Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

# Gestão de Riscos em Computação em Nuvem para a Gestão de Identidade e Acessos aplicada ao Sistema Decom Digital do Ministério da Economia

Claudio Augusto Novais Ferraz

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Orientador
Prof. Dr. Edgard Costa Oliveira

Brasília
2019

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

NF381g

Novais Ferraz, Claudio Augusto
Gestão de Riscos em Computação em Nuvem para a Gestão de Identidade e Acessos aplicada ao Sistema Decom Digital do Ministério da Economia / Claudio Augusto Novais Ferraz; orientador Edgard Costa Oliveira. -- Brasília, 2019.
171 p.

Dissertação (Mestrado - Mestrado Profissional em Computação Aplicada) -- Universidade de Brasília, 2019.

1. Gerenciamento de Identidade e Acessos. 2. Computação em Nuvem. 3. Autenticação por Contexto. 4. Autenticação por Comportamento. 5. Gestão de Riscos. I. Costa Oliveira, Edgard, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

# Gestão de Riscos em Computação em Nuvem para a Gestão de Identidade e Acessos aplicada ao Sistema Decom Digital do Ministério da Economia

Claudio Augusto Novais Ferraz

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Prof. Dr. Edgard Costa Oliveira (Orientador)
CIC/UnB

Prof. Dr. Ari Melo Mariano
EPR/UnB

Dr. Altino José Mentzingen de Moraes
Ministério da Economia

Prof.a Dra. Aletéia Patrícia Favacho de Araújo Von Paumgartten
Coordenadora do Programa de Pós-graduação em Computação Aplicada

Brasília, 31 de julho de 2019

# Dedicatória

Primeiramente a Deus que me deu essa oportunidade e forças para buscar essa realização.

Aos meus pais por todo amor, oportunidades e ensinamentos.

A minha família, em especial a minha amada esposa Taíse Ferraz, pelo amor e apoio incondicional.

As minhas filhas Mel e Clara, grandes bênçãos em nossas vidas, pela compreensão e apoio durante toda a jornada.

Aos meus irmãos e amigos que nos apoiam para alcançar essas grandes conquistas.

# Agradecimentos

Agradeço principalmente ao orientador e amigo, Prof. Dr. Edgard Costa, pela confiança, paciência e serenidade.

Agradeço aos meus colegas do PPCA por todo apoio prestado.

Agradeço especialmente ao PPCA (Programa de Pós-Graduação em Computação Aplicada) e a Universidade de Brasília-UNB por todo conhecimento e apoio ao longo de toda trajetória de acadêmica. O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), por meio do Acesso ao Portal de Periódicos.

# Resumo

As informações e os dados inseridos nos sistemas e serviços digitais do Governo devem ser protegidos contra fraudes e ataques de identidade e acesso que afetam a confidencialidade, integridade e disponibilidade dessas informações, principalmente dados sigilosos quando os ativos da informação são migrados para o ambiente de computação em nuvem. Diante desta necessidade, este trabalho realiza uma pesquisa exploratória e qualitativa a fim de realizar uma gestão de riscos em computação em nuvem considerando o Gerenciamento de Identidades e Acessos (GIA) aplicado ao Sistema Decom Digital (SDD) do Ministério da Economia. O Governo Federal adotou uma política de Governo Digital que tem como uma meta ousada a digitalização de boa parte dos serviços públicos. Por outro lado, cresce exponencialmente os casos de fraudes digitais e vazamento de informações que afetam qualquer tipo de organização inserida no mundo digital. Para oferta desses serviços o governo também passa a utilizar a computação em nuvem, o que aumenta o desafio de proteger dados sensíveis ou sigilosos. Legislações recentes têm surgido como forma de estabelecer diretrizes e metas para o tratamento dos riscos e efetivação de controles de segurança, como a Lei Geral de Proteção aos Dados (LGPD) e as políticas de gestão de riscos dos órgãos. Diante deste cenário, o governo precisa mitigar os riscos de concretização dessas ameaças adotando robustos controles de segurança a fim de proteger as informações inseridas em seus sistemas e serviços digitais. O Ministério da Economia possui uma ampla plataforma de sistemas e serviços, dentre estes o Sistema Decom Digital, que processa informações sigilosas e é um dos candidatos a migrar para a nuvem. A solução de GIA reúne políticas e tecnologias para tratar riscos como o de acessos indevidos, identidades ilegítimas e privilégios excessivos. A partir do resultado da avaliação de riscos serão identificadas e caracterizadas tecnologias de GIA e será aplicada computacionalmente uma dessas tecnologias, no caso a Autenticação por Contexto ou Autenticação por Comportamento, que é uma tecnologia que autentica o usuário de forma transparente a partir de seu contexto de acesso ou perfil comportamental, ela tem um funcionamento dinâmico para se adequar as mudanças de perfil de acesso no processo de autenticação dos usuários e estabelece uma camada adicional de segurança, podendo ser usada com outros mecanismos de autenticação. O uso de soluções de segurança mais eficazes no Sistema Decom Digital tem a finalidade de preservar as informações que muitas vezes são de terceiros e garantir maior confiabilidade no uso dos serviços e sistemas do Governo Federal.

**Palavras-chave:** Gerenciamento de Identidade e Acessos, Autenticação por Contexto, Computação em Nuvem, Autenticação, Riscos.

# Abstract

Information and data entered into Government digital systems and services must be protected against fraud and identity and access attacks that affect the confidentiality, integrity, and availability of such information, particularly sensitive data when information assets are migrated to the computing environment. in the cloud. Given this need, this work conducts an exploratory and qualitative research in order to perform a risk management in cloud computing considering the Identity and Access Management (IAM) applied to the Decom Digital System (SDD) of the Ministry of Economy. The Federal Government has adopted a Digital Government policy that has as its bold goal the digitization of most public services. On the other hand, cases of digital fraud and information leaks that affect any type of organization in the digital world grow exponentially. To provide these services, the government also uses cloud computing, which increases the challenge of protecting sensitive data. Recent legislation has emerged as a way to set guidelines and targets for risk management and enforcement of security controls, such as the General Data Protection Act and agency risk management policies. Given this scenario, the government needs to mitigate the risks of realizing these threats by adopting robust security controls to protect the information entered into its digital systems and services. The Ministry of Economy has a broad platform of systems and services, including the Decom Digital System, which processes sensitive information and is a candidate to migrate to the cloud. The IAM solution brings together policies and technologies to address risks such as improper access, illegitimate identities and excessive privileges. From the result of the risk assessment, IAM technologies will be identified and characterized and one of these technologies will be computationally applied, in this case Context Authentication or Behavior Authentication, which is a technology that transparently authenticates the user from their context access or behavioral profile, it has a dynamic functioning to suit the changes of access profile in the user authentication process and establishes an additional layer of security and can be used with other authentication mechanisms. The use of more effective security solutions in the Decom Digital System is intended to preserve information that is often from third parties and ensure greater reliability in the use of Federal Government services and systems.

**Keywords:** Identity and Access Management, Context Authentication, Cloud Computing, Authentication, Risks.

# Sumário

# Lista de Figuras

# Lista de Tabelas

# Lista de Abreviaturas e Siglas

**APF** Administração Pública Federal.

**CCONV** Coordenação de Contratos e Convênios.

**CGU** Controladoria Geral da União.

**COBIT** Control Objectives for Information and related Technology.

**COPLI** Coordenação de Processos Licitatórios.

**CSA** *Cloud Security Alliance*.

**CSIC** Comitê de Segurança da Informação e Comunicações.

**DSIC** Departamento de Segurança da Informação e Comunicações.

**EGD** Estratégia de Governança Digital.

**GDPR** General Data Protection Regulation.

**GIA** Gerenciamento de Identidades e Acessos.

**GSI/PR** Gabinete de Segurança Institucional da Presidência da República.

**GSIC** Gabinete de Segurança Institucional.

**IA** Inteligência Artificial.

**IAM** *Indentity and Accesss Management*.

**LAI** Lei de Acesso à Informação.

**LGPD** Lei Geral de Proteção aos Dados.

**MDIC** Ministério da Indústria, Comércio Exterior e Serviços.

**ME** Ministério da Economia.

**MFA** Autenticação MultiFator.

**NC** Nível de Confiança.

**NIST** *National Institute of Standards and Technology.*

**NRI** Nível de Risco Inerente.

**PDTIC** Plano Diretor de Tecnologia da Informação e Comunicações.

**PEAD** Programa Eletrônico de Acesso Digital.

**PNSI** Plano de Segurança Nacional de Segurança da Informação.

**POSIC** Política de Segurança da Informação e Comunicações.

**RC** Risco de Controle.

**RNI** Risco Inerente Identificado.

**SDD** Sistema Decom Digital.

**SIC** Segurança da Informação e Comunicações.

**SPOA** Subsecretaria de Planejamento Orçamento e Administração.

**SSO** *Single Sign-On.*

**TCU** Tribunal de Contas de União.

**TIC** Tecnologia da Informação e Comunicações.

# Capítulo 1

# Introdução

O Ministério da Economia (ME) atua em diversas áreas e subáreas da Economia do país, tratando de diversos aspectos como sistema monetário, políticas de preços e cambial, previdência, trabalho, orçamento e também com o desenvolvimento de políticas para o Comércio Exterior do país. O recentemente criado ME, pelo Decreto nº 9.679, de 2 de janeiro de 2019, revogado pelo Decreto nº 9.745, de 08 de abril de 2019 [1], unificou diversas pastas em uma única pasta para tratar de diversos temas, isso fez com que o novo órgão passasse a atuar com diversos serviços para o cidadão e uma grande arquitetura tecnológica e portfólio de sistemas. O ME tem em sua plataforma digital o Sistema Decom Digital (SDD) que transaciona e armazena informações sigilosas de entidades que lidam com Comércio Exterior e Serviços.

O Governo Digital [2] objetiva transformar a relação do governo com a sociedade e promover interatividade com cidadãos, empresas e órgãos governamentais, melhorar o processo de democratização do país, dinamizar os serviços públicos e proporcionar uma administração pública mais eficiente, já que, agora, a sociedade possui meios digitais para interagir mais facilmente e se manifestar em relação às ações governamentais. Países como a Estônia, no Leste Europeu, apostaram alto na tecnologia para reduzir a burocracia. Nesse país, praticamente todos os serviços públicos estão online [3]. A plataforma digital do país conecta bancos de dados de 950 instituições públicas e empresas do país, permitindo o cruzamento de informações e tornando o atendimento muito mais ágil. No Brasil, o emaranhado de regras e procedimentos exigidos pela legislação do país atrapalha tanto a rotina das empresas quanto a do cidadão comum, apesar do avanço no índice da Organização da Nações Unidas (ONU) de desenvolvimento do Governo Eletrônico onde se encontre na 44ª posição, enquanto que a Estônia é o 16º pais [4]. O excesso de burocracia tem impedido o Brasil de avançar mais no ranking mundial de competitividade. Apesar da evolução do Governo Digital em países como a Estônia, a iniciativa é criticada por grandes potências como os Estados Unidos que adotam uma postura mais cautelosa, pois

apesar de também serem um dos expoentes em Governo Digital, para alguns serviços que precisam preservar a confidencialidade dos dados, os aspectos de Segurança da Informação e Comunicações são de fundamental importância e precisam evoluir na mesma velocidade para garantir um serviço mais confiável para o cidadão e usuários dos serviços digitais [5].

A progressiva digitalização do setor público no Brasil durante a última década permitiu o surgimento de projetos emblemáticos a nível federal, o que contribuiu para mudar significativamente a relação entre os cidadãos e o setor público. O Governo brasileiro adotou uma Estratégia de Governança Digital (EGD) e desburocratização dos serviços públicos, alicerçado pela adoção de novas tecnologias e do crescimento e democratização do uso da Internet. A EGD tem como um dos indicadores principais a digitalização dos serviços públicos, que impulsiona a iniciativa de adoção de um Governo Digital que coloca o país em ascendência na escala de nível mundial de desempenho digital dos países em oferta de serviços públicos [2].

Diante desse novo cenário de crescimento da plataforma digital de serviços públicos, a Segurança da Informação e Comunicações (SIC) passa a ser uma grande preocupação para a ampliação de serviços digitais no governo. A SIC compreende um conjunto de ações que busca proteger e preservar os ativos de informação, assegurando-lhes disponibilidade, integridade, confidencialidade e autenticidade no trato das informações. Segurança é o estado em que se está livre de perigos e incertezas. Nas instituições governamentais, a segurança está relacionada a proteger tudo aquilo que possui valor para o órgão ou entidade da Administração Pública Federal, ou seja, os ativos de informação, as pessoas e a sua imagem [6].

Modelos como o do Control Objectives for Information and related Technology (COBIT), mundialmente reconhecido como um dos principais modelos de Governança e Gestão de Tecnologia da Informação [7], trata a Segurança da Informação e a Gestão dos Riscos com alta relevância para atender as partes interessadas, agregar valor e alcançar os objetivos das organizações. No âmbito da Governança, no domínio "Avaliar, Dirigir e Monitorar" (EDM), existe o processo "Garantir a Otimização dos Riscos" e no âmbito de Gestão, existe no domínio "Alinhar, Planejar e Organizar" (APO) os processos "APO12 - Gerenciar Riscos" e "APO13 - Gerenciar Segurança". Devido à importância desses temas para a Governança e Gestão de TIC o COBIT ainda publicou dois guias específicos para tratar com mais detalhes e aprofundamento esses temas, o "COBIT 5 para Segurança da Informação" e o "COBIT 5 para Risco" [8].

Com o crescente número de fraudes digitais, ações de pessoas mal-intencionadas e de criminosos cibernéticos [9], os aspectos de segurança da informação tornam-se cada vez mais relevantes para um governo que busca aumentar sua plataforma de serviços digitais. Em particular, o uso de soluções e tecnologias de controle de acesso como a autenticação

e a autorização, que buscam proteger às informações de acessos indevidos garantindo a confidencialidade e integridade dos dados. Os crimes digitais estão cada vez mais eficientes e diversificados e afetam até grandes empresas de tecnologia, que teoricamente, possuem grandes investimentos em segurança e proteção dos dados e informações dos seus clientes. Esses crimes cibernéticos exploram potenciais vulnerabilidades dos ativos de informação causando enormes prejuízos financeiros e de imagem. Esse é o caso de uma grande empresa de nível mundial que é umas das redes sociais mais conhecidas e utilizadas do mundo, que descobriu uma violação de segurança que afetou cerca de 50 milhões de contas de usuários, o que poderia permitir que hackers assumissem o controle das contas, implicando em um grande vazamento de informações pessoais que deveriam ser mantidas em sigilo e somente compartilhadas a quem os usuários concedessem esse direito. Esse é um caso explícito de vazamento de informações por ações de pessoas mal-intencionadas [10]. Essa realidade não é diferente no governo que lida e armazena informações pessoais e sigilosas de empresas e cidadãos, e ao disponibilizar os serviços no mundo digital deve cuidar para que essas ações de hackers não comprometam a confiabilidade e disponibilidade dos serviços digitais do governo.

O controle de acesso atua desde o processo de identificação do usuário quando este tenta acessar um sistema ou serviço, no processo de autenticação que consiste em validar o acesso solicitado pelo usuário, na autorização que controla quais dados o usuário pode acessar e por fim na auditoria que levanta informações de acessos indevidos e possíveis comprometimentos gerados por esses acessos. A gestão de identidades e o controle de acesso são de grande importância para evitar acessos não legítimos, criando controles cada vez mais eficazes para proteção dos ativos de informação, ambos fazem parte de um conjunto de tecnologias e processos que visam à proteção de identidade e acessos, o que é chamado de Gerenciamento de Identidades e Acessos (GIA).

A GIA é um conjunto de processos e tecnologias para proteção dos ativos de informação contra ataques e fraudes digitais. As novas tecnologias utilizadas pela GIA têm contribuído de forma eficaz para dificultar as ações e resultados pretendidos pelos criminosos digitais. São soluções que dificultam as fraudes digitais por meio do fortalecimento das tecnologias de acesso e novos tipos de verificação do comportamento dos usuários ou contexto de acesso quando tentam se autenticar para utilizar um determinado serviço digital. Atuam por meio de uma correlação de fatores que identificam o perfil comportamental e contextual de acesso de cada conta de usuário ou por meio de relação de confiança entre provedores de serviços. O GIA, do acrônimo em inglês *Indentity and Accesss Management* (IAM) passa a ser considerado pelo Governo nesse processo de ampliação e melhoria de seus serviços digitais, pois otimiza e cria novos controles de segurança evitando acessos ilegítimos e fraudes digitais *online*.

O Governo a fim de racionalizar custos com a hospedagem e a manutenção das infraestruturas de Tecnologia da Informação editou normativo recomendando que os órgãos não invistam em estruturas locais de datacenter ou salas cofres e passem utilizar serviços de nuvem, que além de proporcionar custos mais módicos devido ao compartilhamento de sua infraestrutura, oferecem uma estrutura de maior resiliência com instalações e equipamentos redundantes e de contingência [11]. A computação em nuvem (*cloud computing*) é um modelo computacional que deve prover, a partir de uma rede de dados, uma estrutura tecnológica por meio de serviços que são caracterizados por uma necessidade de maior flexibilidade, escalabilidade e benefícios de custo [12]. Como o ME não dispõe de uma infraestrutura de hospedagem que possa garantir alta disponibilidade aos sistemas se comparado a um provedor de serviços em nuvem, além do alto custo de implantação e manutenção de uma infraestrutura deste tipo, é desejável a migração dos seus sistemas mais críticos para a nuvem.

Essa possível migração torna ainda mais latente as lacunas de segurança dos sistemas, ou seja, suas vulnerabilidades, por estarem em um ambiente não controlado pelo órgão e acessíveis a partir de qualquer ponto do globo.

Apesar da computação em nuvem reduzir o escopo geral de segurança e não exigir que os clientes gerenciem parte da pilha de computação em um modelo de responsabilidade compartilhada, esta é uma boa oportunidade para novos tipos de abordagens e adoção de novos métodos para proteger as informações. A nuvem exigirá uma abordagem diferente para a segurança – os hábitos e projetos de segurança da estrutura de armazenamento local não funcionam bem para informações armazenadas na nuvem por tratar-se de outro ambiente com outras políticas e tecnologias de Segurança da Informação e Comunicações (SIC). As organizações não devem presumir que usar um serviço de nuvem significa que tudo o que eles fazem dentro dessa nuvem será seguro. Os requisitos de segurança devem ter maior atenção com uso da computação em nuvem, pois além dos controles tradicionais de segurança da infraestrutura local os provedores de serviços em nuvem e seus clientes devem se preocupar mais com o controle de acesso interno e externo e o vazamento de informações compartilhadas e disponíveis em um ambiente de nuvem.

Nesse sentido é de extrema importância que o ME realize uma Gestão de Riscos para minimizar essa mudança do ambiente interno para o ambiente de computação em nuvem e minimizar as possíveis fraudes digitais, conforme recomendação da Norma Completar nº 14 do Departamento de Segurança da Informação e Comunicações (DSIC) da Presidência da República [13]. Dessa forma o ME poderá identificar vulnerabilidades, em especial às que podem afetar o SDD ou outros sistemas que abrigam informações de caráter sigiloso, e implantar melhorias e novas tecnologias para diminuir a probabilidade ou mitigar a possibilidade do risco vir a se materializar e causar grande impacto financeiro e de imagem

para o Governo.

A Gestão de Riscos é uma recomendação do Governo para ser adotada diante de qualquer ação que haja possibilidade de ocorrência de riscos de quaisquer naturezas. Essa política de gestão passou a ser adotada e implantada no Governo Federal em grande escala de forma institucional ou em diversas áreas, e com a área de Tecnologia da Informação e Comunicações (TIC) não é diferente. O Gabinete de Segurança Institucional da Presidência da República avalia que qualquer ação que possa comprometer a Segurança da Informação ou que envolva a movimentação e hospedagem de dados do governo para o ambiente de nuvem deve ser precedida pela elaboração de uma Gestão de Riscos a fim de municiar os gestores de informações para tomada de decisão [13]. Informações como o nível, tipo, avaliação, probabilidade e consequências da materialização do risco negativo, possíveis ações mitigadoras e custo de implantação dessas ações são de grande importância para o gestor público e para o planejamento estratégico dos órgãos. No âmbito do Governo Digital, sistemas estruturantes e finalísticos e das TIC, as iniciativas de proteção aos dados das empresas e cidadãos e a mitigação dos riscos de segurança da informação são extremamente importante para a implantação da plataforma de sistemas e serviços digitais e para a transformação digital e desburocratização dos processos na Administração Pública.

Não faz parte do escopo desse trabalho identificar ou discorrer sobre os protocolos de autenticação usados pelas tecnologias ou soluções de autenticação.

## 1.1 Problema de Pesquisa

O ME tem a intenção de hospedar o SDD em um ambiente de nuvem para prover maior resiliência e confiabilidade para esse sistema, o que é uma tendência que deve ser seguida pela esfera governamental.

Diante do atual cenário político e financeiro, diversas empresas, órgãos de governo, universidades e até mesmo fundações e institutos de pesquisa vem aderindo ao modelo de computação em nuvem. A decisão de migrar os sistemas existentes para as soluções de nuvem pode ser complicada, uma vez que requer a avaliação dos benefícios, riscos e custos que não são muito simples [14].

Para o NIST [15] a computação em nuvem se refere a um modelo prático para permitir o acesso via rede a um conjunto compartilhado de recursos computacionais configuráveis sob demanda (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que podem ser rapidamente provisionados e liberados com esforço mínimo de gerenciamento ou interação com o provedor de serviços.

Com isso, o sistema passa a funcionar em um ambiente não controlado e aspectos de segurança da informação devem ser considerados, bem como a incidência de fraudes. Um desses aspectos é o sistema de autenticação, pois o SDD somente possui um fator de autenticação simples que é do tipo usuário e senha, o que é considerado insuficiente para tornar o sistema mais confiável, seguro e menos vulnerável a fraudes cibernéticas. Esses aspectos precisam ser considerados para qualquer sistema de governo, seja em ambiente de nuvem ou ambiente interno dos órgãos, a fim de garantir serviços de maior confiabilidade, o que se torna ainda mais relevante ao se considerar a nova plataforma digital do governo a fim de atender a demanda do cliente-cidadão e a organismos nacionais e internacionais.

O SDD precisa de maiores controles de segurança em vista do caráter sigiloso de suas informações. Um vazamento de informações do sistema pode gerar descrédito perante seus usuários e fragilizar a imagem do ME com perda de confiabilidade e reputação para o órgão. Dentre esses controles um dos mais importantes é o de acesso, pois apenas um fator de autenticação como usuário e senha pode ser facilmente fraudado com Engenharia Social, ataques de força bruta, dentre outros métodos de ataques cibernéticos, e a consequência pode ser desde a perda de confidencialidade e integridade dos dados até um abalo significativo à imagem do ME, e consequentemente, do Governo Federal.

A necessidade de melhores controles de segurança é a realidade de muitos sistemas da Administração Pública em todas as suas esferas: federal, estadual e municipal. Os demais sistemas do ME também carecem de uma arquitetura de segurança mais robusta e adequada para garantir maior nível de segurança aos seus usuários.

O Ministério está em processo de homologação de um Portal de Acesso Único (*Single Sign-On*) aos sistemas, esse portal é denominado Programa Eletrônico de Acesso Digital (PEAD) que servirá inclusive ao SDD, porém o PEAD apesar de prover uma autenticação mais forte para alguns desses sistemas por meio de certificado digital não garante evitar os acessos fraudulentos de diversos tipos por meio de vazamento ou posse desses certificados.

A Segurança da Informação e Comunicações (SIC) passa a ter uma importância cada vez maior nos processos que envolvem tecnologia e na oferta de serviços digitais. Com a adoção do programa de Governo Digital e da Estratégia de Governança Digital e outras iniciativas com o Portal de Serviços do Governo, o Plano de Dados Abertos, o processo de desburocratização do Governo, a grande oferta de serviços e processos por meio digital, inclusive sistemas da área de Comércio Internacional, um dos problemas é como tornar o SDD mais resiliente a ataques cibernéticos relacionados ao controle de acesso e a autenticação e consequentemente às fraudes digitais a partir de tentativas de acessos indevidos com origem a partir do ambiente de rede do próprio órgão ou a partir de qualquer rede ou usuário conectado em qualquer parte do mundo.

Para isso o trabalho irá responder a seguinte questão de pesquisa: como tratar as

vulnerabilidades de segurança no âmbito do controle de identidade e acessos ao SDD que poderão ser potencializadas com a migração para o ambiente de nuvem?

Nesse sentido esse estudo buscará por meio da aplicação de uma tecnologia de GIA, o controle mais robusto e eficaz para mitigar ou evitar acessos não legítimos e fraudes digitais em sistema ou serviços do Governo, como o SDD, que armazena dados sigilosos.

## 1.2 Objetivos

### 1.2.1 Objetivo Geral

Propor uma solução de tratamento dos riscos de Gestão de Identidade e Acessos aplicada ao Sistema Decom Digital do Ministério da Economia (ME).

### 1.2.2 Objetivos Específicos

- Estabelecer o contexto da gestão de riscos;
- Avaliar os riscos considerando a Gestão de Identidades e Acessos para o SDD no ambiente de computação em nuvem;
- Identificar as principais tecnologias de Gestão de Identidade e Acessos;
- Desenvolver uma aplicação computacional para o uso de uma tecnologia de GIA para o SDD, como forma de tratamento dos riscos.

## 1.3 Justificativa

A utilização da Computação em Nuvem para hospedar os recursos de TI das organizações é uma prática amplamente utilizada nos dias de hoje. Os benefícios de utilização da Computação em Nuvem são inúmeros, como o ganho de economia de escala, agilidade na obtenção de recursos de TI e resiliência, porém a adoção desta arquitetura traz riscos para o negócio, sobretudo riscos operacionais relacionados à Segurança da Informação e Comunicações.

A gestão dos riscos de SIC aplicada à computação em nuvem passa a ser importante para qualquer organização e para os órgãos governamentais, com o o ME não é diferente. O Governo Federal busca com a contratação da computação em nuvem a redução de custos, padronização e confiabilidade no acesso aos serviços públicos que são ofertados cada vez mais por meio das TIC. Os riscos operacionais relacionados à segurança da informação e comunicações no ambiente de nuvem é um fator inibidor para a contratação

desses serviços, outro fator inibidor é a legislação do Governo Federal, como o Decreto nº 8135/2013 [16], que aplacou as intenções dos órgãos em adotar a computação em nuvem devido à preocupação com segurança. A falta de clareza da legislação sobre o tema e de um modelo padrão que incentive a adoção da nova arquitetura são outros fatores a considerar.

Porém, iniciativas recentes surgem no sentido de viabilizar a contratação da computação em nuvem pelo Governo, impulsionadas pelos benefícios da arquitetura e principalmente pelos altos custos de manutenção das infraestruturas de TIC internalizadas nos órgãos, além da importância da TIC para o aumento da oferta e da qualidade dos serviços públicos digitais ao cidadão.

O Sistema Decom Digital (SDD) é um dos principais sistemas do antigo Ministério de Indústria, Comércio Exterior e Serviços que passou a integrar o Ministério da Economia, pois trata dos processos de Defesa Comercial das organizações. O mesmo recebe e armazena peças processuais de cunho sigiloso, com prazos pré-definidos de apresentação, para serem analisados e julgados pelo Ministério. Por ser um sistema notadamente crítico e que consequentemente exige resiliência do ambiente hospedeiro é um dos elegíveis para o Ministério migrar inicialmente para o ambiente de computação em nuvem, porém por tratar de informações sigilosas das empresas, os riscos operacionais, como vazamento e falhas de integridade das informações, precisam ser geridos para que o Ministério possa adotar esta arquitetura com maior grau de confiabilidade. O DECOM Digital é um sistema desenvolvido com o objetivo de conferir acesso remoto aos autos dos processos de investigação conduzidos pelo Departamento de Defesa Comercial – DECOM [17].

Um dos maiores desafios para o Governo Federal na adoção da computação em nuvem e para o Governo Digital é proteger as informações sensíveis, restritas ou sigilosas dos sistemas e portais de serviços do governo contra fraudes digitais e vazamento de informações [18]. Para a Agência Brasileira de Inteligência (ABIN) [19] a informação sensível é aquela sigilosa ou estratégica, cujo acesso não autorizado pode comprometer a consecução dos objetivos nacionais e resultar em prejuízos ao País, necessitando de medidas especiais de proteção. A Lei de Acesso à Informação [20] define informação sigilosa como aquela submetida temporariamente à restrição de acesso público em razão da sua imprescindibilidade para a segurança da sociedade e do Estado. A mesma Lei define como informações de acesso restrito qualquer tipo de informação pessoal de posse do Governo ou qualquer sistema que contenha, utilize ou veicule conhecimento ou informação classificada em qualquer grau de sigilo, informação econômica ou informação científico-tecnológica cuja divulgação implique risco ou dano aos interesses da sociedade e do Estado.

O ME, preocupado com a segurança no acesso a seus sistemas e aplicações, desenvolveu um portal do tipo *Single-Sign On* (Acesso Único) chamado de Programa Eletrônico

de Acesso Digital (PEAD) que trata da transmissão mais segura de arquivos, auditoria e autenticação e controle de acesso aos sistemas do Ministério. O PEAD disponibiliza no módulo de autenticação a Autenticação MultiFator (MFA) que garante maior segurança no acesso às aplicações por meio de autenticação por senha e certificado digital. O PEAD ainda está em fase de testes e homologação e mesmo após a sua implantação, ainda existirão lacunas importantes para prover maior segurança devido à ausência de algumas tecnologias, como maiores controles de autenticação com uso da solução de autenticação baseada em comportamento (*Behavior Authentication*) ou contexto (*Context-aware Authentication*). Essas tecnologias no âmbito de autenticação e controle de acesso provêm maiores controles de segurança, e fazem parte do grupo de controles de segurança que comumente é chamado de Gerenciamento de Identidades e Acessos (GIA) ou *Indentity and Accesss Management* (IAM).

A Gestão de Identidades e Acessos é o grupo de controles de segurança de suma importância para a gestão de riscos em computação em nuvem, pois envolve procedimentos e tecnologias para evitar acessos indevidos e garantir maior proteção às informações dos clientes hospedadas na infraestrutura de nuvem dos provedores de serviços.

Os crimes cibernéticos estão se proliferando no mundo digital em grande escala e estão cada vez mais sofisticados, pois buscam incessantemente explorar vulnerabilidades dos sistemas, arquiteturas tecnológicas, protocolos e serviços digitais [9]. Em um mundo que cada vez mais dependemos de uma identidade e serviços digitais, em que muitos dos serviços de empresas privadas ou do governo somente estão sendo oferecidos nesse tipo de plataforma, a necessidade de preocupação com a segurança dos dados e informações se torna exponencial. Nesse contexto, as maiores empresas do mundo, inclusive de tecnologia, já sofreram com a ação de criminosos digitais, sequestrando informações ou acessando e comercializando as mesmas de forma ilegal.

Para o Governo esse aspecto também é muito preocupante por lidar com informações sigilosas de pessoas e empresas, e o cuidado com a proteção à informação, recentemente revelado por normativos como a Lei de Acesso à Informação (LAI) – Lei nº 12.527 [20] e a ainda mais recente Lei Geral de Proteção aos Dados (LGPD) - Lei nº 12.965 [21] que estabelece maior rigor para com que as empresas privadas e órgãos governamentais tratam as questões de privacidade e proteção de dados dos cidadãos brasileiros.

O Brasil busca melhorar sua eficiência por meio de programa de Governo Digital que se baseia na maior oferta de serviços públicos digitais e também na desburocratização de seus processos o que reflete diretamente em um serviço mais ágil e de melhor qualidade para o cidadão e empresas que se relacionam com o Governo [2]. Os sistemas e serviços oferecidos pelo Governo, na maioria das vezes, ainda não possuem uma arquitetura tecnológica robusta quando se trata de segurança da informação, esse quadro precisa ser alterado

para que o cliente do Governo possa utilizar sistemas e serviços mais confiáveis e que sua informação seja resguardada com controles de segurança mais eficazes. O cidadão precisa ter sua informação protegida para que não seja usada para fins criminosos ou de exposição da privacidade dos indivíduos, ao passo que as empresas também precisam confiar ao Governo a proteção de seus dados, muitas vezes segredos comerciais e outras informações valiosas e de reputação que são armazenadas pelo Governo e somente devem ser reveladas tempestivamente para que não gerem favorecimentos competitivos de mercado para um ou outrem.

Dessa forma, percebe-se a importância do Governo investir em controles mais eficazes de Segurança da Informação e Comunicações ao tempo que cresce sua plataforma e portfólio digital de sistemas e serviços. Nesse interim estão os sistemas de Comércio Exterior e Serviços, e em particular os sistemas de defesa comercial, onde está inserido o Sistema Decom Digital do ME. Este sistema processa e armazena informações sigilosas de empresas que atuam com Comércio Exterior e Serviços e ainda não possui uma arquitetura de segurança da informação que contemple controles eficazes de acesso, autenticação e autorização. O SDD necessita de uma evolução para que o Governo possa proporcionar aos usuários desse sistema a segurança requerida nas suas transações e para seus dados, sem esse tipo de ação as vulnerabilidades do sistema poderão ser exploradas e o vazamento de informações será um risco com maior probabilidade de ocorrência. As tecnologias e processos de GIA podem ser utilizados para evitar perdas financeiras e de reputação e mitigar o risco de vazamento de informações, e em consequência tornar o SDD mais confiável para seus usuários.

A Avaliação de Riscos deve ser considerada quando se trata de Segurança da Informação. No caso do SDD o processo de avaliação de riscos será importante, pois possibilitará identificar as lacunas de segurança do sistema, os riscos a serem tratados e opções de tratamento desses riscos. O GIA poderá ser utilizado como mecanismo de prevenção e mitigação do risco de vazamento ou perda de integridade das informações.

Por fim, para os profissionais de TIC a Segurança da Informação e Comunicações em particular, a GIA representa um grande campo de estudo e de uso de novas tecnologias. Os desenvolvedores de sistemas e soluções de TIC devem considerar os aspectos de SIC em seus projetos, sobretudo os aspectos de GIA, como controle de acessos, protocolos e fatores de autenticação, processo de autorização e auditoria, para que essas soluções estejam em conformidade com o que se requer de segurança para a plataforma digital de empresa privadas e do governo, seja em ambiente local ou de computação em nuvem.

## 1.4 Estrutura do Trabalho

Este trabalho está divido em sete capítulos. O primeiro capítulo apresenta o contexto da pesquisa, problema, justificativa e os objetivos do trabalho; o segundo capítulo aborda a revisão de literatura que visa identificar as fontes e normas para o processo de Gestão de Risco, Gestão de Identidade e Acessos e suas tecnologias e a Autenticação baseada em Contexto ou Comportamento, também aborda os seguintes tópicos complementares: computação em nuvem, segurança da informação em nuvem, autenticação, *behavior analytics e context-aware authentication*, ainda traz as principais fontes de referências utilizadas, no desenvolvimento deste trabalho; o terceiro capítulo apresenta o Estabelecimento do Contexto da Gestão de Riscos para o SDD considerando a GIA no ambiente de nuvem; o quarto capítulo apresenta a avaliação dos Riscos para o SDD considerando a GIA no ambiente de nuvem; o quinto capítulo apresenta as principais tecnologias de GIA, o sexto capítulo apresenta uma aplicação de solução baseada em comportamento ou contexto e o sétimo capitulo apresenta os resultados e a conclusão do trabalho.

## 1.5 Metodologia de pesquisa

Essa seção apresenta a metodologia aplicada ao trabalho, onde serão apresentados, o ambiente, os métodos utilizados e os procedimentos para o alcance do objetivo geral e de cada um dos objetivos específicos propostos nesta pesquisa.

O tipo desta pesquisa é exploratória qualitativa, e utiliza a revisão bibliográfica e a Teoria de Enfoque Meta Analítico Consolidado – TEMAC, de Mariano e Rocha [22], que é fundamentada em três passos simples para identificação de literatura de impacto e análises segundo as regras da bibliometria.

Na primeira etapa definiu-se como termo de pesquisa as *string "Identity and Access Management"*, *"Behaviour Atuthentication"* e *"Context-Aware Authentication"* , *"Adaptive Authentication"*, *"Authentication based risk"*, *"Multifactor Authentication"*, "OFD"e *"Authentication based context"*, como base de dados a base *Web of Science*, com raio de busca de 1991-2019, englobando as áreas de conhecimento *"Computer Science"*, *"Telecommunications"*, *"Engineering" and "Business"*. O resultado foram 270 trabalhos, que compõe a amostra desta pesquisa.

O software bibliométrico utilizado para a formação de redes e mapas foi o *Vosviewer 1.6.11*, que realiza uma leitura dos dados da base *Web of Science* e, por meio de técnicas de clusterização, separa os autores em grupos.

Trata-se de pesquisa com o objetivo de produzir informações ilustrativas e aprofundadas, capaz de responder aos objetivos gerais e específicos, por meio da produção de

novas informações. De acordo com [23] a pesquisa exploratória proporciona maior familiaridade com o problema, tendo em vista torná-lo mais explícito. Quanto a abordagem a pesquisa é qualitativa, pois se preocupa com aprofundamento e de como o tema será entendido pelos leitores e quanto à natureza trata-se de pesquisa aplicada, objetivando gerar conhecimentos para aplicação prática, dirigidos à identificação e possível solução de problemas de gestão de riscos de interesse do ME. Quanto aos objetivos trata-se de pesquisa exploratória, pois busca entender melhor o problema, com a meta de estabelecer o contexto interno e externo bem como buscar identificar os fatores de risco para adoção da arquitetura de computação em nuvem pelo governo brasileiro. Pesquisas bibliográficas foram realizadas nas principais bases acadêmicas como Biblioteca Eletrônica Científica *Online* (*Scielo*), *Web of Science*, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes), Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), *Google* Acadêmico, *Directory of Open Access Journals* (DOAJ) dentre outros.

O método que é composto por um conjunto rigoroso de procedimentos intelectuais e técnicos, sistemáticos e racionais, adotados para se atingir o conhecimento, é denominado método científico [23], [24]. Por sua vez a pesquisa é o processo formal e sistemático de desenvolvimento do método científico que tem por objetivo fundamental descobrir respostas para problemas ou obter novos conhecimentos mediante o emprego de procedimentos científicos [23].

O método baseou-se em levantamento bibliográfico e análise de conceitos por meio de livros, artigos e publicações sobre GIA e Autenticação, levantamento sócio técnico e análise documental de normativos e documentos técnicos do Ministério e do Governo Federal, análise das diretrizes de gestão de riscos e de publicações e artigos que discorrem sobre a implementação de autenticação e tecnologias de GIA.

Para o primeiro objetivo específico o método foi utilizar para o contexto interno uma pesquisa sobre a estrutura organizacional, documentação física e eletrônica, dos planos táticos e estratégicos da área de TIC e do Planejamento Estratégico do órgão. Para o contexto externo realizou-se uma pesquisa em portais governamentais, normas e legislação sobre o tema do trabalho, decretos sobre a criação do órgão e da Secretaria de Comércio Exterior onde está localização a Diretoria de Defesa Comercial responsável pelo Sistema Decom Digital.

Para o segundo objetivo realizou-se um estudo e pesquisa sobre as principais normas, modelos e guias para avaliação de riscos. A pesquisa envolveu as normas ISO 31.000, 31.010 e 27.005, o COSO, o guia *COBIT Value to Risk*, o Manual de Gestão de Riscos do TCU e o Manual de Gestão de Riscos da CGU, a política, portarias e modelos do Ministério que implementam a Gestão de Riscos institucionalmente e outros modelos utilizados no mercado público e privado.

Para o terceiro objetivo foi feita uma vasta revisão de literatura acerca do tema de GIA para identificar as suas tecnologias, potenciais vulnerabilidades e opções de tratamento de risco. Por meio do conhecimento de cada tecnologia foi possível identificar como cada uma pode contribuir no processo de mitigação dos riscos.

Para o quarto objetivo o método foi pesquisar por meio de uma revisão de literatura e levantamento documental as soluções e produtos de GIA existentes no mercado e suas formas de funcionamento e implementação. Após a seleção da tecnologia o estudo aplicou computacionalmente a mesma por meio de pesquisa sobre as principais formas de implementação da autenticação por comportamento ou contexto, e ainda por meio de pesquisa bibliográfica identificou a plataforma e as formas de funcionamento das aplicações e algoritmos que implementam esse tipo de tecnologia.

De acordo com Gil [23], "o elemento mais importante para a identificação de um delineamento é o procedimento adotado para a coleta de dados". O autor define dois grandes grupos de delineamento: "aqueles que valem das chamadas fontes de papel e aqueles cujos dados são fornecidos por pessoas". A coleta de informações ocorreu por meio de exploração documental e baseada em conhecimentos específicos. Assim, por meio dos procedimentos metodológicos citados, pretende-se atingir os resultados esperados para o alcance dos objetivos traçados no trabalho.

A coleta de informações ocorreu mais precisamente por meio da opinião de especialistas, levantamento documental, análise de cenários, análise da legislação e de casos práticos, análise de publicações sobre temas como segurança da informação, ataques e fraudes cibernéticas, Gestão de Identidade e Acessos, controle de acesso, autenticação e computação em nuvem e consulta a algumas bases de dados de informações de segurança e do SDD.

O levantamento documental considerou o Plano Diretor de Tecnologia da Informação e Comunicações (PDTIC)) do órgão para o triênio de 2017-2019, os documentos de arquitetura e de ambiente do sistema Decom Digital, a política de desenvolvimento de sistemas do órgão, as ferramentas produzidas no órgão e seus aspectos de segurança da informação, relatórios de consultorias sobre a segurança aplicada aos sistemas do órgão, a política de Gestão de Riscos do órgão e o alinhamento ao planejamento estratégico do ME.

Para o desenvolvimento do protótipo foram coletados dados de algoritmos similares que implementam autenticação por contexto e de publicações de sítios especializados, livros e repositórios de construções de algoritmos e sistemas [25].

Os dados foram tratados por meio da análise documental, ferramentas como matrizes e digramas e utilização de planilhas. No caso do protótipo alguns trechos de códigos foram selecionados por motores de busca na Internet, identificados pela similaridade com os requisitos propostos e serviram de base técnica para a construção do protótipo.

# Capítulo 2

# Referencial Teórico

Este estudo apresenta a revisão de literatura considerando a Gestão de Identidade e Acessos, Autenticação, Autenticação baseada em Comportamento (*Behavior Authentication*), Autenticação baseada em Contexto (*Context-Aware Authentication*), Autenticação Multifator e Computação em Nuvem.

Considerando a Teoria de Enfoque Meta Analítico Consolidado – TEMAC foi realizado o detalhamento da análise dos autores e dos artigos, ou seja, uma visualização da estrutura conceitual da área e optou-se pelo uso de gráficos chamados mapas de calor. Por meio do software *VOSviewer 1.6.11* foram elaborados os mapas de calor, facilitando a visualização da análise de co-citation e de palavras com base nos registros encontrados em *Web of Science* dos temas deste trabalho. Na análise de citação é possível compreender quais autores foram mais citados e quais costumam ser citados simultaneamente, indicando similaridade entre as linhas de pesquisa dos mesmos. A figura abaixo ilustra o mapa de *cocitation*:

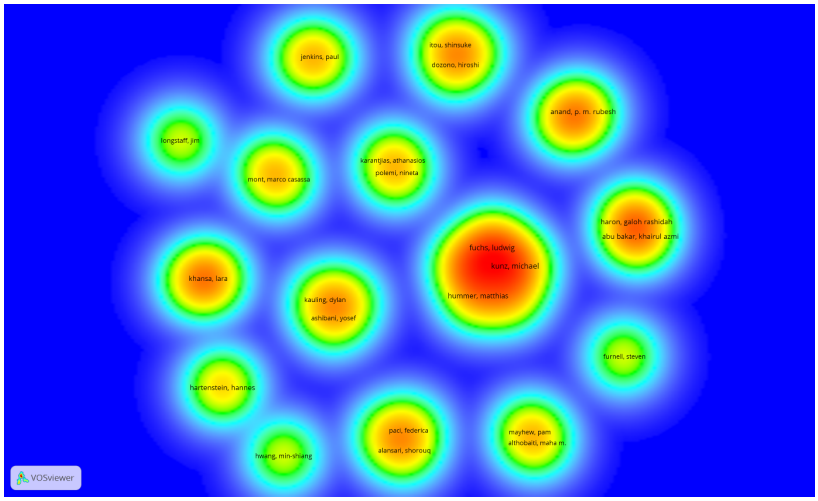


Figura 2.1: Mapa de Calor de citação dos Autores. Elaboração própria. Extraído do *VOSviewer*.

Para balizar este referencial teórico, foi elaborado o mapa de calor acima dos autores que abordam o tema de Gestão de Identidades e Acessos e Autenticação por Comportamento ou Contexto, que visa estabelecer a proximidade dos estudos mais abordados e estabelecer suas principais contribuições ou enfoques teóricos.

