RIPE

Idealizamos o projeto da aplicação web para agir de maneira eficaz e com fácil utilização. O layout simples e didático das telas tem esse objetivo torná-la acessível para o maior público possível.

A divisão das telas age conforme o comportamento e funcionalidade específica, seja o cadastro de um novo usuário, como a tela de questionário ou a exibição do relatório avaliativo, há uma nova interface para cada etapa.

2.2.6.1. TELA DE APRESENTAÇÃO

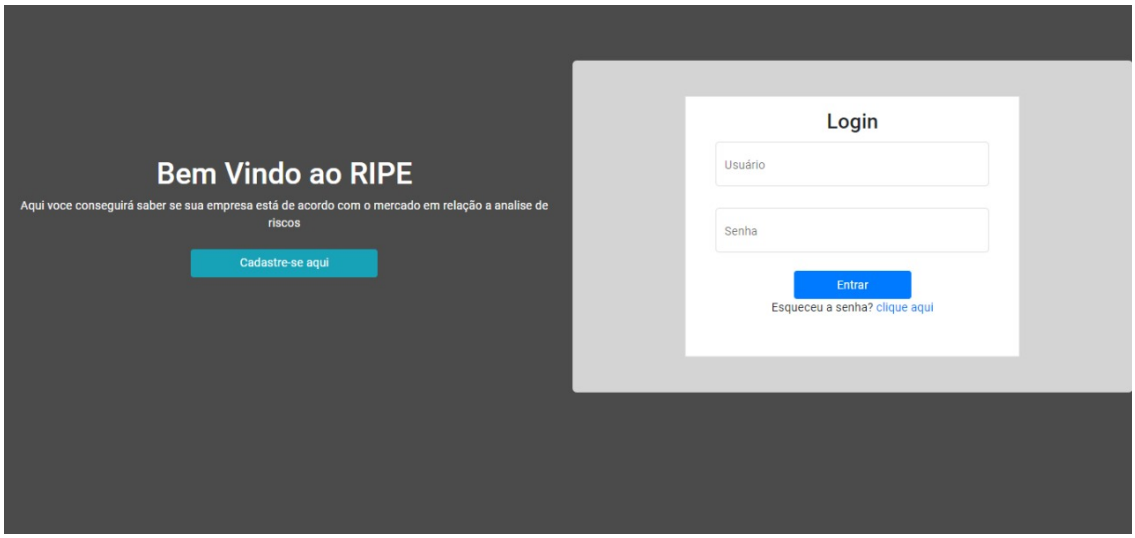
Figura 7: Tela de apresentação



A tela de apresentação do site, exibindo a definição de alguns conceitos importantes para a nossa aplicação.