A Figura 2.1 retrata um mapa de calor de citação entre 1990-2019. Quanto mais próximos os autores, maior a similaridade dos trabalhos e quanto maior ou em negrito for seu nome, mais citado ele foi. No caso, os autores Ludwig Fuchs, Michael Kunz e Matthias Hummer são bem citados no tema pesquisado e seus trabalhos tem um grau de similaridade.

A figura abaixo é do mapa de calor de palavras gerado no *VOSviewer*:

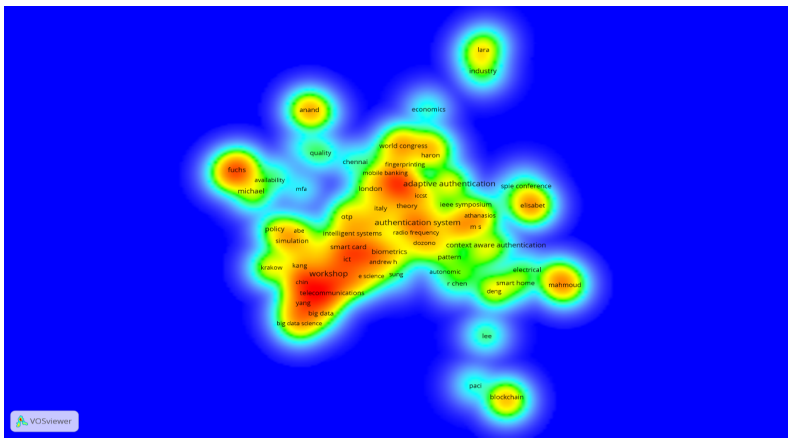


Figura 2.2: Mapa de palavras. Elaboração própria. Extraído do *VOSviewer*.

O mapa de calor destaca as palavras que mais aparecem nos artigos pesquisados sobre o tema na *base Web of Science: Context-aware Authentication, Adaptive Authentication, Authentication System, Biometrics* e *Intelligent Systems*.

A pesquisa realizada na base *Web of Science* foi elaborada a partir das seguintes *strings: "Identity and Access Management", "Behaviour Atuthentication" , "Context-Aware Authentication" , "Adaptive Authentication", "Authentication based risk", "Multi-factor Authentication", "Online Fraud Detection"* e *"Authentication based context"*, com raio de busca de 1990-2019, englobando as áreas de conhecimento *"Computer Science", "Telecommunications", "Engineering" and "Business"*. O resultado foram 270 trabalhos, que compõe a amostra desta pesquisa. Após a pesquisa os resultados foram analisados e refinados, o resultado foi exportado em formato de arquivo e importado pelo software *Vosviewer* onde foram realizadas as configurações necessárias e gerado o mapa de calor acima com base nos autores e temas pesquisados.

A pesquisa da base bibliográfica utilizada neste trabalho considerou a busca por livros, teses, dissertações, normas e artigos nas seguintes fontes especializadas: *Web of Science,*

*Scopus, IEEE (Institute of Electrical and Electronics Engineers), SciELO*, BDTD (Biblioteca Digital Brasileira de Teses e Dissertações), Repositório de Dissertações do PPCA e outras bases de dados científicas. Tornou-se necessário ainda, a pesquisa junto a órgãos de governo como o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), o antigo MPDG (Ministério do Planejamento, Desenvolvimento e Gestão) que se integrou ao Ministério da Economia, o Tribunal de Contas de União (TCU), a Controladoria Geral da União (CGU) e a legislação sobre os temas abordados por este trabalho.

## 2.1 Gestão de Riscos

O termo "Risco" apresentado na norma ABNT NBR ISO 31000:2009 [26] está definido como o "Efeito da incerteza sobre os objetivos". Por isso é importante identificar e analisar os potenciais impactos da migração do ativo para a nuvem considerando os objetivos e o contexto interno e externo do ME. Na Norma ABNT NBR ISO 31010 [27] são apresentadas várias técnicas de mapeamento dos riscos. É importante levantar as possíveis causas associadas às incertezas mapeadas, associar o risco com uma causa, por meio da associação de probabilidade e consequência. A etapa de "Analisar Riscos" é a que se determina, de forma combinada, a probabilidade e as consequências do risco em termos do seu impacto. O processo de "Avaliar o Risco" deve ser feito com base nos resultados da análise de risco e nos critérios de risco, onde se deve decidir quais riscos serão tratados, a estratégia de tratamento mais adequada para cada risco e a prioridade para à implementação do tratamento. Por fim, o "Tratamento dos Riscos" diz respeito à implementação da estratégia de risco e dos controles que visam modificar os riscos.

Gestão de Riscos é definida por [26] como um conjunto de processos consistentes em uma estrutura abrangente que pode ajudar a assegurar que o risco seja gerenciado de forma eficaz, eficiente e coerentemente ao longo de uma organização. Essa norma define risco como o efeito da incerteza sobre se e quando as organizações de todos os tipos e tamanhos atingirão seus objetivos considerando-se que enfrentam influências de fatores internos e externos.

Para o guia de Gerenciamento de Riscos Corporativos - Estrutura Integrada do *Committee of Sponsoring Organizations of the Treadway Commission* (ERM/COSO) [28] a Gestão de Riscos é definida a partir da premissa que toda organização existe para gerar valor às partes interessadas. Todas as organizações enfrentam incertezas, e o desafio de seus administradores é determinar até que ponto aceitar essa incerteza, assim como definir como essa incerteza pode interferir no esforço para gerar valor às partes interessadas. Incertezas representam riscos e oportunidades, com potencial para destruir ou agregar valor. O gerenciamento de riscos corporativos possibilita aos administradores tratar com

eficácia as incertezas, bem como os riscos e as oportunidades a elas associadas, a fim de melhorar a capacidade de gerar valor.

Com a adoção pelo Governo Federal da Lei Geral de Proteção aos Dados (LGPD), Lei nº 13.709 de 14 de agosto de 2018 [21], que entrará em vigor em agosto de 2020, e que é muito similar ao General Data Protection Regulation (GDPR) [29] em vigor na Europa desde 25 de maio de 2018, o país busca trazer maior rigor para a forma com que as empresas privadas e órgãos governamentais tratam as questões de privacidade e proteção de dados dos cidadãos brasileiros. As novas regras afetarão todas as atividades que envolvam a utilização de dados pessoais em empresas brasileiras, que têm até 2020 para se adequarem. As regras buscam proteger os dados contra as vulnerabilidades e vazamentos de dados e informações. O artigo 3º da LGPD diz que a Lei será aplicada a qualquer operação de tratamento de dados realizada por pessoa física ou por pessoa jurídica de direito público ou privado. Desta forma, a LGDP delimitou um capítulo (art. 23 a 30) exclusivo que definem as regras para o tratamento de dados pelo poder público. A Lei no seu artigo 46º determina que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Com isso torna-se fundamental revisar as políticas de segurança dos órgãos públicos para criar mecanismos de controle mais efetivos e seguros a fim de proteger os dados custeados pelo Governo e nesse âmbito a Gestão e Avaliação de Riscos de segurança em diversos níveis, incluindo o risco de vazamento de informações e a necessidade de proteção a acessos indevidos, seja em ambiente local ou em nuvem, torna-se de fundamental importância para que os órgãos estejam em conformidade com a nova legislação.

A NBR ISO 31010 [27] fornece orientações sobre a seleção e aplicação de técnicas sistemáticas para o processo de avaliação de riscos. A figura abaixo demonstra seu fluxo de atividades:

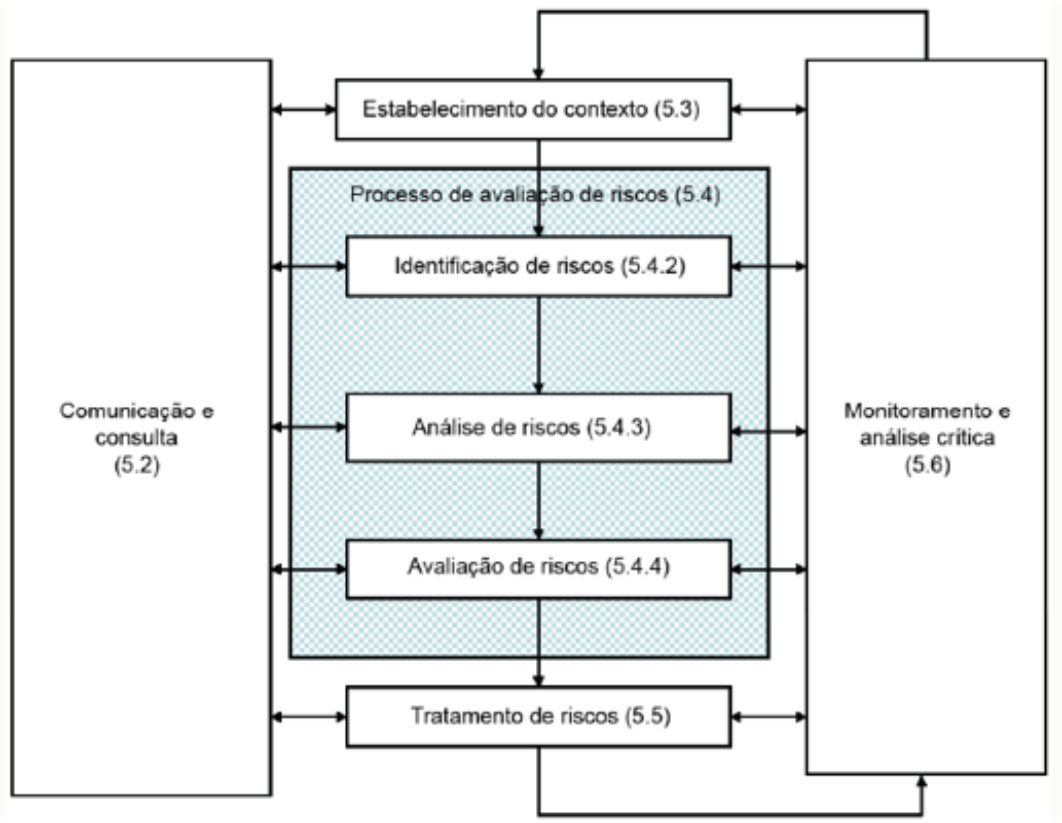


Figura 2.3: Processo de Avaliação de Riscos.
[27]

Uma abordagem sistemática de gestão de riscos de segurança da informação é necessária para se identificar as necessidades da organização em relação aos requisitos de segurança da informação e para criar um sistema de gestão de segurança da informação (SGSI) que seja eficaz. Convém que essa abordagem seja adequada ao ambiente da organização e em particular esteja alinhada com o processo maior de gestão de riscos corporativos. Convém que os esforços de segurança lidem com riscos de maneira efetiva e no tempo apropriado, onde e quando forem necessários. Convém que a gestão de riscos de segurança da informação seja parte integrante das atividades de gestão da segurança da informação e aplicada tanto à implementação quanto à operação cotidiana de um SGSI. Convém que a gestão de riscos de segurança da informação seja um processo contínuo. Convém que o processo defina o contexto interno e externo, avalie os riscos e trate os riscos usando um plano de tratamento a fim de implementar as recomendações e decisões. Convém que a gestão de riscos analise os possíveis acontecimentos e suas consequências, antes de decidir o que será feito e quando será feito, a fim de reduzir os riscos a um nível aceitável [30].

A portaria nº 1.001-SEI, de 30 de junho de 2017 [31], que dispõe sobre a Política de

Gestão de Riscos do Ministério da Indústria, Comércio Exterior e Serviços (MDIC) em seu Art. 1º. Institui a Política de Gestão de Riscos, no âmbito do Ministério da Indústria, Comércio Exterior e Serviços (MDIC), com o objetivo de definir conceitos, fixar princípios e diretrizes, estabelecer a estrutura de gestão de risco, suas atribuições e responsabilidades, e orientar a identificação, a análise, a avaliação, o tratamento, o monitoramento, a análise crítica e a comunicação dos riscos institucionais. Essa portaria é um normativo interno e tornou obrigatória a realização da Gestão de Riscos para o projeto do SDD e também serviu como iniciativa institucional para a gestão de riscos do Ministério estabelecendo as diretrizes para essas iniciativas.

A política de Gestão de Riscos do MDIC determina no seu Artigo 10 o processo de gerenciamento de riscos e suas etapas conforme segue:

> Art. 10 - O Processo de Gerenciamento de Riscos tem caráter contínuo e consiste no estabelecimento de contexto, na avaliação de riscos e no tratamento de riscos, interligadas essas atividades pelo monitoramento e análise crítica e amparados em fluxo de comunicação e consulta entre os interlocutores [31].

Dessa forma o processo de gerenciamento de riscos considerando a GIA para o SDD em ambiente de nuvem seguirá o estabelecido nessa portaria.

## 2.2 Segurança da Informação e Comunicações

Para contextualizar a Segurança da Informação e Comunicações (SIC) é preciso definir primeiramente o que é informação no contexto de tecnologia. A Administração Pública Federal (APF) segue o conceito utilizado por [32] que considera a informação um ativo importante para a manutenção dos negócios de qualquer organização:

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização, e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades [32].

Segundo [6] a informação, em qualquer dos seus formatos, é o principal ativo das instituições, públicas ou privadas e, considerando o cenário globalizado em que vivemos, está cada vez mais exposta a riscos de segurança. A Segurança da Informação e Comunicações compreende um conjunto de ações que buscam proteger e preservar os ativos de informação, assegurando-lhes disponibilidade, integridade, confidencialidade e autenticidade (DICA). A informação tornou-se um recurso de importância crescente para qualquer setor e atividade do Estado brasileiro. Informação e conhecimento são fatores determinantes para a gestão governamental, e os órgãos e entidades da Administração Pública Federal utilizam grande volume de informações para promover de forma eficiente a prestação de serviço público ao cidadão, bem como para a tomada de decisões estratégicas. Disponibilidade, Integridade, Confidencialidade e Autenticidade - problemas decorrentes da falta desses atributos nos ativos de informação levam à necessidade de desenvolver ações permanentes de segurança nas organizações governamentais, inscritas no Orçamento da União. São diversos os desafios relacionados à Segurança da Informação e Comunicações como:

(a) Redes Sociais;

(b) Computação em nuvem;

(c) Aumento exponencial da utilização de dispositivos móveis;

(d) Aumento da exposição;

(e) Problemas tecnológicos;

(f) Aumento da demanda de informações pelos cidadãos;

(g) Convergência digital;

(h) Leis, regulamentações e normas incompletas relacionadas ao tema.

O Governo Federal define a Segurança da Informação da seguinte forma:

> Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento [33].

No âmbito do Governo Federal existe uma estrutura de SIC, na qual o Departamento de Segurança da Informação e Comunicações (DSIC) tem entre suas incumbências planejar, orientar, coordenar e desenvolver as políticas e ações de segurança da informação no âmbito da Administração Pública Federal, além de outras atribuições relacionadas à SIC [34].

O DSIC responde estruturalmente ao Gabinete de Segurança Gabinete de Segurança Institucional da Presidência da República (GSI/PR) que coordenou a proposta de elaboração do Plano de Segurança Nacional de Segurança da Informação (PNSI) [34]. Ainda temos o Comitê Gestor de Segurança da Informação (CGSI) que assessora a Secretaria Executiva do Conselho de Defesa Nacional, exercida pelo GSI/PR, auxilia na consecução das diretrizes da Política de Segurança da Informação, nos órgãos e nas entidades da Administração Pública Federal [34].

O DSIC e o GSI determinam diretrizes e normas de SIC a serem seguidas pelos órgãos que compõem à Administração Pública Federal, estres esses normativos estão a Política de Segurança da Informação e Comunicações (POSIC) estabelecida por meio da Instrução Normativa GSI Nº 1, de 13 de junho de 2008 e da Norma Complementar nº 03/IN01/DSIC/GSIPR e Norma Complementar nº 14/IN01/DSIC/GSIPR [35]. A POSIC deve ser elaborada por cada órgão da APF e objetiva estabelecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações [34].

## 2.3 Computação em Nuvem

A computação em nuvem é a distribuição de serviços de computação – servidores, armazenamento, bancos de dados, redes, software, análises, inteligência e muito mais pela Internet ("a nuvem"), proporcionando inovações mais rápidas, recursos flexíveis e economia na escala. Você normalmente paga apenas pelos serviços de nuvem que utiliza, ajudando a reduzir os custos operacionais, a executar sua infraestrutura com mais eficiência e a dimensionar conforme as necessidades da sua empresa mudam [36].

A computação em nuvem é um modelo para permitir um acesso à rede onipresente (ubíqua), conveniente e sob demanda, para um "*pool*" compartilhado de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços). A computação em nuvem é uma tecnologia disruptiva que tem o potencial de aumentar a colaboração, a agilidade, o dimensionamento e a disponibilidade e, fornece as oportunidades de redução de custos através da computação otimizada e eficiente. O modelo em nuvem prevê um mundo onde os componentes podem ser rapidamente orques-

trados, provisionados, implementados e desativados e, escalados para cima ou para baixo para fornecer um modelo utilitário de alocação e consumo sob demanda [37].

Segundo a NC 14/IN01/DSIC/GSIPR [13] do GSI - Gabinete de Segurança Institucional da Presidência da República - a Computação em Nuvem é um modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços.

Segundo [12], a computação em nuvem (*cloud computing*) remete-se a um modelo computacional que proverá a partir de uma rede de dados, uma estrutura tecnológica por meio de serviços. Serviços que são caracterizados por uma necessidade de maior flexibilidade, escalabilidade e benefícios de custo.

O *National Institute of Standards and Technology* (NIST) [15] destaca que a computação em nuvem se refere a um modelo prático para permitir o acesso via rede a um conjunto compartilhado de recursos computacionais configuráveis sob demanda (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que podem ser rapidamente provisionados e liberados com esforço mínimo de gerenciamento ou interação com o provedor de serviços. A instituição ainda destaca que as principais características da nuvem são:

(a) Auto-atendimento sob demanda - Um consumidor pode unilateralmente fornecer capacidades de computação;

(b) Amplo acesso à rede - As capacidades estão disponíveis na rede e são acessadas por meio de mecanismos padrão;

(c) Agrupamento de recursos - Os recursos de computação do provedor são agrupados para atender múltiplos consumidores com recursos dinamicamente atribuídos e reatribuídos de acordo com a demanda;

(d) Rapidez de elasticidade - As capacidades podem ser elasticamente provisionadas e liberadas, dando a ideia de recursos ilimitados;

(e) Serviço medido - Os sistemas em nuvem controlam e otimizam automaticamente o uso de recursos.

Segundo [38] a consolidação de centros de dados e o compartilhamento mais agressivo de recursos de computação levam a benefícios chaves para computação em nuvem, tais como: menor custo de uso de recursos computacionais, menor custo de provisionamento de recursos computacionais e redução do tempo de colocação no mercado.

Para [39] a computação em nuvem representa uma convergência de duas grandes tendências em tecnologia da informação: (a) eficiência de TI, por meio da qual o poder dos computadores modernos é utilizado de forma mais eficiente através de recursos altamente escaláveis de hardware e software e (b) agilidade de negócios, competitiva através da rápida implantação, processamento em lote paralelo, uso de computação intensiva analítica de negócios e aplicações móveis interativas que respondem em tempo real aos requisitos do usuário.

A computação em nuvem é um novo serviço e tem algumas das suas características próprias em comparação com as redes de computadores:

(a) O número de usuários é muito maior. A tecnologia de rede serve principalmente para resolver o problema de compartilhamento de recursos de informação em diferentes organizações. A computação em nuvem não é apenas capaz de alcançar o compartilhamento de recursos, mas também capaz de alcançar a integração em grande escala uma computação escalável, armazenamento, dados e aplicação de computação distribuída para o trabalho colaborativo. Além disso, está preparada para acomodar e atrair mais usuários.

(b) O comportamento do usuário é mais diversificado. O ambiente de Computação em Nuvem pode fornecer mais serviços. Os usuários terão um comportamento mais interativo na utilização desses serviços. Portanto, o controle de acesso de comportamento interativo é muito importante.

(c) Problemas de segurança são mais proeminentes. A Computação em Nuvem enfrenta uma maior variedade de ameaças de segurança, como disponibilidade de serviço, bloqueio de dados, confidencialidade e auditabilidade dos dados, estrangulamentos na transferência de dados, imprevisibilidade de desempenho, bugs em sistemas distribuídos em grande escala, destino de reputação compartilhamento, privacidade e segurança, e acesso ao controle.

Nessa perspectiva o ME busca prover serviços de forma cada vez mais dinâmica e ágil para os cidadãos com alta disponibilidade, qualidade e racionalização de custos para o Governo, com isso a Computação em Nuvem passa a ser de grande importância para alcance desses objetivos.

## 2.4 Gestão de Riscos em nuvem

Um modelo de Gestão de Risco bem delineado se torna crucial para garantir que a informação está ao mesmo tempo disponível, protegida e segura. Os processos de negócios

e procedimentos precisam levar em conta a segurança, e os gerentes de segurança da informação precisam ajustar suas políticas e procedimentos de segurança para atender às necessidades do negócio. Um exemplo de risco de computação em nuvem para a empresa que precisa ser gerenciado é o acesso de terceiros às informações sensíveis cria um risco de comprometimento das informações confidenciais. Na nuvem, isto pode representar uma ameaça significativa para a proteção da propriedade intelectual e de segredos comerciais [40]. Segue abaixo uma tabela adaptada de [40] que relaciona os princípios de Segurança da Informação e Comunicações com os riscos de segurança em um modelo de nuvem:

Tabela 2.1: Princípios da Segurança da Informação em um modelo de Nuvem. Adaptado.

| Princípios da Segurança | Cenário do Risco | Questões |
|---|---|---|
| Integridade | Invasões por hackers aos ambientes da nuvem. Violação de leis de proteção de dados. | Quais são as garantias sobre a preservação da integridade dos dados? |
| Confidencialidade | Aplicações de diversos usuários coabitam nos mesmos sistemas de armazenamento. | Como é realizada a segregação de dados? Como é protegida a propriedade intelectual e segredos comerciais? |
| Disponibilidade | Recuperação de dados gerenciados por terceiros. | Como é garantida a arquitetura de disponibilidade? A recuperação de informações críticas está sujeita a atrasos? |
| Autenticidade | Verificação da autenticidade das entidades comunicantes. | Que recursos são utilizados na autenticação e controle de acesso dos usuários? |
| Não-repúdio | Auditabilidade das ações executadas por usuários no sistema. | Os usuários do modelo são capazes de negarem suas ações? |

Segundo o ISACA [41] o acesso de terceiros às informações confidenciais cria um risco de comprometimento dessas informações. Na computação em nuvem, isso pode comprometer a proteção da propriedade intelectual e os segredos comerciais.

A figura abaixo demonstra os riscos de segurança em nuvem identificados pela *Cloud Security Alliance* (CSA) [37], dentre estes aparece no grupo nº 11, as questões gerenciamento de identidade e gerenciamento de acessos.

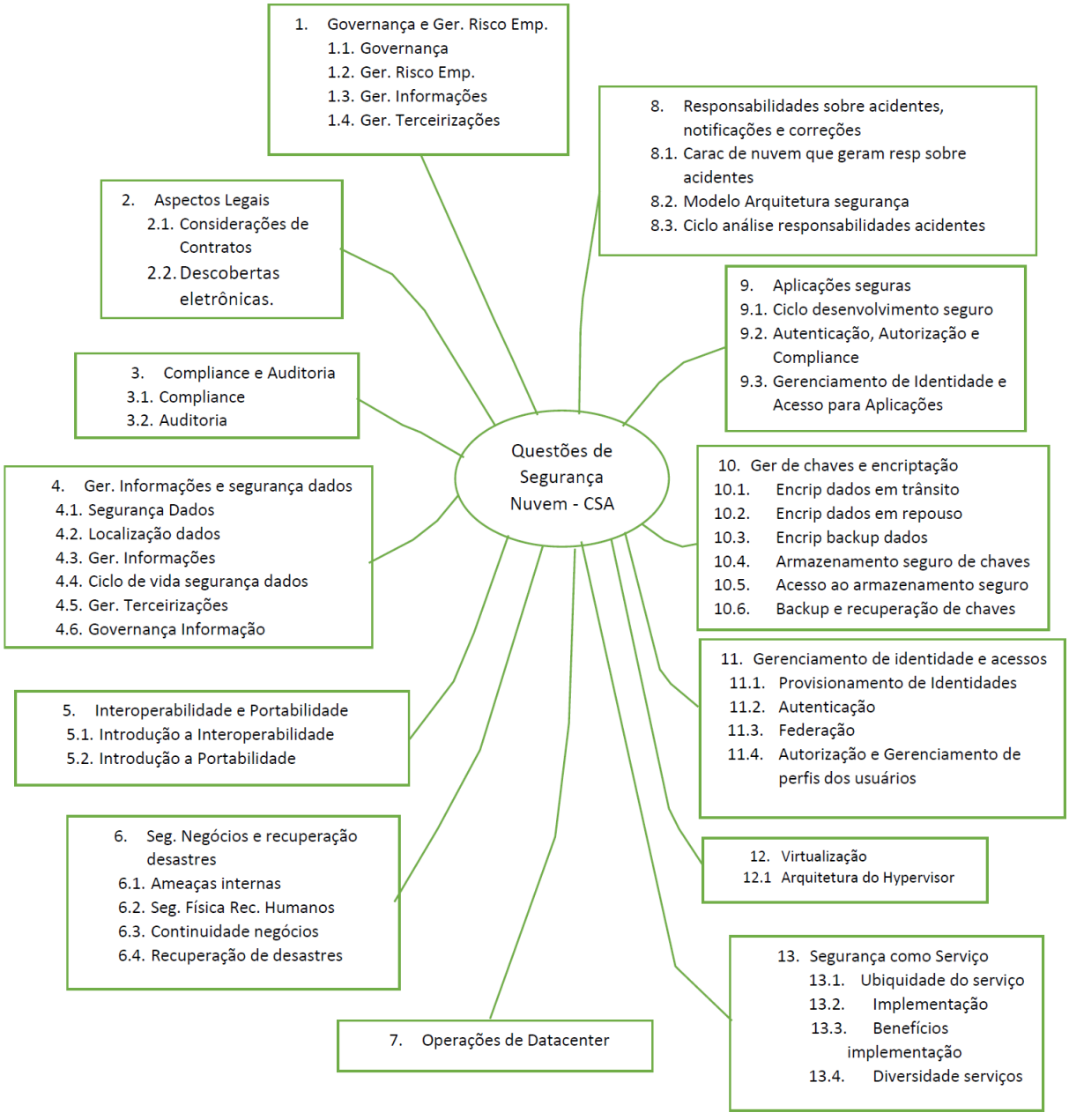


Figura 2.4: Tipos de Riscos de Segurança na nuvem. Adaptado. [37]

De acordo com [42] a segurança computacional se apresenta como um recurso indispensável para garantir o acesso em ambientes de Computação em Nuvem, e destaca à

proteção à privacidade, já que os dados sensíveis passam a ficar sob custódia de terceiros. Nesse contexto, o gerenciamento de identidades cresce em importância conforme crescem os serviços que precisam utilizar autenticação e autorização para controlar o acesso de usuários.

## 2.5 Identificação dos Riscos

Identificação de riscos é o processo de busca, reconhecimento e descrição de riscos, tendo como base o contexto estabelecido e apoiado na comunicação e consulta com as partes interessadas, internas e externas [26].

Para [43] a identificação de riscos é o processo de descoberta, reconhecimento e documentação de riscos que uma organização enfrenta.

Segundo [44] a identificação de riscos pode se basear em dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, necessidades das partes interessadas.

O Acórdão TCU 1.793/2015-Plenário [45] identificou diversos riscos para a adoção da arquitetura de Computação em Nuvem pela Administração Pública e os dividiu em Temas e Categorias de Riscos e alinhou a critérios do *framework* COBIT de governança de TI, no caso o risco que alinhado ao tema deste trabalho é o seguinte:

Tabela 2.2: Risco de acesso para aplicação em nuvem.

| **Risco específico** | |
|---|---|
| 8 - Acesso indevido à medida que os serviços de computação em nuvem são amplamente acessíveis, independentemente de localização. | |
| **Controles possíveis** | **Critérios** |
| O provedor deve garantir controles eficazes e compatíveis com as políticas e procedimentos do cliente para gerenciamento de identidades de usuários e controle de acessos. | COBIT DSS05 - Manage Security Services |

A tabela acima demonstra, segundo [45], a identificação de um risco específico e controles possíveis, alinhados a um dos processos do domínio Entrega, Serviço e Suporte (DSS) do modelo COBIT que é o de Gerenciamento de Serviços de Segurança - DSS05.

## 2.6 Análise dos Riscos

Segundo [27] a análise de riscos diz respeito ao entendimento do risco. Ela fornece uma entrada para o processo de avaliação de riscos e às decisões sobre se os riscos necessitam

ser tratados e sobre as estratégias e métodos de tratamento mais apropriados. A análise de riscos consiste na determinação das consequências e suas probabilidades para eventos identificados de risco, levando em consideração a presença (ou não) e a eficácia de quaisquer controles existentes. As consequências e suas probabilidades são então combinadas para determinar um nível de risco.

Dependendo das circunstâncias, a análise de riscos pode ser semi-quantitativa, qualitativa ou quantitativa, ou uma combinação destas, e ser mais ou menos detalhada [26].

A análise do risco se refere ao desenvolvimento da compreensão sobre o risco e a determinação do nível do risco. Geralmente, utilizam-se escalas qualitativas de probabilidade e de impacto que podem variar de acordo com o objeto de gestão e com o grau de precisão na definição dos níveis de probabilidade e impacto [46].

O resultado final do processo de análise de riscos será o de atribuir, para cada risco identificado, uma classificação tanto para a probabilidade como para o impacto do evento, cuja combinação determinará o nível do risco [27].

A análise de risco é a etapa em que os riscos são entendidos e o nível desses riscos é determinado a partir da utilização de escalas qualitativas, como as se probabilidade e impacto.

De acordo com [44], em análises qualitativas e semi-quantitativas, considerando que a lógica subjacente ao nível de risco seja proporcional tanto em relação à probabilidade quanto ao impacto, a função 'Risco' será essencialmente um produto dessas variáveis, conforme equação abaixo:

$$Risco = P(Probabilidade) * I(Impacto) \tag{2.1}$$

Ainda segundo [44] para refletir uma relação linear é necessário incluir um fator de ponderação para uma das duas variáveis (probabilidade ou impacto, de modo a atingir a escala relativa necessária entre eles) e ou um operador exponencial para uma ou para ambas as variáveis. Considerando um fator de ponderação na variável 'Impacto' a equação ficaria da seguinte forma, onde 'x' e 'y' são as variáveis:

$$Risco = (P)^x.(I * FatordePonderação)^y \tag{2.2}$$

A matriz seguinte demonstra a relação entre o nível de risco e as variáveis que o compõe em sua forma qualitativa mais simples [44]:


Figura 2.5: Relação entre as variáveis de probabilidade e impacto.
[44]

Essa abordagem, mais simples, é geralmente utilizada na avaliação inicial de riscos num nível geral ou superior, de modo a estabelecer prioridades de identificação e análise em nível mais específico ou quando dados numéricos, tempo e recursos não estão disponíveis. Análises semi-quantitativas geralmente utilizam escalas, como a exemplificada a seguir, para fornecer um entendimento comum das classificações de probabilidades e impacto [44].

Tabela 2.3: Exemplo de Escala de Probabilidades/Impacto. Adaptado.

| **Probabilidade/Impacto** | **Descrição Probabilidade/Impacto** | **Peso** |
|---|---|---|
| Muito baixa | Improvável/Mínimo | 1 |
| Baixa | Rara/Pequeno | 2 |
| Média | Possível/Moderado | 5 |
| Alta | Provável/Significativo | 8 |
| Muito Alta | Praticamente certa/Catastrófico | 10 |

Na tabela acima baseada em [44] temos um exemplo de Escala de Probabilidade e Impacto desconsiderando qualquer tipo de controle, essas escalas são elaboradas de modo compatível com o contexto e os objetivos específicos da atividade objeto da gestão de riscos.

Para o processo de análise é recomendado estabelecer tipos e níveis de riscos para medir condições do risco e de confiança nos controles existentes. Segundo [47] o risco inerente é o risco que uma organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos. Risco residual é aquele que ainda permanece após a resposta da administração.

De acordo com [44] o nível de risco inerente (NRI) de um evento é o nível de risco antes da consideração das respostas que a gestão adota, incluindo controles internos, para reduzir a probabilidade do evento e ou os seus impactos nos objetivos. Resulta da combinação da probabilidade com o impacto. A política de gestão de riscos da organização geralmente estabelece categorias para classificar os níveis de risco resultantes do processo de análise, sejam inerentes ou residuais, de modo consistente com o seu apetite a risco, como as exemplificadas na figura abaixo:

| **RB** (Risco Baixo) | **RM** (Risco Médio) | **RA** (Risco Alto) | **RE** (Risco Extremo) |
|---|---|---|---|
| **0 – 9,99** | **10 – 39,99** | **40 – 79,99** | **80 – 100** |

Figura 2.6: Níveis de classificação de risco.
[44]

A partir do estabelecimento dos níveis de riscos é possível elaborar uma matriz de riscos combinado esses níveis de risco com a probabilidade e impacto. Com a elaboração dessa matriz o NRI pode ser definido conforme se segue:

| RISCOS IDENTIFICADOS | PROBABILIDADE | | IMPACTO | | NÍVEL DE RISCO INERENTE (NRI) |
|---|---|---|---|---|---|
| Risco 1 – Descrição do risco 1 | Alta | 8 | Muito Alto | 10 | 80 RE (Extremo) |
| Risco 2 – Descrição do risco 2 | Média | 5 | Alto | 8 | 40 RA (Alto) |
| Risco 3 – Descrição do risco 3 | Baixa | 2 | Médio | 5 | 10 RM (Médio) |
| Risco ***n*** – Descrição do risco ***n*** | Muito Baixa | 1 | Médio | 5 | 5 RB (Baixo) |

Figura 2.7: Registro de riscos parcial com níveis de risco inerente calculado.
[44]

A análise de riscos só se completa quando as ações que a gestão adota para respondêlos são também avaliadas, chegando-se ao nível de risco residual, o risco que remanesce depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e ou o impacto dos riscos, incluindo controles internos e outras ações.

Uma forma de avaliar o efeito dos controles na mitigação de riscos consiste em determinar um nível de confiança (NC), mediante análise dos atributos do desenho e da implementação dos controles, utilizando uma escala como a exemplificada a seguir.

| NÍVEL DE CONFIANÇA (NC) | AVALIAÇÃO DO DESENHO E IMPLEMENTAÇÃO DOS CONTROLES (ATRIBUTOS DO CONTROLE) | RISCO DE CONTROLE (RC) |
|---|---|---|
| Inexistente NC = 0% (0,0) | Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais. | Muito Alto **1,0** |
| Fraco NC = 20% (0,2) | Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas. | Alto **0,8** |
| Mediano NC = 40% (0,4) | Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas. | Médio **0,6** |
| Satisfatório NC = 60% (0,6) | Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente. | Baixo **0,4** |
| Forte NC = 80% (0,8) | Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco. | Muito Baixo **0,2** |

Figura 2.8: Exemplo de escala para avaliação de controles.
[48]

Uma vez determinado o Nível de Confiança (NC), pode-se determinar o Risco de Controle (RC), isto é, a possibilidade de que os controles adotados pela gestão não sejam eficazes para prevenir, detectar e permitir corrigir, em tempo hábil, a ocorrência de eventos que possam afetar adversamente a realização de objetivos. O RC é definido como complementar ao NC:

$$RC = 1 - NC \tag{2.3}$$

Pela fórmula é possível deduzir que quanto mais eficaz for o desenho e a implementação dos controles, ou seja, quanto maior for o NC, menor será o RC e vice-versa, porém este nunca será "zero", uma vez que o nível de confiança jamais será 100%. Uma vez estabelecido o RC, é possível estimar o nível de risco residual (NRR), ou seja, o risco que

permanece após o efeito das respostas adotadas pela gestão, incluindo controles internos e outras ações, para reduzir a probabilidade e ou o impacto do evento. Para isso, deduz-se do Nível de Risco Inerente (NRI) o percentual de confiança (NC) atribuído ao controle, o que equivale a multiplicar o NRI pelo RC, utilizando a seguinte fórmula:

$$NRR = NRI * RC \tag{2.4}$$

Segue-se na figura 2.9 um exemplo de um registro de riscos (parcial) com a determinação dos níveis dos riscos residuais (NRR) de alguns riscos identificados, de acordo com o método apresentado.

| RISCOS IDENTIFICADOS | P | I | NÍVEL DE RISCO INERENTE (NRI) | EFICÁCIA DO CONTROLE | RISCO DE CONTROLE (RC) | NÍVEL DE RISCO RESIDUAL (NRR) |
|---|---|---|---|---|---|---|
| Risco 1 | Alta - 8 | M. Alto - 10 | RE - 80 | Inexistente | 1,0 | RE - 80 |
| Risco 2 | Média - 5 | Alto - 8 | RM - 40 | Mediano | 0,6 | RM - 24 |
| Risco 3 | Baixa - 2 | Alto - 5 | RM - 10 | Fraco | 0,8 | RB - 8 |

Figura 2.9: Registro de riscos parcial com níveis de risco residual calculado. [44]

Na figura 2.10 temos um exemplo de um registro de riscos (parcial) com a determinação dos níveis dos riscos inerentes (NRI), de acordo com o método apresentado.

| RISCOS IDENTIFICADOS | PROBABILIDADE | | IMPACTO | | NÍVEL DE RISCO INERENTE (NRI) |
|---|---|---|---|---|---|
| Risco 1 – Descrição do risco 1 | Alta | 8 | Muito Alto | 10 | 80 RE (Extremo) |
| Risco 2 – Descrição do risco 2 | Média | 5 | Alto | 8 | 40 RA (Alto) |
| Risco 3 – Descrição do risco 3 | Baixa | 2 | Médio | 5 | 10 RM (Médio) |
| Risco ***n*** – Descrição do risco ***n*** | Muito Baixa | 1 | Médio | 5 | 5 RB (Baixo) |

Figura 2.10: Registro de riscos parcial com níveis de risco inerente calculados. [44]

A figura 2.11 apresenta os riscos residuais classificados por categorias, conforme os critérios da entidade para a classificação dos níveis de risco (Figura 2.5) para alguns níveis de risco inerentes selecionados da figura 2.6.

| NÍVEL DE RISCO INERENTE (NRI) | | | | | | |
|---|---|---|---|---|---|---|
| | 100 Extremo | 20 RM | 40 RA | 60 RA | 80 RE | 100 RE |
| | 80 Extremo | 16 RM | 32 RM | 48 RA | 64 RA | 80 RE |
| | 50 Alto | 10 RM | 20 RM | 30 RM | 40 RA | 50 RA |
| | 25 Médio | 5 RB | 10 RM | 15 RM | 20 RM | 25 RM |
| | 8 Baixo | 2 RB | 3 RB | 5 RB | 6 RB | 8 RB |
| | | 0,2 Muito baixo | 0,4 Baixo | 0,6 Médio | 0,8 Alto | 1 Muito alto |
| | | RISCO DE CONTROLE (RC) | | | | |

Figura 2.11: Matriz de riscos residuais.
[48], [49]

O propósito da matriz de riscos residuais é demonstrar o efeito dos controles (RC) sobre os riscos inerentes (NRI), por meio do cálculo do Nível de Risco Residual que aponta o grau do risco após a aplicação dos controles de segurança.

## 2.7 Avaliação dos Riscos

Segundo [26] a finalidade da avaliação de riscos é auxiliar na tomada de decisões com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento. A avaliação de riscos envolve comparar o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos quando o contexto foi considerado. Com base nesta comparação, a necessidade do tratamento pode ser considerada.

Para [50], a avaliação de risco é um processo usado para identificar e avaliar os riscos e seus efeitos potenciais. Já para o [47] a avaliação de riscos permite que uma organização considere até que ponto eventos em potencial podem impactar a realização dos objetivos.

Este trabalho avalia os riscos identificados com base no Modelo de Gestão de Riscos do Tribunal de Contas de União (TCU) - Manual de Gestão de Riscos e Avaliação de Maturidade da Gestão de Riscos [46] - que é baseado no COSO ERM, ISO 31000 e

frameworks de referência a nível mundial em Gestão de Riscos organizacionais. O então Ministério do Planejamento, Orçamento e Gestão produziu o Guia de Orientação para o Gerenciamento de Riscos, para apoiar o Modelo de Excelência do Sistema de Gestão Pública (GESPÚBLICA) e prover uma introdução ao tema gerenciamento de riscos [51].

Em 2009, o governo britânico divulgou o *Risk Management Assessment Framework: a Tool for Departments* [52], uma ferramenta para aferir a gestão de riscos nas organizações governamentais daquele país e identificar oportunidades de melhoria, derivada de um modelo de excelência de gestão utilizado por mais de trinta mil organizações, principalmente na Europa – *The EFQM Excellence Model* [53]. A ferramenta é estruturada em sete componentes e, assim como este roteiro do TCU, pode ser aplicada por examinadores externos ou auto aplicada pelos gestores. Por ter sido desenvolvido especificamente para o setor público e por tratar-se de ferramenta com a mesma finalidade pretendida pelo TCU (avaliar a gestão de riscos e identificar oportunidades de melhoria), o modelo foi considerado no desenvolvimento da base conceitual do modelo de avaliação da maturidade em gestão de riscos do TCU.

A avaliação do risco envolve a comparação do seu nível com o limite de exposição a riscos, a fim de determinar se o risco é aceitável. O limite de exposição de uma organização ao risco é o nível de risco que acima deste deve ser aplicado o tratamento ao risco, até que após o tratamento o risco residual esteja abaixo desses limites [46].

A figura abaixo demonstra uma matriz de gerenciamento de riscos da Secretaria do Conselho do Tesouro do Canadá [54] com ações a serem consideradas na etapa de tratamento do risco, conforme a classificação do mesmo.

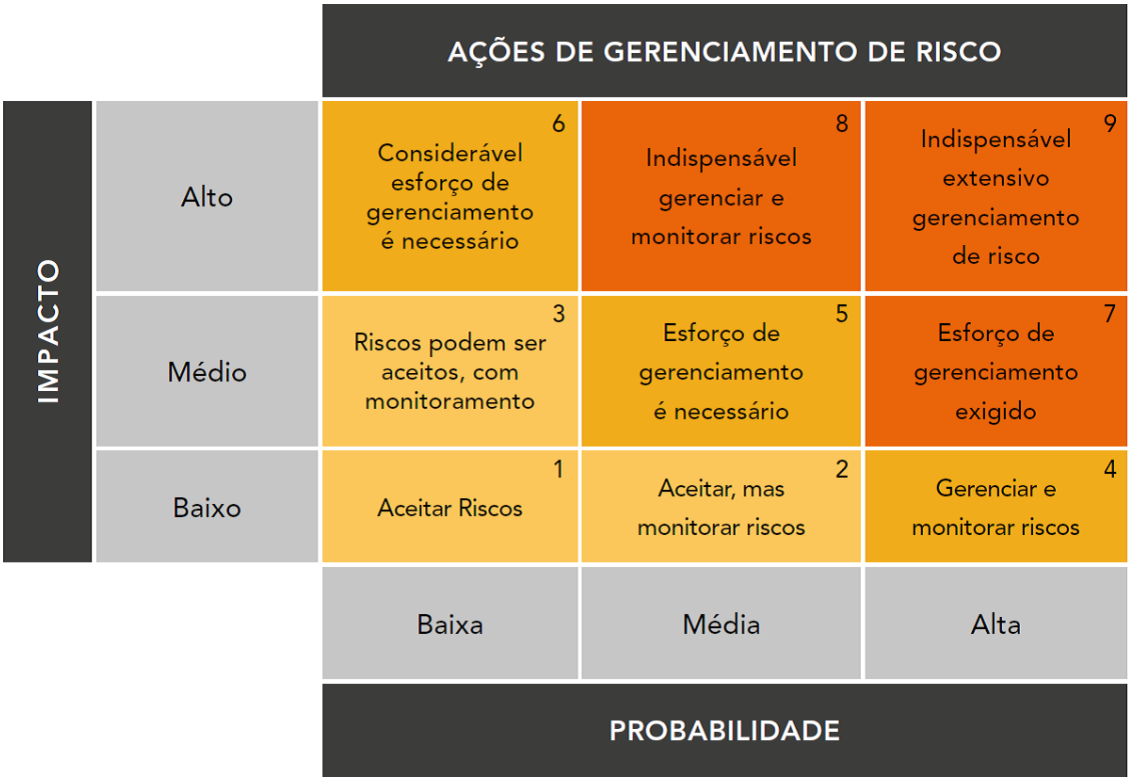


Figura 2.12: Matriz de gerenciamento de riscos.
[54]

Uma boa prática para apoiar o processo de avaliação de riscos é estabelecer critérios para priorização e tratamento (apetite a risco, nível recomendado de atenção, tempo de resposta requerido, comunicação etc.) associados aos níveis de risco. Os limites de tolerância ao risco devem ser definidos e podem ser demonstrados conforme figura abaixo:

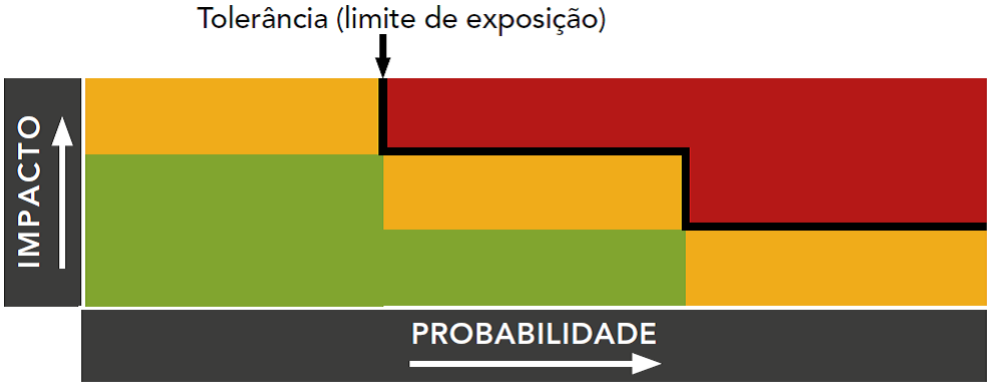


Figura 2.13: Matriz de avaliação dos riscos.
[55]

Conforme o posicionamento do risco na matriz acima, será determinada a ação e o tipo de tratamento para esse risco. Segunda [46] a avaliação dos riscos fornece subsídios para a tomada de decisão, não se constituindo em fator determinante para eventual tratamento do risco. Ou seja, cabe ao gestor, diante da lista de riscos ordenados por nível de risco, decidir quais merecerão ações mitigadoras. Para [56] a avaliação do risco permitirá enumerar as prioridades e apresentar as informações para tomada de decisão sobre a forma como os riscos devem ser controlados.

## 2.8 Gerenciamento de identidade e Acessos

O Gerenciamento de Identidades e Acessos (GIA) é uma função essencial para proteger a privacidade da informação, aprimorando a experiência do usuário, permitindo a prestação de contas e controlando o acesso aos ativos de uma organização. À medida que as organizações crescem e se adaptam as mudanças do mercado, elas acumulam vários sistemas, aplicativos, padrões e processos de armazenamento, gerenciamento e uso de identidades digitais para força de trabalho de empregados, trabalhadores terceirizados (contratados) e clientes. GIA é a coleção de processos e tecnologias usadas para gerenciar essas identidades digitais e acessos aos recursos fornecidos através delas. GIA é melhor descrito definindo seus principais componentes, o gerenciamento de identidade e o gerenciamento de acessos [57].

Segundo [58] a identidade é considerada digital quando surgem propriedades que são únicas e digitais, e/ou ainda pode se estabelecer fatos que relacione uma identidade a um indivíduo, ou seja, certificação de que determinado usuário é realmente quem ele garante ser.

O processo de estabelecer uma identidade de usuário é conhecido como identificação e autenticação. O objetivo é ter apenas usuários autorizados acessando um computador sistema, uma rede ou um serviço específico [59].

No Gerenciamento de Identidades e Acessos (GIA), o comportamento do usuário é monitorado e analisado em relação aos direitos de acesso já estabelecidos, com o objetivo de identificar privilégios excessivos ou um acesso anormal. Isso vale para todos os tipos de usuários e contas, incluindo usuários privilegiados e contas de serviço. As organizações também usam o modelo denominado Análise de Comportamento de Entidades e Usuários do acrônimo em inglês UEBA (*User and Entity Behavior Analytics*) para ajudar a limpar contas inativas e privilégios de usuário que são definidos como mais altos do que precisam ser [60].

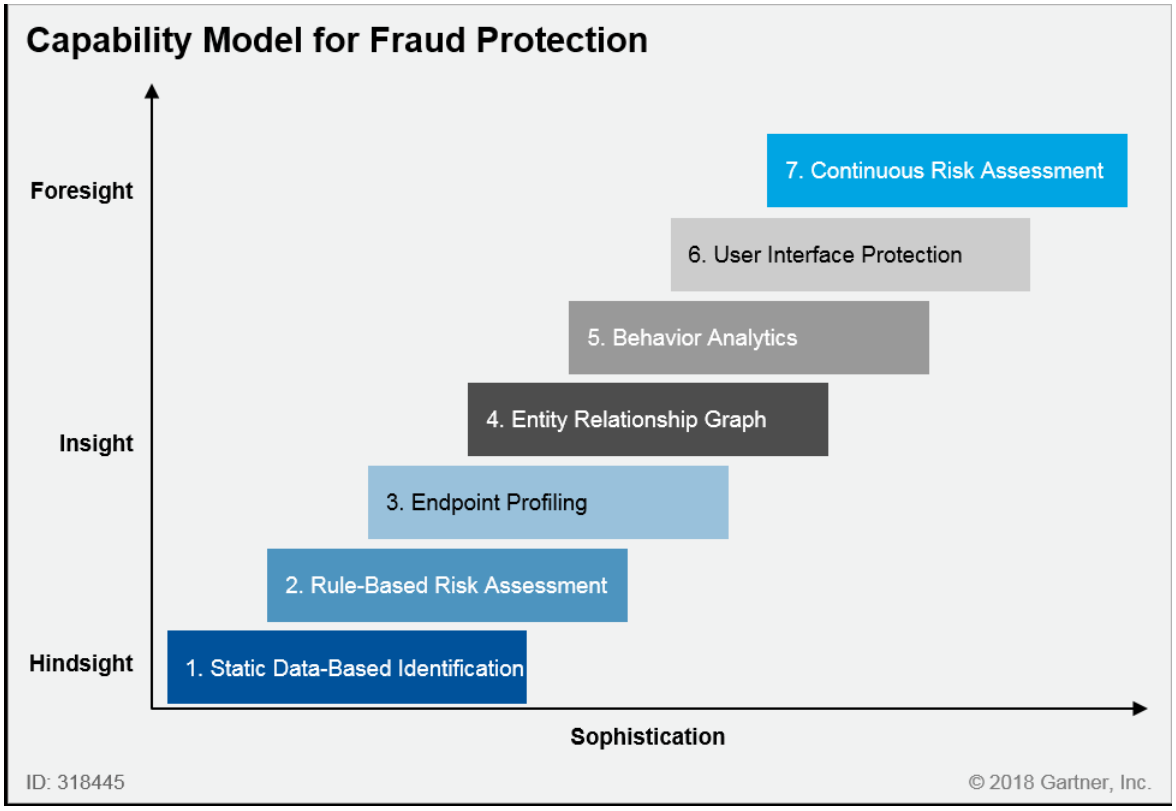


Figura 2.14: Modelo de Capacidade de OFD (*Online Fraud Detection*). [60]

O modelo de capacidade acima publicado pelo Gartner [60] para a categoria de soluções de OFD (*Online Fraud Detection*) que são tecnologias que atuam no combate a prevenção de fraudes, aponta a Análise de Comportamento como um dos principais fatores de combate às fraudes e sequestro de informações.

As tecnologias do modelo de capacidade detectam com mais precisão os ataques de identidade, como fraude de identidade. Além disso, há um afastamento dos métodos de detecção de fraudes pontuais (por exemplo, no momento do cadastro) para um modelo de avaliação contínua de riscos, baseado em atividades precursoras identificáveis e atributos não transacionais da interação com o cliente.

À medida que as técnicas se tornam mais sofisticadas, surgem métodos que detectam padrões históricos de fraude, e tentam impedir que esses padrões tornem-se recorrentes. A tendência é em direção a métodos que forneçam *insight* e inteligência orientada para a ação quanto ao risco de cada interação com o cliente [61].

O gerenciamento de identidade e acesso pode ser fornecido como serviços de nuvem; ou seja, segurança entregue através da nuvem. O Gerenciamento de Identidades consiste no gerenciamento, criação e exclusão de identidades digitais. O gerenciamento de acesso é mais granular, consiste na autorização de acesso da entidade a recursos protegidos [62].

Para [60] o Gerenciamento de Identidade e acessos refere-se às "tecnologias, processos, políticas e infraestruturas de suporte necessárias para a implantação, controle e manutenção de identidades digitais e acesso a seus recursos".

Segundo [63], ao contrário das tecnologias de segurança de conteúdo e de rede, as tecnologias de GIA podem complementar várias camadas do modelo OSI. O GIA complementa a camada 8 (oito) do modelo OSI por meio da avaliação abrangente de ameaças e gerenciamento de riscos, licenciamento (incluindo autoria, assinaturas e certificados) e unificação de políticas de segurança e governança (incluindo gerenciamento de privacidade e forense) que visam limitar violações de privacidade e garantir conformidade regulatória.

Nas camadas de aplicativos e apresentações, o GIA oferece gerenciamento de identidades seguro (incluindo identidade federada, gerenciamento de credenciais, *single signon*, infraestrutura de chave pública e serviços de diretório), acesso e gerenciamento de funções corporativas incluindo autenticação (por exemplo, autenticação forte, autenticação baseada em conhecimento e autenticação multifator, etc.), autorização e auditoria [64].

Isso é seguido pelo gerenciamento de contas, que abrange o gerenciamento de senhas e o provisionamento e o desprovisionamento de usuários. Nessas duas camadas do modelo OSI, o GIA também abrange o gerenciamento de confiança (incluindo escalonamento de privilégios e gerenciamento de direitos digitais). Na camada de sessão, o GIA fornece recursos de *secure sockets layers* (SSL) que permitem a verificação das identidades dos servidores, usando criptografia de chave pública (PKI) e clientes usando autenticação no lado do cliente. Nas camadas de transporte e de rede, o GIA oferece tecnologias de avaliação de riscos para redes corporativas, análise de políticas de terminais, aplicação de conformidade e capacidades de autorização de acesso, e soluções de segurança de acesso à rede baseadas em padrões. Na camada de *link* de dados, o GIA consiste em listas de controle de acesso e protocolos de qualidade de serviço, e na camada física, o GIA oferece tecnologias de identificação, incluindo cartões inteligentes, *tokens* e biometria, e pode ser usado para gerenciamento e recuperação de desastres.

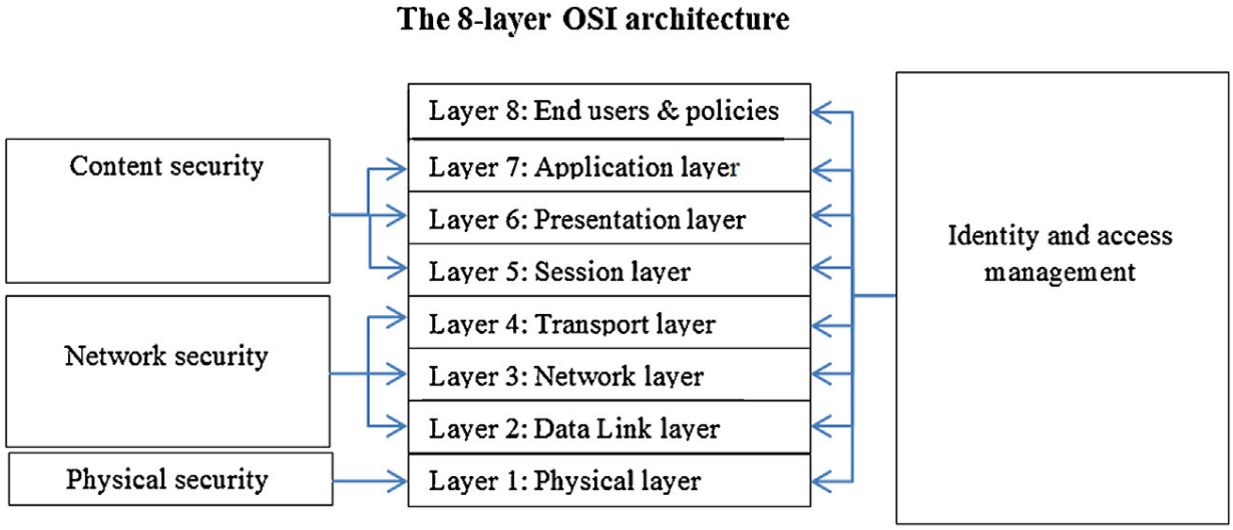


Figura 2.15: Mapeamento das tecnologias de segurança da informação em relação as camadas de TI.

[64]

Na figura acima é demonstrado segundo [63] o relacionamento das tecnologias de segurança da informação com as camadas de rede do modelo OSI (Open System Interconnection), onde as políticas de usuários finais estão numa nova camada.

Um sistema de gerenciamento de identidades consiste na integração de políticas e processos de negócios, resultando em um sistema de autenticação de usuários aliado a um sistema de gerenciamento de atributos. De acordo com [65], o sistema de gerenciamento de identidades é caracterizado pelos seguintes elementos:

(a) Usuário – aquele que deseja acessar algum serviço;

(b) Identidade – conjunto de atributos de um usuário. Pode ser seu nome, endereço, filiação, data de nascimento, etc;

(c) Provedor de Identidades (*Identity Provider* – IdP) – responsável por emitir a identidade de um usuário. Após o usuário passar por um processo de autenticação, este recebe uma credencial, dita identidade, que é reconhecida como válida pelos provedores de serviço;

(d) Provedor de Serviços (*Service Provider* – SP) – oferece recursos a usuários autorizados, após verificar a autenticidade de sua identidade e após comprovar que a mesma carrega todos os atributos necessários para o acesso.

De acordo com [66], o gerenciamento de identidades apresenta diferentes modelos. Esses modelos são dispostos de acordo com a sua arquitetura, apresentando-se, portanto como: tradicional, centralizado, centrado no usuário e federado.

(a) Modelo Tradicional.

Também conhecido como Silo ou Modelo Isolado, onde o Provedor de Serviço (SP) funciona como Provedor de identidade (IdP). Neste modelo o usuário do serviço é o principal responsável por criar e administrar sua identidade. Os usuários apresentam grandes dificuldades quanto à utilização deste modelo, pelo fato dos mesmos terem que gerir diversas contas bem como diversas senhas, muitas vezes não obedecendo às regras de segurança. A figura 2.16 mostra o modelo em questão:

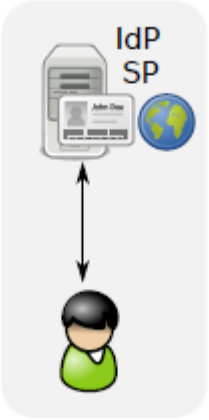


Figura 2.16: GIA - Modelo tradicional.

(b) Modelo Centralizado.

Como o modelo tradicional não se apresentava muito flexível surgiu como proposta de solução o modelo centralizado, onde se passa a centralizar tudo em um único Provedor de Identidade, onde todos os serviços o consultam para a realização da autenticação dos usuários. Não é necessário possuir diversas identidades como no modelo tradicional, neste modelo é utilizado o conceito de autenticação única conhecido por *Single Sign-On* (SSO) que lhe dá direito a usufruir de todos os serviços com apenas uma autenticação. Caso o Provedor de identidade seja acometido por alguma falha, todos os sistemas estarão comprometidos. A figura 2.17 ilustra o modelo Centralizado:

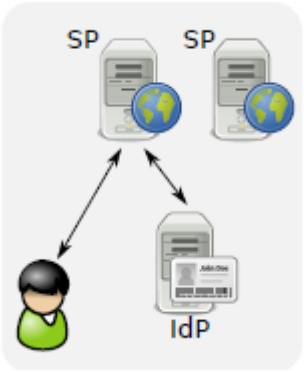


Figura 2.17: GIA - Modelo centralizado.

(c) Modelo Federado.

Neste modelo a autenticação do usuário ocorre de maneira descentralizada através de múltiplos provedores de identidades, que se encontram distribuídos em diferentes domínios administrativos. Um domínio administrativo é composto de diversos provedores de serviços enquanto há somente um único provedor de identidade. Em um determinado domínio um provedor de identidade que possui uma identidade de usuário cadastrado, pode partilhar com outros domínios, desde que tenha uma relação de confiança com outros domínios, não sendo necessário ter uma identidade em cada domínio. A figura seguinte mostra a relação:

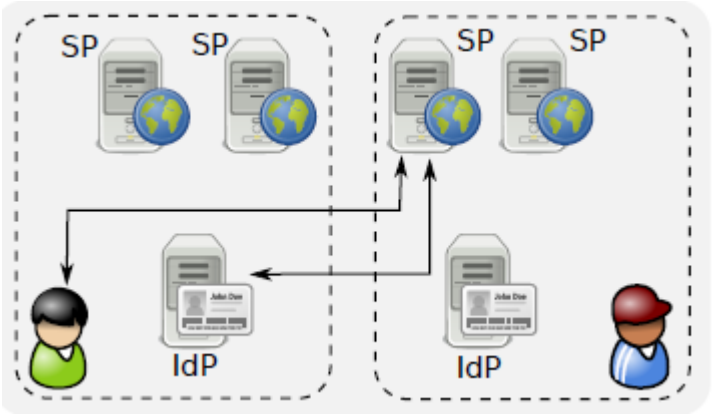


Figura 2.18: GIA - Modelo federado.

(d) Modelo Centrado no usuário.

O modelo centrado no usuário objetiva dar ao usuário o total controle sobre suas identidades digitais, contudo as principais propostas e implementações deste modelo fazem uso de um dos modelos apresentados anteriormente, sendo o modelo de identidade federado o mais usado. As identidades dos usuários, destinadas a diferentes

provedores de serviços, são armazenadas em um dispositivo físico que fica em poder do usuário, como um *smartcard* ou mesmo um telefone celular. O usuário se autentica neste dispositivo físico e cabe a este liberar as informações do usuário para cada provedor de serviços que o usuário acessar, respeitando totalmente as preferências de privacidade do usuário.

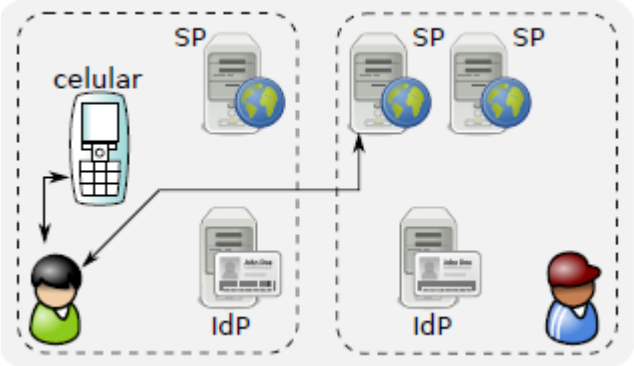


Figura 2.19: GIA - Modelo centrado no usuário.

Na figura 2.19 temos a representação do modelo centrado no usuário, onde as identidades do usuário ficam em dispositivos como os telefones inteligentes, estes autenticam o usuário e se relacionam com cada provedor de serviços (SP) para liberar as informações para o usuário.

## 2.9 Controle de Acesso

O Controle de Acesso é o elemento central de segurança de computadores, pois os principais objetivos da segurança de computadores são impedir que usuários não autorizados consigam acesso a recursos, impedir que usuários legítimos acessem recursos de maneira não autorizada e permitir que usuários legítimos acessem recursos de maneira autorizada [67].

Para [68], o controle de acesso é uma área da segurança da informação que controla a forma como os dados devem ser acessados. O Controle de Acesso ganha cada vez mais importância, pois além de ser altamente importante e crítico para a segurança da informação, existem muitas más prática em seu gerenciamento.

Segundo [69], os quatro componentes do controle de acesso são:

(a) Identificação (também chamada de registro): "Quem é você?- o usuário fornece informação para se identificar, por ex. endereço de e-mail, usuário ID, nome ou nome de usuário;

(b) Autenticação "Você é quem você diz que é?- o usuário verifica sua identidade ou de qual organização ele vem;

(c) Autorização "O que você pode fazer?- o processo de determinar o que o usuário identificado e autenticado tem permissão para acesso e quais operações ele pode realizar. No caso de recursos de informação licenciados, isto é baseado em perfis de usuário e permissões de licenciamento;

(d) Auditoria: O processo de coleta de estatísticas e/ou dados de faturamento. As mesmas ferramentas também podem ser usadas para investigar quais as contas de usuário podem ser comprometidas devido a acesso não autorizado.

## 2.10 Autenticação

Autenticação é o processo de verificar as credenciais de um usuário que está tentando acessar um recurso protegido. Uma autenticação baseada em senha do ID (identificador) do usuário é a solução predominantemente implementada. Enquanto isso serve como um mecanismo suficiente para a maioria das necessidades de negócios e é suscetível a muitas ameaças conhecidas. A autenticação é fundamental para proteger os recursos da nuvem. Ele verifica a identidade da entidade (usuário ou máquina) que deseja acessar os recursos da nuvem, e isso deve ser feito de maneira segura, confiável e gerenciável [70].

Autenticação é o processo de verificação das credenciais de uma entidade que tenta acessar um recurso protegido. A autenticação deve ser feita de maneira segura, confiável e gerenciável. Para contas que exigem níveis mais altos de segurança, podem ser necessárias autenticações de múltiplos fatores. Sistemas de autenticação devem ter a capacidade de usar a definição de risco de transação comercial como orientação e fornecer autenticação adaptativa baseada no nível de risco da transação.

Para [71] a autenticação visa estabelecer confiança na identidade das entidades e serviços em todas suas interações. Técnicas de autenticação baseadas no *Analytics* (Análise de Dados), incluindo autenticação biométrica comportamental contínua, estão alinhadas com a verificação de identidade e prevenção de fraude, e permitem abordagens adaptativas.

Segundo [72], a Autenticação é o processo de verificação de uma identidade alegada por ou para uma entidade do sistema. Um processo de autenticação consiste em duas etapas: etapa de identificação que consiste em apresentar um identificador ao sistema de segurança, essas identidades autenticadas são base para o controle de acesso, e a etapa de verificação que consiste em apresentar ou gerar informações de identificação que corroboram o vínculo entre a entidade e o identificador. Existem quatro meios gerais de

autenticação da identidade de um usuário, que podem ser usados isoladamente ou em combinação:

(a) Algo que o indivíduo sabe: alguns exemplos são uma senha, um número de identificação pessoal (PIN, do acrônimo em inglês para personal *identification number*) ou respostas a um conjunto de perguntas pré-estipuladas;

(b) Algo que o indivíduo possui: alguns exemplos são chaves criptográficas, cartões de senha eletrônica, *smart cards* e chaves físicas. Esse tipo de autenticador e conhecido como um *token*;

(c) Algo que o indivíduo é (biometria estática): alguns exemplos são reconhecimento por impressão digital, retina e face;

(d) Algo que o indivíduo faz (biometria dinâmica): alguns exemplos são reconhecimento pelo padrão de voz, características de escrita manual e ritmo de digitação.

Autenticação do usuário é a confirmação em tempo real (com uma confiança implícita ou um nível de confiança) da reivindicação de uma pessoa a uma identidade previamente estabelecida para permitir seu acesso a um ativo eletrônico ou digital [73].

A autenticação é a identificação segura de entidades em que uma prova de possuir uma identidade é verificada. O acesso de uma entidade a um sistema é encapsulado o que ficou conhecido como uma conta. Envolver-se em um ato de autenticação pode ocorrer em todas as tentativas de acessar um sistema de computação controlado, conhecido como *login*, quando um serviço de um aplicativo é solicitado no tempo em que um acesso à rede é executado.

A evidência resultante de uma identidade estabelecida é mantida pelo dispositivo de computação no que é chamado de contexto de segurança. O último permanece firmemente ligado a cada unidade de trabalho solicitada pela entidade. Um contexto de segurança pode ser trocado localmente pelos espaços de endereço e pode ser transmitido através de uma rede incorporada no pedido com o qual está associado [74].

Autenticação tradicional por senha e autenticação de segurança elevada através do uso de um segundo fator (por exemplo, um token SecurID) ficam aquém no contexto de autenticação em dispositivos móveis, onde as limitações do dispositivo e a atitude do consumidor exigem uma maior integração e uma experiência conveniente e mais segura [74].

Os métodos modernos de autenticação geralmente usam dois ou vários fatores de autenticação, em que diferentes fatores de pelo menos duas categorias são examinados para verificar a identidade de um usuário ou dispositivo - "quanto mais fatores empregados, mais robusta a autenticação do sistema [75]".

### 2.10.1 Autenticação Contínua

A autenticação contínua surge como uma solução para assegurar a identidade do usuário durante toda sua sessão e não somente no início.

A autenticação contínua também pode ser feita de forma implícita, ou seja, sem que o usuário fique ciente que está passando pelo processo de autenticação. Em [76] é feito uso do padrão de digitação do usuário como uma forma de autenticá-lo continuamente de forma implícita. Com o advento da popularização dos telefones inteligentes e pela riqueza de sensores que esses possuem, a autenticação contínua implícita poderia ser obtida com base na geolocalização contexto do acesso, por reconhecimento facial, etc [77].

Com o processo de autenticação é possível assegurar que um sujeito é realmente quem dizer, tendo como bases as credenciais fornecidas por esse. Geralmente os usuários só precisam passar pelo processo de autenticação antes de terem acesso ao recurso desejado. Uma vez autenticados, esses poderão usufruir dos recursos até o fim de sua sessão.

## 2.11 Autenticação por Comportamento ou por Contexto

O emergente paradigma de computação móvel torna viável o acesso a recursos de qualquer lugar e em qualquer momento. Porém, ao mesmo tempo, que esse acesso ubíquo proporciona os seus benefícios, ele cria desafios particulares para prover segurança às entidades participantes. Tais desafios não são tratados de forma apropriada por abordagens tradicionais de segurança [78].

Os mecanismos tradicionais de autenticação são ineficazes para satisfazer as necessidades de ambientes altamente dinâmicos como os ambientes móveis e pervasivos [79]. Ainda, segundo [80], a eficácia da maioria dos mecanismos de autenticação para computação móvel depende da força dos identificadores utilizados para a autenticação dos usuários.

Um ambiente pervasivo é caracterizado pela riqueza de contextos, no qual usuários, dispositivos e agentes se deslocam entre diversos lugares e diversas entidades, como serviços, aplicações e recursos alternando sua disponibilidade sobre o tempo [81].

A computação pervasiva tem como objetivo dar às pessoas acesso conveniente a informações relevantes e a capacidade para agir com base nessa informação a qualquer momento e em qualquer lugar [82].

Consequentemente, autenticação sensível ao contexto, que utiliza a mudança de contexto para permitir a adaptação dos mecanismos de segurança baseada na situação atual, é essencial para prover segurança de forma efetiva para ambientes pervasivos [78].

O acesso contextual é, em sua essência, uma evolução da autenticação adaptativa que substitui o uso de regras estáticas e listas negras por aprendizado de máquina para avaliar o risco com base no comportamento e no contexto do usuário [83].

Inicialmente, o sistema de autenticação passa por uma fase de aprendizado do comportamento do usuário, os padrões de comportamento são coletados e, em seguida, aprendidos como um modelo de usuário. Com base neste modelo de usuário e em alguns dados recentes do comportamento do usuário, podemos fazer uma comparação para decidir se a autenticação é permitida ou não. A comparação depende de um valor de probabilidade que reflita uma pontuação de autenticação que aumente ou diminua de acordo comportamentos observados. Eventos habituais e tarefas habituais são julgados como eventos positivos que aumentam a pontuação. Quando o a pontuação diminui e fica abaixo de um limite predefinido, o usuário é solicitado a autenticar explicitamente.

Um esquema de autenticação, baseado em transações móveis, chamado TBAS (Transação-Baseada no Esquema de Autenticação) foi proposto por [80], esse esquema opera no nível do aplicativo para classificar o comportamento e as transações do usuário com a ajuda de agentes inteligentes para perceber a informação no ambiente e raciocinar sobre estas percepções.

A figura 2.20 abaixo apresenta o modelo TBAS que é um sistema baseado na análise comportamental do usuário:

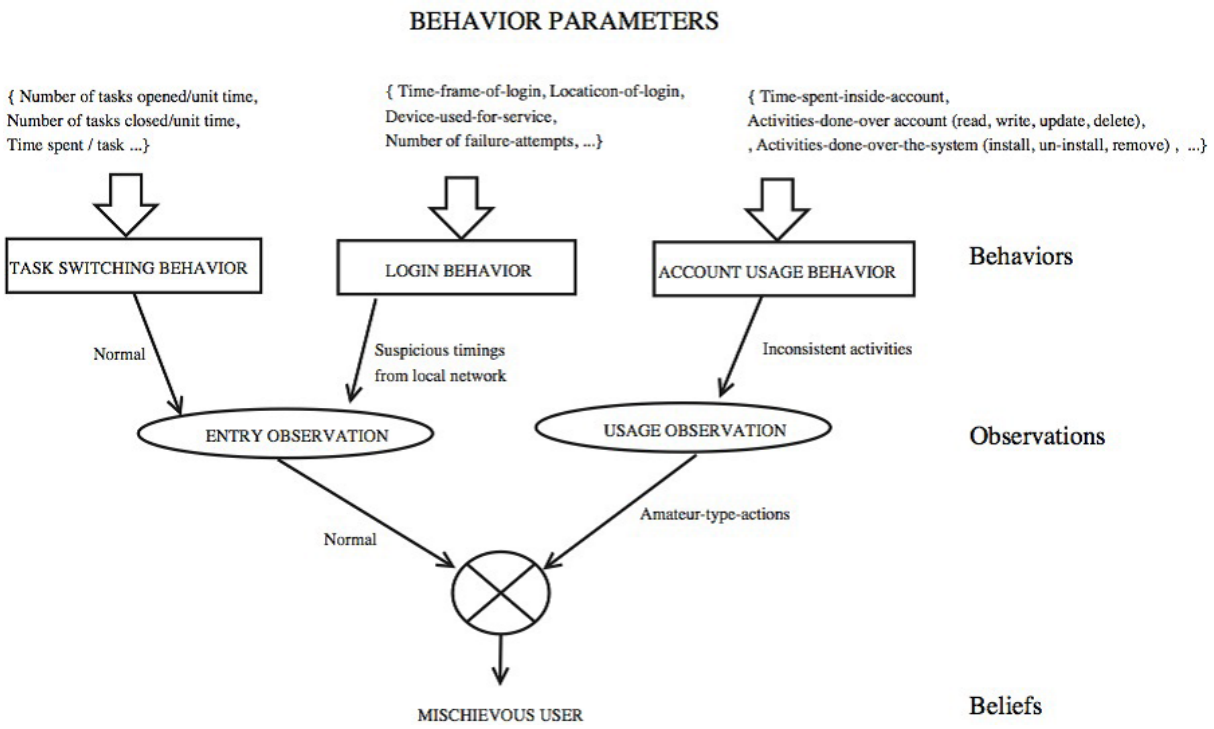


Figura 2.20: Análise comportamental do usuário.
[80]

Autenticação por Contexto funciona coletando informações sobre o usuário e sobre seu padrão de uso comum. Quando usado fora de padrões conhecidos, o sistema gera desafios adicionais para o usuário passar antes que ele possa acessar suas informações. Uma maneira de trabalhar é através do gerenciamento de *cookies* e informações sobre o sistema que está acessando o site. Por exemplo, o tipo e versão do navegador usado para iniciar a sessão pode ser um fator que desencadeia níveis adicionais de autenticação. Uma vez que o mecanismo de autenticação percebe um novo computador, ou padrão de acesso, o sistema busca métodos de autenticação. Um componente de gerenciamento de risco no sistema de autenticação traduz a política organizacional em decisões de controle e ações por meio de um mecanismo de imposição de regras. Ajusta dinamicamente desafios de autenticação necessários para um usuário com base nos indicadores de risco (coletadas em tempo real), informações sobre políticas e entrada de dados do sistema de fraude [84].

Existem diferentes maneiras de usar recursos de autenticação por contexto. Algumas implementações simplesmente transmitem leituras de sensor para o seu parceiro de comunicação para avaliar [85], enquanto outros esquemas geram seu fator de autenticação do ambiente [86] ou a partir de eventos [87], [88].

Contexto inclui qualquer informação relacionada para a situação de um usuário, como

localização, status do dispositivo e qualquer informação relacionada ao ambiente, como temperatura, volume e brilho. Outra classificação de contexto contextual relevante para a segurança são os atributos que incluem o contexto do ambiente físico (por exemplo, hora ou temperatura); contexto do tipo de serviço (por exemplo, serviço premium ou básico); contexto do usuário (por exemplo, localização); contexto da plataforma (por exemplo, o estado confiável da plataforma); e transação particular (por exemplo, um token eletrônico ou recibo eletrônico) [89]. Além do que, informação contextual inclui contextos pessoais (por exemplo, preferências); contextos de atividade (por exemplo, reunião, agenda ou lista de compras); contextos físicos (por exemplo, hora e localização); contextos do dispositivo (por exemplo, e tamanho de exibição); contextos sistemáticos (por exemplo, largura de banda de rede); contextos de aplicação (por exemplo, agente e serviço); e contextos ambientais (por exemplo, nível de luz) [90], [91].

O comportamento do usuário é complexo e os modelos são muitas vezes construídos para corresponder aos comportamentos de vários usuários. Como resultado, a computação baseada em contexto é um aspecto importante que deve ser considerado em ambientes difusos com o objetivo de entender a relação entre os usuários, os dispositivos e ambientes. Mais especificamente, a quantidade significativa de informação em uma configuração abrangente pode ajudar na compreensão do comportamento do usuário [92].

Segundo [78], ambientes altamente dinâmicos, tais como ambientes difusos, necessitam de reconhecimento de contexto mecanismos de segurança, porque a mudança de contexto permite esses mecanismos para ajustar com base no status atual.

A Autenticação Baseada em Contexto é uma resposta dinâmica às condições variáveis da classificação de risco um determinado usuário (agente) e a transação em um determinado momento. Quanto maior a classificação de risco da transação, maior o nível de autenticação exigido do agente, em para concluir a transação. O nível de risco do agente é determinado examinando contextos comportamentais, como um histórico de solicitações semelhantes, localização do agente, transação e tempo da solicitação. Quaisquer anomalias comportamentais podem desencadear uma reação, variando de uma solicitação de autenticação adicional a uma negação da transação [70].

Mecanismos de segurança adaptativos são capazes de responder dinamicamente a mudanças ambientais reconfigurando suas funções de segurança. Além disso, eles apoiam a ideia de que a segurança pode ser mais eficaz se vários níveis variáveis de segurança forem apresentados aos usuários e aos sistemas. Os serviços de segurança exigem uma infraestrutura sensível ao contexto para a detecção e interpretação de informações de contexto, a fim de permitir uma segurança adaptativa controlada quando necessário. As informações de contexto podem incluir qualquer tipo de dados, como fatores humanos (hábitos do usuário, estado mental, ambiente social, atividades relacionadas à tarefa), o

ambiente físico (localização, conectividade de rede, energia da bateria), dados de negócios (atividades direcionadas a objetivos, confiança) e tempo. Um contexto de segurança pode ser definido como a informação coletada do usuário e seu ambiente de aplicação que é relevante para a infraestrutura de segurança do usuário e do aplicativo. A informação de contexto forma assim, além dos tradicionais serviços de segurança, um elemento adicional importante do contexto de segurança. Um exemplo ilustrativo é o uso de informações de localização e velocidade para inferir que um usuário é um viajante de trem e, portanto, é concedido acesso aos serviços oferecidos no trem [93].

Diante do exposto pelos autores, a autenticação por contexto ou comportamento é um método adaptativo considerado eficaz para ambientes pervasivos, caracterizado pela dinamicidade e mudança constante de contexto ou comportamento. O contexto é formado por características do perfil de acesso, do ambiente e dos usuários. A partir da análise desse contexto o acesso pode ser negado ou validado com uso de técnicas de confirmação de legitimidade.

## 2.12 Autorização

Autorização é o processo de concessão de direitos de acesso (direitos) a um usuário, programa ou processo [84].

Autorização garante que um usuário autenticado somente tenha acesso aos recursos que foram autorizados. Tendo estabelecido (para um nível apropriado de certeza) que um usuário *on-line* é de fato o indivíduo que eles afirmam ser, autorização é o processo de determinar se esse indivíduo deve ter acesso a esse recurso. Para alguns recursos (como um *wiki* editável), pode haver vários possíveis níveis de autorização aos quais diferentes utilizadores têm direito ("ler", "gravar", "editar", etc.), e diferentes tipos de usuários podem ter acesso a diferentes partes de um recurso (por exemplo, funcionários e alunos provavelmente poderão ver recursos em um ambiente de aprendizado virtual).

Autorização refere-se a direitos e privilégios concedidos a um indivíduo ou processo que permitem o acesso a recursos do computador e ativos de informação. Depois que a identidade e a autenticação de um usuário são estabelecidas, os níveis de autorização determinam a extensão dos direitos do sistema que um usuário pode ter [94].

Enquanto a Autenticação é o mecanismo de aplicação pelo qual os sistemas validam o acesso com a segurança corporativa. A autorização, pelo contrário, é o mecanismo de aplicação que um sistema determina qual nível de acesso um determinado usuário autenticado deve ter e direcionar recursos controlados pelo sistema. Uma vez que a identidade seja reconhecida e validada, o aplicativo autorizará a usuário para executar funções no aplicativo com base nos direitos de acesso associado à identidade do usuário.

Por exemplo, um aplicativo pode ser concebido de modo a proporcionar a determinados indivíduos específicos a capacidade de recuperar informações do aplicativo, mas não a capacidade de alterar dados armazenados nos sistemas de back-end, ao mesmo tempo em que capacidade de alterar dados [84].

A autorização relaciona-se à concessão de permissões a um determinado indivíduo que deseja obter acesso um determinado recurso. Esta se encontra ligada diretamente com a autenticação. O usuário, após realizar a validação da sua identidade, para que acesse aos recursos, tem que saber quais restrições se encontram dirigidas a estes, como por exemplo, o que se pode fazer com esta autorização, o que está tentando fazer, etc.

## 2.13 *Single Sign-On (SSO)*

De acordo com [42] o *Single Sign-On* (SSO) permite que os usuários finais acessem múltiplos serviços com um conjunto único de credenciais.

Os sistemas de autenticação podem ser implementados para fornecer serviços de SSO, que agregam identidades e permitem acesso a vários sistemas por meio do método de autenticação do sistema. Os usuários podem fornecer uma senha, uma vez e trabalhar o tempo necessário conforme limite de tempo determinado pela organização [84].

O *Single Sign-On* (SSO), permite autenticação única, em que a mesma autenticação de um usuário possa ser compartilhada simultaneamente por diversos provedores de serviço [95].

O *Single Sign-On* (SSO) é a funcionalidade do gerenciamento de acesso em que o usuário é autenticado uma vez e as credenciais para a sessão são confiáveis para diferentes aplicativos dentro de um domínio de segurança. Isso é tipicamente feito dentro de um domínio de segurança ou risco. O SSO é um requisito crítico dentro das organizações que operam aplicativos em uma infraestrutura de nuvem específica.

Segundo [96] uma organização pode executar várias aplicações web que requerem controle de acesso. Integrando componentes de controle de acesso em todas aplicações resultaria em altos custos de gerenciamento e inconveniências para os usuários que tenham que lembrar de todas as suas credenciais.

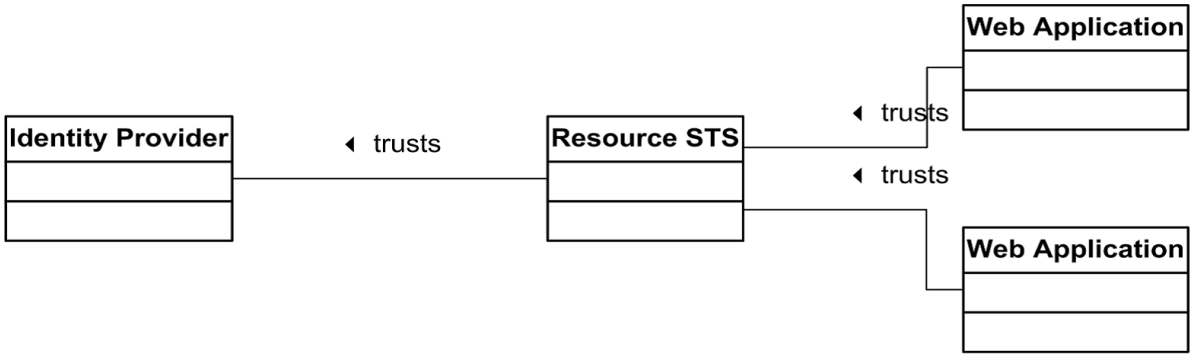


Figura 2.21: Arquitetura de *Single Sign-On*.
[96]

A figura acima é de arquitetura de serviço de SSO onde um *Identity Provider* (IP) e um *security token services* (STS) estão configurados. Todas as aplicações estão configuradas para enviar solicitações de recursos dos usuários para o STS. O STS redireciona o usuário novamente, agora para seu IP configurado que exibe um formulário de login. Caso as credenciais válidas tenham sido fornecidas, *token* de segurança é gerado e transmitido para o STS. O STS determina as permissões para a identidade declarada na entrada do token, gera um novo *token* e redireciona para a aplicação original. Quando o usuário acessa outras federações, aplicações são ativadas dentro da mesma sessão, o IP não terá para mostrar o formulário de *login* novamente, pois ele já autenticou o usuário e o token emitido ainda estão disponíveis como dados da sessão [96].

Tradicionalmente, o *Single Sign-On* é um processo que permite ao usuário acessar vários aplicativos que exigem autenticação passando suas credenciais apenas uma vez. O usuário primeiro se autentica em alguma autoridade confiável e, em seguida, é concedido acesso a todos os aplicativos que confiam nessa autoridade. As aplicações só recebem informações sobre se elas podem deixar o usuário entrar ou não. Como o usuário autentica apenas uma vez, a exposição de informações confidenciais pela rede é limitada. Sistemas SSO geralmente preservam o estado do usuário por algum período de tempo, para que o usuário possa acessar repetidamente esses aplicativos sem a necessidade de autenticar repetidas vezes.

O SSO na nuvem é uma extensão do SSO local na *Web*. Como as empresas se expandem além de seus limites locais, há demanda em expansão para a nuvem. O resultado é implementação do SSO entre os aplicativos corporativos locais e os aplicativos baseados em nuvem.

O SSO Federado utiliza a tecnologia denominada de Federação que fornece a capacidade de compartilhar a identidade do usuário e acessar informações entre vários domínios, o que podem estar dentro das mesmas ou diferentes infraestruturas e organizações de TI.

O *Single Sign-On* Federado permite várias organizações fornecerem seus serviços em um ambiente colaborativo de maneira segura. O SSO Federado, quando implementado corretamente em um domínio de autenticação forte, fornece segurança para a organização e a facilidade de uso para o consumidor da nuvem.

## 2.14 Federação

Os serviços de identidade federada permitem que uma organização gerencie a identidade e o acesso de seus usuários a recursos de organizações parceiras que fornecem serviços autorizados para esses usuários específicos. Enquanto os processos de gerenciamento de identidades federada ajudam a gerenciar o ciclo de vida das identidades e contas dos usuários nos sistemas de parceiros, o Single Sign-On federado ajuda na autenticação dos usuários internamente e, em seguida, transmite essa identidade para seu provedor de serviços em nuvem, como um token confiável. Isso permite que a organização mantenha o controle do processo de autenticação.

A identidade federada indica que indivíduos (pessoas ou entidades) podem usar suas credenciais (id local, senha biométrica, etc.) para acessar redes de diferentes entidades (governos, empresas, etc.) sem aderir para um sistema centralizado de logon único.

Uma federação de identidades permite acesso transparente a seus usuários aos serviços oferecidos pelos membros e parceiros. Esta federação é apoiada por padrões de comunicação e troca de mensagens, como o SAML (*Security Assertion Markup Language*). Em uma federação de identidade, o usuário tem apenas uma credencial, criada em instituição de origem, que permite a transparência e a solidez no acesso único [97].

(a) Gerenciamento de identidade federada

O gerenciamento de identidade federada fornece as políticas, processos e mecanismos para gerenciar a identidade e acesso confiável à sistemas nas organizações. Isso permite reutilizar as identidades dos usuários nos limites da organização, e garante gerenciamento eficiente do ciclo de vida do usuário, conformidade e congruência de informações de usuários relevantes entre duas organizações parceiras sem sobrecarga administrativa excessiva. O objetivo principal do gerenciamento de identidade federada é fornecer aos usuários de um domínio de segurança a capacidade de acessar os sistemas de outro domínio de maneira contínua, permitindo assim o *Single Sign-On* federado [70].

Os sistemas de gerenciamento de identidade e acesso devem suportar a cooperação entre organizações, principalmente para fornecer recursos como SSO. As identidades utilizadas nesse contexto são denominadas identidades federadas [98].