2.2.6.2. TELA DE LOGIN

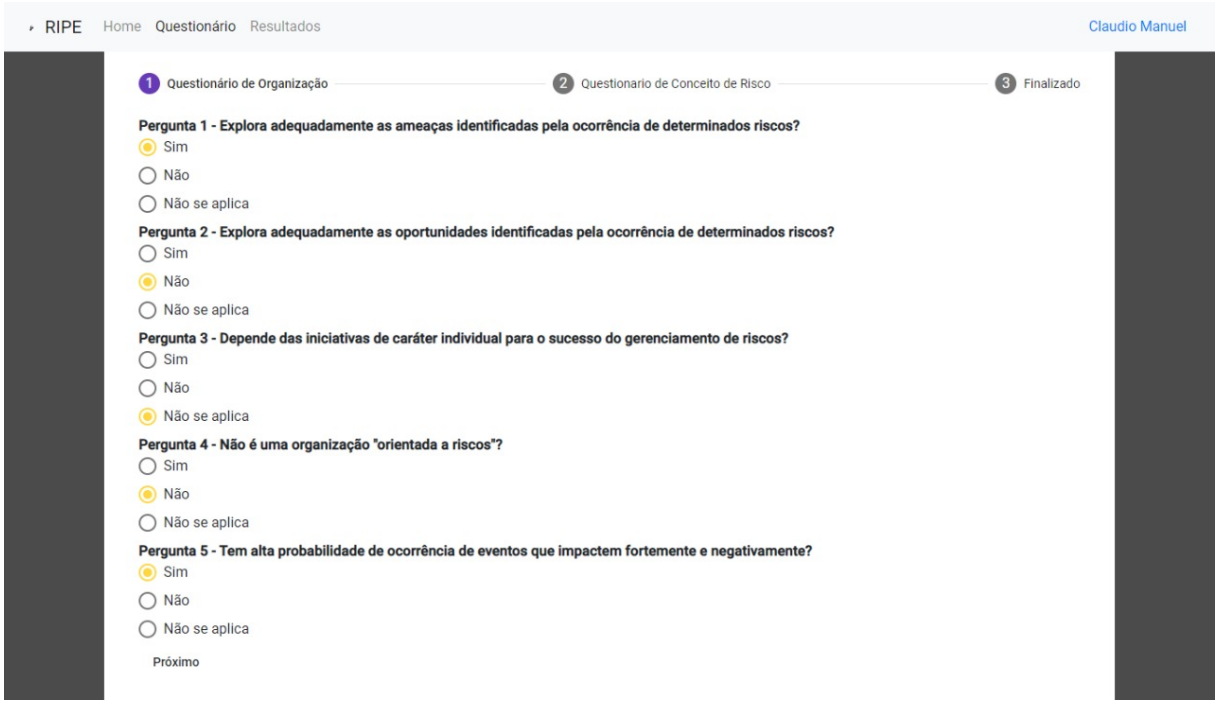
Figura 8: Tela de Login



A tela de cadastro do usuário. Com a opção de criar um registro ou efetuar o *login* para obter acesso ao questionário e aos relatórios avaliativos.

2.2.6.3. TELA DE EXIBIÇÃO QUESTIONÁRIO

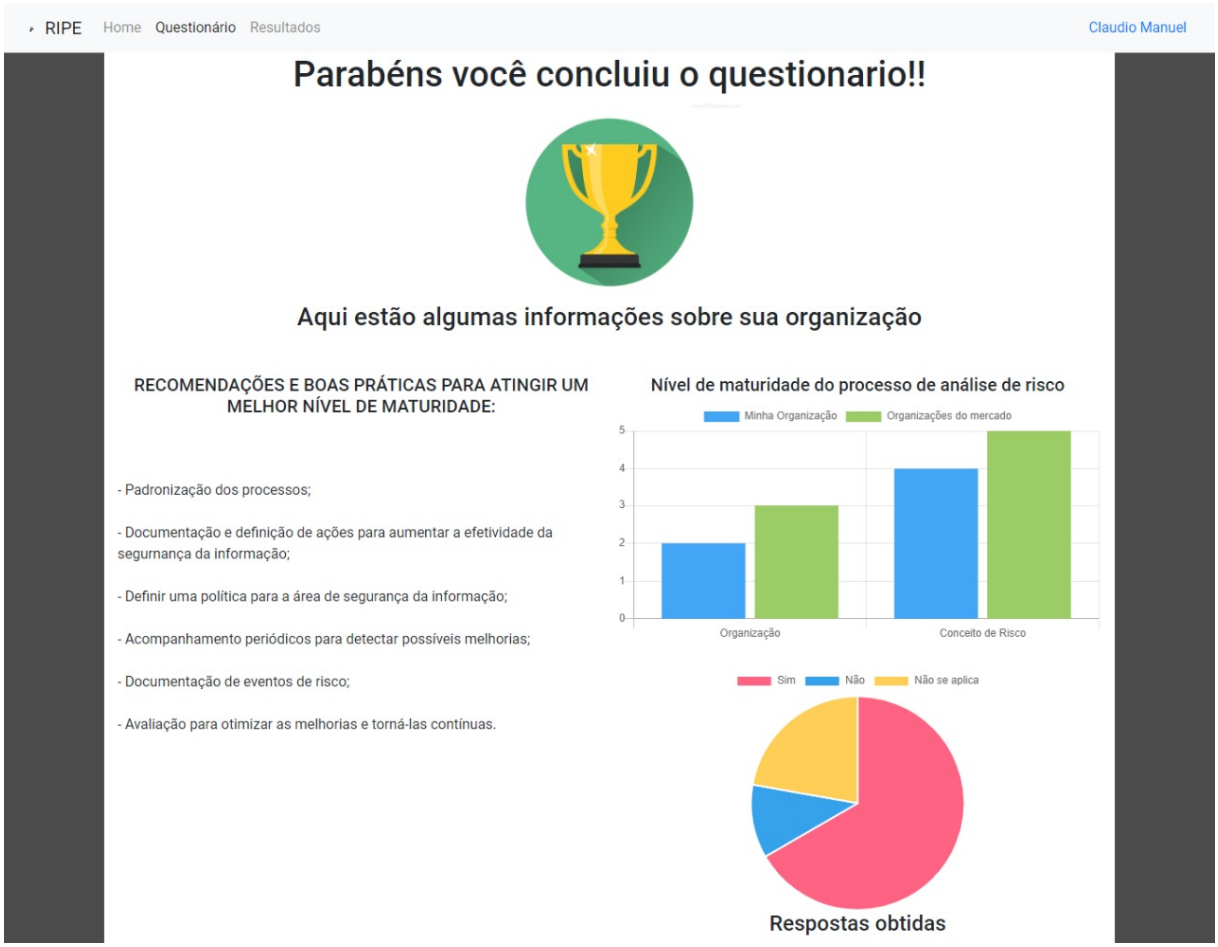
Figura 9: Tela de exibição do questionário