O Gerenciamento de Identidade Federada (FIM - *Federated Identity Management*) visa facilitar a gestão da identidade, processos e políticas entre as entidades colaboradoras com um controle descentralizado. Um framework FIM consiste em processos e todas as tecnologias subjacentes para a criação, gerenciamento e uso de identidades digitais compartilhadas entre várias organizações [96].

(b) *Single Sign-On* Federado (SSO)

O *Single Sign-On* federado (SSO) permite que a autenticação de um usuário em um domínio seja confiável em todos os domínios diferentes (por exemplo, diferentes provedores de serviços). Isso proporciona conveniência aos usuários e melhor segurança, se o domínio de autenticação mantém uma forte postura de segurança. O *Single Sign-On* federado é necessário como uma funcionalidade padrão para facilitar o acesso de domínio interorganizacional e intersegurança aos recursos aproveitando o gerenciamento de identidade federada [70].

O *Single Sign-On* federado pode ser alcançado usando algoritmos padrões do setor que não são parte do escopo deste trabalho, como o *SAML*, *WS-Security*, *Open ID* e *OAuth*. Ao implantar o SSO federado, é importante decidir qual padrão usar, com base nos casos de uso a serem suportados [70]. Na figura abaixo é representado um processo de autenticação federada, onde um provedor de identidade fornece um *ticket* usando o protocolo *SAML* para acesso a aplicações de um provedor de serviços confiável.

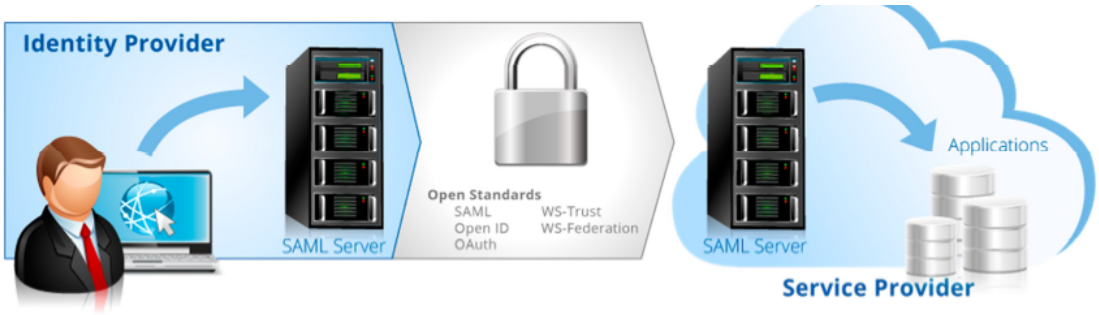


Figura 2.22: Processo de autenticação federado.
[70]

No ambiente de nuvem, muitas vezes há vários aplicativos e serviços da *Web* projetados para ajudar os usuários, requerendo autenticação. Em alguns casos, pode ser conveniente e seguro usar uma infraestrutura de SSO centralizada vinculado à autoridade central de autenticação. O SSO na *Web* fornece infraestrutura de SSO para aplicações *web*. No entanto, o SSO da *Web* provou ser um mecanismo muito

frágil para o gerenciamento de acesso. *Web* SSO pode ser usado para autenticação de usuários para sistemas genéricos, mas para aplicativos de negócios, um SSO federado é altamente recomendado [70].

Uma das funções básicas oferecidas por essas soluções de federação de identidades é a autenticação única (*Single Sign-On* (SSO)) [99]. Esta autenticação traz facilidades para os usuários, pois permite que esses passem pelo processo de autenticação uma única vez e usufruam das credenciais obtidas por todos os serviços que desejarem acessar. Garantir tal conceito dentro de um único domínio administrativo e de segurança não é algo complexo, porém garantir o SSO em uma federação com diferentes tecnologias de segurança é algo desafiador [100].

Os autores evidenciaram que o SSO é um sistema de acesso único onde o usuário se autentica apenas uma vez para acessar diversas aplicações em um domínio ou entre vários domínios confiáveis entre si. A Federação permite acesso confiável aos domínios relacionados e o gerenciamento de identidade federadas define políticas e processos para a gestão de identidade e acessos em uma federação. Nesse contexto, o SSO federado provê acesso em um ambiente de federação, por meio de protocolos específicos, à aplicações em domínios diferentes e confiáveis.

# Capítulo 3

# Estabelecimento do contexto da gestão de riscos

A avaliação de riscos para o SDD, considerando a GIA no ambiente de computação em nuvem, seguirá os preceitos da Norma ISO 31.000 [26] e o modelo de Gestão de Riscos do TCU [46] que é baseado na Norma ISO 31.010 [27], no COSO [28] e no *Orange Book* [55]. Além disso, seguirá o estabelecido pela portaria nº 1.001-SEI, de 30 de junho de 2017 [31] sobre a Política de Gestão de Riscos do Ministério da Indústria, Comércio Exterior e Serviços (MDIC) que define conceitos, princípios, diretrizes e a estrutura de gestão de risco.

O estabelecimento do contexto define os parâmetros básicos para a avaliação de riscos e define o escopo e os critérios para o restante do processo. O estabelecimento do contexto inclui considerar os parâmetros internos e externos relevantes para a organização como um todo, bem como o conhecimento dos riscos específicos a serem avaliados.

## 3.1 Contexto Externo

O contexto externo é o ambiente externo no qual a organização busca atingir seus objetivos, podendo incluir o ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, seja internacional, nacional, regional ou local; os fatores–chave e as tendências que tenham impacto sobre os objetivos da organização; e as relações com partes interessadas externas e suas percepções e valores.

Para o ME e qualquer organização, entender esse contexto externo é de fundamental importância para assegurar que os objetivos e as preocupações das partes interessadas externas sejam considerados no desenvolvimento dos critérios de risco. O contexto externo para o ME é baseado principalmente em requisitos legais e regulatórios e as percepções das partes interessadas.

O contexto externo do ME envolve seus clientes, ou seja, a sociedade, fornecedores e provedores de serviços, o Estado, o ambiente político e econômico e todas as organizações públicas e privadas, nacionais ou estrangeiras, que consomem serviços do Ministério. Além disso, no âmbito de requisitos legais e regulatórios e no espaço do contexto estabelecido, temos a Norma Complementar NC14/IN01/DSIC/GSIPR [13] do Gabinete de Segurança Institucional (GSIC) da Presidência da República que regulamenta a utilização da Computação em Nuvem no âmbito do Governo Federal e o Acordão nº 1.739/15 [45] do Tribunal de Contas da União que versa sobre a contratação e riscos de utilização dos serviços de Computação em Nuvem.

Dessa forma, considerando o escopo da Computação em Nuvem para a Gestão de Identidades e Acessos aplicada ao Sistema Decom Digital para o ME, o contexto externo é constituído por:

(a) Requisitos legais e regulatórios e normativos do Governo Federal que tratam desse escopo. A NC14/IN01/DSIC/GSIPR de 19 de março de 2018 [13], o Acordão 1.739/15 do TCU [45] e a Lei Geral de Proteção aos Dados [21];

(b) A sociedade brasileira, pois o cidadão é um dos principais clientes do MDIC e usuários do Sistema Decom Digital;

(c) Os organismos nacionais e internacionais e as empresas nacionais e estrangeiras que prestam informações de defesas comerciais importantes a partir do Sistema Decom Digital;

(d) Os provedores de serviços de Computação em Nuvem (CSP – *Cloud Services Providers*) que podem fornecer os serviços para o Governo Federal;

(e) Os organismos políticos, sociais, culturais e financeiros nacionais e estrangeiros que poderão usufruir de serviços de qualidade e confiáveis e em conformidade com a legislação;

(f) Normas relacionadas ao processo de Gestão de Riscos como a ISO 31.000 [26] e a ISO 31.010 [27];

(g) Normas de Segurança como as da família ISO 27.000;

(h) Normas de exportação e importação do país;

(i) Ambiente político e econômico do país

No contexto externo é preciso destacar a política de Governo Digital do Governo que tem como alguns dos objetivos a ampliação dos serviços digitais e a implantação da

Estratégia de Governança Digital, que deve ser seguida pelo ME e se traduz na maior oferta de serviços digitais e destacar também a Lei Geral de Proteção aos Dados (LGPD) que estabelece que o Governo proteja os dados pessoais sob sua custódia por meio de algumas medidas, dentre elas a implantação de controles efetivos de segurança, que serão auditados a partir do ano de 2020.

## 3.2 Contexto Interno

O Ministério da Economia (ME) no âmbito do Ministério da Indústria, Comércio Exterior e Serviços (MDIC), um dos Ministérios que o compuseram depois da reestruturação ministerial promovida pelo atual governo, dispõe de uma área de TI organizada por meio de uma Coordenação-Geral de TI (CGTI) e as seguintes coordenações subsidiárias: Coordenação de Serviços de TI (COSTI), Coordenação de Sistemas (COSIS) e Coordenação de Governança (COGTI). A CGTI está ligada à Subsecretaria de Planejamento Orçamento e Administração (SPOA) que por sua vez está ligada à Secretaria Executiva (SE) que responde ao gabinete do Ministro. O organograma da CGTI é apresentado na figura a seguir:

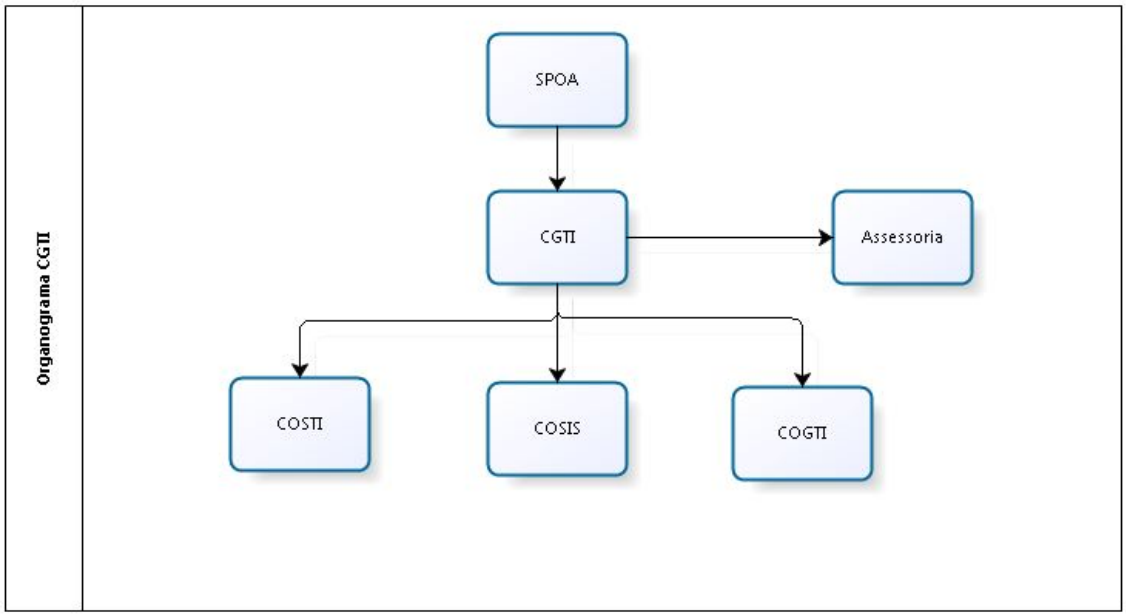


Figura 3.1: Organograma da CGTI.
[17]

O processo de migração do Sistema Decom Digital para a "nuvem" é de competência da COSTI. A COSTI desenvolve atividades de sustentação do ambiente de TI, divididas em áreas de conhecimento, tais como: Redes e Comunicações de Dados, Bancos de Dados e

Segurança da Informação. A COSTI também é responsável pelo atendimento dos serviços de TI em geral e está em busca de um nível de maturidade maior ao desenvolver políticas, processos e atividades alinhados ao Planejamento Estratégico Institucional do MDIC e ao PDTIC do MDIC para o triênio 2017-2019 [101], implantar a Governança de TI alinhado ao *framework* COBIT, e no caso do gerenciamento de serviços de TI procura alinhamento ao *framework* do ITIL [102] que é o mais aceito como boa prática no mercado de TI. Os planos e ações devem seguir a política de Gestão de Riscos do Ministério, adotada por meio da Portaria nº 1.001, de 30 de junho de 2017 [31] que estabelece diretrizes para gestão de riscos dos planos e projetos táticos e estratégicos do órgão.

A COSTI e a CGTI têm um histórico de poucos processos desenvolvidos ou revisados, o que implica em ações e atividades a serem executadas de forma desestruturada e sem métricas e controle. Além disso, os processos de contratação e execução dos serviços de TI estão mais alinhados aos normativos e requisitos legais. A CGTI está em busca de melhoria na padronização dos requisitos, métricas para gerenciar a área de TI e a qualidade dos serviços prestados pelos fornecedores. Os processos e a prestação dos serviços contam com requisitos mínimos de sustentabilidade no planejamento da contratação, o que implica na existência da gestão do conhecimento de TI no órgão, continuidade de ações entre contratações, processos perenes, metodologias e padrões.

Nesse cenário, a CGTI e junto com a COSTI implantou um Comitê de Segurança, o Comitê de Segurança da Informação e Comunicações (CSIC) que implantou a Política de Segurança da Informação e Comunicações (POSIC) [103] do MDIC contendo algumas Normas Complementares do Departamento de Segurança da Informação e Comunicações (DSIC) do Governo Federal, o SGSI (Sistema de Gestão de Segurança da Informação). A CGTI institucionalizou também uma área de Governança e junto com a COSTI implantou processos de gerenciamento de serviços baseados no framework ITIL (*Infrastructure Technology Information Library*) [102], como o Gerenciamento de Incidentes, Problemas, Cumprimento de Requisições, Gerenciamento de Mudanças para avaliar e aprovar mudanças e permitir que mudanças benéficas sejam feitas com o mínimo de interrupção dos serviços de TI, Gerenciamento de Demandas para levantar as demandas do negócio relativas a TI de maior complexidade e subsidiar processos como o Gerenciamento de Portfólio e Gerenciamento de Capacidade e por fim o Gerenciamento da Melhoria Contínua que consiste em analisar e melhorar continuamente os processos, e a função da Central de Serviços de TI. Desses processos do ITIL, apenas estão maduros os de Incidentes, que consiste em reestabelecer a operação normal do serviço o mais rápido possível e Mudanças e Requisições, além da função da Central de Serviços que consiste em um único ponto de contato para atender aos chamados dos usuários e clientes, os demais processos necessitam de aperfeiçoamento e institucionalização.

As ações de Segurança da Informação do MDIC estão alinhadas ao Planejamento Estratégico do Ministério por meio do Plano Diretor de Tecnologia da Informação e Comunicações (PDTIC) 2017-2019 [103], para o triênio de 2017 a 2019. O MDIC não conta com uma área de Segurança da Informação e Comunicações (SIC) o que dificulta a execução de ações necessárias para o estabelecimento das diretrizes das políticas internas e externas. Para a sustentação da TI a CGTI/COSTI celebrou um novo contrato para atender plenamente aos requisitos e níveis de serviço do MDIC, melhorar o atendimento aos usuários e clientes internos e externos, implantar o gerenciamento de Serviços de TIC no Ministério e elevar a maturidade de TIC. O Ministério com o novo contrato celebrado a pouco mais de um ano conta com especialistas em Segurança da Informação, redes locais e de longa distância, gerenciamento de serviços, banco de dados transacionais e analíticos, ativos de rede e em projetos de TI.

As funções e responsabilidades para a contratação dos serviços de TIC são da CGTI, da área de contratos do órgão Coordenação de Contratos e Convênios (CCONV) e da área de licitações Coordenação de Processos Licitatórios (COPLI), essas duas últimas ligadas a outra Coordenação Geral, e todas essas áreas subordinadas a Subsecretaria de Planejamento Orçamento e Administração (SPOA). A responsabilidade de elaborar o Planejamento da Contratação e Análises e Tratamento de Riscos de Segurança é da CGTI. A reponsabilidade sobre o processo licitatório é da COPLI e pela celebração do contrato é da CCONV. Todas essas áreas devem trabalhar em conjunto para que o processo tenha sucesso e atenda aos requisitos internos e externos.

Já as funções e reponsabilidade para a gestão da segurança das contratações de TIC são da CGTI que nomeia o gestor e fiscal técnico do contrato, e do CGD (Comitê de Governança Digital) que nomeia o Gestor de Segurança da Informação e Comunicações do Ministério, com funções de validar a execução as ações de segurança institucionais.

A COSTI é responsável pelas ações que direcionam a contração de um provedor de serviços de nuvem e também pela gestão dos riscos que envolvem essa contratação e a hospedagem de ativos críticos na nuvem.

Para o MDIC contratar um serviço que atenda aos requisitos e as expectativas das partes interessadas é preciso ter um orçamento para tal fim, para lançar um processo de contratação que identifique previamente riscos na fase de execução contratual, avalie e trate esses riscos, além de atender aos requisitos internos de gestão de riscos após a institucionalização dessa prática por meio da Portaria nº 1.001, de 30 de junho de 2017 [31], e dos requisitos legais e regulatórios, como a Norma Complementar nº 14 [13] do DSIC, que trata também da gestão de riscos em computação em nuvem, e dos níveis e qualidade de serviços exigidos pelo Ministério.

O quadro de pessoal da CGTI também é reduzido, por isso é preciso nomear uma

equipe que fique dedicada ao processo. O MDIC institucionalizou o plano de Teletrabalho, onde os servidores trabalham remotamente, o que também impulsiona o uso de tecnologias de computação em nuvem. O parque tecnológico do MDIC é bem heterogêneo, com redes locais e delonga distância, banco de dados *Oracle* e *SQL Server*, linguagens *PHP* e *Java*, servidores de aplicação e *web*, *firewalls CheckPoint*, roteadores *Cisco*, *switches Cisco* e *Enterasys*, sistemas operacionais *Windows* e *Linux*, dentre outras tecnologias.

Os valores do Ministério estão voltados para a qualidade de atendimento ao cidadão e de seus clientes, enquanto a sua cultura está voltada para a melhoria contínua dos processos, planos e atividades e das entregas ao cidadão e clientes internos e externos. O uso da tecnologia é de fundamental importância para a inovação, agregação de valor ao negócio e melhor atuação do Ministério que precisa seguir as políticas de governança digital e os normativos de segurança e tecnologia na prestação de serviços. Por isso, a cultura também está voltada para a inovação tecnológica com projetos como o de dados abertos, uso de serviços em nuvem, análise e inferência de dados para gerar informações relevantes, big data e adoção de processos digitais. Ainda é preciso melhorara a interface entre as áreas, inclusive da TI com as áreas de negócio, a implantação, transformação maturidade e gestão dos processos e a institucionalização das diretrizes do nível estratégico para toda a organização.

### 3.2.1 Análise Documental

A análise documental considerou documentos importantes no âmbito interno e externo ao órgão. No âmbito interno considerou o PDTIC (2017-2019) [101], o Planejamento Estratégico Institucional e o Mapa Estratégico do órgão [104], a Política de Segurança da Informação e Comunicações (POSIC) [103] do órgão e suas Normas Complementares (NC) [13], a política de gestão de riscos do Ministério [31] e as documentações técnicas do SDD e do PEAD (Anexo I). No âmbito externo considerou normas e publicações como as normas ISO 31.000 [26] e 31.010 [27], ISO 27.005 [30], o Manual de Gestão de Riscos do TCU, a Metodologia de gestão de Riscos do TCU, as Instruções Normativas, as Normas Complementares do Departamento de Segurança da Informação e Comunicações (DSIC) da Presidência da República e a recente Lei Geral de Proteção aos Dados (LGPD) [21].

### 3.2.2 Sigilo e confidencialidade do SDD

O sigilo e confidencialidade que as informações e dados armazenados no SDD são oriundos de sua natureza. Trata-se de informações de processos comerciais das empresas que não devem ser acessadas por outras empresas, pessoas ou organizações.

O SDD é um sistema de formação de autos digitais que permite o envio eletrônico de documentos no âmbito de processos de defesa comercial, bem como a visualização desses documentos a qualquer momento. Esse sistema está programado para receber petições relativas aos procedimentos previstos no Decreto nº 8.058 [105], inclusive aqueles de avaliação de escopo e de nova determinação. O sistema abrange as fases de petição e de processo. Em linhas gerais, a dinâmica do SDD se dá por meio dos usuários externos submetendo documentos e elementos de prova por meio do referido sistema e com investigadores analisando esse material, solicitando mais informações, caso seja necessário, e disponibilizando seus pareceres e determinações [106].


Figura 3.2: Tela de Acesso ao Sistema Decom Digital.
[106]

O SDD dispõe de um sistema de autenticação simples, com uso de senha, e uso de certificados digitais para envio de arquivos. Porém não conta com fatores de autenticação adicionais e nem soluções de gestão de identidade e acessos, o que evidencia a necessidade de fortalecimento da segurança nessa área a fim de evitar fraudes digitais e vazamento de informações, uma das grandes preocupações em ambientes de computação onipresente caracterizada por perfis de acesso dinâmicos.

### 3.2.3 Programa Eletrônico de Acesso Digital (PEAD)

O PEAD é um sistema de Single *Sign-on* que foi desenvolvido para elevar a segurança dos sistemas do MDIC, sobretudo o SDD, porém o mesmo não entrou em produção em

razão da descontinuidade do serviço pela empresa que o concebeu. O PEAD traria para o SDD os aspectos de autenticação mais forte, autorização e auditoria, itens fundamentais na gestão de identidade e acessos.

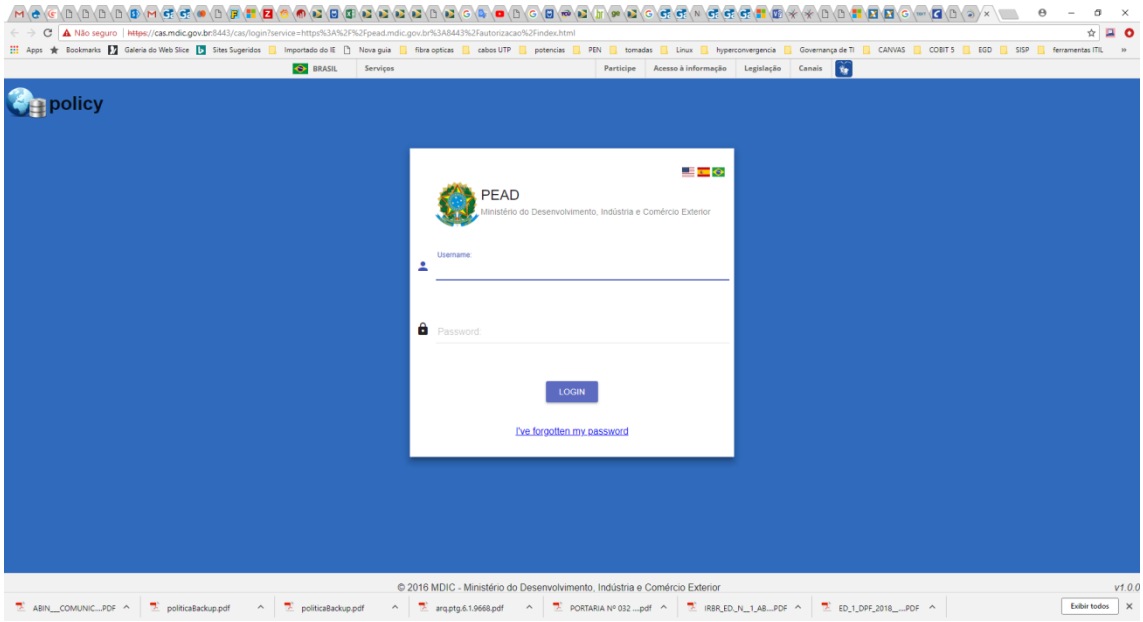


Figura 3.3: Tela de Acesso ao PEAD.
[17]

A figura acima demonstra a tela de aceso ao PEAD, porém como sofreu descontinuidade não poderá ser aproveitado pelo órgão como solução de acesso único aos sistemas.

## 3.3 Conclusões do capítulo

O capítulo demonstrou que o ME tem uma forte dependência de fatores externos como a legislação e dos cidadãos. No contexto interno demonstrou-se que o órgão possui forças como a estrutura da área de TIC, políticas e comitês implantados e atuantes, porém identificou-se como fraquezas a existência de sistemas que tratam informações sigilosas, como o SDD, e que carecem de ações para gerir os riscos representados por explorações de vulnerabilidades tecnológicas. Com o estabelecimento do contexto interno e externo, os riscos do SDD poderão ser identificados, analisados, avaliados e tratados, o que será abordado nos próximos capítulos.

# Capítulo 4

# Avaliação dos riscos considerando a Gestão de Identidade e Acessos para o SDD no ambiente de computação em nuvem

A norma ISO 31010 [27] versa sobre a gestão de risco, em especial com relação às ferramentas e técnicas que podem ser apropriadas em diferentes contextos. O processo de avaliação de riscos possibilita um entendimento dos riscos, suas causas, consequências e probabilidades. Isso proporciona uma entrada para decisões sobre a realização de uma atividade; maximização de oportunidades; se os riscos necessitam ser tratados; a escolha entre opções de riscos; a priorização de opções de tratamento de riscos; a seleção mais apropriada de estratégias de tratamento de riscos que trará riscos adversos a um nível tolerável. Dessa forma, este trabalho realizará o processo de Avaliação de Riscos no contexto da Gestão de Identidade e Acessos para hospedar o Sistema Decom Digital no ambiente de Computação em Nuvem.

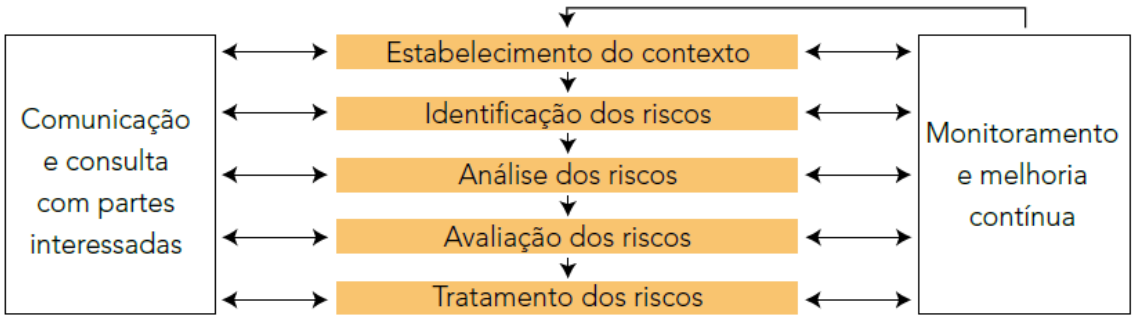


Figura 4.1: Processo de Gestão de Riscos.
[26]

A avaliação dos riscos é baseada no estabelecimento do contexto produzido no capítulo anterior do trabalho e no Modelo de Gestão de Riscos do Tribunal de Contas da União, nos documentos de Manual de Gestão de Riscos [46] e Avaliação de Maturidade da Gestão de Riscos [44] deste órgão. Esse modelo é baseado no COSO ERM [28], ISO 31.000 [26] e no Orange Book [55] que são modelos e frameworks de referência a nível mundial em Gestão de Riscos organizacionais.

A primeira iniciativa para avaliar riscos institucionais no Governo Federal surgiu no então Ministério do Planejamento, Orçamento e Gestão que produziu o Guia de Orientação para o Gerenciamento de Riscos, para apoiar o Modelo de Excelência do Sistema de Gestão Pública (GESPÚBLICA) e prover uma introdução ao tema gerenciamento de riscos [51].

O Tribunal de Contas de União (TCU), Controladoria Geral da União (CGU) e outros órgãos dos três poderes, estabeleceram gradualmente as práticas de Gestão de Riscos na Administração Pública. O Tribunal de Contas de União (TCU) começou, em 2012, a mapear a situação da gestão de riscos de entidades da administração indireta. Em 2017, essa avaliação abrangeu todas as entidades do setor público no âmbito do Índice Geral de Governança do Setor Público (IGG), incluindo-se aí o TCU. Na esfera federal o processo de gestão de riscos passou a ser obrigatório desde 2017. Nesse ano o TCU intensificou esforços no contexto da Gestão de Riscos e em 2018 lançou o Manual de Gestão de Riscos do TCU [46] e a segunda versão do documento "Gestão de Riscos - Avaliação de Maturidade" [44].

Em 2016, foi expedida a Instrução Normativa Conjunta nº 01 [107], com participação do Ministério do Planejamento, Desenvolvimento e Gestão (MPDG), e a então Controladoria Geral da União (CGU), que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. O MPDG lançou, em 2017, o Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão. O Decreto nº 9.203,

de 22 de novembro de 2017 [108], dispõe sobre a política de governança da administração pública federal, que trata, entre outros temas, da gestão de riscos na administração pública.

O objeto da avaliação dos riscos deste trabalho é de classificar e priorizar os riscos e apontar os que mais precisam de tratamento considerando o contexto da Gestão de Identidade e Acesso para o Sistema Decom Digital no ambiente de Computação em Nuvem. O processo de avaliação de riscos possui as etapas de identificação dos riscos, análise dos riscos e avaliação dos riscos.

## 4.1 Identificação dos Riscos para o uso de ativos em computação em nuvem

Identificação de riscos é o processo de busca, reconhecimento e descrição de riscos, tendo como base o contexto estabelecido e apoiado na comunicação e consulta com as partes interessadas, internas e externas [26].

O objetivo é produzir uma lista abrangente de riscos, incluindo causas, fontes e eventos, que possam ter um impacto na realização dos objetivos identificados na etapa de estabelecimento do contexto.

Em uma etapa preliminar, pode-se adotar uma abordagem do tipo "*top-down*" para a identificação de riscos, indo do mais geral para o mais específico. Primeiro, identificam-se riscos em um nível geral ou superior, como ponto de partida para estabelecer prioridades para, em um segundo momento, identificarem-se e analisarem-se riscos em nível específico e ou mais detalhado. A identificação de riscos pode se basear em dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, necessidades das partes interessadas. Convém que pessoas com conhecimento adequado sejam envolvidas na identificação de riscos e que a organização utilize ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos, às suas capacidades e aos riscos enfrentados. Envolver a equipe diretamente responsável pela execução do processo, do projeto ou da atividade que está tendo os riscos identificados, também ajuda a criar a responsabilidade em relação ao processo de gestão de riscos e o comprometimento em relação ao tratamento dos riscos [44].

A documentação dessa etapa de identificação dos riscos geralmente inclui pelo menos:

(a) o escopo do processo, projeto ou atividade coberto pela identificação;

(b) os participantes do processo de identificação;

(c) a abordagem ou o método utilizado para identificação dos riscos e as fontes de informação consultadas;

(d) o registro dos riscos identificados em sistema, planilha ou matriz de avaliação de riscos, descrevendo os componentes de cada risco separadamente com, pelo menos, suas causas, o evento e as consequências.

Para este trabalho consideramos a seguinte documentação para a etapa de identificação dos riscos:

Tabela 4.1: Documentação do processo de identificação dos riscos. Elaboração própria.

| | |
|---|---|
| **Escopo** | Hospedar o SDD em ambiente de nuvem. |
| **Responsável** | Gestor de SIC do órgão, opinião de especialistas. |
| **Método** | Modelo de Gestão de Riscos do TCU que se baseia na ISO 31.000, 31.010, 27005, Orange Book e no COSO. |
| **Premissas** | a) Informações Sigilosas;<br>b) Acessos em ambiente não controlado pelo órgão;<br>c) Computação pervasiva ou ubíqua. |

A partir da coleta de opiniões em relação ao ativo objeto de estudo, de especialistas do órgão em computação e segurança da informação e de colaboradores da Diretoria de Defesa Comercial (DECOM) responsáveis pelo SDD foram identificadas possíveis ameaças, controles, vulnerabilidades e impactos. As seguintes etapas foram consideradas para o processo de identificação de riscos:

(a) Identificar ativos;

(b) Identificar ameaças;

(c) Identificar controles existentes;

(d) Identificar vulnerabilidades;

(e) Identificar as consequências.

A tabela abaixo identifica o ativo alvo do estudo, suas vulnerabilidades ou pontos fracos que podem ser explorados por ameaças do mundo digital, as principais ameaças que exploram esses tipos de vulnerabilidades, o risco que pode se materializar e o risco específico ou mais granular e os tipos de controles existentes atualmente para este ativo.

Tabela 4.2: Identificação de Riscos e Controles. Elaboração própria.

| **Ativo** | **Vulnerabilidade** | **Ameaças** | **Risco** | **Risco específico** | **Controles existentes** |
|---|---|---|---|---|---|
| SDD na nuvem | Autenticação simples e fraca | Ataques de personificação | Acessos indevidos | Vazamento de Informações | Senha |
| | Privilégios indevidos | Ataques de personificação | Privilégios excessivos | Perda de Informações e Aplicações Alteração de Informações | Controle de acesso simples |
| | Perímetro de rede desprotegido | Ataques digitais diversos | Invasões de perímetro | Indisponibilidade de ativos | *Firewall* |
| | Ausência de controles de acesso físico | Ataques diversos | Acessos indevidos locais | Indisponibilidade de ativos | Sem controle de acesso |
| | Ausência de plano de continuidade e de alta disponibilidade | Evento que cause incidente na infraestrutura e/ou instalações | Indisponibilidade da aplicação | Perda de imagem e confiabilidade, interrupção dos serviços | Plano de continuidade e alta disponibilidade parcial |
| | Ausência de Auditoria de Acessos | - | Não detecção de eventos suspeitos | Maior tempo de exposição a ameaças | *Logs* de acesso |

Os riscos identificados na tabela acima a partir das vulnerabilidades e ameaças detectadas foram os seguintes: acessos indevidos, privilégios excessivos, invasões de perímetro, acessos locais indevidos, indisponibilidade da aplicação e a não detecção de eventos suspeitos.

As etapas para a identificação dos riscos foram construídas a partir da opinião do Gestor de SIC do Ministério e outros membros de TIC do órgão, além de membros do Comitê de Segurança da Informação e Comunicações (CSIC) e do Comitê de governança Digital (CGD) do órgão. Além disso, foram consideradas as opiniões de servidores do Departamento de Defesa Comercial – gestor do SDD – e técnicos da empresa terceirizada que mantém e construíram o sistema. Por fim, também foram analisados documentos técnicos e de arquitetura do sistema (Anexo I) e a pesquisa bibliográfica sobre o tema.

Com os principais riscos identificados a próxima etapa do processo global de Avaliação dos Riscos pode ser iniciada. Essa próxima fase consiste na análise dos riscos que foram identificados.

## 4.2 Análise dos riscos considerando a GIA para o SDD na nuvem

A análise de riscos é o processo de compreender a natureza do risco e determinar o nível de risco, fornecendo a base para a avaliação e para as decisões sobre o tratamento de riscos [26].

O risco pode ser descrito como uma função da sua probabilidade relacionada as suas consequências, então, o nível do risco é expresso pela combinação da probabilidade de ocorrência do evento e de suas consequências, em relação a relevância do impacto nos objetivos organizacionais. A equação que melhor define o risco é a seguinte:

$$Risco = função(Probabilidade\ e\ Impacto) \tag{4.1}$$

A probabilidade é a medida da frequência da qual um evento pode ocorrer, que depende da existência de uma fonte potencial para o evento (ameaça), e a medida em que um tipo particular de evento pode afetar seu alvo (vulnerabilidade), levando em consideração os controles ou contramedidas que a organização criou para reduzir sua vulnerabilidade [43]. O impacto mede o potencial comprometimento de um objetivo ou resultado organizacional.

Então, para avaliar os riscos, primeiro é preciso definir uma escala de probabilidade e impacto. A escala de probabilidades e impactos utilizada neste trabalho está demonstrada na tabela abaixo:

Tabela 4.3: Escala de probabilidades e impactos. Elaboração própria.

| **Probabilidade/ Impacto** | **Descrição Probabilidade/Impacto** | **Peso** |
|---|---|---|
| Muito Baixa | Improvável: ocorrência do risco em situações excepcionais/ Mínimo impacto nos objetivos | 1 |
| Baixa | Rara: ocorrência de forma casual ou inesperada/ Pequeno impacto nos objetivos | 2 |
| Média | Possível: ocorrência do risco possível, moderada/ Moderado impacto nos objetivos, porém recuperável. | 5 |
| Alta | Provável: ocorrência de forma esperada/ Relevante impacto nos objetivos, difícil recuperação. | 8 |
| Muito Alta | Praticamente certa: ocorrência do risco de forma inequívoca/ Catastrófico impacto nos objetivos, irreversível. | 10 |

A tabela acima demonstra que a probabilidade de ocorrência do risco vai de improvável, quando ocorre somente em situação excepcionais, até a praticamente certa, quando o risco ocorrerá de forma inequívoca. Quanto ao impacto, ele pode ser desde mínimo nos objetivos estratégicos, operacionais, de informação, comunicação, divulgação ou de conformidade, até o impacto relevante e catastrófico em relação a esses mesmos objetivos.

A partir da do grau de probabilidade e impacto podemos então calcular a função de risco que servirá para sua análise e posterior avaliação, indicando sua relevância para que o Ministério possa determinar possíveis formas de tratamento a partir do seu apetite ao risco, ou seja, o quanto esse risco é tolerável pelo órgão. Os resultados das combinações de probabilidade e impacto, classificados de acordo com a escala de níveis de risco, podem ser expressos em uma matriz, como a seguir:

Tabela 4.4: Matriz de Riscos. Elaborada pelo autor.

| | | | | | | |
|---|---|---|---|---|---|---|
| IMPACTO | Muito Alto<br>10 | 10<br>Risco Médio | 20<br>Risco Médio | 50<br>Risco Alto | 80<br>Risco Elevado | 80<br>Risco Elevado |
| | Alto<br>8 | 8<br>Risco Baixo | 16<br>Risco Médio | 40<br>Risco Alto | 64<br>Risco Alto | 80<br>Risco Elevado |
| | Médio<br>5 | 5<br>Risco Baixo | 10<br>Risco Médio | 25<br>Risco Médio | 40<br>Risco Alto | 50<br>Risco Alto |
| | Baixo<br>2 | 2<br>Risco Baixo | 4<br>Risco Baixo | 10<br>Risco Médio | 16<br>Risco Médio | 20<br>Risco Médio |
| | Muito Baixo<br>1 | 1<br>Risco Baixo | 2<br>Risco Baixo | 2<br>Risco Baixo | 8<br>Risco Baixo | 10<br>Risco Médio |
| | | Muito Baixa<br>1 | Baixa<br>2 | Média<br>5 | Alta<br>8 | Muito Alta<br>10 |
| | PROBABILIDADE | | | | | |

A partir de matriz de probabilidade e impacto pode-se medir o Nível de Risco Inerente (RNI) dos riscos identificados na seção anterior do trabalho que é o resultado do produto dos graus aferidos a partir de uma escala pré-definida da probabilidade pelo impacto aferidos:

Tabela 4.5: Registro de riscos com níveis de risco inerentes calculados. Elaborada pelo autor.

| Risco Identificado | Probabilidade | Impacto | Nível de Risco Inerente (NRI) |
|---|---|---|---|
| Acessos indevidos | MUITO ALTA<br>10 | MUITO ALTO<br>10 | **RE**<br>**100** |
| Privilégios excessivos | ALTA<br>8 | MUITO ALTO<br>10 | **RE**<br>**80** |
| Invasões de perímetro | MÉDIA<br>5 | ALTO<br>8 | **RA**<br>**40** |
| Indisponibilidade da aplicação | MEDIO<br>5 | MUITO ALTO<br>10 | **RA**<br>**50** |
| Não detecção de eventos suspeitos | MEDIA<br>5 | MÉDIO<br>5 | **RM**<br>**25** |
| Acessos indevidos locais | BAIXA<br>2 | ALTO<br>8 | **RM**<br>**16** |

Na tabela acima o NRI é o produto do nível de probabilidade e impacto identificado para determinado risco e de acordo com o resultado do produto pode ser classificado como um Risco Elevado (RE), Risco Alto (RA), Risco Médio (RM) ou um Risco Baixo (RB).

Para este trabalho definiu-se a seguinte escala: 1 < Risco < 10 (Baixo), 9,99 < Risco < 40 (Médio); 39,9 < Risco < 80 (Risco Alto) e 79,9 < Risco <= 100 (Risco Elevado).

Para analisar os riscos outro parâmetro importante é a definição dos controles que aplicam formas de resposta a risco. Essas respostas podem variar entre reduzir, evitar, compartilhar ou aceitar o risco.

A avaliação das respostas a riscos e atividades de controle correspondentes – ou simplesmente controles – é parte integrante da análise de riscos. Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações e medidas que a gestão adota com o objetivo de modificar o nível de risco [26].

As atividades de controle são as ações estabelecidas por meio de políticas e procedimentos, desempenhadas em todos os níveis da organização, em vários estágios dentro do processo organizacional e no ambiente tecnológico, que ajudam a garantir o cumprimento das diretrizes determinadas pela administração para mitigar os riscos a realização dos objetivos [109]. As atividades de controle também são geralmente referidas como controles internos.

Os controles podem ser medidos em níveis de confiança existentes em relação a esses controles quando aplicados a um determinado ativo, o que determina o risco de controle que é o grau de risco existente considerando a aplicação de um determinado controle ao risco.

Tabela 4.6: Níveis de controle. Elaborada pelo autor.

| **Riscos** | **Nível de Confiança (NC)** | **Avaliação dos Controles** | **Risco de Controle (RC)** |
|---|---|---|---|
| Acessos indevidos | Inexistente NC = 0% (0,0) | Controles inexistentes ou pouco eficientes para tratar o risco. | Muito Alto 1,0 |
| Privilégios excessivos | Fraco NC = 20% (0,2) | Controles e procedimentos ad hoc, aplicados caso a caso e dependem de ação e conhecimento dos envolvidos. | Alto 0,8 |
| Invasões de perímetro | Mediano NC = 40% (0,4) | Controles implementados mitigam parte do risco, mas não contemplam todos aspectos do risco, são mal desenhados e as ferramentas mal utilizadas. | Médio 0,6 |
| Indisponibilidade da aplicação | Satisfatório NC = 60% (0,6) | Controles sustentados por ferramentas adequadas que embora passíveis de melhorias mitigam o risco satisfatoriamente. | Baixo 0,4 |
| Não detecção de eventos suspeitos | Forte NC = 80% (0,8) | Controles implementados podem ser considerados a "melhor prática", mitigam todos os aspectos relevantes do risco. | Muito Baixo 0,2 |

Na tabela acima estão evidenciados os níveis de controle aplicados para cada tipo de risco que impacta o SDD. O Nível de Confiança (NC) representa os níveis de confiança do controle de cada risco identificado para o SDD na situação atual de do sistema. O Risco de Controle (RC) é o risco existente após a aplicação do controle ao SDD. Observa-se que o NC e o RC são inversamente proporcionais (RC = 1 – NC), se o nível de confiança do controle implementado é alto então o RC será baixo, pois quanto mais eficiente for o controle menor será o risco para o ativo.

Na tabela anteriormente apresentada, observa-se, que o controle mais bem avaliado apresentou um NC = 80% (0,8). Isso ocorre, pois os controles têm limitações e não conseguem ser totalmente eficazes, pois estão sujeitos a eventos como erros humanos, falhas de instalações ou tecnologias e eventos que possam mitigar a ação desses controles. O controle somente poderá fornecer uma segurança razoável, nunca absoluta, portanto, não se deve atribuir 100% de confiança a um controle.

Observa-se que o SDD atualmente somente tem controle de autenticação simples, os demais controles são inexistentes no sistema.

Após o cálculo do NRI e do RC pode-se calcular outro indicador importante para análise dos riscos que é o Nível de Risco Residual (NRR), obtido pelo produto do NRI pelo RC. O NRR é o nível de risco que permanece após a aplicação dos controles, por isso obtém-se a partir do produto do nível de risco do ativo em uma determinada situação identificada (NRI) com o Risco de Controle (RC) após aplicação de alguma forma de tratamento do risco. Então o NRR é o nível de risco após aplicações de controles para se chegar a uma situação desejada perante determinados riscos. A tabela abaixo demonstra o cálculo do NRR:

Tabela 4.7: Registro de riscos com níveis de riscos inerentes calculados. Elaborada pelo autor.

| Risco Identificado | Probabilidade | Impacto | Nível de Risco Inerente (NRI) | Eficácia do Controle | Risco de Controle (RC) | Nível de Risco Residual (NRR) |
|---|---|---|---|---|---|---|
| Acessos indevidos | MUITO ALTA 10 | MUITO ALTO 10 | **RE 100** | **Fraco** | **0,8** | **RE 80** |
| Privilégios excessivos | ALTA 8 | MUITO ALTO 10 | **RE 80** | **Mediano** | **0,6** | **RA 48** |
| Invasões de perímetro | MÉDIA 5 | ALTO 8 | **RA 40** | **Alto** | **0,4** | **RM 16** |
| Indisponibilidade da aplicação | MÉDIA 5 | MUITO ALTO 10 | **RA 50** | **Mediano** | **0,6** | **RM 30** |
| Não detecção de eventos suspeitos | MÉDIA 5 | MÉDIO 5 | **RM 25** | **Fraco** | **0,8** | **RM 20** |
| Acessos locais indevidos | BAIXA 2 | ALTO 8 | **RM 16** | **Fraco** | **0,8** | **RM 13** |

A probabilidade classificada como “MUITO ALTA” e “ALTA” para dois riscos identificados, justifica-se pela ausência de um sistema de Gerenciamento de Identidades e Acessos no SDD e o mecanismo de autenticação simples do sistema. A probabilidade “MÉDIA” é devido ao órgão contar com equipamentos de proteção de perímetro como os firewalls, planos parciais de continuidade e alta disponibilidade e da ausência de auditorias recorrentes para detectar eventos suspeitos e finalmente a probabilidade “BAIXA” deve-se ao órgão contar com sistemas de restrição de acesso físico e acesso controlado e monitorado por câmeras, sensores e dispositivos biométricos.