A tela de exibição do questionário com um layout em *steps*, ou seja, o questionário será dividido em etapas, onde cada etapa tem um tema principal a ser abordado, como na imagem, o primeiro passo as questões tem o objetivo de obter dados sobre a organização de forma geral, já o segundo tem o objetivo de entender como a empresa define e compreende o conceito de risco.

2.2.6.4. TELA DE EXIBIÇÃO DO RELATÓRIO

Figura 10: Tela de exibição do relatório



A tela de exibição do relatório terá a lógica baseada nas respostas obtidas no questionário. Será demonstrado a porcentagem das respostas, com um gráfico pizza, além de exibir o nível de maturidade do processo de análise de risco, conforme a nossa regra de avaliação e algumas ações e melhorias possíveis de acordo com o nível obtido na avaliação

3. CONCLUSÃO

Uma das constatações mais importantes trazidas pelo COBIT para o cenário de TI mundial é o fato de que o profissional de TI precisará cada vez mais entender sobre o negócio da organização ao qual ele faz parte.

Percebeu-se que a utilização da Informática, nas mais diversas áreas das organizações, está passando de um diferencial para um requisito. A partir deste fato, tem-se um aumento na demanda por tecnologias inovadoras, todas com o objetivo de reduzir custos, auxiliando os colaboradores em suas atividades.

Com base nos estudos realizados sobre as melhores práticas sugerida pelo COBIT, este trabalho de conclusão teve como foco desenvolver uma ferramenta que auxilie no processo de avaliação de um processo de análise de risco, com a exposição e acompanhamento dos níveis de maturidade alcançados pelo departamento de segurança de TI em relação às melhores práticas sugeridas pelo COBIT.

Por se tratar de uma ferramenta construída para plataforma Web, a “RIPE” permite que as avaliações e os resultados obtidos de acordo com o questionário, possam ser facilmente disseminadas entre as pessoas responsáveis.

A partir dos testes e validações realizados durante o desenvolvimento deste trabalho, pode-se afirmar que a ferramenta “RIPE” possui plenas condições de informar o nível de maturidade e possíveis ações para otimizar um processo tão relevante no contexto de segurança de uma organização como a análise de risco.

4. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação**. ABNT NBR ISO/IEC 27002. Rio de Janeiro: ABNT, 2013.

ARAÚJO, NONATA. "**Segurança da Informação: Sobre a Necessidade de Proteção de Sistemas de Informações"**. Revista Espaço Acadêmico n. 42. 2004. Disponível em: <https://administradores.com.br/artigos/seguranca-da-informacao-ti>. Acesso em: 10/01/2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação.** ABNT NBR ISO/IEC 27005. Rio de Janeiro: ABNT, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da Informação – Técnicas de segurança – Sistema de gestão da segurança da informação.** ABNT NBR ISO/IEC 27001. Rio de Janeiro: ABNT, 2013.

BACKER, B. **"Business Modeling with UML: The Light at the End of the Tunnel"**, 2001. Disponível em: <http://www106.ibm.com/developerworks/rational/library/content/RationalEdge/archives/dec01.html>. Acesso em: 20/05/2020.