O NRR calculado foi maior para dois dos riscos, o que indica um NRI e um RC alto para esses riscos devido a controles fracos e níveis de confiança baixos. Nesses casos específicos o motivo é que o SDD não conta com camadas ou fatores adicionais de proteção contras esses riscos.

## 4.3 Avaliação dos riscos considerando a GIA para o SDD na nuvem

A finalidade da avaliação de riscos é auxiliar na tomada de decisões com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade

para a implementação do tratamento. Envolve comparar o nível de risco com os critérios de risco estabelecidos quando o contexto foi considerado, para determinar se o risco e ou sua magnitude é aceitável ou tolerável ou se algum tratamento é exigido [26].

Os riscos identificados são analisados com a finalidade de determinar a forma como serão administrados e, depois, serão associados aos objetivos que podem influenciar. Avaliam-se os riscos considerando seus efeitos inerentes e residuais, bem como sua probabilidade e seu impacto [109].

A etapa de avaliação de riscos, conforme destaca as afirmações acima, é importante para determinar as medidas adotadas perante aos riscos classificados na etapa de análise dos riscos. As organizações adotam essas medidas conforme o grau de exposição àqueles riscos e a capacidade de administrá-los.

Para a etapa de avaliação dos riscos, utiliza-se o nível de risco obtido na análise realizada na seção anterior deste trabalho para determinar se se um dos riscos identificados para o SDD precisa de tratamento e a prioridade que deve ser definida para este tratamento, se controles atuais devem ser modificados ou apenas mantidos e se novos controles devem ser considerados e implementados.

Uma boa prática para apoiar o processo de avaliação de riscos é estabelecer critérios para priorização e tratamento (apetite a risco, limite de exposição, nível recomendado de atenção, tempo de resposta requerido, comunicação, etc.) associados aos níveis de risco.

Para definição da prioridade e o tratamento do risco estabelecemos critérios como o apetite ao risco, limite de exposição ao risco, nível de atenção recomendado, tempo de reposta e comunicação à organização, esses critérios são relacionados aos níveis de riscos identificados após análise dos mesmos. O limite de exposição a riscos representa o nível de risco acima do qual é desejável o tratamento do risco [46]. Já o apetite ao risco é o nível de risco que uma organização está disposta a aceitar enquanto persegue seus objetivos [110]. Na tabela abaixo adaptada de [51] demonstra-se os os níveis de risco e critérios para classificação desses riscos.

Tabela 4.8: Critérios para priorização e tratamento dos riscos. Adaptado.

| **NÍVEL DE RISCO** | **CRITÉRIOS PARA PRIORIZAÇÃO E TRATAMENTO DE RISCOS** |
|---|---|
| Risco Elevado (RE) | Nível de riscos muito superior ao apetite de risco da organização. Os riscos desse nível devem ser comunicados à Governança e a Alta Adiminstração e requer uma resposta imediata. |
| Risco Alto (RA) | Nível de risco superior ao apetite de risco da organização. Riscos devem ser comnicados a Alta Administração e uma ação tomada em período determinado. |
| Risco Médio (RM) | Nível de risco dentro do apetite de risco da organização. Requer atividades de monitoramento e matença na manutenção de respostas e controles para manter o risco nesse nível ou reduzí-lo sem custos adicionais. |
| Risco Baixo (RB) | Nível de risco dentro do apetite de risco da organização, procura-se avaliar a relação custo benefício e diminuir o nível de controle. |

A ISO 31.010 [27] destaca diversos métodos para avaliação dos riscos e dentre esses métodos se destaca a utilização dos indices de risco como fortemente aplicáveis para o processo de avaliação dos riscos. Os índices de riscos são calculados com base no processo de Análise de Riscos.

As organizações podem usar os resultados da avaliação de risco para identificar implementações alternativas de controles de segurança selecionados (por exemplo, considerando vulnerabilidades inerentes a uma implementação de controle de segurança versus outra). Alguns produtos de tecnologia da informação, componentes do sistema ou configurações de arquitetura podem ser mais suscetíveis a certos tipos de fontes de ameaças; essas suscetibilidades são abordadas posteriormente durante o desenvolvimento e a implementação do controle de segurança. Além disso, a força dos mecanismos de segurança selecionados para implementação pode levar em consideração os dados de ameaças das avaliações de risco. Configurações individuais para produtos de tecnologia da informação e componentes do sistema podem eliminar vulnerabilidades identificadas durante a análise de eventos de ameaça. Os resultados da avaliação de risco também ajudam a informar decisões relacionadas a custos, benefícios e riscos na utilização de um tipo de tecnologia versus outra ou como controles de segurança são efetivamente implementados em ambientes operacionais específicos (por exemplo, quando controles de compensação devem ser usados devido à indisponibilidade de certas tecnologias). À medida que as avaliações de risco são atu-

alizadas e refinadas, as organizações usam os resultados para ajudar a determinar se as implementações de controle de segurança atuais permanecem eficazes, dadas as mudanças no espaço de ameaças [111].

Para classificar o risco utilizamos o cálculo do NRI (Nível de Risco Inerente) a partir da probabilidade e impactos determinados. Conforme a tabela de identificação dos níveis de riscos inerentes da etapa de Análise de Riscos descrita na seção anterior deste trabalho, temos:

Tabela 4.9: Classificação dos Riscos. Elaborada pelo autor.

| **ID** | **Risco Identificado** | **Probabilidade** | **Impacto** | **Nível de Risco Inerente (NRI)** |
|---|---|---|---|---|
| R1 | Acessos indevidos | MUITO ALTA 10 | MUITO ALTO 10 | 100 RE |
| R2 | Privilégios excessivos | ALTA 8 | MUITO ALTO 10 | 80 RE |
| R3 | Invasões de perímetro | MÉDIA 5 | ALTO 8 | 40 RA |
| R4 | Indisponibilidade da aplicação | MEDIO 5 | MUITO ALTO 10 | 50 RA |
| R5 | Não detecção de eventos suspeitos | MÉDIA 5 | MÉDIO 5 | 25 RM |
| R6 | Acessos indevidos locais | BAIXA 2 | ALTO 8 | 16 RM |

Os riscos com NRI entre 80 e 100 estão na faixa do nível de risco extremo que estão muito além do apetite de riscos da organização e requerem comunicação e ação imediata da alta administração e a implantação de mecanismos de controle. Os riscos com NRI entre 40 e 80 estão na faixa do nível de risco alto que estão muito além do apetite de riscos da organização e ação imediata da alta administração e a implantação de mecanismos de controle. Esses riscos estão na faixa de exposição inaceitável.

Os riscos com NRI entre 10 e 40 estão na faixa do nível de risco médio que estão dentro do apetite a riscos da organização e requerem atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais. Esses riscos estão na faixa de exposição inaceitável.

Os riscos na com NRI entre 0 e 10 estão na faixa do nível de risco baixo que estão dentro do apetite a risco da organização e em que se pode diminuir o nível de controle. Esses riscos estão na faixa de exposição aceitável.

Outro método de avaliação de riscos segundo [112] consiste em determinar o seu efeito potencial, ou seja, o grau de exposição da organização àquele risco. Esse grau leva em consideração pelo menos dois aspectos: a probabilidade de ocorrência e o seu impacto (em geral medido pelo impacto no desempenho econômico-financeiro do período), e o impacto "intangível" Na figura abaixo é demonstrado um gráfico da relação probabilidade e impacto onde temos uma área de exposição aceitável, outra com exposição inaceitável e uma faixa de alerta ente as duas anteriores.

O grau de exposição financeira é calculado simplesmente pelo valor aproximado do impacto financeiro multiplicado pela probabilidade de ocorrência do evento. Os riscos associados a estes eventos podem ser controlados para cada processo isoladamente. Incorpora-se ainda na abordagem o impacto intangível de cada um dos processos, tal como ilustrado nas figuras abaixo:

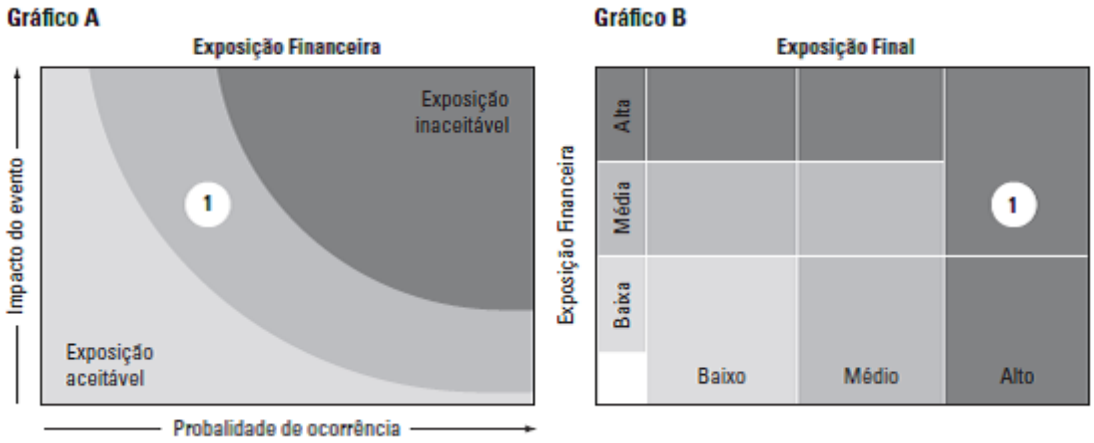


Figura 4.2: Mapa de avaliação de riscos.
[112]

O gráfico "A" demonstra eventos identificados e calculados a partir da probabilidade e do impacto do evento, no caso o "Evento 1" é de médio impacto e probabilidade. A faixa com tom mais escuro demonstra os riscos de exposição inaceitáveis e que necessitam de tratamento imediato. No gráfico "B" temos a Exposição Financeira calculada pela relação de probabilidade e impacto, resultado que advém do gráfico "A", e a Exposição Final (Exposição Financeira + Impacto Intangível) que é considerada alta para esse evento (1) devido ao impacto intangível ser alto.

## 4.4 Conclusões do capítulo

O capítulo demonstrou que a Avaliação de Riscos é realizada a partir do nível de riscos identificados na etapa de Análise de Riscos e definição de critérios de priorização e tratamento de acordo com esses níveis de risco. A partir da classificação dos riscos ou de uma matriz de riscos é possível determinar a forma de tratamento dos riscos.

De acordo com a avaliação, os riscos R1 "Acessos Indevidos" e R2 "Privilégios excessivos", foram avaliados como de Alta Relevância. Eles estão muito além do apetite de riscos do Ministério e precisam ser imediatamente comunicados e de uma atenção e ação imediata da alta administração da organização. É indispensável tratar e gerenciar esses riscos, pois a sua exposição é inaceitável. Conforme a avaliação de riscos realizada é recomendável para a organização, no caso o ME, um plano de tratamento de risco e a utilização de controles adequados para o risco de "Acessos Indevidos" em relação ao SDD em ambiente de nuvem.

# Capítulo 5

# Identificação das principais tecnologias de Gestão de Identidade e Acessos

Este capítulo trata das possíveis formas de tratamento dos riscos de "Acessos Indevidos" e de "Privilégios Excessivos" identificados no capítulo anterior para a situação atual do Sistema Decom Digital considerando um cenário do sistema em ambiente de nuvem. Enfatiza as principais tecnologias de Gestão de Identidade e Acessos e propõe uma solução de tratamento desses riscos.

## 5.1 Plano de tratamento do risco

O plano de tratamento para os riscos identificado de acessos indevidos e privilégios excessivos ao SDD em ambiente de nuvem, a partir de fraudes digitais e as suas consequências que são o vazamento e a perda de integridade das informações, consiste em adoção de tecnologias de Gestão de Identidades e Acessos, em particular a Autenticação por Comportamento ou Contexto.

Segundo [47], [110] as opções de tratamento dos riscos são as seguintes:

Tabela 5.1: Opções comuns de tratamento de riscos. Adaptado.

| **Opções de Tratamento de Riscos** | **Descrição** |
|---|---|
| Mitigar ou reduzir | Um risco normalmente é mitigado quando é classificado como "Alto" ou "Extremo". A implementação de controles, neste caso, apresenta um custo/benefício adequado, por exemplo, tomar ações para reduzir o tempo de indisponibilidade de um sistema crítico. |
| Compartilhar | Um risco normalmente é compartilhado quando é classificado como "Alto" ou "Extremo", mas a implementação de controles não apresenta um custo/benefício adequado. As técnicas comuns compreendem a aquisição de produtos de seguro ou a terceirização de uma atividade. |
| Evitar | Um risco normalmente é evitado quando é classificado como "Alto" ou "Extremo", e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco. Descontinuação das atividades que geram os riscos, por exemplo, uma organização decide se desfazer de uma unidade de negócios. |
| Aceitar | Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos. |

O plano para tratar o risco é baseado na criação de controles para identificar quem está solicitando o acesso. Esses controles são baseados em uma autenticação multifator que utilizará além dos meios mais comuns de autenticação, como o usuário e senha, as características comportamentais e de contexto de uso da conta que está tentado acessar o SDD. Essas características incluem a geolocalização da origem do acesso, *hardware*, sistemas operacionais e navegadores utilizados para o acesso.

A Gestão de Identidade e Acessos complementa a autenticação de fator único que suporta o Sistema Decom Digital, que funciona somente com senha. O sistema usa *token* somente para a funcionalidade de *upload* de arquivos. Com a adoção da GIA o sistema estará menos vulnerável às tentativas de fraudes e mais alinhado as políticas e tecnologias de detecção de fraudes digitais.

A análise de comportamento de entidades e usuários é de grande importância na prevenção de fraudes e acessos indevidos, pois propicia uma nova camada de proteção baseada no contexto e no perfil de acesso dos usuários. O ME pode mitigar essas vulnerabilidades ao adotar a tecnologia de GIA denominada de Autenticação por Comportamento ou Contexto, tornando mais seguro o acesso aos sistemas e às informações sigilosas de seus sistemas, como é o caso do Sistema Decom Digital, por meios da implementação dessas tecnologias na nuvem e on premises (tecnologias que funcionam no ambiente controlado da organização).

## 5.2 Identificar alternativas de tratamento do risco

Com o fenômeno da Transformação Digital, muitas mudanças começaram a acontecer nas organizações, que entraram em um processo de virtualização em busca da otimização de seu desempenho de mercado. Entre as mudanças que mais marcaram as empresas está a necessidade de garantir a segurança das identidades e acessos digitais para conquistar a confiança de clientes e colaboradores. Garantir a segurança dos ativos corporativos e pessoais, então, é uma postura estratégica essencial e que deve estar refletida na cultura da organização, garantindo que todos participem da construção e manutenção dessa proteção de dados. É possível adotar uma série de soluções para garantir a segurança das identidades digitais e acessos à rede, desde softwares até políticas a serem seguidas pelos usuários. Nas próximas seções serão apresentadas as tecnologias de GIA para tratar os riscos de acessosindevidos e privilégios excessivos.

### 5.2.1 Gerenciamento de Identidades e Acessos

Entre as possibilidades de proteção que as tecnologias oferecem está o IAM, sigla para *Identity and Access Management*, ou Gerenciamento de Identidades e Acessos (GIA). O IAM é uma função essencial para proteger a privacidade da informação, aprimorando a experiência do usuário, permitindo a responsabilização e controlando acessos aos ativos de uma organização. Gerenciamento de identidade refere-se às pessoas, processos e tecnologia necessários para gerenciar todo o ciclo de vida de identidades e perfis digitais. O gerenciamento de acesso, também conhecido como gerenciamento de permissões do usuário, refere-se aos processos e tecnologia utilizados para controlar o acesso a um ativo de informação específico fornecido por uma identidade específica. As permissões dos usuários são conjuntos de atributos que especificam os direitos de acesso e privilégios de uma identidade autenticada. Por exemplo, grupos de segurança e direitos de acesso são permissões [84].

O Gerenciamento de Identidade e Acessos é um *framework* desenvolvido para processos de negócios que garante maior controle para o registro e segurança de identidades digitais ou eletrônicas. O controle oferecido por essa estrutura permite a integração entre tecnologias e políticas de suporte aos acessos, principalmente de dados críticos. A proteção oferecida pelo IAM ocorre por meio de diferentes sistemas de autenticação utilizados em conjunto ou isoladamente: *logon* único, multifator, uma camada de proteção e gestão de acesso, somados a um processo de governança de dados, que não permite que eles sejam compartilhados a menos que recebam autorização. Para que este gerenciamento seja eficiente, ele deve ser supervisionado e controlado, motivo pelo qual seus serviços de diretório são centralizados.

### 5.2.2 Autenticação

Autenticação é o processo de verificação das credenciais de uma entidade que tenta acessar um recurso protegido. A autenticação deve ser feita de maneira segura, confiável e gerenciável. Para contas que exigem níveis mais altos de segurança, podem ser necessárias autenticações de múltiplos fatores. Sistemas de autenticação devem ter a capacidade de usar a definição de risco de transação comercial como orientação e fornecer autenticação adaptativa baseada no nível de risco da transação. A autenticação adaptativa é a que oferece controle baseado em características e comportamentos de um perfil dinâmico de acesso.

Autenticação é o processo de verificar a identidade ou outros atributos reivindicados por uma entidade ou verificar a origem dos dados apresentados. A entidade pode ser um usuário, processo ou dispositivo. A autenticação acontece toda vez que usamos nossos computadores. Grande parte da autenticação é transparente para o usuário e tratada por meio de processos de comunicação computacional sem que o usuário, mesmo perceba o que está acontecendo [84].

A autenticação, no âmbito da segurança digital, é o procedimento que confirma a legitimidade do usuário que realiza a requisição de um serviço, para o controle de acesso identificado. Este procedimento é baseado na apresentação de uma identidade junto com uma ou mais credenciais de confirmação e verificação.

Existem diversos tipos e fatores de autenticação, os tipos podem variar da autenticação simples que utiliza um único mecanismo de autenticação até a autenticação multifator que utiliza mais de um meio de autenticação: como algo que o usuário sabe combinado com algo que o usuário possui. Novos fatores de autenticação surgem a todo momento como forma de proporcionar maiores garantias de proteção aos dados.

#### 5.2.2.1 Autenticação de fator único

A abordagem de autenticação mais básica é a autenticação de fator único. A autenticação de fator único geralmente se baseia em uma senha estática e reutilizável (algo que o usuário sabe) em combinação com um ID de usuário. As senhas são um segredo compartilhado, conhecido pelo usuário e pelo sistema [84].

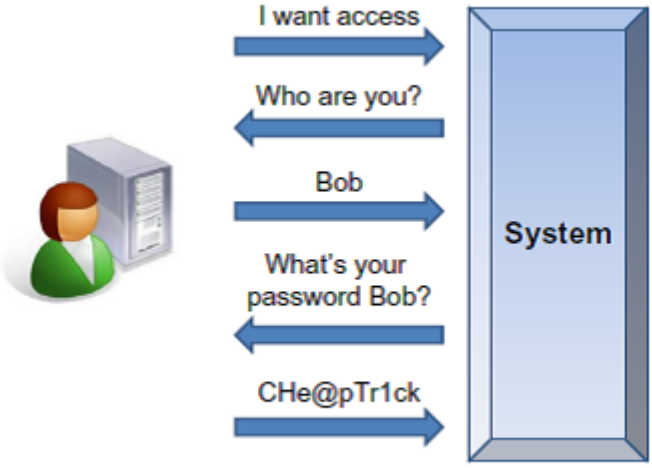


Figura 5.1: Autenticação de fator único.
[84]

A abordagem de autenticação mais básica é a autenticação de fator único. O fator único de autenticação geralmente se baseia em uma senha estática e reutilizável (algo que o usuário sabe) em combinação com um ID de usuário. As senhas são um segredo compartilhado, conhecido pelo usuário e pelo sistema. Nos primórdios da computação, muitos sistemas limitavam senhas a seis caracteres, e ainda existem algumas organizações que usam seis caracteres como o comprimento base da senha. No entanto, como as senhas podem ser facilmente adivinhadas, muitas organizações impõem padrões para implementá-las. No decorrer dos anos, a duração e a força das senhas mudaram consideravelmente, e muitas organizações agora exigem que as senhas contenham uma combinação letras e numerais, especificando o número mínimo de caracteres, exigindo senhas com caracteres especiais ou exigindo que sejam atualizadas regularmente. A maioria dos sistemas modernos tem a capacidade de impedir a reutilização de senhas e forçar os usuários a mudarem suas senhas com alguma frequência. O desafio é estabelecer um equilíbrio entre a capacidade de lembrar do usuário e a vontade de digitar com algum nível de frequência e segurança. O desafio de fazer senhas mais longas e mais complexas é que quanto mais longa e complexa a senha, maior a probabilidade de o usuário anotá-la [84].

Conforme destacado pelo autor no trecho acima, a autenticação de único fator, que é o caso de usuário e senha, é simples e apesar de ter se aperfeiçoado ao logo do tempo não

deixa de ser uma forma de autenticação fraca, pois o usuário precisa lembrar da senha a todo momento e muitas vezes anota a própria senha, além de poder ser descoberta por meio de ataques digitais, como a força bruta em que um algoritmo testa as combinações até identificar a senha e também a Engenharia Social, onde os fraudadores solicitam aos usuários suas credencias de acesso por meios que parecem legítimos.

A autenticação mais comum é a combinação de *login* e senha, ou seja, a que utiliza apenas um fator. A senha memorizada, contudo, tem sua fragilidade. Tanto a identificação (*login*) quanto a senha (este fator "algo que você sabe") podem ser revelados ou descobertos, permitindo a fraude de utilização ilegítima de identidade de uma pessoa por outra. Pode ainda ser esquecida, causando transtornos ao usuário, pois exigirão alguma forma de redefinição ou reposição de uma nova senha.

#### 5.2.2.2 Autenticação MultiFator (MFA)

A segurança da verificação em duas etapas baseia-se na sua abordagem em camadas. O comprometimento de vários fatores de autenticação apresenta um desafio significativo para os invasores. Mesmo que um invasor consiga descobrir a senha do usuário, ela será inútil se ele também não estiver de posse do método de autenticação adicional. Isso funciona exigindo dois ou mais métodos de autenticação. Os fatores de autenticação para humanos são normalmente classificados em três casos:

(a) Algo que o usuário sabe: senha, PIN (número de identificação pessoal), frase de segurança ou frase-passe, que normalmente deve ser apenas memorizada e não escrita, para garantir o segredo que torna o fator seguro;

(b) Algo que o usuário possui/tem: certificado digital A3 (*token* ou *smart card*), cartão de códigos numéricos, token de segurança (gerador eletrônico de senhas únicas temporais), *token* por *software*, códigos enviados por telefone celular (SMS) etc.;

(c) Algo que o usuário é: impressão digital, padrão de retina, sequência de DNA, padrão de voz, padrão de vasos sanguíneos, reconhecimento facial, reconhecimento de assinatura, sinais elétricos unicamente identificáveis produzidos por um corpo vivo, ou qualquer outro meio biométrico.

Na figura abaixo temos um gráfico que demonstra no eixo horizontal a força do fator ou da combinação de fatores de autenticação e no eixo vertical os tipos de autenticação: autenticação única, dupla ou de três fatores combinados. Percebemos que quanto mais fatores combinados, maior a força de autenticação.

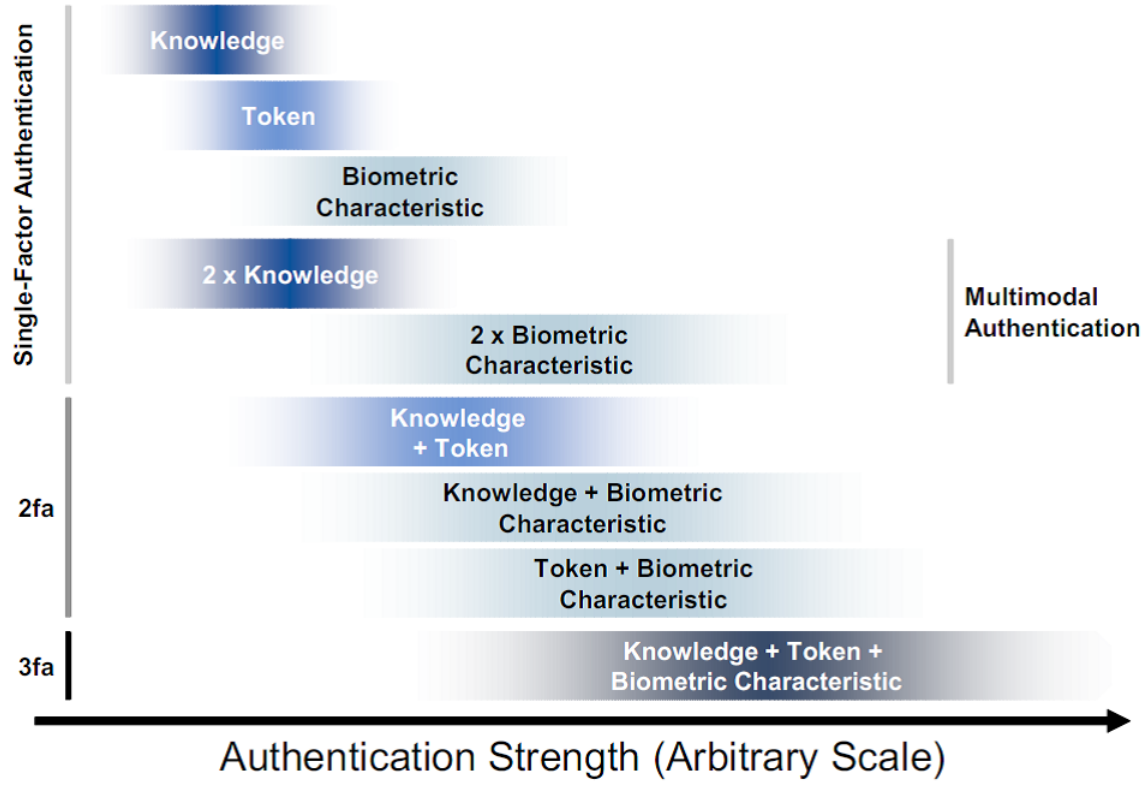


Figura 5.2: Força de Autenticação de diferentes combinações de atributos de autenticação. [113]

Abordagens de autenticação que dependem de mais de um fator são mais difíceis de comprometer do que as abordagens de fator único. As abordagens de autenticação de vários fatores combinam algo que um usuário conhece, algo que usuário é, ou de algo que um usuário possui. Por exemplo, uma transação de terminal bancário requer autenticação multifator: algo que o utilizador possui (isto é, o cartão) combinado com algo que o utilizador conhece (isto é, o seu número de identificação pessoal (PIN)). A autenticação multifatorial, também conhecida como autenticação forte, pode usar várias técnicas para verificar uma identidade [84].

#### 5.2.2.3 Autenticação biométrica

A biometria, como técnica de autenticação multifatorial, mede e analisa as características exclusivas do corpo humano de cada indivíduo com fins de autenticação [84].

Segundo [114] a autenticação pode ser biométrica utilizando impressão digital e outras características do corpo do indivíduo que o torna único, a biometria também pode ser

utilizada no aspecto comportamental que usa, por exemplo, as características de como o indivíduo usa o mouse ou digita no teclado.

(a) Autenticação biométrica física.

A biometria, como técnica de autenticação multifatorial, mede e analisa as características do corpo humano exclusivas de cada indivíduo fins de autenticação [84].

A autenticação biométrica física é estática por natureza e baseada nas características físicas de um indivíduo como a face, impressão digital, padrões de íris e retina. Esse tipo de autenticação é bastante precisa e difícil de ser comprometida, porém exige dispositivos com sensores, scanners e leitores das características físicas, softwares específicos para coleta, transporte e gerenciamento das credenciais e uma base de armazenamento das características físicas dos indivíduos.

(b) Autenticação biométrica comportamental.

Assim como geramos um traçado pessoal e distintivo quando escrevemos à mão, uma série de características únicas também pode ser detectada quando digitamos ou usamos o *mouse*. Essa característica é um traço biométrico conhecido como dinâmica de pressionamento de tecla ou de utilização do mouse e pode ser usado para fortalecer os processos de autenticação.

A biometria comportamental é a medição e registro de padrões comportamentais humanos para verificar e autenticar um usuário de computador individual seja em tempo real ou retrospectivamente. Em vez de se concentrar em o resultado de uma atividade, a biometria comportamental se importa como um usuário conduz a atividade especificada. Não verifica se o nome do usuário e a senha são inseridos corretamente, por exemplo, mas como um usuário acessa: ele está digitando rapidamente ou devagar, como ele altera entre janelas do sistema usando a tecla tab ou o mouse, como ele usa o mouse e o teclado.

#### 5.2.2.4 OTP (*Ontime Passsword*)

OTP são senhas de uso único em um sistema baseado em dispositivos de *hardware*. Os sistemas OTP criam senhas válidas para um uso único ou para uso dentro de um período de tempo específico. Para acessar recursos protegidos pela tecnologia OTP, os usuários combinam seu PIN (*Personal Identication Number*) ou senha secreta com um código de *token* gerado pelo sistema OTP - geralmente em uma exibição de dispositivo de hardware, como uma chave *SecurID* e às vezes através de um aplicativo em seu dispositivo. Um dispositivo *SecurID* usa um algoritmo proprietário para gerar códigos de acesso que mudam regularmente e que estão vinculados ao número de série do dispositivo. O método

de autenticação OTP é predominante em muitos ambientes de acesso. No entanto, por meio de uma avaliação de risco pode-se identificar que em razão dos sistemas de acesso remoto disponibilizarem acesso a sistemas corporativos através da Internet, pode ser uma oportunidade para indivíduos não autorizados detectarem e capturar senhas, o que torna o risco significativo [84].

Conforme destacado por [84] o OTP é o processo de autenticação baseado em senha única que é válida somente para uma sessão de *login* ou transação, em um sistema de computadores ou outros dispositivos digitais. OTPs evitam uma série de deficiências que estão associadas às autenticações tradicionais (estáticas), baseada em uma senha; uma série de implementações também incorporam autenticação de dois fatores, garantindo que a senha de uso requeira acesso a algo que uma pessoa tem (como um pequeno chaveiro OTP ou um telefone inteligente específico), bem como algo que a pessoa sabe (como um PIN).

A vantagem mais importante que é dada pelas OTPs é que, em contraste com as senhas estáticas, elas não são vulneráveis a ataques *replay*. Isso significa que um potencial intruso que consiga capturar uma OTP que já foi usada para fazer *login* em um serviço ou uma transação, não conseguirá utilizá-la, uma vez que ela não será mais válida. Uma segunda maior vantagem é que um usuário que usa a mesma senha (ou similar) para múltiplos sistemas, não fica vulnerável em todos eles, se a senha de um deles for conseguida pelo atacante.

Porém, os OTPs são enviados pela Internet aos dispositivos dos usuários e caso as senhas sejam capturadas por um atacante o acesso poderá ser feito por um usuário ilegítimo, esse tipo de ataque muitas vezes é chamado de ataque *man-in-the-middle* (homem do meio), pois intercepta as informações, quando estão sendo transmitidas, para uso não autorizado.

A tabela abaixo demonstra segundo [15] as vantagens e desvantagens de cada fator de autenticação:

Tabela 5.2: Fatores de autenticação: vantagens e desvantagens.

| **Senhas** | **Tokens** | **Biometria** |
|---|---|---|
| São fáceis de implementar e de baixo custo. | Pode exigir habilidade especial para interagir com o dispositivo leitor. Pode ser caro implementar. | Requer habilidade especial para interagir com o equipamento. Caro para implementar. |
| Precisa ser memorizado. | Precisa ser carregado com o usuário, tamanho do *token* é um fator a considerar. | Estão naturalmente presentes com o usuário. |
| São suscetíveis de adivinhar e serem comprometidos por terceiros. | Duplicado apenas pelo fabricante. | Usuário pode ser comprometido apenas quando vitimizado. Geralmente muito difícil de comprometer. |
| Usuário não tem consciência de um ativo comprometido por algum tempo, talvez até que o dano seja feito. | Usuário imediatamente ciente do comprometimento potencial ao perceber que o textittoken desapareceu. | Usuário imediatamente ciente de comprometimento. |
| Requer canais de comunicação seguros. | Geralmente destinado ao uso com um sistema ou dispositivo local, ainda vulnerável a ataques com o de textitreplay. | O mesmo que para textittokens. |
| Pode ser facilmente reutilizado por vários sistemas e aplicações. | Requerer dispositivos de entrada específicos e isso pode ser uma limitação para usuários móveis em todos sistemas. | Requerer dispositivos de entrada específicos. |
| Fornece precisão nas implementações. | Preciso, mas o dispositivo é propenso a desgaste e perda de informação. | São propensos a confusão e erro. |
| Uso por usuários em diversas localizações remotas. | Requerem dispositivos específicos de entrada, pode ser uma limitação para usuários em textitroaming. | O mesmo que para textittokens. |
| Pode ser compartilhado entre os usuários e sistemas. | Pode ser replicado pelo fabricante, mas geralmente não são compartilhados entre usuários. | Não pode ser compartilhado entre os usuários. |

A tabela compara três tipos de fatores de autenticação: o que você sabe (senha), o que você possui (*token*) e o que você é (biometria). As senhas são fáceis de implementar e de baixo custo, porém podem ser facilmente descobertas ou comprometidas e podes ser compartilhada facilmente. No caso dos *tokens*, são mais precisos e difíceis de comprometer, porém ainda vulneráveis a ataques de *replay* como o "homem do meio" que captura as informações quando estão sendo transmitidas. O *token* precisa ser carregado pelo usuário e sem ele não é possível autenticar. Quanto a biometria é o mais difícil de ser comprometido, porém necessita de dispositivos leitores do lado do acesso e são mais caros para implementar devido a utilização de dispositivos específicos.

### 5.2.3 Autenticação por Comportamento ou por Contexto

O emergente paradigma de computação móvel torna viável o acesso a recursos de qualquer lugar e em qualquer momento. Porém, ao mesmo tempo que esse acesso ubíquo proporciona os seus benefícios, ele cria desafios particulares para prover segurança às entidades participantes. Tais desafios não são tratados de forma apropriada por abordagens tradicionais de segurança [78].

Os mecanismos tradicionais de autenticação são ineficazes para satisfazer as necessidades de ambientes altamente dinâmicos como os ambientes móveis e pervasivos [79]. Ainda, segundo Babu and Venkataram [80], a eficácia da maioria dos mecanismos de autenticação para computação móvel depende da força dos identificadores utilizados para a autenticação dos usuários.

Segundo [78] a autenticação sensível ao contexto, que utiliza a mudança de contexto para permitir a adaptação dos mecanismos de segurança baseada na situação atual, é essencial para prover segurança de forma efetiva em ambientes pervasivos.

A autenticação por comportamento ou contexto utiliza uma espécie de identidade digital do indivíduo por meio da correlação de propriedades comportamentais ou características que formam um perfil desse indivíduo. A autenticação por contexto pode ser utilizada em conjunto com outras tecnologias de autenticação já que é uma camada ou nível adicional para o sistema de segurança. Esse tipo de tecnologia funciona como se fosse um "DNA" digital da pessoa. Esse perfil do usuário pode ser formado pela correlação de diversas características de comportamento, geolocalização e *hardware* utilizado pelo indivíduo que acessa determinado serviço ou sistema.

Como forma de complementar a autenticação por comportamento ou contexto alguns mecanismos de validação podem ser utilizados, como a Autenticação por Conhecimento, que pode validar ou não um acesso suspeito utilizando informações pessoais do indivíduo através do envio de confirmações por meio de plataformas como SMS (*Short Message Service*) ou ligações para dispositivos móveis.

A autenticação por contexto utiliza determinadas características e dados do ambiente em que o processo de autenticação ocorre, incluindo o dispositivo, a rede de conexão, o local, o intervalo de tempo e outros dados sobre o comportamento do usuário. Se ao longo de várias autenticações, o contexto permanecer constante ou estiver sujeito apenas a pequenas variações, a probabilidade de que o usuário autenticado seja o proprietário legítimo das credenciais é maior do que se ocorrer o oposto, ou seja, o contexto muda consideravelmente em diferentes processos de autenticação. A distância entre os contextos é determinada na fase de análise de contexto e fornece, como resultado, o nível de risco da autenticação. Basicamente, uma distância maior entre os contextos significa que há um risco maior de que uma tentativa seja feita para usar fraudulentamente a identidade do usuário legítimo.

A autenticação por contexto ou por comportamento tem muitas vantagens [115], incluindo a capacidade de ser continuamente verificada sem o conhecimento do usuário e funcionar sem hardware adicional. Como por exemplo, o uso de aplicativos (apps) [116], [117] e rastreamento de localização pode ser empregado para usuários com autenticação continua. A autenticação multifator, que requer dois ou mais fatores de autenticação, como senha, *token* ou característica do usuário solicitante, pode ser dificultada, pois o uso de alguns desses fatores, que envolvem *tokens* físicos ou estáticos, que são considerados apenas como um ponto de entrada e não realizam a autenticação continua, são suscetíveis a roubo ou perda, além de não considerar a prestação de autenticação contínua para toda a sessão de acesso.

A captura e análise dos fatores de contexto não afetam a experiência do usuário. Portanto, a redução do risco e a melhoria na segurança da autenticação são alcançadas de uma forma quase que totalmente transparente.

A análise por contexto pode ser usada em conjunto com outros fatores de autenticação, a autenticação multifator que adota outros fatores de autenticação além do fator que você conhece, ou seja, a senha do usuário. A autenticação por contexto é uma tecnologia que pode ser vista como uma camada adicional de segurança que fortalece o processo de autenticação e aprimora a proteção do sistema.

Além da análise individual de cada um dos fatores acima, uma análise cruzada pode ser realizada, correlacionando vários fatores e comparando-os com o histórico de atividade de autenticação do usuário. Essas correlações são combinações diferentes envolvendo o dispositivo de acesso, geolocalização, navegador, sistema operacional usado, endereços lógicos e intervalo de tempo, essas características criam o perfil de acesso comportamental do usuário. A figura abaixo mostra a arquitetura geral de um sistema de autenticação por contexto baseado em atributos de um dispositivo como: GPS (Sistema de Posicionamento Global), timezone, aplicações instaladas, processos e tarefas em execução, descrição e

versão do sistema operacional [118].

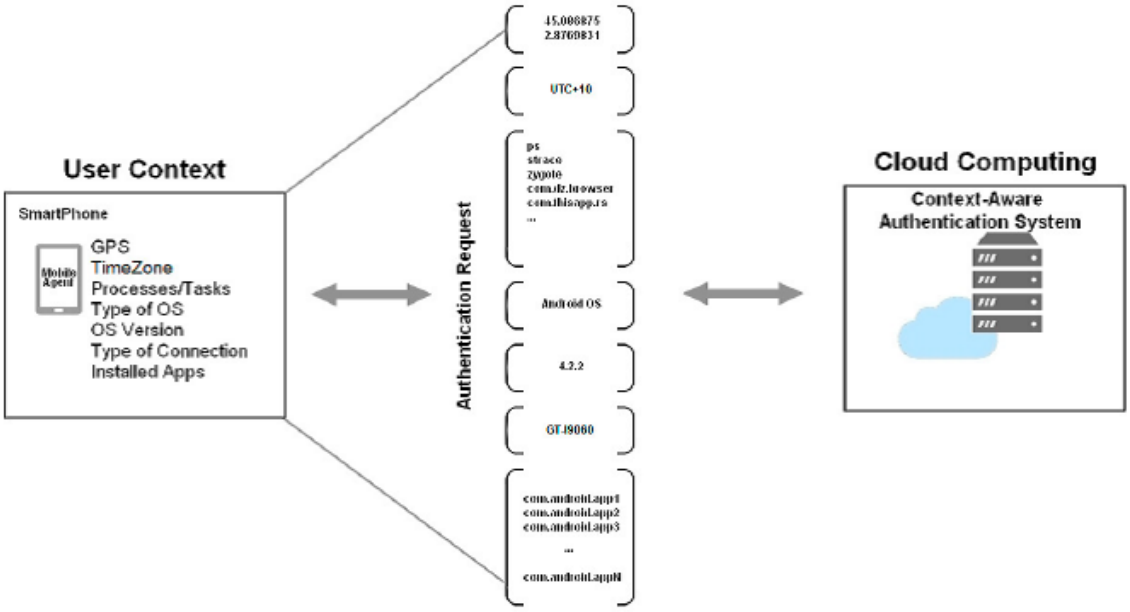


Figura 5.3: Arquitetura geral de Autenticação.
[118]

A autenticação por comportamento ou contexto analisa o contexto no qual a autenticação ocorre e avalia o risco de uma tentativa de fraude e roubo de identidade. Essa análise pode ser realizada sem afetar a experiência normal do usuário. Ela pode enriquecer qualquer processo de autenticação no qual um nome de usuário, uma senha, *tokens* ou outros fatores de autenticação são usados. Portanto, é especialmente útil em ambientes em que pode não ser possível usar métodos mais fortes, por exemplo, por motivos de usabilidade (como geralmente ocorre em cenários de compras *on-line*) ou porque o custo de implementação de métodos mais fortes (como *hardware OTP – One Time Password*) que geram senhas descartáveis de uso em um único acesso, ou o custo de implementação de dispositivos biométricos em grande escala, podem ser custos proibitivos em determinados cenários, como o de um sistema em um ambiente em nuvem que é acessado por usuários de diversas partes do globo.

O sistema armazena informações detalhadas sobre todos os fatores de contexto dos processos de autenticação. Além disso, quando uma situação anômala é detectada, o sistema gera um evento que é registrado no sistema de auditoria. Esse evento pode ser convertido em um alerta ou configurado para ativar um fator de autenticação adicional, como o fator baseado no conhecimento para verificar se o usuário é o proprietário das credenciais.

Assim, a análise de contexto detecta anomalias nos processos de autenticação, aumenta o nível de segurança fornecido por senhas ou outros fatores combinados, reduz o risco de roubo de identidade ou fraudes digitais e oferece um maior grau de confiança na proteção de recursos.

### 5.2.4 *Single Sign-On*

O *Single Sign-On* (SSO) é a funcionalidade do gerenciamento de acesso em que o usuário é autenticado uma vez e as credenciais para a sessão são confiáveis para diferentes aplicativos dentro de um domínio de segurança. Isso é tipicamente feito dentro de um domínio de segurança ou risco. O SSO é um requisito crítico dentro das organizações que operam aplicativos em uma infraestrutura de nuvem específica.

Os sistemas de autenticação podem ser implementados para fornecer serviços de SSO, que agregam identidades e permitem o acesso a vários sistemas por meio de um método de autenticação do sistema de destino. Os usuários podem fornecer uma senha somente uma vez e trabalhar durante todo o dia. Pode ser permitido que os usuários mantenham essas credenciais por um dia inteiro; no entanto, dentro de qualquer organização, pode ser determinado algum prazo razoável dentro do qual os usuários sentirão que têm o acesso de que precisam e os profissionais de segurança sentirão que protegeram o ambiente adequadamente [84].

Uma organização pode executar várias aplicações web que requerem controle de acesso. Integrar componentes de controle de acesso em todas aplicações resultaria em altos custos de gerenciamento e inconveniências para os usuários que tenham que lembrar de todas as suas credenciais.

Tradicionalmente, o *Single Sign-On* é um processo que permite ao usuário acessar vários aplicativos que exigem autenticação passando suas credenciais apenas uma vez. O usuário primeiro se autentica em alguma autoridade confiável e, em seguida, é concedido acesso a todos os aplicativos que confiam nessa autoridade. As aplicações só recebem informações sobre se elas podem deixar o usuário entrar ou não. Como o usuário autentica apenas uma vez, a exposição de informações confidenciais pela rede é limitada. Sistemas SSO geralmente preservam o estado do usuário por algum período de tempo, para que o usuário possa acessar repetidamente esses aplicativos sem a necessidade de autenticar repetidas vezes.

O SSO na nuvem é uma extensão do SSO local na *Web*. Como as empresas se expandem além de seus limites locais, há demanda em expansão para a nuvem. O resultado é implementação do SSO entre os aplicativos corporativos locais e os aplicativos baseados em nuvem.

O SSO é uma tecnologia representada pela sincronização de senhas na medida em que permite que um usuário estabeleça sua identidade apenas uma vez. Depois disso, o acesso a outros aplicativos e sistemas conectados em rede torna-se simples e evita o esforço de autenticar novamente. Várias implementações de SSO foram desenvolvidas em ambientes homogêneos onde uma única tecnologia de autenticação é usada. No modelo de identidade local com um registro do usuário o SSO é alcançado automaticamente. O usuário autentica uma vez para o sistema; depois disso, um contexto de segurança é estabelecido e passado para sistemas diferentes pelas funções de tempo de execução do sistema [15].

### 5.2.5 *Single Sign-On* Federado

O *Single Sign-On* (SSO) Federado utiliza a tecnologia denominada de Federação que fornece a capacidade de compartilhar a identidade do usuário e acessar informações entre vários domínios, que podem estar dentro das mesmas ou diferentes infraestruturas e organizações de TI. O *Single Sign-On* Federado permite a várias organizações fornecerem seus serviços em um ambiente colaborativo de maneira segura. O SSO Federado, quando implementado corretamente em um domínio de autenticação forte, fornece segurança para a organização e a facilidade de uso para o consumidor da nuvem.

Proporcionar aos usuários de sistemas heterogêneos multinuvens uma experiência de acesso homogênea a estes serviços é um grande desafio. Federações de identidade proporcionam o *Single Sign-On* (SSO) Federado, em que os usuários são identificados e autenticados por provedores de identidade (IdPs) uma única vez e, através de protocolos como *OpenID Connect* ou SAML, recebem acesso a serviços federados com os quais possuem relação de confiança [119].

### 5.2.6 Federação

Os serviços de identidade federada permitem que uma organização gerencie a identidade e o acesso de seus usuários a recursos de organizações parceiras que fornecem serviços autorizados para esses usuários específicos. Enquanto os processos de gerenciamento de identidades federada ajudam a gerenciar o ciclo de vida das identidades e contas dos usuários nos sistemas de parceiros, o *Single Sign-On* Federado ajuda na autenticação dos usuários internamente e, em seguida, transmite essa identidade para seu provedor de serviços em nuvem, como um *token* confiável. Isso permite que a organização mantenha o controle do processo de autenticação.

O uso de federações também permite que o usuário se autentique uma única vez e obtenha acesso a vários serviços e sistemas diferentes através do mecanismo de *Single*

*Sign-On* (SSO). Ao unificar a autenticação, os usuários passam a ter menos senhas para lembrar, podendo escolher senhas mais fortes e seguras [120].

(a) Gerenciamento de identidade federada.

O gerenciamento de identidade federada fornece as políticas, processos e mecanismos para gerenciar a identidade e acesso confiável à sistemas nas organizações. Isso permite reutilizar as identidades dos usuários nos limites da organização, e garante gerenciamento eficiente do ciclo de vida do usuário, conformidade e congruência de informações de usuários relevantes entre duas organizações parceiras sem sobrecarga administrativa excessiva. O objetivo principal do gerenciamento de identidade federada é fornecer aos usuários de um domínio de segurança a capacidade de acessar os sistemas de outro domínio de maneira contínua, permitindo assim o *Single Sign-On* Federado.

O *Single Sign-On* Federado permite que a autenticação de um usuário em um domínio seja confiável em todos os domínios diferentes (por exemplo, diferentes provedores de serviços). Isso proporciona conveniência aos usuários e melhor segurança, se o domínio de autenticação mantém uma forte postura de segurança. Essa tecnologia é necessária como uma funcionalidade padrão para facilitar o acesso de domínio interorganizacional e inter-segurança aos recursos aproveitando o gerenciamento de identidade federada.

O *Single Sign-On* federado pode ser alcançado usando padrões do setor como os algoritmos SAML, *WS-Security*, *Open ID* e *OAuth*. Ao implantar o SSO federado, é importante decidir qual padrão usar, com base nos casos de uso a serem suportados.

No ambiente de nuvem, muitas vezes há vários aplicativos e serviços da *Web* projetados para ajudar os usuários, requerendo autenticação. Em alguns casos, pode ser conveniente e seguro usar uma infraestrutura de SSO centralizada vinculado à autoridade central de autenticação. O SSO na *Web* fornece infraestrutura de SSO para aplicações *web*. No entanto, o SSO da Web provou ser um mecanismo muito frágil para o gerenciamento de acesso. *Web* SSO pode ser usado para autenticação de usuários para sistemas genéricos, mas para aplicativos de negócios, um SSO federado é altamente recomendado.

## 5.3 Principais soluções de mercado

As principais soluções de Autenticação por Contexto ou Comportamento originalmente foram concebidas para a área financeira, porém com a proliferação e sofisticação dos ataques, esse tipo de solução passou a ser mais comum em outros nichos de mercado. Com o fortalecimento da legislação de segurança e proteção dos dados e informações e o crescimento dos serviços digitais, já se inicia um processo de adoção no Governo.

### 5.3.1 *Microsoft Azure Active Directory*

O *Azure* é a arquitetura de nuvem da *Microsoft* e pode ser utilizada para hospedar soluções dos clientes ou para fornecer soluções e recursos em ambiente de nuvem para esses clientes. O *Azure Active Directory* (AD) é a solução de Gerenciamento de Identidade e Acessos disponível para os clientes da empresa. Essa solução utiliza métodos de autenticação baseados em comportamento e risco para validar os acessos solicitados à infraestrutura de nuvem.

Para manter o ambiente protegido, convém bloquear a conexão de usuários suspeitos. A proteção de identidade do Azure AD analisa cada *login* e calcula a probabilidade de uma tentativa de conexão não ter sido realizada pelo proprietário legítimo de uma conta de usuário. A probabilidade (baixa, média, alta) é indicada na forma de um valor calculado chamado de níveis de risco de entrada. Definindo a condição de risco de entrada, você pode configurar uma política de acesso condicional para responder aos níveis de risco de entrada específicos.

A solução utiliza um recurso de Política de Acesso Condicional que poderá bloquear acessos de acordo com o nível de risco pré-definido. Para isso, o nível de risco poderá ser classificado considerando o modo e o comportamento do perfil de autenticação, usando fatores como o endereço IP (geolocalização), dentre outros.

O *Azure Active Directory* B2C (*Business to Consumer*) é outro serviço do *Azure*. Esse serviço é de identidade em nuvem que permite que o usuário se conecte a qualquer cliente e que coloque sua marca em primeiro lugar. Governos e empresas em todo o mundo estão usando o *Azure Active Directory* B2C para disponibilizar seus aplicativos para os cidadãos e clientes com experiências totalmente personalizáveis, protegendo simultaneamente as identidades destes. Criado com base no *Azure Active Directory*, a plataforma de identidade em nuvem é altamente segura e lida com bilhões de autenticações por dia. O *Azure Active Directory* B2C oferece a mesma escala, confiabilidade e disponibilidade para seus aplicativos voltados para o cliente. A plataforma Azure possui vários recursos de GIA, entre eles o SSO e o *logon* único contínuo do Azure que conecta usuários automaticamente quando estiverem nos respectivos dispositivos conectados à rede corporativa.

O acesso condicional do Azure é um hub de política de segurança de identidade que ajuda implementar a estratégia de confiança no ponto de acesso. O acesso condicional é baseado no usuário, na localização geográfica, no endereço IP, em dispositivos registrados e aprovados para que possam acessar dados corporativos, baseado em aplicativo e baseado em risco. O *Azure* reduz proativamente o risco em seu ambiente com políticas para evitar ataques de identidade antes que eles se instalem. A figura abaixo é da tela de acesso condicional do Azure onde são definidas faixas de endereços IP e geolocalização por país.

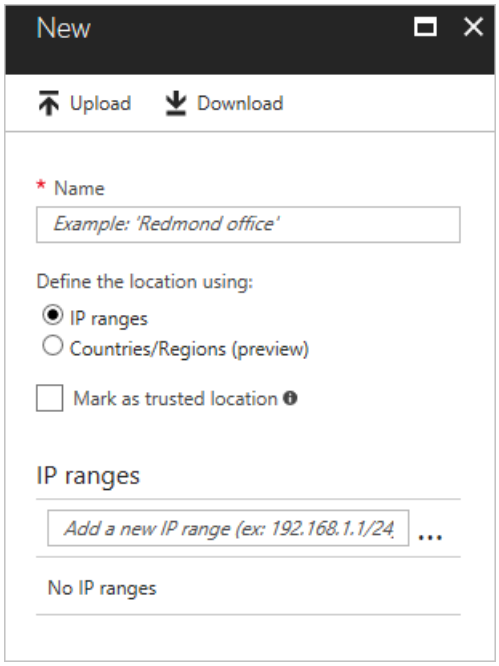


Figura 5.4: Tela de acesso condicional do *Azure* baseado em IP.
[121]

O *Azure* disponibiliza recursos de GIA como o acesso condicional, configuração de dispositivos para suportar as condições de acesso e o uso pelos dispositivos da última versão do sistema operacional para garantir conformidade.

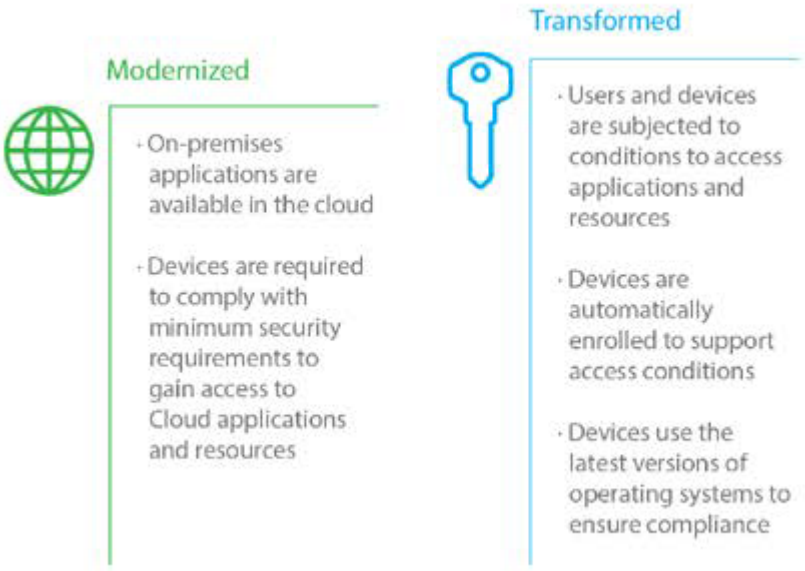


Figura 5.5: Características do controle de acesso no Azure.
[121]

A figura acima demonstra algumas características do gerenciamento de acesso no *Azure* que utiliza os dispositivos e contas de usuários para condicionar o acesso as aplicações e recursos e as políticas de conformidade dos dispositivos para acessar o *Azure* [121].

### 5.3.2 AWS (*Amazon Web Services*)

O AWS é a solução de "nuvem" da Amazon que disponibiliza o serviço AWS *Indentity and Accesss Management* (IAM) que permite gerenciar com segurança o acesso aos serviços e recursos da AWS. O IAM permite criar e gerenciar usuários e grupos da AWS e usar permissões para conceder e negar acesso a recursos da AWS [122].

O IAM permite que os usuários controlem o acesso às APIs (*Application Programming Interface*) de serviço e a recursos específicos da AWS. O IAM também permite adicionar condições específicas para controle do acesso, como a hora certa para controlar como o usuário pode usar a AWS, seu endereço IP de origem, se estão usando certificados SSL (*Security Socket Layer*) ou se fizeram a autenticação com um dispositivo de autenticação multifator.

A solução AWS IAM permite que o usuário:

(a) Gerencie os usuários do IAM e seus acessos. É possível criar usuários no AWS IAM, atribuir a eles credenciais de segurança individuais (ou seja, chaves de acesso, senhas e dispositivos de autenticação multifator) ou solicitar credenciais de segurança temporárias para disponibilizar aos usuários acessos a serviços e recursos da AWS. É possível gerenciar permissões para controlar quais operações um usuário pode desempenhar;

(b) Gerencie a função do IAM e suas permissões. É possível criar funções no IAM e gerenciar as permissões para controlar quais operações podem ser realizadas pela entidade ou pelo serviço da AWS que assumir a função. É possível também definir qual entidade tem permissão para assumir a função. Além disso, você pode usar funções vinculadas a serviços para delegar permissões a serviços da AWS que criam e gerenciam recursos da AWS em seu nome;

(c) Gerencie usuários federados e suas permissões. É possível habilitar a federação de identidades para permitir que as identidades atuais (usuários, grupos e funções) na sua empresa acessem o Console de Gerenciamento da AWS, chamem as APIs da AWS e acessem recursos, sem a necessidade de criar um usuário do IAM para cada identidade. Use qualquer solução de gerenciamento de identidade que ofereça suporte ao SAML 2.0 ou use os recursos de federação do AWS (SSO do Console AWS ou federação por meio de APIs).

Com a ferramenta de IAM do *Azure* é possível criar políticas de acesso condicional, por meio de critérios de liberação e bloqueio do acesso conforme o perfil dos usuários. O AWS *Identity and Access Management*, ajuda a configurar usuários e grupos e mostra como proteger recursos com políticas de controle de acesso. Além disso, mostra como conectar-se a outros serviços de identidade para permitir que usuários externos acessem recursos da AWS.

### 5.3.3 OKTA

A OKTA é uma empresa americana que oferece um portfólio de soluções de segurança e acesso. Dentre dessas soluções está a Autenticação Adaptativa Multifator, que é dividida em três soluções:

(a) Política baseada em contexto. Aplicar a autenticação multifator somente quando necessário, com base em uma ampla gama de sinais. A solução define um acesso inteligente e políticas de autenticação com base no contexto de *login*;

   I. Contexto de localização: nova cidade, estado ou país, nova localização geográfica, padrões de viagens impossíveis;

   II. Contexto do Dispositivo: reconhecimento de dispositivo conhecido e gerenciamento de dispositivo;

   III. Contexto de Rede: novo IP, zonas de IP especificadas, anonimizadores de rede;

   IV. Contexto de risco: cria políticas com base nos sinais de risco observados em todo o conjunto de dados global, como endereços IP de alto risco.

(b) MFA incorporável. Adiciona um segundo nível de segurança ao seu aplicativo com autenticação de vários fatores;

   Suporte para uma variedade de fatores: *e-mail*, SMS, voz, pergunta de segurança, *Google Authenticator*, *Okta Verify*, *Okta Verify* com *Push*, *tokens* OTP e autenticadores, Provedores de MFA (*Multi Factor Authentication*) de terceiros, *faceID*, *touchID* e biometria *Android*.

(c) Relatório robusto: fornece o histórico de autenticação multifator do usuário para investigações de aquisição de conta ou análise de risco.

### 5.3.4 *Diebold Nixdorf*

As soluções antifraude Diebold Nixdorf existem para minimizar os riscos de fraude no ambiente digital, tornando o acesso a informações e transações o mais simples e seguro para os usuários das instituições.

Atualmente, qualquer sistema que necessite de monitoramento para segurança da informação precisa de alguma forma de autenticação e identificação dos usuários finais. É assim que o gestor da solução consegue determinar quem é confiável e quem pode interagir com o sistema.

A maneira mais comum de fazer a autenticação é utilizar um nome virtual e uma senha definidos pelo próprio usuário final. O que ocorre é que, muitas vezes, a pessoa configura as mesmas credenciais em diferentes sistemas, o que pode prejudicar a segurança.

A *Diebold Nixdorf* atua no desenvolvimento de mecanismos para aperfeiçoar a identificação e autenticação em diferentes canais. Identificadores de dispositivos, criptografia sofisticada, dispositivos de bolso e ferramentas de monitoramento de acessos e comportamentos dos usuários finais são a base das soluções hoje ofertadas pela empresa.

Por meio dessa tecnologia, é possível desenvolver uma camada de autenticação de usuário tão sofisticada a ponto de eliminar a necessidade de utilização de nome de usuário virtual e senhas para acesso. Apenas com o uso de um dispositivo móvel é permitido acessar qualquer canal de comunicação, sem necessidade de teclado ou *mouse*.

## 5.4 Comparação entre tecnologias de GIA

Na tabela resumo abaixo é realizada uma comparação entre as tecnologias de autenticação, com base no estudo de [15] e com as tecnologias de GIA.

Tabela 5.3: Comparação entre as tecnologias de GIA. Adaptado.

| **Tecnologia** | **Função** | **Prós** | **Contras** | **Interação do usuário** | **Ponto de controle** |
|---|---|---|---|---|---|
| SSO | Única validação de acesso para todas as aplicações do mesmo domínio. | Minimiza o risco de acessos indevidos, pois basta um único processo de autenticação para várias aplicações ou domínios. | Verifica apenas o nível de acesso e não toda a cadeia de acesso ao sistema. | Sim. | Momento do Acesso. |
| SSO Federado | Única validação de acesso para todos os domínios confiáveis entre si. | | | | |
| Federação | Gerencia acesso confiável entre organizações. | | Implementação pode ser complexa. | Não. | Momento do Acesso. |
| Autenticação Simples: usuário e senha | Utiliza fator único para o acesso. | São fáceis de implementar e de baixo custo. | São suscetíveis de adivinhar e serem comprometidos por terceiros. | Sim. | Momento do Acesso. |
| Autenticação por *Token* / OTP | Baseada no envio de código de acesso para um dispositivo. | As informações do *token* são sempre precisas Senha ou código descartável. | Pode exigir habilidade especial para interagir com o dispositivo e ser caro implementar Precisa ser carregado com o usuário Suscetíveis a perdas e roubos. | Sim. | Momento do Acesso. |
| Autenticação por Biometria | Autentica com característica física do usuário. | Difícil de comprometer o sistema, somente ser o usuário for vitimizado. Naturalmente presentes com o usuário. | Requer habilidade especial para interagir com o equipamento. Alto custo de implementação. | Sim. | Momento do Acesso. |
| Autenticação adaptativa por contexto ou comportamento | Adaptativa, baseada no perfil dinâmico de contexto ou comportamento do usuário. | Autenticação dinâmica, adequada para ambientes pervasivos. Difícil de comprometer. | Pode ser complexa a manutenção da solução ou criação de algoritmos. | Não. | Pode ser contínua. |

Conforme demonstrado na tabela acima e neste trabalho o *Single Sign-On* (SSO)) é a tecnologia que permite o acesso a vários sistemas ou aplicativos a partir de um único processo de *login*, porém o SSO implementa originalmente o acesso de fator único e precisa de outras tecnologias adicionais para ser mais confiável diante dos riscos de fraudes digitais. No caso do SSO Federado ou da solução de "Federação", a diferença é que a autenticação passa a ser confiável para várias organizações enquanto que no caso do SSO é somente em seu próprio domínio organizacional.

A autenticação simples e de fator único, geralmente por usuário e senha, que é o método de autenticação ainda mais comum, pode ser comprometida facilmente pela descoberta da senha, a vantagem é que a implementação é fácil e de baixo custo, porém, são suscetíveis a fraudes digitais e ataques diversos. A autenticação por token é precisa e também muito usada, porém apresenta dificuldades para o uso como a dependência de um dispositivo e riscos como a eventual perda ou roubo do mesmo. É um fator adicional de autenticação, pois além da senha o usuário precisa confirmar com o código enviado, além de usar no caso do OTP (*OnTime Passwords*) senhas descartáveis, o que mitiga o risco da interceptação do código ou senha para uso posterior.

A autenticação biométrica é muito difícil de ser comprometida por pessoas mal-intencionadas, pois a validação é feita com características do corpo humano, como por exemplo a impressão digital. Porém, ainda existe o risco da pessoa ser vitimizada e ser compelida a realizar o acesso contra a sua vontade. O custo de implementação é alto, pois requer sempre um dispositivo no lado do acesso para capturar as informações físicas do usuário. Combinada com outras tecnologias pode ser bastante eficaz contra fraudes digitais.

Por fim, a autenticação por contexto ou comportamento, onde sua principal característica é ser adaptativa, como uma camada adicional de segurança consegue a partir de padrões dinâmicos validar a legitimidade do acesso. Em razão de ser adaptativa consegue funcionar muito bem em ambientes pervasivos, que se caracterizam pela computação onipresente e a dinamicidade do acesso, onde os usuários são predominantemente móveis e podem acessar aplicações de várias localizações do globo. Com o crescimento da computação em nuvem e dos negócios pela internet este cenário pervasivo é o mais atual. Essa tecnologia é transparente para o usuário, pois ela detecta automaticamente as informações de perfil, o atualiza, e compara com as informações de perfil da conta. Também é difícil de comprometer, pois em caso de tentativa de fraude o sistema vai poder bloquear acessos considerados anormais ou suspeitos. Caso combinada com o processo de autorização passa a ser eficiente no tratamento de riscos de privilégios excessivos, pois realizará continuamente a verificação dos direitos de acesso dos usuários naquela determinada sessão de *login* ao sistema. Com isso, a autenticação por contexto ou comportamento, mostrou-se a

mais adequada para combater as tentativas de fraudes digitais que podem levar a perdas dados sigilosos e da imagem da organização.

## 5.5 Conclusões do capítulo

Neste capítulo foram apresentadas as formas de tratamento para os riscos de "Acessos Indevidos" e "Privilégios Excessivos", que foram identificados como de alta relevância para o Sistema Decom Digital. Foi também apresentada a maior adequação da solução de GIA como camada adicional para tratamento desses riscos que podem resultar em fraudes digitais e vazamento de informações. Foram apresentadas as características das principais tecnologias de GIA, como se inserem como formas de tratamento de riscos, comparação de fatores de autenticação, melhores formas de tratamento dos riscos mencionados e a forma de utilização recomendada para prover um sistema de segurança mais forte.

Além disso, o capítulo demonstrou as principais soluções de mercado que adotam a GIA como requisito de segurança e prevenção contra acessos indevidos, privilégios excessivos e fraudes digitais.

# Capítulo 6

# Desenvolvimento de uma aplicação computacional para o uso de uma tecnologia de GIA para o SDD, como forma de tratamento dos riscos.

Este capítulo apresenta uma tecnologia de GIA para o SDD e o ambiente, requisitos e implementação de um protótipo desenvolvido para validar a abordagem proposta. O objetivo dessa implementação e é possibilitar a autenticação do usuário, através da utilização da riqueza de contextos encontrada em ambientes de computação, sobretudo a computação móvel e pervasiva.

## 6.1 Contexto para construção do protótipo

Conforme demonstrado no capítulo 4, no processo de avaliação de riscos, o risco de "Acessos Indevidos" foi classificado como um risco extremo e no capítulo 5 evidenciou-se que um dos controles mais efetivos possíveis para esse tipo de risco é a utilização das tecnologias de Gestão de Identidade e Acessos, pois disponibilizam mecanismos para que o acesso seja mais confiável. O capítulo cinco também evidenciou a Autenticação por Comportamento, Contexto ou Risco como uma das mais efetivas tecnologias de GIA para controle dos riscos de Acessos Indevidos e Privilégios Excessivos em qualquer ambiente, principalmente em ambiente de nuvem.

Considerando as análises realizadas, principalmente a análise de riscos para uso do Sistema Decom Digital na nuvem, selecionou-se como lacuna para tratar o risco de vazamento e falha na integridade das informações, a adoção da tecnologia de GIA denominada Autenticação por Contexto (*Context-awareness Authentication*) ou Comportamento (*Behavior*

*Authentication*), que analisa os padrões de comportamento dos usuários e características comuns dos acessos, como redes origem de acesso, endereços IP de origem, tecnologias usadas nos dispositivos de acesso como navegadores e sistemas operacionais, os próprios dispositivos, geolocalização, timezones (horários de acesso), e correlaciona todos esses eventos para identificar padrões e evitar fraudes e vazamentos de informações.

Como o Sistema Decom Digital trata de informações sigilosas, e é acessado por organizações do mundo todo, a Autenticação baseada em comportamento ou contexto é bastante importante para garantir a segurança dos acessos. Por meio de uma análise adicional e transparente das solicitações de acesso ao SDD esta tecnologia torna o acesso mais confiável e auditável por meio de processos de autenticação mais robustos e que podem ser verificados a partir de acessos de qualquer tipo de dispositivos, como smartphones, notebooks, desktops, em qualquer parte do globo.

## 6.2 Tecnologia de GIA proposta

A tecnologia de GIA proposta a partir da análise de riscos e do estudo realizado nos capítulos quatro e cinco é a autenticação baseada em comportamento ou no contexto que consiste em analisar os acessos ao SDD considerando padrões e características de acessos dos usuários. Nas tentativas de acesso, em caso de convergência com os padrões daquela conta, o acesso será permitido. Já em caso de divergência dos padrões ou diante da identificação de uma correlação de eventos considerada suspeita, como acessos em períodos curtos de tempo a partir de redes geograficamente distantes, alguma ação é requerida, inclusive até o próprio bloqueio imediato do acesso. No caso de uma ação, pode ser usada a Autenticação por Conhecimento, ou seja, envio de um desafio para o solicitante do acesso composto por respostas a perguntas previamente cadastradas quando da criação da conta pelo usuário legítimo ou o uso de mensagens de texto para o dispositivo móvel do usuário.

A autenticação por contexto é uma camada adicional de segurança no processo de gestão de identidade e acessos e não dispensa a utilização de outros mecanismos de autenticação. Essas tecnologias não são excludentes e sim complementares, pois quanto mais níveis de segurança a aplicação puder contar, maiores serão os controles para evitar fraudes digitais.

## 6.3 Problema a ser resolvido pelo protótipo

O problema é que o SDD possui um sistema de autenticação simples, o que torna frágil a proteção contra acessos indevidos, esse problema é maximizado quando o SDD passa a

funcionar em um ambiente de nuvem, pois estará em um ambiente não controlado pelo cliente e continuará a ser acessado por dispositivos diversos em qualquer área do globo, essa maior exposição influencia em maior risco em razão de ataques e apropriação indevida de senhas e uso de técnicas como a Engenharia Social. É uma necessidade fortalecer o sistema de autenticação do Sistema Decom Digital para mitigar eventos de fraudes, vazamento de informações e falha de integridade dos dados em razão de vulnerabilidades que elevam os riscos de acessos indevidos. Essas vulnerabilidades são representadas principalmente por um sistema de autenticação simples de usuário e senha, o que tornam as tentativas de fraudes e acessos indevidos mais prováveis de ocorrerem e com maior probabilidade de sucesso.

## 6.4 Planejamento do Protótipo

Este estudo implementou um protótipo concebido por meio de uma rotina de aplicação computacional baseada na Autenticação por Contexto ou Comportamento. Para isso foi construída uma aplicação de validação de acesso a partir de algumas características deste perfil de acesso, tais como: faixa de endereço lógico de origem, tipo de navegador e sistema operacional utilizado durante o acesso. Ao comparar os elementos que formam o contexto do acesso, ou seja, as informações de endereço IP, navegador e sistema operacional utilizado, que compõem o perfil de acesso daquela conta, a aplicação pode permitir ou negar acesso, ou ainda tomar alguma ação para validação deste acesso.

### 6.4.1 Requisitos

Um requisito é uma condição necessária para satisfazer um objetivo, portanto, um requisito é um aspecto que o sistema proposto deve fazer ou uma restrição no desenvolvimento do sistema [123]. Para o protótipo implementado alguns requisitos precisaram ser atendidos para que o mecanismo de controle seja efetivo. Para contextualizar o funcionamento da aplicação descrevemos uma arquitetura de autenticação baseada em comportamento ou contexto.

As soluções de Autenticação por Contexto geralmente possuem os subsistemas de autenticação, validação e desafio [50]. O subsistema de autenticação executa o controle de acesso e valida o acesso dos usuários a partir de um perfil conhecido que é atualizado quando o subsistema correlaciona fatores de acordo com a evolução do comportamento das contas de acesso. O subsistema de validação compara as características de acesso com a base de perfis armazenados para validar ou não o acesso. O subsistema de desafio gera confirmações quando o subsistema de validação considera o acesso como suspeito.

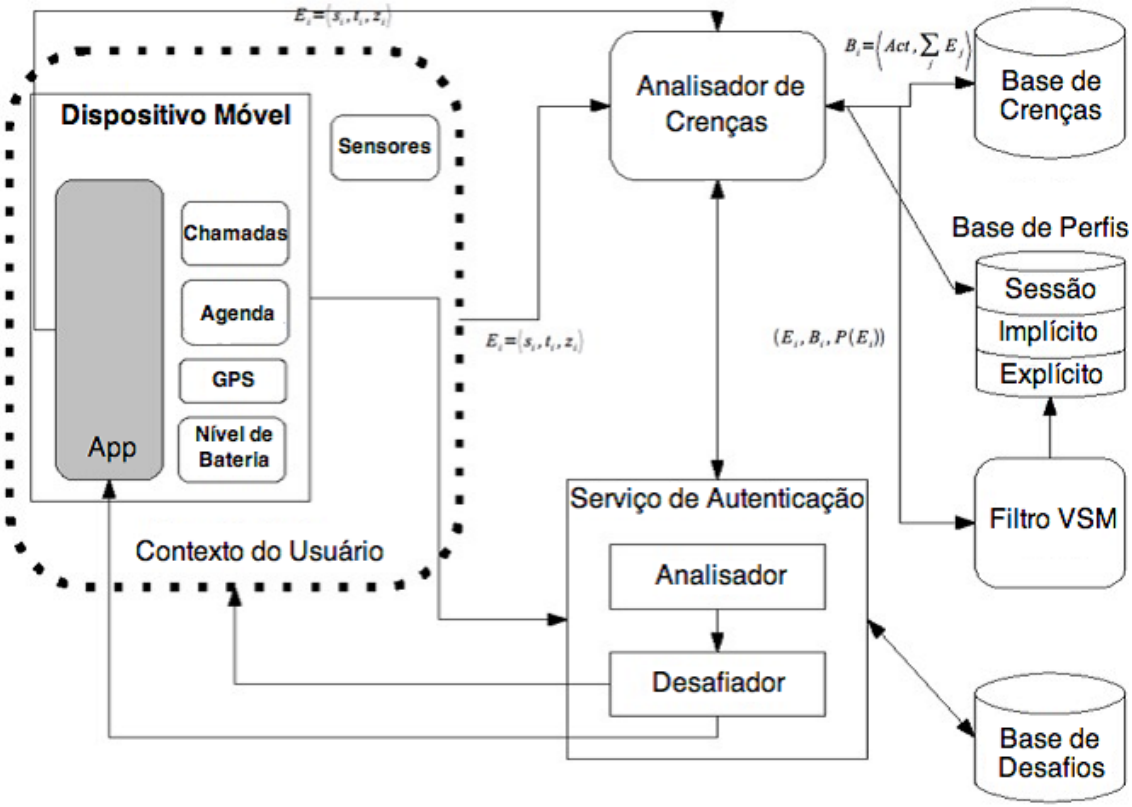


Figura 6.1: Arquitetura geral de Autenticação por Contexto.
[92]

Na figura acima existe o Sistema de Contexto do Usuário que junto ao Serviço de Autenticação formam o subsistema de autenticação, o Analisador de Crenças que junto ao Analisador, o filtro VSM (Modelo de Espaço Vetorial) e as bases de crenças e perfis formam o subsistema de validação, e o Desafiador que junto ao Analisador de Crenças e a base de desafios forma o subsistem de desafio.

O subsistema de contexto, ou contexto do usuário, é responsável por capturar todas as situações que determinam a ocorrência de um novo evento. O Analisador de Crenças é responsável pela definição de comportamentos, ou crenças, assim como pela classificação de eventos e inferência de comportamentos através das atividades, dos perfis armazenados e eventos que são percebidos e registrados. O Filtro VSM (Modelo de Espaço Vetorial) é um filtro que utiliza o modelo de espaço vetorial para calcular a relevância da informação, utiliza um tratamento formal através de vetores para o cálculo de similaridade entre os perfis em análise. O Filtro VSM tem como objetivo determinar os novos perfis implícitos através do modelo de vetor de similaridade. Por fim, o subsistema de desafios, ou Desafiador, determina como o usuário será questionado a fim de provar sua identidade no sistema.

Para o protótipo, o subsistema de autenticação será representado pela rotina própria de autenticação simples, somente usuários pré-cadastrados e validados podem acessar ao sistema. Esse subsistema não é um objetivo principal do trabalho, pois o SDD já possui o mecanismo de autenticação simples baseado em usuário e senha.

Na rotina desenvolvida, o programa de acesso cuida da verificação do acesso por usuário e senha e coleta os dados de entrada para comparar com o perfil de acesso, para validar esse perfil e consequentemente o acesso. A construção de uma base de perfis é desejável para que sua atualização seja dinâmica e possa atender a um ambiente computacional pervasivo. No protótipo o acesso é validado de forma estática e compara as informações armazenadas com as de solicitação de acesso.

#### 6.4.1.1 Subsistema de autenticação

A rotina possui um controle de acesso e de contas de usuários cadastrados. Cada conta deve ter um perfil e base de contexto conforme os controles de validação informados abaixo:

(a) *Range* de IP;

(b) Sistema operacional utilizado para o acesso;

(c) *Browser* utilizado pelo acesso.

Os atributos acima foram selecionados, pois são comumente usados e fornecem características únicas quando combinados os três fatores, porém podem ser usados atributos como: horário de acesso (*timezone*), aplicativos mais acessados, identificador único do dispositivo em que a aplicação reúne informações do dispositivo de acesso, tornando único esse identificador digital, dentre outros atributos.

O sistema de autenticação consulta uma base de endereços IPs e uma base ou informações de perfis de comportamento ou contexto para validar o acesso. A aplicação simula esse comportamento com um usuário e senha pré-cadastrado que é comparado com a entrada de dados de autenticação para validar a primeira etapa do acesso.

#### 6.4.1.2 Subsistema de validação

O subsistema de validação deve comparar as características de acesso ao perfil armazenado para que o acesso seja liberado. Caso o acesso daquela conta de usuário seja considerado suspeito, o sistema deve verificar o tipo de acesso (privilégio da conta) e acionar o subsistema de desafio para aplicar o desafio conforme grau de privilégio da conta de acesso.

A aplicação realiza a comparação dos atributos de IP de origem, sistema operacional e tipo de navegador, individualmente ou correlacionados, com as informações armazenadas pela aplicação para cada conta do sistema.

#### 6.4.1.3 Subsistema de desafio

O subsistema de desafio deve enviar o desafio ao usuário e caso o desafio seja respondido corretamente o acesso será permitido. Caso o desafio não seja respondido ou respondido incorretamente o acesso deve ser negado.

No caso do protótipo o sistema enviará um desafio composto de perguntas se na tentativa de acesso mais de um fator de autenticação não coincida com os dados cadastrados daquela conta. A simulação computacional passa a considerar o acesso como suspeito e utiliza o sistema de desafio para validação do acesso.

#### 6.4.1.4 Correlação de fatores

Além do fator de usuário e senha o protótipo disponibilizará outros fatores de atributos do usuário que poderão ser analisados a partir dos registros de login das tentativas de acesso, neste caso de estudo, apenas os três fatores (faixa de endereço IP, sistema operacional e tipo de navegador) serão considerados e poderão ser correlacionados para validação do acesso.

#### 6.4.1.5 Auditoria dos acessos

O protótipo disponibilizará *logs* de acesso com os registros das ações efetuadas mediante as tentativas de acessos. Por meio desses logs deverá ser possível auditar as tentativas de acesso e possíveis indícios de contas que podem estar sendo usadas de forma fraudulenta.

#### 6.4.1.6 Requisitos especificados para o protótipo

Os requisitos especificados para o protótipo estão relacionados na tabela abaixo:

Tabela 6.1: Especificação de requisitos do protótipo

| **REQUISITOS DO PROTÓTIPO** | | |
|---|---|---|
| Subsistema de Autenticação | Possuir rotina própria de autenticação simples | |
| Subsistema de validação | Controles por faixa de IP, navegador e sistema operacional. | Validação estática pela comparação dos atributos do acesso com os atributos da aplicação. |
| Subsistema de desafio | Enviará perguntas no caso de insucesso de alguma comparação do subsistema de validação | |
| **Requisitos funcionais** | | |
| A validação de usuário/senha é obrigatória | | |
| As validações adicionais por IP, sistema operacional e navegador poderão ser realizadas em conjunto ou isoladamente. | | |
| Caso dois ou mais atributos adicionais sejam violados o acesso será negado. | | |
| Caso um atributo adicional seja violado, será disparado o desafio. | | |
| Caso as respostas ao desafio sejam válidas o acesso será concedido, caso contrário será negado. | | |
| **Requisitos não funcionais** | | |
| A aplicação disponibilizará logs de acesso com os registros das ações efetuadas mediante as tentativas de acessos. | | |
| Protótipo será desenvolvido em linguagem PHP e servidor de aplicação Apache | | |

A tabela acima relaciona os requisitos funcionais e não funcionais do protótipo segregando primeiro por subsistema e posteriormente pelo tipo de requisito. Segundo [123] os requisitos funcionais referem-se sobre o que o sistema deve fazer, ou seja, suas funções e informações. Os requisitos não funcionais referem-se aos critérios que qualificam os requisitos funcionais. Esses critérios podem ser de qualidade para o software, ou seja, os requisitos de performance, usabilidade, confiabilidade, robustez, etc. Ou então, os critérios podem ser quanto a qualidade para o processo de software, ou seja, requisitos de entrega, implementação, etc. Portanto, requisitos funcionais preocupam-se com a funcionalidade e os serviços do sistema e os requisitos não funcionais definem propriedades e restrições do sistema como tempo, espaço, linguagens de programação, sistema operacional, etc.

#### 6.4.1.7 Processo de funcionamento do protótipo

A partir dos requisitos estabelecidos é possível elaborar um fluxo do processo de funcionamento do sistema, na figura abaixo está demonstrado esse fluxo:

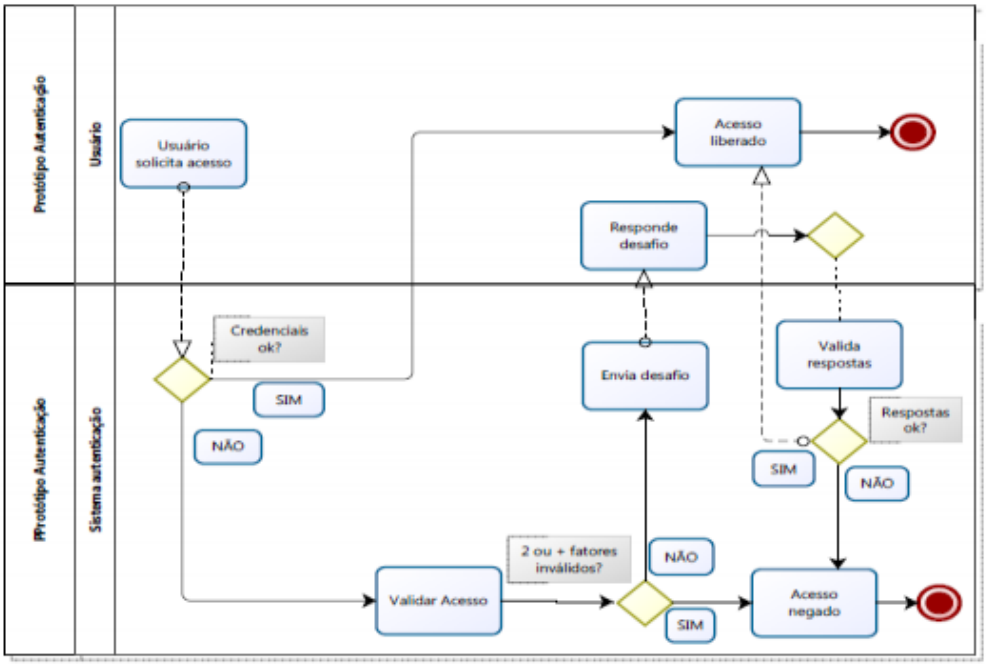


Figura 6.2: Fluxo de funcionamento do protótipo. Elaboração própria.

A figura acima demonstra as atividades e pontos de decisão determinados pelos requisitos funcionais do protótipo e as ações tomadas após cada ponto de decisão.

### 6.4.2 Metodologia

Esta seção apresentará a metodologia de desenvolvimento do protótipo.

#### 6.4.2.1 Método de construção do protótipo

A metodologia de desenvolvimento aplicada ao projeto da solução foi a chamada XP (*Extreme Programming*), que se baseia principalmente na possibilidade de alteração rápida dos requisitos caso necessário. Seu emprego é geralmente utilizado em projetos de curta duração, onde o foco principal é a apresentação de resultados físicos e interativos de relevância. Como organização de processos, foi utilizada a metodologia ágil, com desenvolvimento em microciclos.

#### 6.4.2.2 Etapas de construção do protótipo

A construção da aplicação foi dividida em 3 (três) etapas:

(a) Conhecimento: leitura da documentação base e levantamento dos requisitos para funcionamento da solução;

(b) Validação: validação técnica dos requisitos propostos para possível avaliação;

(c) Desenvolvimento: real desenvolvimento do código fonte, testes e compilação da aplicação.

Para a etapa de Conhecimento o método utilizado foi de levantamento de documentações e dos requisitos funcionais da solução, ou seja, os requisitos de funcionalidades que devem ser cumpridos pela aplicação. Na etapa de validação dos requisitos técnicos foi realizada uma análise dos requisitos propostos e levantadas formas de desenvolver tecnicamente a solução.

Na etapa de desenvolvimento se deu a construção e documentação do código fonte, testes unitários e funcionais de código, compilação da solução e a validação preliminar dos resultados.

Na etapa de validação foram realizados testes da solução considerando diversos cenários. Para complementar a validação foram gerados logs de validação e bloqueio dos acessos à aplicação.

#### 6.4.2.3 Modelo de teste do protótipo

Para os testes foi utilizada a metodologia V&V (Verificação e Validação), que divide-se em estática e dinâmica, na primeira são realizadas análises de representação estática do sistema com o objetivo de descobrir problemas e na segunda o teste de software é uma atividade dinâmica com o intuito de executar o programa com entradas especificas e verificar se seu comportamento está de acordo com o esperado. Ele é utilizado também para demonstrar a confiabilidade do software. Validação significa que o software deve estar de acordo com sua especificação e Verificação indica que o software deve fazer exatamente o que o usuário deseja [124].

O processo básico de testes deve envolver uma mistura de testes manuais e automatizados. De acordo com [124] os testes automatizados são mais rápidos que os manuais, pois o fluxo segue a codificação dos testes em um programa e a execução sempre que necessário. Já no teste manual, o testador deve executar o programa desenvolvido com os dados de teste preparados e comparar os mesmos com o resultado esperado.

Neste trabalho serão utilizadas as seguintes técnicas de testes:

(a) Teste Unitário: tem a função de descobrir defeitos nas menores unidades do sistema. A execução dos testes unitários fornece uma garantia ao programador de que os resultados esperados sejam iguais aos resultados retornados pelo sistema;

(b) Teste de Funcional: é utilizado para testar as funções do sistema, garantindo que estão de acordo com o especificado nos requisitos funcionais.

A metodologia de testes inclui um plano de testes que funciona como um integrador entre diversas atividades de testes no projeto e é um guia para execução e controle

das atividades de testes. O Plano de testes elaborado para o protótipo tem a seguinte estrutura:

(a) Os itens a serem testados: serão testadas as funcionalidades de controle de acesso por meio da autenticação por contexto. Os testes deverão identificar se as funcionalidades de validação de acesso descritas nos requisitos serão atendidas;

(b) Atividades e recursos a serem empregados: os testes serão realizados por meio de simulações de acesso em situações considerando vários perfis de acesso, selecionando atributos da aplicação que simulam os atributos de composição de um perfil;

(c) Os tipos de testes a serem realizados serão unitários funcionais na seguinte ordem: acesso de fator único com usuário e senha, acesso com dois fatores (senha e endereço IP), acesso com senha e navegador, acesso com senha e sistema operacional e acesso com todos os atributos de autenticação, testes com sistema de desafio;

(d) Critérios para avaliar os resultados obtidos: observação do comportamento do protótipo e as mensagens na tela que informam se o acesso foi permitido ou bloqueado e resultados das mensagens de log no arquivo de *logs* do protótipo.

Por meio do plano de teste é possível provisionar os recursos necessários nos momentos adequados. Isto significa coordenar o processo de teste de modo a perseguir a meta de qualidade do protótipo.

## 6.5 Construção do Protótipo

O protótipo desenvolvido simula uma solução de Autenticação por Contexto ou por Comportamento e nesta seção serão demonstradas todas suas características e modelo de implementação.