DOURADO, Luzia. "**Apostila COBIT 5, Framework de Governança e Gestão Corporativa TI**", 2014. Disponível em: <http://www.gestaoporprocessos.com.br/wp-content/uploads/2014/06/2APOSTILA-COBIT-5-v1.1.pdf>. Acesso em: 02/08/2019.

FERNANDES, Jorge H. C. “**Sistemas Complexos.”** Universidade de Brasília, Curso de Especialização em Gestão de Segurança da Informação e Comunicações, CEGSIC, Brasília, 2008, Apostila.
Disponível em: <https://cic.unb.br/~jhcf/MyBooks/cegsic/2007_2008/livro_gsic.pdf>
Acesso em: 02/03/2020

FIDALGO, José Jorge Caramelo. “**Implementar COBIT em empresas TI**”, 2017. Disponível em: <https://repositorioaberto.uab.pt/bitstream/10400.2/6592/1/TMISE_JoseFidalgo.pdf>. Acesso em: 04/08/2019

ISACA: **Process Assessment Model (PAM):** Using COBIT® 5, 2013. Disponível em: http://www.isaca.org/COBIT/Pages/COBIT-5-PAM.aspx. Acesso em: 04/08/2019.

ISACA: **Self-assessment Guide:** Using COBIT® 5, 2013. Disponível em: http://www.isaca.org/COBIT/Pages/Self-Assessment-Guide.aspx. Acesso em: 04/08/2019

ISACA: **COBIT 5: Implementation**, 2012, p.2. Disponível em: http://www.isaca.org/COBIT/Pages/COBIT-5-Implementation-product-page.aspx. Acesso em: 04/08/2019

ISACA: **COBIT 5: A Business Framework for the Governance and Management of Enterprise IT**, 2012, pp. 41–45. Disponível em: <https://www.researchgate.net/publication/247778781_COBIT_5_and_Enterprise_Governance_of_Information_Technology_Building_Blocks_and_Research_Opportunities>. Acesso em: 04/08/2019.

ISACA, “**Implementação COBIT 5**”, 2012. Disponível em: <http://www.isaca.org/COBIT/focus/Pages/importance-of-cmmi-dev-in-cobit-based-it-governance.aspx>. Acesso em: 04/08/2019

ISACA, “**Modelo Corporativo para a Governança e Gestão de TI da Organização**”, 2012. Disponível em: <http://www.isaca.org/COBIT/Pages/COBIT-5-portuguese.aspx>. Acesso em: 04/08/2019.

IT Governance Institute, “**Mapping of CMMI for Development With COBIT**” V1.2, 2016, Disponível em: <https://www.worldcat.org/title/cobit-mapping-mapping-of-cmmi-for-development-v12-with-cobit-41/oclc/713538288>. Acesso em: 03/08/2019

MANOEL, Sérgio da Silva, “**Governança de Segurança da Informação: Como criar oportunidades para o seu negócio**”, São Paulo, Brasport, 2014.

MASSARI, Vitor “**Gerenciamento Ágil de Projetos**”, 2014. Disponível em: <https://www.projectbuilder.com.br/Downloads/ebook-gratuito-scrum-pmbok.pdf>. Acesso em: 04/08/2019

PASQUINI, Alex. GALIÈ, Emidio. “**COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process**”,2013. Disponível em: <https://www.researchgate.net/publication/321016045_Process_Capability_Model_Based_on_COBIT_5_Assessments_Case_Study>. Acesso em: 03/08/2019

RENAUD, Paul E. **“Introdução aos Sistemas Cliente/Servidor: Guia Prático para Profissionais de Sistemas”**, 1994

RAMOS, Patrícia Edí. **“Vivendo uma nova era: a tecnologia e o homem, ambos integrantes de uma sociedade que progride rumo ao desenvolvimento”.** Disponível em: **<**http://www2.seduc.mt.gov.br/-/vivendo-uma-nova-era-a-tecnologia-

e-o-homem-ambos-integrantes-de-uma-sociedade-que-progride-rumo-ao-desenvolvimen-1>**.** Acesso em 13/04/2020

SFALSIN, Eliana. **"A importância da Governança Corporativa"**, 2018**.** Disponível em: <http://administradores.com.br/artigos/a-importancia-da-governanca-corporativa> Acesso em: 04/08/2019

SOMMERVILLE, Ian. **Engenharia de software. 8 Edição.** Editora: Pearson, 2007.