### 6.5.1 Arquitetura do protótipo

O padrão de arquitetura utilizada no desenvolvimento da solução é o padrão MVC (Modelo, Visualização, Controle) que define basicamente todo desenvolvimento em três camadas:

(a) Camada de apresentação ou visualização: camada que adiciona os elementos de exibição ao usuário: HTML, ASP, XML, Applets. É a camada de interface com o usuário. É utilizada para receber a entrada de dados e apresentar visualmente o resultado;

(b) Camada de lógica da Aplicação - É a camada nuclear da execução. Responsável por tudo que a aplicação executa e pelo controle de um ou mais elementos de dados, responde às perguntas sobre sua condição e responde as instruções para mudar de posição. O modelo sabe o que o aplicativo quer fazer e é a principal estrutura computacional da arquitetura, pois é ele quem modela o problema que está se tentando resolver. Modela os dados e o comportamento por atrás do processo de negócio. Essa camada se preocupa apenas com o armazenamento, manipulação e geração de dados. É um encapsulamento de dados e de comportamento independente da apresentação;

(c) Camada de Controle - É responsável por interpretar as ações de entrada realizadas pelo usuário através do mouse e do teclado. O Controle (*Controller*) envia essas ações para o Modelo (*Model*) e para a janela de visualização (*View*) onde serão realizadas as alterações necessárias.

O modelo de três camadas MVC é uma arquitetura de projeto onde seu objetivo é separar seu código em três camadas fazendo com que cada área só trabalhe com itens que competem a elas. Cada um só faz o que foi desenvolvido para fazer. Haverá uma separação em seu código, as regras de negócio ficarão separadas da lógica e da interface do usuário [125]. No caso do protótipo os códigos de interface com o usuário estão separados dos códigos das regras de negócio.

### 6.5.2 Pseudocódigos para os sistemas de validação e desafio

Os subsistemas de validação e desafio da solução de autenticação por contexto ou comportamento são construídos como módulos de uma aplicação principal e podem ser desenvolvidos de muitas formas de acordo com a regra de negócio adotada, como ponto de partida para essa codificação pode-se adotar um pseudocódigo que traduz em linhas gerais o funcionamento de cada sistema.

O pseudocódigo abaixo é para o subsistema desafiador, onde a base de desafios é consultada a partir de um evento suspeito de acordo com o nível de autenticação, se o evento for anormal será pesquisado na base o desafio de acordo com o nível de autenticação para essa severidade. Após seleção do desafio, o mesmo é enviado para o usuário, em seguida o subsistema valida a resposta ao desafio e permite o acesso se a resposta for correta, caso contrário fecha a aplicação.

```
1 Início
2 if NaturezaUsuario is USUARIO_SUSPEITO then
3 Pesquisar na Base de Desafios o desafio referente ao nível da autenticação
4 exigida pela aplicação para comportamentos suspeitos
5 else if NaturezaUsuario is USUARIO_ANORMAL then
6 Pesquisar na Base de Desafios o desafio referente ao nível da autenticação
7 exigida pela aplicação para comportamentos anormais
8 end if
9 Enviar desafio para o usuário
10 if Resposta do desafio está correta then
11 Realizar a operação requerida pelo usuário
12 Definir o evento E como Perfil de Sessao do usuário
13 Inserir o evento E ao Perfil Implicito do usuário
14 else
15 Fechar a aplicação
16 end if
17 Fim
```

Figura 6.3: Algoritmo para o Funcionamento do Desafiador.

No trecho de código acima a linha '2' inicia uma estrutura condicional que é executada se o usuário for considerado "anormal" comparando com critérios de classificação pré-definidos pelo programa. Caso seja executada, a estrutura realizará pesquisa na base de desafios conforme linha '7' e enviará o desafio para o usuário (linha '9'), finalmente outra estrutura condicional é iniciada '10' para validar a resposta do usuário.

### 6.5.3 Níveis de autenticação

Os níveis de autenticação podem determinar os níveis de controle e medidas a serem executadas no momento da solicitação de acesso. Conforme [80], todas as operações executadas em um ambiente pervasivo não podem ser classificadas em uma única categoria. Portanto, a natureza das operações deve ser envolvida a fim de categorizar os níveis de autenticação.

O tipo de perfil ou tipo de privilégio determinaram a ação e o nível dessa ação. Caso o acesso seja considerado suspeito poderá ser enviado um desafio ao solicitante do acesso

e o nível do acesso solicitado determinará também o nível do desafio. O nível de desafio varia entre alto e baixo e é determinado pelos tipos de perguntas enviadas ao solicitante do acesso.

Em um ambiente de computação pervasiva e móvel busca-se identificar as categorias de níveis de autenticação conforme exemplo abaixo:

(a) Alto: representa um risco elevado às operações do usuário realizadas através da aplicação utilizada;

(b) Médio: apresenta um risco moderado às operações realizadas pelo usuário. Exemplos são: submissão de tarefas para realização de reserva de recursos; e

(c) Baixo: apresenta um risco mínimo às operações do usuário realizadas através da aplicação em questão. Pode-se citar como exemplos: monitoramento da de reservas de recursos realizadas.

A partir dessa categorização procura-se relacionar o nível de autenticação e a natureza do usuário aos desafios propostos para cada categoria a fim de validar o processo de autenticação dos usuários conforme proposto por [92] na tabela abaixo:

Tabela 6.2: Relação entre os níveis de autenticação, natureza do usuário e desafios propostos.

| **Nível** | **Natureza do Usuário** | **Desafio** |
|---|---|---|
| Alto | Suspeito Anormal | "Por favor, digite o nome de seu primeiro animal de estimação"<br>"Por favor, digite a cidade de nascimento de usa mãe" |
| Médio | Suspeito Anormal | "Por favor, digite sua cor favorita"<br>"Por favor, digite o nome de sua primeira escola" |
| Baixo | Suspeito Anormal | "Por favor, digite sua data de nascimento"<br>"Por favor, digite seu CEP" |

Dessa forma estabeleceu-se que quanto mais alto o nível de autenticação mais complexo será o desafio, pois trata-se de um risco maior para a organização baseado na possibilidade de um perfil de acesso crítico ser comprometido e usado de forma fraudulenta.

Para a aplicação o nível de autenticação foi relacionado a quantidade de fatores de entrada que diferem do perfil de acesso armazenado. A partir um fator de entrada, além

de usuário e senha, o protótipo enviar o desafio. Qualquer que seja o atributo de entrada, endereço IP, tipo de navegador, sistema operacional ou o navegador diferente da base de perfis, o acesso é considerado suspeito e o sistema de desafio é acionado.

### 6.5.4 Fases e Entregas

Na primeira fase do projeto foram especificados os requisitos da aplicação, depois foi realizada uma etapa de projeto onde foi estabelecida a forma de construção e testes da aplicação. Na fase seguinte a execução foi realizada com entregas medidas pelos subsistemas que compõem a solução. Após a fase de execução foram realizados testes para validar se as saídas do programa estavam conformes aos requisitos levantados e validados. Após a fase de testes, foi realizada a fase de conclusão com o encerramento do projeto de construção da aplicação.

Tabela 6.3: Validação das fases do projeto de construção do protótipo.

| **Fase** | **Entrega** | **Validação** |
|---|---|---|
| I – Planejamento | Requisitos de alto nível | Revisão |
| II - Requisitos | Requisitos especificados e validados | Revisão |
| III - Execução | Códigos entregues | Compilação do código |
| A - Sistema | Códigos entregues | Compilação do código |
| B - Sistema de validação | Códigos entregues | Compilação do código |
| C - Sistema de desafio | Códigos entregues | Compilação do código |
| IV - Testes | Código testado | Execução dos testes |
| V - Conclusão | Aplicação homologada | Testes de integração |

A tabela acima demonstra que para cada fase do projeto foram realizadas entregas e validações por meio de testes diversos, tais como: testes unitários das entregas, funcionais, não funcionais e e de integração de toda a aplicação.

### 6.5.5 Implementação

Este trabalho implementou um protótipo que foi desenvolvido na linguagem PHP (um acrônimo recursivo para PHP: Hypertext Preprocessor) que é uma linguagem de *script open source* de uso geral, muito utilizada, e especialmente adequada para o desenvolvimento *web*. A aplicação utilizou como entrada parâmetros que representam características

de um acesso. O acesso é concedido caso seja considerado legítimo pela aplicação que operacionaliza a autenticação por comportamento ou contexto. No entanto, diante de outra entrada em que as características sejam consideradas suspeitas ou fora dos padrões, o acesso não será permitido. Esses parâmetros de acessos serão as faixas dos endereços IP de origem e as tecnologias usadas nos dispositivos de acesso como navegadores e sistemas operacionais.

#### 6.5.5.1. Entrada de dados

Na aplicação implementada, o usuário deverá entrar com as credenciais de acesso (*login* e senha) e, por motivos de implementação e testes, campos adicionais foram incluídos para validar o modelo proposto, como a faixa de endereços IPs e o país de origem dessa faixa de endereços IPs. A aplicação identifica automaticamente o endereço IP de origem por meio de consulta a uma base de endereços IP de um site que referencia o bloco de IP informado a um determinado país ou região. Os endereços IPs válidos na rede mundial de computadores nos permitem identificar a área e o país de acesso, pois cada bloco de endereços IPs válidos é registrado para um determinado país, região ou sistema autônomo que pode ser de uma empresa ou universidade.

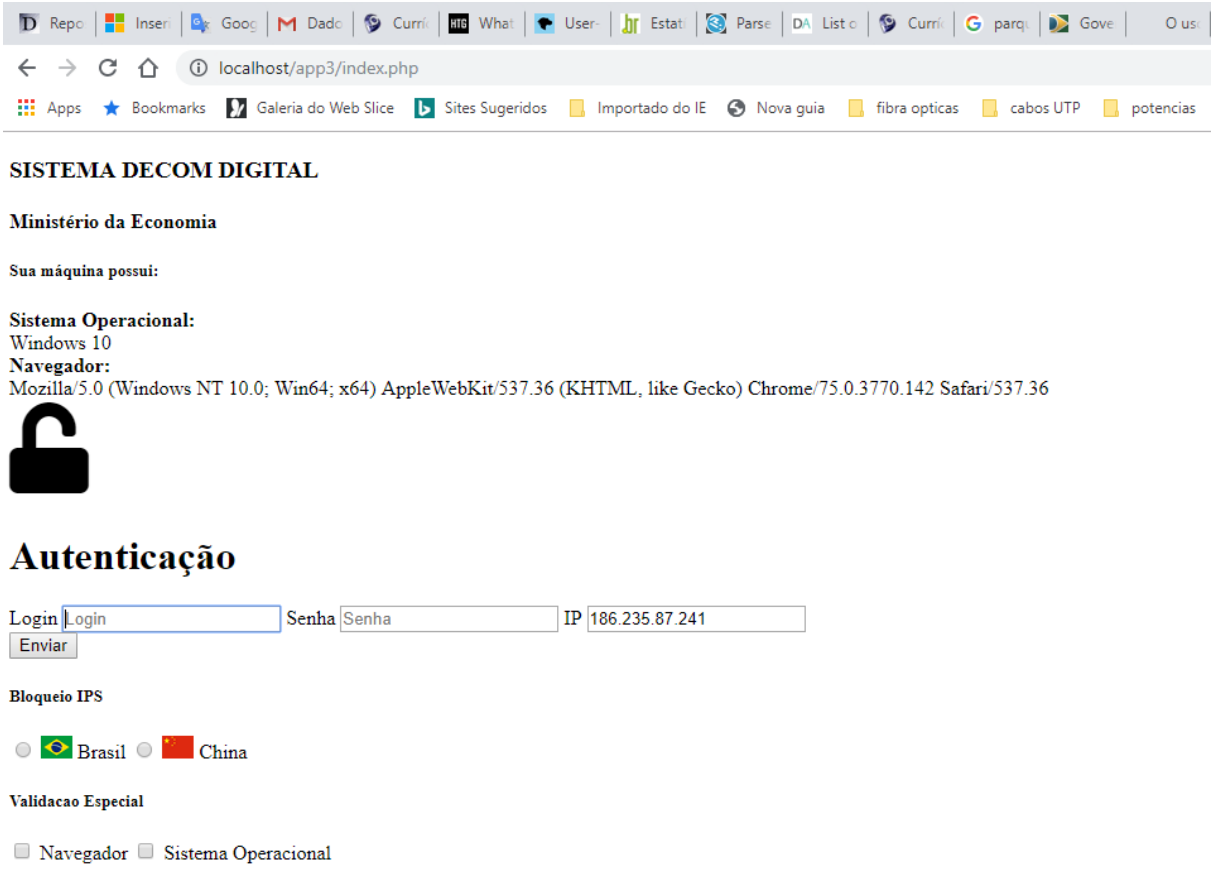


Figura 6.4: Tela inicial com campos para entrada de dados.

Na tela de entrada de dados acima são apresentados os campos para validação do acesso, como o usuário e a senha. De forma automática a aplicação detecta qual o endereço IP (endereço IP – *Internet Protocol*), sistema operacional e tipo de browser do dispositivo onde está sendo executada.

#### 6.5.5.2. Validação por endereço IP

No caso de validação por endereço IP originário de determinado país, é utilizada a base de dados do *site* `https://ipapi.com/` demonstrado na figura baixo, que a partir dos endereços IPs fornecidos pela aplicação que consome o serviço, retorna para aplicação o país de origem do endereço IP informado como entrada. Para o experimento utilizamos as faixas de endereços IPs da China e do Brasil para realizar a simulação.

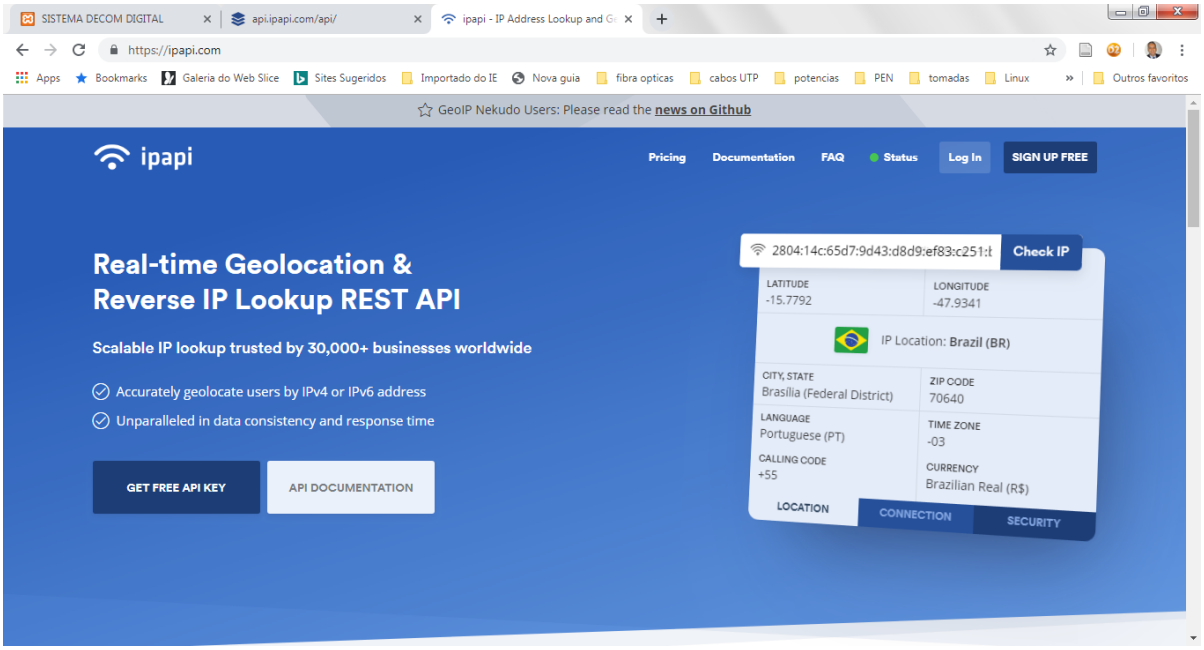


Figura 6.5: Tela de acesso da base de dados de IPs mundiais.

A aplicação realizará uma verificação pelo endereço IP detectado na máquina onde está sendo executada e o usuário poderá selecionar a faixa de endereços IPs do Brasil ou China para verificar a conformidade do acesso. Essa verificação é estática para o experimento, porém em um sistema mais complexo e robusto em ambiente de produção o controle deve ser baseado em perfis dinâmicos de acesso, para que a base seja dinâmica e constantemente atualizada a fim de analisar de forma efetiva os acessos de uma grande base de usuários do sistema. O experimento traz uma demonstração de como essa funcionalidade pode ser útil para a confiabilidade dos acessos, em razão de se tornar um dos fatores de autenticação que pode se correlacionar a outros fatores para a construção de um perfil ou "identidade eletrônica" daquela conta ou usuário. A partir dessa condição a aplicação pode fazer um bloqueio de acesso ao usuário, não permitindo então que ele acesse a aplicação. A aplicação faz uma verificação eletrônica de um, dois ou até três fatores, que são o bloco de endereço IP de origem, o sistema operacional e o browser do dispositivo de acesso, além do fator de autenticação simples que é de usuário e senha.

O trecho de código abaixo é o da função da aplicação proposta que identifica o endereço IP da máquina hospedeira a fim de servir como entrada para composição de perfil e para a verificação de acesso.

```
function get_client_ip() {
    $ipaddress = '';
    if (isset($_SERVER['HTTP_CLIENT_IP']))
        $ipaddress = $_SERVER['HTTP_CLIENT_IP'];
    else if(isset($_SERVER['HTTP_X_FORWARDED_FOR']))
        $ipaddress = $_SERVER['HTTP_X_FORWARDED_FOR'];
    else if(isset($_SERVER['HTTP_X_FORWARDED']))
        $ipaddress = $_SERVER['HTTP_X_FORWARDED'];
    else if(isset($_SERVER['HTTP_FORWARDED_FOR']))
        $ipaddress = $_SERVER['HTTP_FORWARDED_FOR'];
    else if(isset($_SERVER['HTTP_FORWARDED']))
        $ipaddress = $_SERVER['HTTP_FORWARDED'];
    else if(isset($_SERVER['REMOTE_ADDR']))
        $ipaddress = $_SERVER['REMOTE_ADDR'];
    else
        $ipaddress = 'UNKNOWN';

    return $ipaddress;
}
```

Figura 6.6: Função para coleta do endereço lógico (IP).

A função do código acima é utilizada em construções em PHP e coletam o IP do dispositivo do cliente ou do servidor *proxy* (procurador) que pode estar intermediando a conexão e armazena o resultado em uma variável chamada "*ipaddress*".

A aplicação validará o IP por país, no caso do experimento se restringe aos IPs do Brasil e China, coletando o IP do dispositivo de origem e comparando com o bloco de IP dos dois países.

O código abaixo demonstra a rotina que executa a comparação e verificação do fator, ou seja, se o IP de origem pertence ao bloco do Brasil ou China. Caso o acesso seja realizado de um dispositivo na faixa de IPs do Brasil e a opção de validação especial "Bloquear IPs do Brasil", for selecionada, a faixa se encontrará no escopo de bloqueio e o acesso será negado ou enviado o desafio.

```
1 if(isset($_POST['bloqueio'])){
2     if($_POST['bloqueio'] == 'china' || $_POST['bloqueio'] == 'brasil'){
3         $regiao = ipDetails($_POST['ip']);
4         if($_POST['bloqueio'] == 'brasil' && $regiao == 'Brazil'){
5             salvarLog('FALHA',$_POST['login'].' Range de IP encontrado no Bloqueio');
6             $tentativas++;
7         }
8
9         if($_POST['bloqueio'] == 'china' && $regiao == 'China'){
10            salvarLog('FALHA',$_POST['login'].' Range de IP encontrado no Bloqueio');
11            $tentativas++;
12        }
13    }
14 }
```

Figura 6.7: Função de bloqueio por IP.

Para verificar o bloco de endereço IP por país, a aplicação consulta uma base de um sítio da Internet que realiza esse serviço de verificação. Para isso no código acima é chamada na linha '3' uma função "*ipDetails*".

```
function ipDetails($ip){
    $url = 'http://api.ipapi.com/api/'.$ip.'?access_key=4e05f3abbc60e497db1734b3010f99eb';
    $content = json_decode(file_get_contents($url), true);
    return $content['country_name'];
}
```

Figura 6.8: Função de consulta ao país a partir do IP de origem.

O código da função "*ipDetails*" é demonstrado acima, ela recebe como parâmetro o IP do dispositivo de origem coletado e consulta o sítio do serviço de identificação de IPs para retornar o país de origem do acesso.

#### 6.5.5.3. Validação por navegador e sistema operacional

A aplicação utiliza informações do browser e sistema operacional utilizado para o acesso ao sistema com a finalidade de compor o perfil digital da conta ou usuário. Para realizar essa validação a aplicação utiliza o recurso *USER AGENT* dos *browsers*. Esse recurso disponibiliza uma cadeia de informações em formato de *string* que vão do tipo de *browser* e sua versão até o tipo de sistema operacional.

O *User Agent* é um cabeçalho do tipo HTTP (*Hyper Transfer Protocol*) que é enviado pelos *browsers* a uma aplicação e que serve como um fator de identificação único daquele *browser*, independentemente do tipo (*Mozilla, Chrome, Internet Explorer, Safari*, ...). Ele contém informações sobre o nome do seu navegador da *Web*, o sistema operacional, o tipo de dispositivo e muitas outras informações úteis.

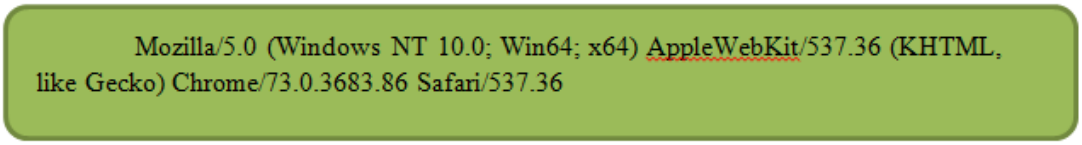


Figura 6.9: *String* do *USER AGENT*.

O *User Agent* acima informa que está sendo utilizado o browser Chrome na versão 73.*0.3683.86* em um sistema operacional *Windows* 10 de 64 *bits*.


Figura 6.10: Campos do *User Agent*.

Na figura acima são demonstrados os campos que formam a *string* do *User Agent*. O campo "*Mozilla*/5.0" é o token geral que diz que o navegador é compatível com o *Mozilla*, o que é comum a quase todos os navegadores atuais.

O campo "*platform*" descreve a sistema nativo em que o navegador está sendo executado (por exemplo, *Windows, Mac, Linux* ou *Android*) e se é ou não um *smartphone* por meio da indicação do tipo do equipamento. Os navegadores *Firefox* simplesmente dizem "*Mobile*"; a *web* é a plataforma. A plataforma pode ser constituída por vários *tokens* separados por ";"conforme a figura 6.9.

O campo "*rv: geckoversion*" indica a versão de lançamento do Gecko (como "17.0"). Nos navegadores recentes, o *geckoversion* é o mesmo que o *firefoxversion*. O campo "*Gecko / geckotrail*" indica que o navegador é baseado no *Gecko*. Na área de trabalho, o *geckotrail* é a *string* fixa "20100101". O campo "*Firefox / firefoxversion*" indica que o navegador é

*Firefox* e fornece a versão (como "17.0"), porém poderia ser *Chrome, Internet Explorer*, etc.

```
1 Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0)    Gecko/20100101 Firefox/47.0
2 Mozilla/5.0 (Macintosh; Intel Mac OS X x.y; rv:42.0) Gecko/20100101 Firefox/42.0
3 Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_1 like Mac OS X) AppleWebKit/603.1.30
(KHTML, like Gecko) Version/10.0 Mobile/14E304 Safari/602.1
```

Figura 6.11: *User Agent*.

Na figura acima o primeiro *User Agent* identifica um navegador *Mozilla*, em um sistema operacional *Windows* 64 *bits*. O *User Agent* seguinte identifica o *Mozilla* e o sistema operacional *Mac* e o terceiro *User Agent* demonstra um *IPhone* com sistema *Mac OS* e navegador *Mozila Firefox*.

O sítio `http://whatsmyuseragent.org/` pode ser usado para acessar as informações do *User Agent* do dispositivo. Caso as informações do dispositivo coincidirem com as do perfil armazenado na aplicação o acesso será liberado, caso contrário será bloqueado.

#### 6.5.5.4. Validação de acessos

A aplicação é executada para validação de acessos, primeiro ela realiza a validação do acesso simples que já existe no Sistema Decom Digital, que é a de usuário e senha. Caso essa primeira validação obtenha sucesso, a aplicação poderá realizar a validação correlacionando entre um e até três fatores, no caso a validação do bloco de endereço IP de origem entre IPs do Brasil e da China, validar o acesso a partir do navegador e do sistema operacional do dispositivo de acesso, seja apenas um desses fatores ou a correlação de dois ou três deles.

A aplicação armazena os parâmetros de acesso daquela conta que seria correspondente ao perfil dinâmico da própria conta de acesso. A partir desses parâmetros de IP, navegador e sistema operacional a aplicação pode validar ou não àquele acesso. Caso o acesso seja permitido, a aplicação disponibilizará a mensagem de sucesso e concederá o acesso, caso existam inconsistências entre os fatores de entrada do acesso e os que estão armazenados para a conta ou *login* correspondente, a aplicação realizará uma ação que pode ser o envio de um desafio para confirmação do acesso ou até o bloqueio imediato do acesso. Esse desafio é composto de perguntas para confirmação da legitimidade do acesso, caso as respostas correspondam as previamente cadastradas pelo usuário legítimo o acesso será liberado, caso contrário ocorrerá o bloqueio daquela tentativa de acesso.

```
if(isset($_POST['bloqueio_navegador'])){
if(trim($_POST['navegador']) != trim($navegador)){
redirect('bloqueio.php','Navegador Inválido');
}
}

if(isset($_POST['bloqueio_os'])){
if(trim($_POST['os']) != trim($os)){
redirect('bloqueio.php','Sistema Operacional Inválido');
}
}
```

Figura 6.12: Código de bloqueio de acesso a partir do sistema operacional e navegador.

O código da figura acima foi construído para a aplicação validar os atributos de navegador e sistema operacional por meio de uma função que chama outras funções que a responde com os parâmetros necessários para verificação do acesso. Primeiro o código compara o navegador armazenado pela aplicação com o retorno de uma função que captura o navegador do dispositivo de acesso e por meio dessa comparação libera ou não o acesso. Em seguida o código realiza o mesmo tipo de comparação para o sistema operacional.

Caso algum dos três parâmetros não seja atendido durante a verificação, o IP, o sistema operacional ou o navegador, a aplicação executará um desafio para confirmação do acesso, porém se mais de um desses parâmetros não seja atendido, a aplicação bloqueará imediatamente o acesso, pois pela regra de negócio implementada esse tipo de violação será considerado de um acesso ilegítimo. Esse desafio consiste no envio de perguntas a partir de um cadastro pré-definido quando da criação da conta de acesso, esse cadastro não faz parte do escopo da aplicação. As perguntas e respostas foram armazenadas na aplicação para realização do experimento, caso as respostas às perguntar coincidam com as respostas armazenadas pela aplicação o acesso será concedido, caso contrário o acesso será bloqueado pela aplicação.

O código abaixo é um trecho da implementação do desafio e compara as entradas fornecidas pelo usuário para confirmação da legitimidade do acesso, no caso o CPF e nome da cidade de nascimento da mãe, por meio da função "*POST*" para captura de dados de entrada. No caso de inconsistência das informações o acesso será negado por

meio da chamada ao programa “bloqueio.php” e será apresentada a mensagem de bloqueio na tela.

```
if(isset($_POST['CPF']) && isset($_POST['mae'])){
   if($_POST['CPF'] != $cpf || $_POST['mae'] != $cidade){
      redirect('bloqueio.php','Seu acesso foi negado, por favor contacte o administrador do sistema!');
   }
```

Figura 6.13: Código de verificação do desafio.

Na tela abaixo houve uma divergência no tipo do browser e foi executado o desafio com envio de perguntas para que o acesso possa ser validado:

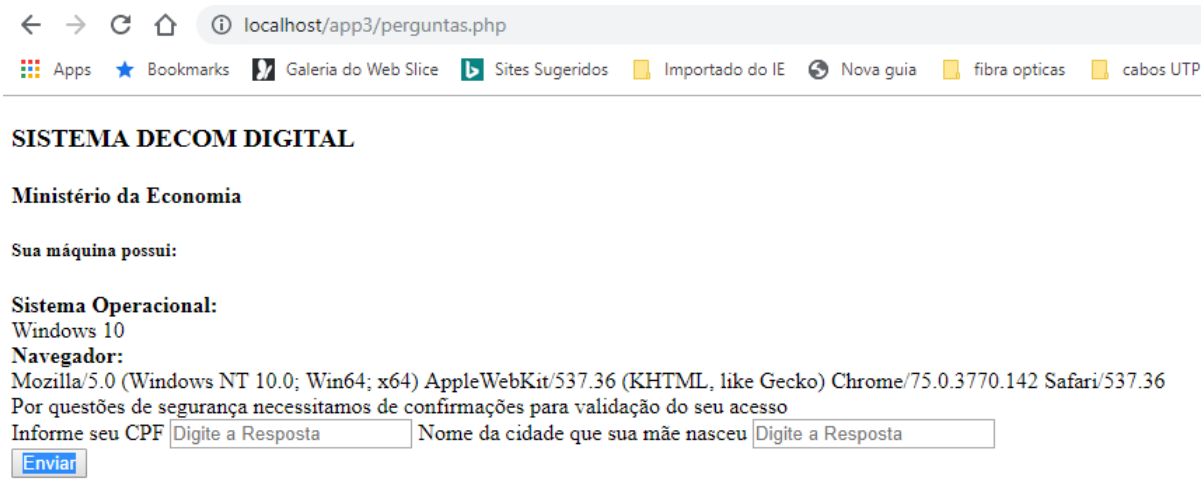


Figura 6.14: Tela de desafio.

A aplicação então simula a Autenticação por Contexto ou Comportamento de forma estática, validando acessos a partir de parâmetros pré-definidos com intuito de demonstrar como o risco de Acessos indevidos e vazamentos de informações do Sistema Decom Digital podem ser mitigados tecnologicamente. O tipo de comportamento pode explicitar o tipo de uso de cada usuário, criando um modelo comportamental para cada tipo de acesso. Na Autenticação por contexto ou comportamento o bloqueio diante de situações suspeitas pode não ser a primeira medida para impedir um possível acesso não legítimo ou suspeito, pode-se utilizar também a autenticação por conhecimento, onde perguntas são enviadas para a sessão que tenta obter o acesso, a partir de um cadastro prévio, como forma de comprovar a autencidade daquele acesso.

### 6.5.6 Validação do protótipo

A validação foi realizada por meio de simulações de tentativas de acessos e o resultado do processo de autenticação por contexto ou comportamento foi exibido em *logs* de acesso.

A aplicação apresentou logs de acesso e bloqueio conforme o caso. Com base nos requisitos definidos, é armazenado em um arquivo físico o processamento da informação em formato *LOG*. Com isso todo histórico e tratamento dos acessos podem ser armazenados e estarem passíveis de auditoria.

A aplicação ao ser executada cria um arquivo de *log* diário com os resultados das tentativas de *login*, onde informa se o acesso obteve sucesso ou falha.

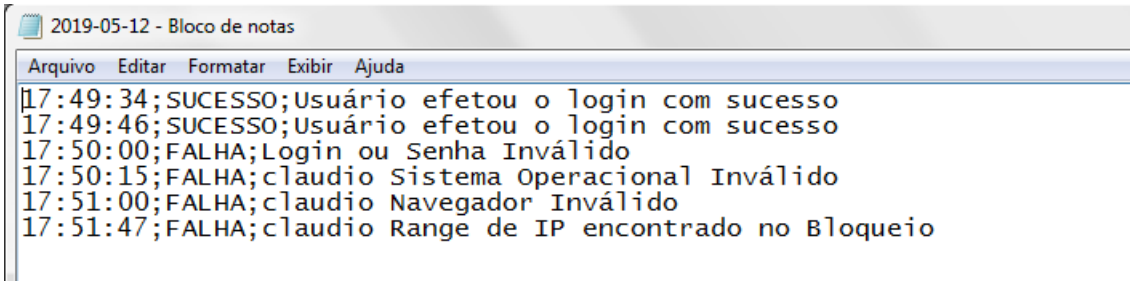


Figura 6.15: Arquivo de *log* com entradas de tentativas de acesso.

Na figura acima é exibido o arquivo de *log* diário da aplicação com as entradas contendo o horário da tentativa de acesso, o resultado da tentativa de acesso, em caso de falha qual a conta que tentou acessar o sistema e o registro do evento que ocorreu durante o acesso, ou seja, a liberação do *login* em caso de sucesso e em caso de falha qual o tipo de evento que ocorreu.

Nesse arquivo de *log*, nos dois primeiros registros o acesso foi permitido, pois as credenciais de acesso coincidiram com as armazenadas na aplicação. Nos demais registros ocorrerem bloqueios de acesso: no terceiro registro ocorreu o bloqueio por falha nas credenciais de login (usuário/senha), no registro seguinte ocorreu bloqueio por sistema operacional inválido, depois ocorreu bloqueio por inconsistência do navegador e por último por bloco de IP inconsistente com o perfil da conta.

#### 6.5.6.1. Testes do protótipo

Pode meio dos testes unitários funcionais, validou-se cada uma das funcionalidades solicitadas no documento de requisitos, e pela análise dos *logs* foi possível validar se a aplicação executa e apresenta os resultados para qual foi construída, e como resultado a validação foi positiva em todos os testes.

Foram realizados testes unitários de validação do acesso com usuário/senha, validação por meio do IP de origem, validação por meios do sistema operacional, validação pelo tipo

de navegador usando o User Agent e testes correlacionando de um a três desses fatores. Para validação forma utilizados os sistemas operacionais *Windows* nas versões 7, 8 e 10, os navegadores *Chrome* e *Mozilla* e os IPs do Brasil confrontados com os blocos do Brasil e China.

Os testes funcionais realizados envolveram também os testes de desafio, primeiramente com as condições para execução do desafio, a validação correta por meio das respostas tanto em caso de falha como sucesso, também foram realizados testes não funcionais onde foram testados a criação e as mensagens de log e as mensagens apresentadas nas telas.

(a) Experimento 1 (teste unitário 1)

Credenciais de login da conta usada no teste:

Usuário: claudio

Senha: 123456

No teste 1 o acesso foi concedido somente com a validação de fator único, no caso o usuário e a senha, pois as outras opções de validação especial não foram selecionadas. Como as credenciais foram digitadas corretamente o acesso foi liberado conforme figura abaixo:


Figura 6.16: Tela de Acesso liberado - Teste 1.

(b) Experimento 2 (teste unitário 2)

O usuário e a senha forma digitados incorretamente, então o acesso foi negado conforme figura abaixo:

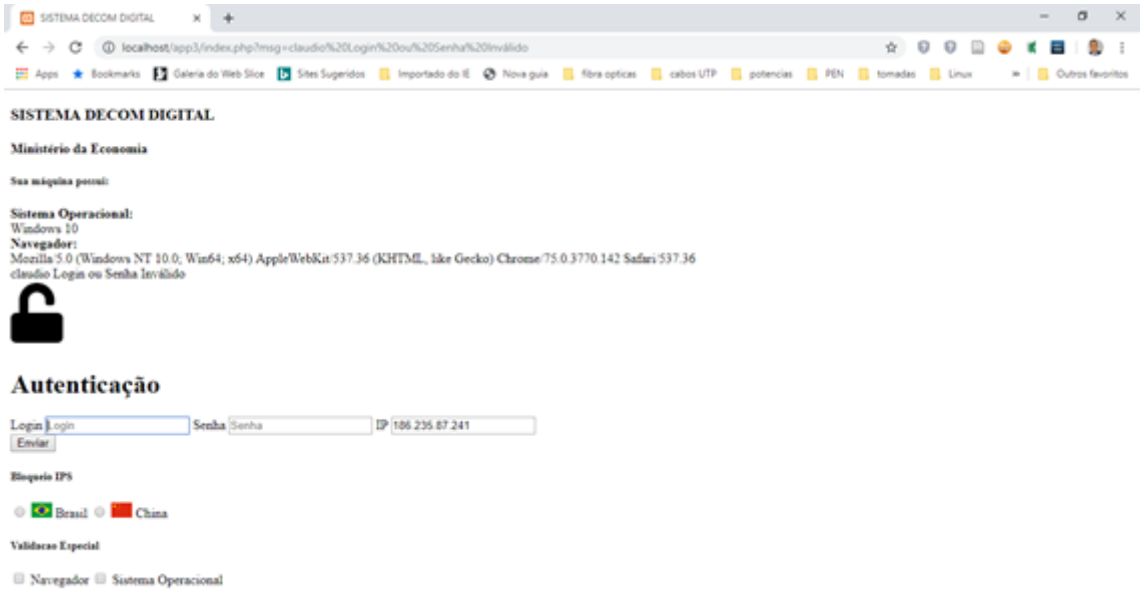


Figura 6.17: Tela de *login* ou senha inválido - Teste 2.

A aplicação retornou *Login* ou Senha inválida, pois a senha foi digitada incorretamente.

(c) Experimento 3 (teste unitário 3)

Nesse teste além das credencias de login digitadas corretamente foi selecionada a opção “Bloquear IPs do Brasil”, como o dispositivo de acesso está dentro da faixa de endereços do Brasil e ocorreu uma diferença no atributo de IPs o desafio é acionado. As respostas ao desafio foram incorretas e então o acesso foi bloqueado conforme figura abaixo:


Figura 6.18: Tela de bloqueio desafio - Teste 3.

As perguntas e respostas corretas para o desafio são as seguintes: “CPF: 59903660510” e “Cidade de nascimento de sua mãe: Itapetinga”.

(d) Experimento 4 (teste unitário 4)

Ao realizar o mesmo processo de *login* do experimento anterior e responder ao desafio corretamente, o acesso foi liberado.

(e) Experimento 5 (teste unitário 5)

Ao entrar com as credenciais corretas de acesso e selecionar “Bloquar IPs da China”, o acesso foi concedido, pois a faixa de IP do dispositivo é do Brasil e não está na faixa de bloqueio.

(f) Experimento 6 (teste unitário 6)

Ao entrar com as credenciais corretas de acesso e selecionar “Navegador” o desafio é acionado, pois as versões dos navegadores do dispositivo de acesso e a armazenada na aplicação são diferentes, conforme segue:

Sistema operacional: Windows 8.1
Navegador (o *user agent* abaixo corresponde ao Chrome versão 73)
Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/73.0.3683.103 Safari/537.36';

Figura 6.19: Perfil aplicação.

Sistema Operacional: Windows 10
Navegador (o *user agent* abaixo corresponde ao Chrome versão 75)
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/75.0.3770.142 Safari/537.36

Figura 6.20: Dispositivo de acesso.

Neste caso a versão do navegador do dispositivo de acesso é diferente da versão armazenada no perfil da conta na aplicação, com isso o acesso foi negado conforme a figura 6.21.

(g) Experimento 7 (teste unitário 7)

Ao entrar com as credenciais corretas e alterar o perfil na aplicação com as mesmas informações do dispositivo de acesso, o atributo de validação especial “Sistema Operacional” foi selecionado e o acesso foi liberado. O mesmo ocorreu ao selecionar simultaneamente os atributos “Sistema Operacional” e “Navegador”.

Os *logs* dos experimentos são demonstrados sequencialmente no arquivo abaixo:


Figura 6.21: *Logs* dos testes.

Após a finalização dos testes evidenciou-se que o protótipo atende aos requisitos elencados para sua construção e, com a exceção do perfil dinâmico de validação que não fez parte do escopo do protótipo e da transparência que no caso da simulação não é adequada para validação do experimento, cumpre o que se espera de uma tecnologia de autenticação baseada em contexto, validando os acessos não somente pela autenticação de usuário e senha, mas pela consistência das informações de perfil e contexto e com confirmações do sistema de desafio. Com isso, os controles passam a ser mais efetivos e o sistema de autenticação do SDD mais confiável.

## 6.6 Resultados da construção do protótipo

Nesta seção serão apresentados os resultados do protótipo construído e executado.

### 6.6.1 Validação da hipótese

A validação da hipótese que consiste no uso da GIA em particular a Autenticação por Contexto para tratar riscos de acessos indevidos e privilégios excessivos, foi possível por meio do experimento e construção da aplicação que demonstrou uma autenticação mais forte e de multifator, pois além de provar a identidade do usuário com o que ele sabe (senha, respostas a perguntas de um cadastro), também prova a identidade com o que ele possui, como o navegador e o sistema operacional do dispositivo de acesso.

O protótipo apresentou resultados que tornam o acesso mais confiável, pois testam se o acesso é legítimo a partir de outros fatores como o perfil da conta que está solicitando

o acesso. Com a autenticação por contexto ou conhecimento o Sistema Decom Digital poderá mitigar riscos de acessos indevidos a informações sensíveis e possíveis fraudes digitais que podem ser realizadas por meio de ataques de Engenharia Social e obtenção das credenciais do usuário. O sistema de autenticação não verifica somente as credenciais, mas também as características do perfil da conta que está solicitando o acesso.

A rotina pode ser perfeitamente adaptada ao Sistema Decom Digital que também é construído em linguagem PHP, usa o servidor de aplicação Apache e um sistema de autenticação simples com apenas um cadastro do usuário conforme documentação do sistema (Anexo I). Em relação ao PEAD, também é adaptável, já que o SSO foi construído na mesma a plataforma, com PHP e Apache. Os sistemas são dessa forma compatíveis tecnologicamente e a aplicação seria um módulo adicional de validação do acesso para o SDD, o que tornaria o sistema mais protegido contra tentativas de acessos ilegítimos. O código da aplicação construída pode substituir a função de autenticação do PEAD a partir do momento que funciona de forma dinâmica e o PEAD funciona somente com autenticação por usuário e senha e utilização de certificados digitais.

## 6.7 Modelo teórico para validação da proposta do trabalho

Nesta seção será apresentado um modelo teórico do trabalho e um modelo de validação teórico da proposta para resolver o problema de segurança do Sistema Decom Digital em ambiente de nuvem por meio da GIA e do protótipo implementado.

### 6.7.1 Modelo de análise teórico

A tabela abaixo demonstra um modelo de validação teórica para a proposta deste trabalho, que foi validado para uma perspectiva de usabilidade no órgão, relacionando premissas importantes com a teoria.

Tabela 6.4: Validação teórica da solução.

| Assunto | Referência | Autor, página |
|---|---|---|
| Autenticação de fator único é simples e fraca. | A abordagem de autenticação mais básica é a autenticação de fator único. O fator único de autenticação geralmente se baseia em uma senha estática e reutilizável (algo que o usuário sabe) em combinação com um ID de usuário. | [84], p. 84 |
| | Figura 5.2: Força de Autenticação de diferentes combinações de atributos de autenticação. | [113], p.81 |
| Autenticação forte | A autenticação multifatorial, também conhecida como autenticação forte, pode usar várias técnicas para verificar uma identidade. | [84], p. 81 |
| | Figura 5.2: Força de Autenticação de diferentes combinações de atributos de autenticação. | [113], p.81 |
| GIA é indicado para melhoria da gestão de acessos e identidades. | GIA é a coleção de processos e tecnologias usadas para gerenciar essas identidades digitais e acessos aos recursos fornecidos através delas. | [57], p. 36 |
| GIA é indicada para o tratamento de riscos de acessos indevidos e privilégios excessivos. | No gerenciamento de identidades e acessos (GIA), o comportamento do usuário é monitorado e analisado em relação aos direitos de acesso já estabelecidos, com o objetivo de identificar privilégios excessivos ou um acesso anormal. | [60], p.37 |
| Autenticação por Contexto é essencial para ambientes pervasivos. | ...autenticação sensível ao contexto, que utiliza a mudança de contexto para permitir a adaptação dos mecanismos de segurança baseada na situação atual, é essencial para prover segurança de forma efetiva para ambientes pervasivos. | [78], p. 87 |
| Autenticação por Contexto pode ser contínua...e funcionar sem hardware adicional | A autenticação por contexto ou por comportamento tem muitas vantagens [96], incluindo a capacidade de ser continuamente verificada sem o conhecimento do usuário e funcionar sem hardware adicional. | [115], p. 87 |

Tabela 6.5: Validação teórica da solução - continuação.

| Assunto | Referência | Autor, página |
|---|---|---|
| Quanto mais fatores utilizados, mais robusta é a autenticação do sistema. | Os métodos modernos de autenticação geralmente usam dois ou vários fatores de autenticação, em que diferentes fatores de pelo menos duas categorias são examinados para verificar a identidade de um usuário ou dispositivo - "quanto mais fatores empregados, mais robusta a autenticação do sistema | [75], p. 45 |
| GIA é indispensável para segurança em computação em nuvem | A segurança computacional se apresenta como um recurso indispensável para garantir o acesso em ambientes de Computação em Nuvem, e destaca à proteção à privacidade, já que os dados sensíveis passam a ficar sob custódia de terceiros. Nesse contexto, o gerenciamento de identidades cresce em importância conforme crescem os serviços que precisam utilizar autenticação e autorização para controlar o acesso de usuários. | [42], p 27 |

Na coluna “Assunto” da tabela 6.5, estão relacionadas as premissas relevantes para o trabalho, que confirmam por meio de publicação dos autores citados e pela extensa revisão de literatura realizada, as hipóteses e afirmações sobre o tema identificados por todo o trabalho. A coluna “Referência” apresenta os trechos de referências citadas no trabalho e a coluna “Autor, página” informa onde encontrar a referência no texto.

Por meio dessa tabela podemos validar as principais premissas sobre os diversos temas apresentados no trabalho, o que representa um fechamento da parte teórica deste trabalho.

### 6.7.2 Diagrama de validação teórica da proposta do trabalho

O diagrama abaixo relaciona e realiza uma validação teórica dos principais temas abordados no trabalho, evidenciando as premissas que servem para validar as hipóteses determinantes e as confirmações necessárias para aceitação dos resultados deste trabalho.

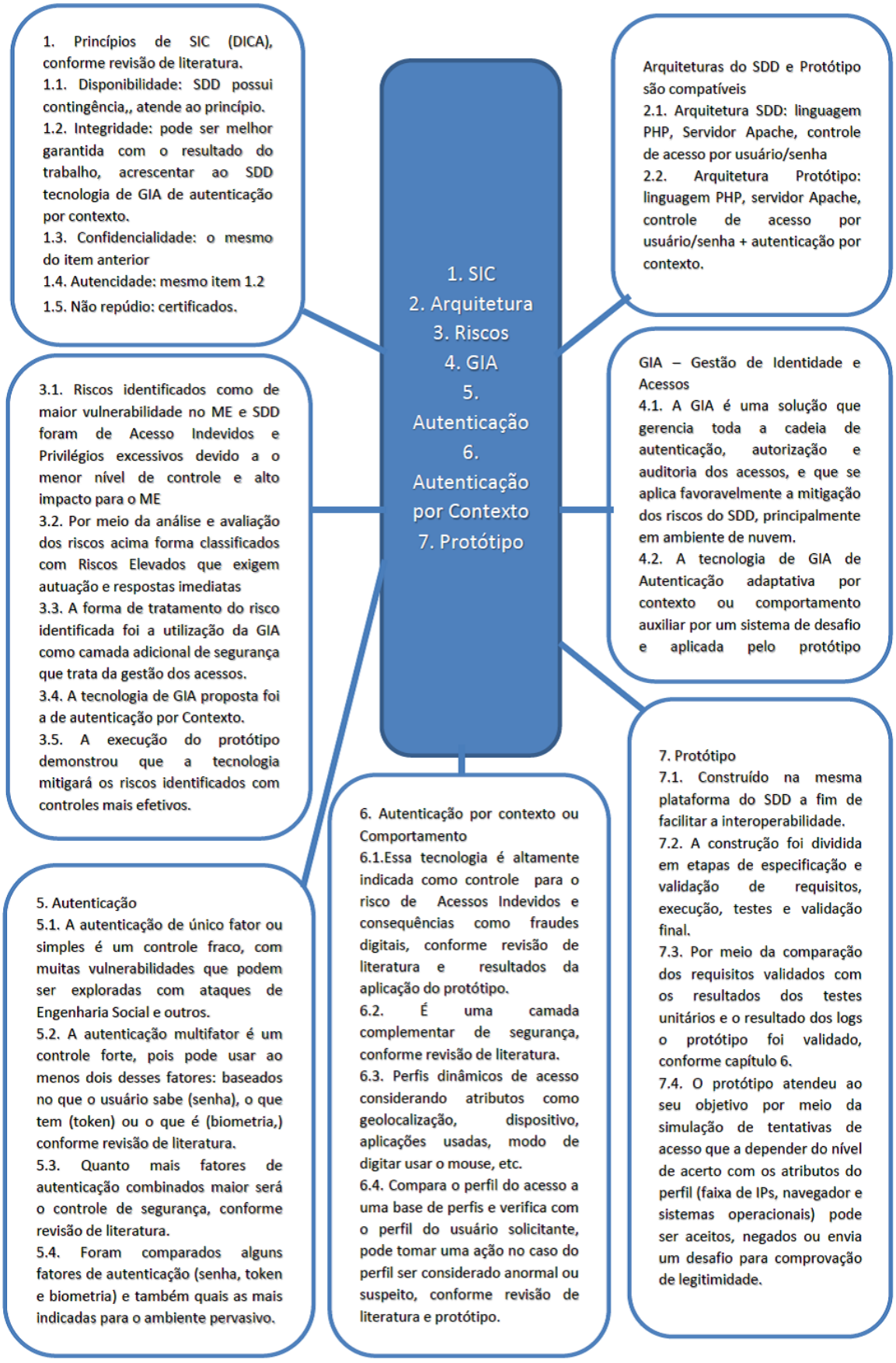


Figura 6.22: Validação teórica dos principais temas abordados no trabalho.

## 6.8 Conclusões do capítulo

A tecnologia sugerida para aplicação da GIA e mitigação dos riscos de acesso indevidos ao Sistema Decom Digital, que foi a autenticação por contexto ou comportamento, mostrou ser um controle essencial para esse risco, pois além de ser utilizada em conjunto com outras tecnologias de autenticação, utiliza em sua essência o contexto ou comportamento de uso de determinada conta de acesso para determinar se o acesso é legítimo ou pode ser considerado suspeito. A aplicação utilizada como experimento demonstrou que a autenticação por contexto cumpre a função de evitar acessos indevidos e consequências graves como o vazamento de informações e fraudes digitais.

A validação dos resultados foi possível devido ao *log* da aplicação e aos testes executados com diversos casos de uso. Ainda que a aplicação não funcione de forma dinâmica como se espera de uma aplicação de autenticação por contexto em ambiente de produção, ela pode fornecer resultados satisfatórios que indicam o uso da autenticação por contexto ou comportamento, independentemente de ser um experimento e funcionar com dados estáticos que simulam o comportamento em produção. Por meio dos *logs* gerados pela aplicação foram evidenciadas as negativas de acesso quando um dos dados de entrada para a validação do acesso era diferente dos atributos previamente cadastrados na aplicação que compõem o perfil de acesso do usuário, simulando dessa forma uma base de perfis de uma aplicação de autenticação por contexto em produção. Também foram validados e permitidos os acessos em que as credenciais de acesso coincidiam com os atributos previamente cadastrados na aplicação. Por meio dos *log* e testes foi possível verificar que quando um dos fatores de contexto era diferente dos atributos cadastrados na aplicação, um desafio de perguntas e respostas era enviado para o usuário e conforme exatidão da resposta em relação à base pré-cadastrada o acesso era permitido, caso contrário era bloqueado.

A aplicação também é tecnologicamente compatível com os sistemas SDD e o PEAD, pois suas arquiteturas são similares e compatíveis tecnologicamente, pois utilizam o mesmo ambiente computacional em nível físico (mesma arquitetura de dispositivos) ou lógico (mesmos servidores de aplicação e linguagem de desenvolvimento).

Dessa forma a solução de Gerenciamento de Identidade e Acessos foi aplicada computacionalmente por meio de simulações de acessos, confirmações, bloqueios e envio de desafios aos usuários, em um ambiente de experimento e simulação que demonstra uma maior proteção em relação ao risco de acessos indevidos que esse tipo de solução pode trazer às aplicações e em especial ao SDD. Foram validados os subsistemas de autenticação, validação e desafio que são parte da estrutura de uma solução de autenticação por contexto ou comportamento.

# Capítulo 7

# Conclusões e trabalhos futuros

Os resultados do trabalho serão apresentados neste capítulo por meio da demonstração das respostas ao objetivo geral e aos objetivos específicos.

A carteira de serviços digitais do Governo Federal se amplia cada vez mais e um dos objetivos do atual governo é o crescimento dos serviços digitais para o cidadão. Para que essa ação tenha sucesso muitas questões precisam de atenção ao transformar esses serviços em digitais, principalmente as relacionadas à Segurança da Informação e Comunicações (SIC). A razão é que o governo costumeiramente trata de dados que muitas vezes são de uma pessoa física, jurídica ou dados sensíveis do próprio governo ou em sua posse. Os sistemas eletrônicos do Governo Federal muitas vezes também fazem parte deste portfólio de serviços digitais e precisam estar conformes com as políticas e normas de segurança do DSIC da Presidência da República e de outros normativos de SIC, políticas de gestão de riscos dos órgãos, além da própria Lei Geral de Proteção aos Dados (LGPD) que passa a auditar os órgãos a partir do ano de 2020 em diversos aspectos, incluindo o de proteção tecnológica às informações sob a guarda desses órgãos.

Este trabalho destacou um dos sistemas do Ministério da Economia, o Sistema Decom Digital, que trata de informações e processos sigilosos das empresas, e realizou uma gestão de riscos considerando o aspecto das tecnologias e soluções de gestão de identidade e acessos em computação em nuvem. O Gerenciamento de Identidades e Acessos (GIA)) é um conjunto de métodos e tecnologias que pode ser utilizada para aumentar o nível de controle de segurança das aplicações e consequentemente mitigar os riscos de acesso indevidos e privilégios excessivos, seja em ambiente local e principalmente em ambiente de nuvem, este com mais atenção por ser um ambiente não controlado pela organização. Esses riscos caso materializados por meio da exploração de vulnerabilidades, como mecanismos de autenticação de fator único e ausência de tecnologias de GIA que possam validar os acessos com maior precisão, podem desencadear ações maliciosas como tentativas de fraudes digitais e vazamento de dados que podem comprometer todo um sistema por

meio do acesso a informações sigilosas e obtenção de privilégio de alteração das mesmas. Essas ações comprometem a integridade das informações e podem levar a uma perda de credibilidade da organização, no caso o Ministério da Economia.

O objetivo geral do trabalho foi atendido por meio da gestão de riscos do SDD em ambiente de computação em nuvem no âmbito da Gestão de Identidade e Acessos em conformidade com a política de gestão de riscos do Ministério e da Norma Complementar nº 14 do DSIC [13] que determina a realização de uma gestão de riscos ao tomar a decisão de levar sistemas e dados sensíveis para o ambiente de computação em nuvem (*cloud computing*), além da determinação institucional do Ministério que todo plano de ação ou projeto deve ser precedido de uma gestão de riscos. Essa política de gestão de riscos do órgão [31] é composta por regras gerais e específicas e por artefatos para atingimento dos objetivos e foi baseada no COSO ERM [28], essa política foi institucionalizada pela portaria nº 1.001 do extinto MDIC [31]. A gestão de riscos seguiu os preceitos da Norma ISO 31.010 [27] e de outros *frameworks* como o COSO ERM e a Metodologia de Gestão de Riscos do TCU. O processo de gestão de riscos dividiu-se em etapas, e por meio de respostas a alguns dos objetivos específicos foi implementado: estabelecimento do contexto interno e externo à organização, identificação, análise, avaliação e tratamento dos riscos.

O primeiro objetivo específico foi atendido por meio do estabelecimento do contexto interno e externo ao Ministério da Economia e que envolve os aspectos de segurança do Sistema Decom Digital no âmbito da Gestão de Identidade e Acessos. Demonstrou-se a estrutura da área de TIC do órgão e o seu nível de maturidade atual, políticas institucionais como a Política de Segurança da Informação e Comunicações (POSIC) e a política de Gestão de Riscos, Mapa Estratégico do órgão, planos como o PDTIC e documentos técnicos dos sistemas. No contexto externo foi demonstrada a situação da conformidade com as legislações de Segurança da Informação e Comunicações (SIC).

O segundo objetivo específico deste trabalho consistiu em realizar uma avaliação de riscos considerando a GIA para o SDD em ambiente de nuvem. Esse objetivo foi alcançado após a realização das três etapas desse processo de avaliação dos riscos: identificação, análise e avaliação dos riscos. Para realização da avaliação de riscos, a metodologia usada baseou-se no processo de avaliação de riscos do TCU, que por sua vez é baseado em importantes *frameworks* do mercado para Gestão de Riscos Corporativos, como o COSO ERM.

Na primeira etapa foram identificados os principais riscos por meio da identificação de ativos, ameaças, controles e vulnerabilidades existentes e consulta as partes interessadas, tais como: Comitê de Comitê de Segurança da Informação e Comunicações (CSIC) do órgão, servidores e especialistas em segurança da informação do órgão. A partir do levantamento dessas informações sobre os ativos foi possível identificar os principais riscos

para o SDD em ambiente de nuvem.

Para analisar os riscos identificados na etapa anterior definiu-se uma escala de probabilidade e impacto e foi produzida uma matriz de riscos. Para realizar a análise dos riscos alguns indicadores foram utilizados, como o Risco Inerente Identificado (RNI), Nível de Risco Inerente (NRI), Nível de Confiança (NC) e Risco de Controle (RC). A partir do cálculo desses indicadores foi possível avaliar de forma semi-quantitativa os riscos em uma escala de riscos com classificação de "baixo" até "elevado". O resultado da análise demonstrou que os riscos de "Acesso Indevidos" e "Privilégios Excessivos" são os mais relevantes e estão muito além do apetite de riscos do órgão e que por essa razão recomenda-se que sejam tratados e tenham uma atenção especial da organização.

A terceira etapa para atingir ao objetivo específico de avaliação dos riscos identificados e analisados nas etapas anteriores estabeleceu critérios de priorização e tratamento dos riscos e os associou ao indicador de nível de risco, calculado durante a etapa de análise de riscos, para determinar o apetite de risco e o grau de exposição ao risco do órgão e a ação recomendada para cada nível de risco. Nessa etapa também foi realizada a classificação dos riscos por meio do cálculo do Nível de Risco Inerente (NRI) que determina a relevância do risco para a organização, no caso do SDD os riscos de acesso indevidos e privilégios excessivos foram apontados como os de maior relevância.

Para atender ao terceiro objetivo específico foram identificadas as principais tecnologias de GIA e as opções para tratamento dos riscos mais relevantes para o SDD em ambiente de nuvem: risco de acessos indevidos e privilégios excessivos. Este trabalho relacionou e caracterizou as principais tecnologias de GIA e demonstrou as de maior aplicabilidade para tratamento dos riscos avaliados como mais significantes considerando o aspecto de gestão de identidade e acessos do SDD. A partir da pesquisa bibliográfica pôde-se constatar que a autenticação por comportamento ou sensível ao contexto é uma solução complementar as tecnologias de autenticação comumente usadas e que oferece um nível de controle apropriado para evitar fraudes digitais e vazamento de informações, portanto com condições de mitigar esses riscos.

Por fim, o último objetivo específico foi atendido por meio da preposição do uso da solução de Autenticação por Comportamento ou Contexto acoplada ao SDD funcionando como uma solução complementar para tratamento dos riscos identificados como de maior relevância considerando a gestão de acessos e identidades em um ambiente de computação em nuvem. Considerando-se que o SDD possui autenticação de fator único e para algumas transações a utilização de *tokens*, inserido o sistema no ambiente de computação pervasiva proposto, a Autenticação por Comportamento ou Contexto pode ser uma camada adicional de proteção ao mesmo. Como forma de demonstrar o funcionamento desta solução, foi construída uma aplicação que simula o comportamento de um sistema, no caso

o SDD, que funciona com autenticação simples e uma camada adicional de proteção. O funcionamento da aplicação demostrou que a partir de atributos que formam um determinado perfil de conta de acesso, as solicitações de acesso podem ser analisadas, permitidas, bloqueadas ou diante de uma transação considerada suspeita podem enviar desafios para confirmação da legitimidade do acesso. A aplicação foi desenvolvida para atender a esses requisitos e após a realização das simulações de acesso evidenciou-se por meio de *logs* das transações e dos testes realizados que ao dar entrada com atributos selecionados na tela: faixa endereço IP de origem, sistema operacional ou navegador, a aplicação comparou os dados de entrada com parâmetros prédeterminados relacionados àquela conta para classificar o acesso como legítimo ou suspeito. A aplicação concedeu acesso ao validar de forma positiva as informações de entrada e no caso de haver inconsistência entre dados de entrada e os atributos do perfil, o acesso foi considerado suspeito. Com intuito de validar o acesso foi enviado ao solicitante um desafio a partir de um cadastro na própria aplicação, caso as respostas demonstrassem conformidade com os atributos do perfil o acesso foi permitido, caso contrário o acesso foi bloqueado.

Demonstrou-se que a aplicação pode ser acoplada facilmente ao SDD, pois são tecnologicamente compatíveis, também se evidenciou o maior nível de controle de segurança na gestão de identidade e acessos, por meio da maior proteção que uma solução de Autenticação por Comportamento ou Contexto trará ao SDD, sobretudo quando o mesmo for utilizado em um ambiente pervasivo e de computação em nuvem.

Como trabalhos futuros recomenda-se o estudo de algoritmos de Inteligência Inteligência Artificial (IA) como os de *Machine Learning* ou outras soluções similares para habilitar a construção de um perfil dinâmico das contas de acesso a fim de implementar a solução de Autenticação por Comportamento e Contexto em um ambiente de produção, o que propiciará o controle de grandes bases de acessos, simultâneos ou não, com grau e nível de controles mais eficazes para esse tipo de ambiente.

Outra possibilidade de trabalho futuro é pesquisar a utilização da solução de Autenticação por Comportamento ou Contexto com outras solução de autenticação e com funções de autorização e auditoria, dessa forma a Gestão de Identidade e Acessos será implantada não somente para a fase de autenticação, mas também realizará uma análise, durante todo o acesso das transações do usuário (Autorização) e investigará na base de acesso os possíveis acessos fraudulentos para tomadas de decisões (Auditoria).

# Referências


[1] Brasil: *Decreto nº 9.745, de 8 de abril de 2019 – dispõe sobre a estrutura regimental do ministério da economia.*, abr 2019. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9745.htm. 1

[2] Brasil: *MinistÉrio da economia. governo digital.* https://www.governodigital.gov.br/. 1, 2, 9

[3] Negócios., Portal Revista Época: *Como a estônia construiu uma sociedade digital.* https://epocanegocios.globo.com/Tecnologia/noticia/2018/08/como-estonia-construiu-uma-sociedade-digital.html. 1

[4] ONU: *Organização das nações unidas. estudo sobre governo eletrônico das nações unidas.* https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_Portuguese.pdf. 1

[5] G1: *Estônia tem projeto pioneiro para acabar com a burocracia e facilitar a vida dos cidadãos.* https://g1.globo.com/fantastico/noticia/2018/11/18/estonia-tem-projeto-pioneiro-para-acabar-com-a-burocracia-e-facilitar-a-vida-dos
ghtml. 2

[6] Brasil: *MinistÉrio da economia. governo digital - segurança da informação.* https://www.governodigital.gov.br/transformacao/compras/orientacoes/seguranca-da-informacao. 2, 20

[7] Devmedia: *Governança de ti e cobit.* https://www.devmedia.com.br/governanca-de-ti-e-cobit/27577. 2

[8] COBIT5: *Modelo corporativo para governança e gestão de ti da organização.*, 2012. http://www.isaca.org/COBIT/pages/cobit-5.aspx. 2

[9] Symantec: *Relatório de crimes cibernéticos norton: O impacto humano.*, 2019. https://www.symantec.com/. 2, 9

[10] Digital, Folha: *Facebook anuncia vazamento de fotos de que afetou até 68 milhões de usuários.* https://www1.folha.uol.com.br/tec/2018/12/facebook-anuncia-vazamento-de-fotos-que-afetou-ate-68-milhoes-de-usuarios.shtml. 3

[11] MP/STI: *Portaria mp/sti nº 20, de 14 de junho de 2016, anexo. boas práticas, orientações e vedações para contratação de serviços de computação em nuvem.*, jun 2016. https://www.governodigital.gov.br/documentos-e-arquivos/Orientacao%20servicos%20em%20nuvem.pdf/view. 4

[12] Wang, Heyong, Wu He e Feng-Kwei Wang: *Enterprise cloud service architectures.* Information Technology and Management, 13(4):445–454, 2012. https://doi.org/10.1007/s10799-012-0139-4. 4, 22

[13] Brasil: *Pesidência da república. nc 14 – norma complementar 14 - diretrizes relacionadas à segurança da informação e comunicações para o uso de computação em nuvem nos órgãos e entidades da administração pública federal*, mar 2018. 4, 5, 22, 55, 58, 59, 136

[14] Alkhalil, Adel, Reza Sahandi e David John: *Migration to cloud computing: a decision process model.* Central European Conference on Information and Intelligent Systems, 2014. 5

[15] Badger, Lee, Tim Grance, Robert Patt-Corner, Jeff Voas *et al.*: *Cloud computing synopsis and recommendations.* NIST special publication, 800:146, 2012. 5, 22, 86, 92, 98

[16] Brasil: *Decreto nº 8.135, de 4 de novembro de 2013. dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.*, mai 2018. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d8135.htm. 8

[17] Brasil: *Ministério da indústria, comércio exterior e serviços.* http://mdic.gov.br/. 8, 56, 61

[18] UOL, Portal: *Vazamento de dados cresce e já é 2º maior ataque digital ao governo federal.* https://www.bol.uol.com.br/noticias/2019/06/16/vazamento-de-dados-cresce-e-ja-e-2-maior-ataque-digital-ao-governo-federal.htm. 8

[19] ABIN: *Proteção de conhecimentos sensíveis e sigilosos.*, 2017. http://www.abin.gov.br/conteudo/%20uploads/2015/05/Prot-Conhec-Sens-e-Sigilosos-jan17.pdf. 8

[20] Brasil: *Lei nº 12.527, de 18 de novembro de 2011. lei de acesso a informação.*, nov 2011. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. 8, 9

[21] Brasil: *Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção aos dados.*, ago 2018. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. 9, 17, 55, 59

[22] MARIANO, Ari Melo e Maíra Santos ROCHA: *Revisão da literatura: Apresentação de uma abordagem integradora.* Em *XXVI Congreso Internacional de la Academia Europea de Dirección y Economía de la Empresa (AEDEM), Reggio Calabria*, volume 26, 2017. 11

[23] Gil, Antonio Carlos: *Métodos e técnicas de pesquisa social.* 6. ed. Ediitora Atlas SA, 2008. 12, 13

[24] Marconi, Marina de Andrade e Eva Maria Lakatos: *Fundamentos de metodologia científica.* 5. ed.-São Paulo: Atlas, 2003. 12

[25] Github: *Github development platform..* `https://github.com/`. 13

[26] ISO, ABNT ABNT NBR: *Iec 31000-2009: Gestão de riscos-princípios e diretrizes.* norma técnica. Technical report, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, Rio de Janeiro, Brasil, 39(4):2, 2009. 16, 26, 27, 32, 54, 55, 59, 63, 64, 67, 70, 73

[27] ISO, ABNT ABNT NBR: *Iec 31010-2012: Gestão de riscos-técnicas para o processo de avaliação de riscos.* ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 46, 2012. 16, 17, 18, 26, 27, 54, 55, 59, 62, 74, 136

[28] COSO, ERM: *Enterprise risk management. integrating with strategy and performance*, 2017. `https://www.coso.org/Pages/default.aspx`. 16, 54, 63, 136

[29] EU, UNIÃO EUROPÉIA: *Gdpr - general data protection regulation, eu.* `https://eur-lex.europa.eu/eli/reg/2016/679/oj`. 17

[30] ABNT, AB de NT: *Nbr iso/iec 27005–tecnologia da informação–técnicas de segurança–gestão de riscos de segurança da informação.* Rio de Janeiro: ABNT, 2008. 18, 59

[31] Brasil: *MinistÉrio da indÚstria, comÉrcio exterior e serviÇos. portaria nº 1.001, de 30 de junho de 2017. política de gestão de riscos do mdic.*, jun 2017. `http://www.lex.com.br/legis_27460575_PORTARIA_N_1001_SEI_DE_30_DE_JUNHO%20DE_2017.aspx`. 18, 19, 54, 57, 58, 59, 136

[32] ISO, ISO e IEC Std: *Iso 27002: 2005.* Tecnologia da Informação – Técnicas de Segurança – Código de práticas para a Gestão da Segurança da Informação. ISO, 2005. 19

[33] Brasil: *Decreto nº 9.637, de 26 de dezembro de 2018. política nacional de segurança da informação.*, dez 2018. `http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm#art22`. 20

[34] Brasil: *Gabinete de segurança institucional da presidência da república. departamento de segurança da informação e comunicações – dsic.* `http://dsic.planalto.gov.br/assuntos/missao-do-dsic`. 21

[35] Brasil: *Portaria 09, gsi, de 09 de março de 2018, nc14 in01. estabelece princípios, diretrizes e responsabilidades relacionados à segurança da informação (si) para o tratamento da informação em ambiente de computação em nuvem.*, mar 2018. http://dsic.planalto.gov.br/assuntos/editoria-c/documentos-pdf-1/portaria-09-gsi-de-9-de-marco-de-2018-nc-14-in01-computacao-em-nuvem.pdf/view. 21

[36] Microsoft, Azure: *O que é computação em nuvem?* https://azure.microsoft.com/pt-br/overview/what-is-cloud-computing/. 21

[37] CSA, Cloud Security Alliance: *Security guidance for critical areas of focus in cloud computing v 4.0. cloud security alliance's security guidance for critical areas of focus in cloud computing v4.0.*, feb 2017. https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL-feb27-18.pdf. 22, 25

[38] Sandholm, Thomas e Dongman Lee: *Notes on cloud computing principles.* J. Cloud Computing, 3:21, 2014. https://doi.org/10.1186/s13677-014-0021-5. 22

[39] Marston, Sean, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang e Anand Ghalsasi: *Cloud computing - the business perspective.* Decision Support Systems, 51(1):176–189, 2011. https://doi.org/10.1016/j.dss.2010.12.006. 23

[40] Castro, Rita de CC de e Verônica L Pimentel de Sousa: *Segurança em cloud computing: Governança e gerenciamento de riscos de segurança.* 2010. 24

[41] ISACA, An: *Cloud computing: Business benefits with security, governance and assurance perspectives*, 2009. 24

[42] BATISTA NETO, Luiz Aurélio *et al.*: *Um mecanismo de integração de identidades federadas entre shibboleth e simplesamlphp para aplicações de nuvens.* 2014. 25, 49, 132

[43] Risk, Certified in e Information Systems Controls CRISK: *Apostila de gerenciamento de riscos preparatório para a certificação isaca.* http://www.isaca.org/chapters9/Brasilia/Certification/Pages/Page4.aspx?utm_referrer=direct%2Fnot%20provided. 26, 67

[44] TCU, Brasil: *Avaliação de maturidade da gestão de riscos do tcu.*, 2018. https://portal.tcu.gov.br/biblioteca-digital/gestao-de-riscos-avaliacao-da-maturidade.htm. 26, 27, 28, 29, 31, 63, 64

[45] União TCU, Tribunal de Contas da: *Acordão 1.739/2015-tcu-plenário. dispõe sobre identificação de riscos relevantes e contratações de serviços de tecnologia da informação, sob o modelo de computação em nuvem.*, jun 2018. https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/destaques/. 26, 55

[46] TCU: *Manual de gestão de riscos do tcu.*, 2018. https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/. 27, 32, 33, 35, 54, 63, 73

[47] Treadway Commission COSO, Committee of Sponsoring Organizations of the: *Gerenciamento de riscos corporativos - estrutura integrada.*, 2017. https://m.isaca.org/Knowledge-Center/Standards/Documents/1202_std_Portuguese_1113.pdf. 29, 32, 78

[48] Avalos, José Miguel Aguilera: *Auditoria e gestão de riscos.* Instituto Chiaventato - São Paulo: Saraiva, 2009. 30, 32

[49] Dantas, José Alves, Fernanda Fernandes Rodrigues, Gileno Fernandes Marcelino e Paulo Roberto Barbosa Lustosa: *Custo-benefício do controle: proposta de um método para avaliação com base no coso.* Revista Contabilidade, Gestão e Governança, 13(2), 2010. 32

[50] ISACA: *Avaliação de riscos no planejamento.* 32, 104

[51] MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO Brasil: *Guia de orientação para o gerenciamento de riscos. secretaria de gestão pública. departamento de inovação e melhoria da gestão. gerência do programa gespÚblica.*, 2013. http://www.gespublica.gov.br/content/guia-de-orienta%C3%A7%C3%A3o-para-o-gerenciamento-de-riscos. 33, 63, 73

[52] UK, Gov: *Risk management assessment framework: a tool for departaments.*, 2009. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191516/Risk_management_assessment_framework.pdf. 33

[53] EFQM: *Excellence model.*, 2013. https://www.efqm.org/index.php/efqm-model-2013/download-your-free-copy/. 33

[54] Canada: *Secretaria do conselho do tesouro do canadá. framework for the management of risk.*, 2010. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422&section=text&id=19422&section=text. 33, 34

[55] UK, Reino Unido: *Hm treasury. management of risk - principles and concepts - the orange book.*, 2004. 34, 54, 63

[56] TCU: *Análise swot e diagrama de verificação de risco aplicados em auditoria.*, 2010. http://www.tcu.gov.br. 35

[57] Benantar, Messaoud: *Access control systems: security, identity management and trust models.* Springer Science & Business Media, 2005. 35, 131

[58] Hovav, Anat e Ron Berger: *Tutorial: identity management systems and secured access control.* Communications of the Association for Information Systems, 25(1):42, 2009. 35

[59] Bussa, T, Avivah Litan e T Phillips: *Market guide for user and entity behavior analytics*. 2018. 35

[60] Care, Phillips Jotathan e Tricia: *Market guide for online fraud detection.* jan 2018. 35, 36, 37, 131

[61] Sharma, Deepak H, CA Dhote e Manish M Potey: *Identity and access management as security-as-a-service from clouds*. Procedia Computer Science, 79:170–174, 2016. 36

[62] Khansa, Lara e Divakaran Liginlal: *Regulatory influence and the imperative of innovation in identity and access management*. Information Resources Management Journal (IRMJ), 25(3):78–97, 2012. 36

[63] Dlamini, Mloses T, Jan HP Eloff e Mariki M Eloff: *Information security: The moving target*. computers & security, 28(3-4):189–198, 2009. 37, 38

[64] Khansa, Lara: *M&as and market value creation in the information security industry.* Journal of Economics and Business, 82:113–134, 2015. 37, 38

[65] Bhargav-Spantzel, Abhilasha, Jan Camenisch, Thomas Gross e Dieter Sommer: *User centricity: a taxonomy and open issues*. Journal of Computer Security, 15(5):493–527, 2007. 38

[66] Wangham, Michelle S, Emerson Ribeiro de Mello, Davi da Silva Böger, Marlon Guerios e Joni da Silva Fraga: *Gerenciamento de identidades federadas*. Minicurso-SBSeg 2010-Fortaleza-CE, 2010. 39

[67] Brown, Lawrie e William Stallings: *Segurança de computadores: princípios e práticas*. Elsevier Brasil, 2014. 41

[68] Diógenes, Yuri e Daniel Mauser: *Security+: da prática para o exame*. Novaterra Editora e Distribuidora LTDA, 2013. 41

[69] Masha Garibyan, Simon McLeish e John Paschoud: *Access and identity management for libraries controlling access to online information.*, 2014. `http://www.facetpublishing.co.uk/`. 41

[70] CSA, Cloud Security Alliance: *Identity and access management - secaas implementation guidance.*, 2012. `https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf`. 42, 47, 51, 52, 53

[71] Felix Gaehtgens, Ant Allan, Jonathan Care: *Identity and access management primer for 2019.*, 2019. 42

[72] Stallings, William: *Criptografia e segurança de redes. princípios e práticas*, 2015. 42

[73] Allan, Ant.: *Iam leader's guide to user authentication.* fev 2018. 43

[74] Garibyan, Masha, John Paschoud e Simon McLeish: *Access and identity management for libraries: controlling access to online information*. Facet Publishing, 2014. 43

[75] Grassi, Paul A, Paul A Grassi, Michael E Garcia e James L Fenton: *Digital Identity Guidelines: Revision 3*. US Department of Commerce, National Institute of Standards and Technology, 2017. 43, 132

[76] Shepherd, SJ: *Continuous authentication by analysis of keyboard typing characteristics*. 1995. 44

[77] Wangham, Michelle Silva, André Marins, Carlos AG Ferraz, Carlos E da Silva, Debora CM Saade, Edelberto F Silva, Emerson Ribeiro de Mello, Fábio B de Oliveira, Flávio Luiz Seixas e Leonardo B Oliveira: *O futuro da gestão de identidades digitais*. Em *Anais Estendidos do XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, páginas 146–166. SBC, 2018. 44

[78] Johnson, Gleneesha M: *Towards shrink-wrapped security: A taxonomy of security-relevant context*. Em *2009 IEEE International Conference on Pervasive Computing and Communications*, páginas 1–2. IEEE, 2009. 44, 47, 88, 131

[79] Malek, Behzad, Ali Miri e Ahmed Karmouch: *A framework for context-aware authentication*. 2008. 44, 88

[80] Sathish Babu, B e Pallapa Venkataram: *A dynamic authentication scheme for mobile transactions*. International Journal of Network Security, 8(1):59–74, 2009. 44, 45, 46, 88, 113

[81] Saha, Debashis e Amitava Mukherjee: *Pervasive computing: a paradigm for the 21st century*. Computer, 36(3):25–31, 2003. 44

[82] IBM: *Computação pervasiva*. `https://www.ibm.com/support/knowledgecenter/pt/ssw_ibm_i_72/rzahg/rzahgebpervasive.htm`. 44

[83] Computerworld: *Forget two factor authentication, here comes context aware authentication*. `https://www.computerworld.com/article/3105866/forget-two-factor-authentication-here-comes-context-aware-authentication.html`. 45

[84] Osmanoglu, Ertem: *Identity and Access Management: Business Performance Through Connected Intelligence*. Newnes, 2013. 46, 48, 49, 80, 81, 82, 84, 85, 86, 91, 131

[85] Shrestha, Babins, Nitesh Saxena, Hien Thi Thu Truong e N Asokan: *Drone to the rescue: Relay-resilient authentication using ambient multi-sensing*. Em *International Conference on Financial Cryptography and Data Security*, páginas 349–364. Springer, 2014. 46

[86] Xiao, Liang, Qiben Yan, Wenjing Lou, Guiquan Chen e Y Thomas Hou: *Proximity-based security techniques for mobile users in wireless networks*. IEEE Transactions on Information Forensics and Security, 8(12):2089–2100, 2013. 46

[87] Gu, Zhonglei e Yang Liu: *Scalable group audio-based authentication scheme for iot devices*. Em *2016 12th International Conference on Computational Intelligence and Security (CIS)*, páginas 277–281. IEEE, 2016. 46

[88] Han, Jun, Albert Jin Chung, Manal Kumar Sinha, Madhumitha Harishankar, Shijia Pan, Hae Young Noh, Pei Zhang e Patrick Tague: *Do you feel what i hear? enabling autonomous iot device pairing using different sensor types*. Em *2018 IEEE Symposium on Security and Privacy (SP)*, páginas 836–852. IEEE, 2018. 46

[89] Covington, Michael J, Manoj R Sastry e Deepak J Manohar: *Attribute-based authentication model for dynamic mobile environments*. Em *International Conference on Security in Pervasive Computing*, páginas 227–242. Springer, 2006. 47

[90] Zhou, Kai e Jian Ren: *Passbio: Privacy-preserving user-centric biometric authentication*. IEEE Transactions on Information Forensics and Security, 13(12):3050–3063, 2018. 47

[91] Qin, Weijun, Daqing Zhang, Yuanchun Shi e Kejun Du: *Combining user profiles and situation contexts for spontaneous service provision in smart assistive environments*. Em *International Conference on Ubiquitous Intelligence and Computing*, páginas 187–200. Springer, 2008. 47

[92] Rocha, Cristiano Cortez da *et al.*: *Uma arquitetura para autenticação sensível ao contexto baseada em definições comportamentais*. 2012. 47, 105, 114

[93] Hulsebosch, RJ, Mortaza S Bargh, Gabriele Lenzini, PWG Ebben e Sorin M Iacob: *Context sensitive adaptive authentication*. Em *European Conference on Smart Sensing and Context*, páginas 93–109. Springer, 2007. 48

[94] Krutz, Ronald L, Russell Dean Vines e Glenn Brunette: *Cloud security: A comprehensive guide to secure cloud computing*. Wiley Indianapolis, 2010. 48

[95] Barreto, Luciano *et al.*: *Controle de autenticação tolerante a intrusões em federações de clouds*. 2017. 49

[96] Gaedke, Martin, Martin Gaedke, Johannes Meinecke e Martin Nussbaumer: *A modeling approach to federated identity and access management*. Em *Special interest tracks and posters of the 14th international conference on World Wide Web*, páginas 1156–1157. ACM, 2005. 49, 50, 52

[97] Silva, Edelberto Franco, Débora Christina Muchaluat-Saade e Natalia Castro Fernandes: *Across: A generic framework for attribute-based access control with distributed policies for virtual organizations*. Future Generation Computer Systems, 78:1–17, 2018. 51

[98] Chadwick, David W: *Federated identity management*. Em *Foundations of security analysis and design V*, páginas 96–120. Springer, 2009. 51

[99] Maler, Eve e Drummond Reed: *The venn of identity: Options and issues in federated identity management*. IEEE Security & Privacy, 6(2):16–23, 2008. 53

[100] De Mello, Emerson Ribeiro, Michelle S Wangham, Joni da Silva Fraga, Edson T De Camargo e Davi da Silva Böger: *A model for authentication credentials translation in service oriented architecture*. Em *Transactions on Computational Science IV*, páginas 68–86. Springer, 2009. 53

[101] Brasil: *MinistÉrio da indÚstria, comÉrcio exterior e serviÇos. plano diretor de tecnologia da informação e comunicações - pdtic 2017/2019 do mdic.*, out 2016. http://www.mdic.gov.br/images/PDTIC_MDIC_2017-19.pdf. 57, 59

[102] ITIL: *Infrastructure technology information library.* https://www.axelos.com/best-practice-solutions/itil. 57

[103] Brasil: *MinistÉrio da indÚstria, comÉrcio exterior e serviÇos. política de segurança da informação e comunicações do ministério da indústria, comércio exterior e serviços (posic/mdic).*, dez 2016. http://www.mdic.gov.br/images/POSIC-MDIC.pdf. 57, 58, 59

[104] Brasil: *MinistÉrio da indÚstria, comÉrcio exterior e serviÇos. planejamento estratégico.* http://www.mdic.gov.br/images/REPOSITORIO/institucional/Gest%C3%A3o_Estrat%C3%A9gica/Planejamento_Estrat%C3%A9gico_Brochura.pdf. 59

[105] Brasil: *Procedimentos administrativos relativos à investigação e à aplicação de medidas antidumping.*, jul 2013. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d8058.htm. 60

[106] Brasil: *MinistÉrio da indÚstria, comÉrcio exterior e serviÇos. sistema decom digital.* http://www.mdic.gov.br/index.php/comercio-exterior/defesa-comercial/849-sistema-decom-digital. 60

[107] Brasil: *Instrução normativa conjunta nº 1, de 10 de maio de 2016.*, mai 2016. http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/21519355/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197. 63

[108] Brasil: *Decreto nº 9.203, de 22 de novembro de 2017 – dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.*, nov 2017. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/D9203.htm. 64

[109] Treadway Commission COSO, Committee of Sponsoring Organizations of the: *Gerenciamento de riscos corporativos - estrutura integrada.*, 2017. https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf. 70, 73

[110] Brasil: *MinistÉrio da transparÊncia e controladoria-geral da uniÃo - cgu. metodologia de gestão de riscos.*, 2018. http://www.cgu.gov.br/Publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf. 73, 78

[111] Dempsey, Kelley, Nirali Shah Chawla, Arnold Johnson, Ronald Johnston, Alicia Clay Jones, Angela Orebaugh, Matthew Scholl e Kevin Stine: *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations: National Institute of Standards and Technology Special Publication 800-137*. CreateSpace Independent Publishing Platform, 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf. 75

[112] IBGC: *Guia de orientação para gerenciamento de riscos corporativos*. Instituto Brasileiro de Governança Corporativa, 2007. 76

[113] Allan, A.: *Defining authentication strength is not as easy.*, mar 2018. https://www.gartner.com/guest/purchase/registration?resId=1796018&srcId=1-3478922230. 84, 131

[114] Saini, Baljit singh, Navdeep Kaur e Kamaljit Bhatia: *Authenticating mobile phone user using keystroke dynamics*. International Journal of Computer Sciences and Engineering, 6:372–377, dezembro 2018. 84

[115] Saevanee, Hataichanok, Nathan L. Clarke e Steven M. Furnell: *Multi-modal behavioural biometric authentication for mobile devices*. Em *Information Security and Privacy Research - 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings*, páginas 465–474, 2012. https://doi.org/10.1007/978-3-642-30436-1_38. 89, 131

[116] Ashibani, Yosef e Qusay H. Mahmoud: *A behavior profiling model for user authentication in iot networks based on app usage patterns*. Em *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, October 21-23, 2018*, páginas 2841–2846, 2018. https://doi.org/10.1109/IECON.2018.8592761. 89

[117] Ashibani, Yosef e Qusay H Mahmoud: *A user authentication model for iot networks based on app traffic patterns*. Em *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, páginas 632–638. IEEE, 2018. 89

[118] Benzekki, Kamal, Abdeslam El Fergougui e Abdelbaki ElBelrhiti ElAlaoui: *A context-aware authentication system for mobile cloud computing*. Procedia Computer Science, 127:379–387, 2018. 90

[119] Howlett, Josh, Sam Hartman, Hannes Tschofenig e Jim Schaad: *Application bridging for federated access beyond web (ABFAB) architecture*. RFC, 7831:1–46, 2016. https://doi.org/10.17487/RFC7831. 92

[120] Revar, Ashish G e Madhuri D Bhavsar: *Securing user authentication using single sign-on in cloud computing*. Em *2011 Nirma University International Conference on Engineering*, páginas 1–4. IEEE, 2011. 93

[121] AZURE: *How hybrid identity allows digital transformation.* https://resources.office.com/ww-landing-M365E-EMS-IDAM-Hybrid-Identity-WhitePaper.html?LCID=EN-US. 95, 96

[122] AWS: *dentity and access management. amazon web services.*, 2019. https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/introduction.html. 96

[123] Devmedia: *Introdução a requisitos de software.*, 2013. https://www.devmedia.com.br/introducao-a-requisitos-de-software/29580. 104, 108

[124] Sommerville, Ian: *Engenharia de software, 9 edição*. Pearson, Addison Wesley, 9, 2011. 110

[125] Devmedia: *Desenvolvimento em 3 camadas (conceitos).* https://www.devmedia.com.br/desenvolvimento-em-3-camadas-conceitos/22277. 112

# Apêndice A

# Código do Protótipo

## Apêndice A – Código do Protótipo

Neste apêndice estão os códigos desenvolvidos em linguagem PHP para concepção do protótipo que validou computacionalmente a proposta deste trabalho.

a) Programa “Acesso.php”: Apresenta a tela de acesso e campos para inserção dos dados de login e validação da simulação

Acesso.php

```
<?php
 $message = (isset($_GET['msg'])) ? $_GET['msg'] : false;
 ?>

 <!doctype html>
 <html lang="pt-BR">
 <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width,
     user-scalable=no, initial-scale=1.0, maximum-scale=1.0,
     minimum-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">

    <link  href="/css/bootstrap.css" rel="stylesheet" />
    <link rel="stylesheet" href="https://use.fontawesome.com/
    releases/v5.8.1/css/all.css" integrity="sha384-  50oBUHEmvpQ+
    1lW4y57PTFmhCaXp0ML5d60M1M7uH2+nqUivzIebhndOJK28anvf"crossorigin=
    "anonymous">

    <link  href="/css/custom.css" rel="stylesheet" />

    <title>SISTEMA DECOM DIGITAL</title>
</head>
<body class="text-center">

<div class="container text-center">

    <div class="row">
        <div class="col-md-12">
            <h3>SISTEMA DECOM DIGITAL</h3>
            <h4>Ministério da Economia</h4>

        </div>
        <div class="col-md-12">
            <h5>Sua máquina possui:</h5>
        </div>
        <div class="col-md-12">
            <strong>Sistema Operacional:</strong> <br>
            <?php echo getOS();?>
        </div>
        <div class="col-md-12">
            <strong>Navegador:</strong> <br><?php echo
$_SERVER['HTTP_USER_AGENT'];?>
        </div>
    </div>
```

```
    <br><br>
    <div class="row">
        <div class="col-md-12">
            <div class="alert alert-success">
               Seu acesso foi liberado!
            </div>
        </div>
    </div>

    <a class="btn btn-success" href="index.php">Voltar ao Login</a>
</div>



</body>

<script src="/js/bootstrap.min.js" type="text/javascript"></script>
</html>


<?php

function getOS() {
    $user_agent = $_SERVER['HTTP_USER_AGENT'];

    $os_array = array(
        'windows nt 10'      =>  'Windows 10',
        'windows nt 6\.3'     =>  'Windows 8.1',
        'windows nt 6\.2'     =>  'Windows 8',
        'windows nt 6\.1'     =>  'Windows 7',
        'windows nt 6\.0'     =>  'Windows Vista',
        'windows nt 5\.2'     =>  'Windows Server 2003/XP x64',
        'windows nt 5\.1'     =>  'Windows XP',
        'windows xp'         =>  'Windows XP',
        'windows nt 5\.0'     =>  'Windows 2000',
        'windows me'         =>  'Windows ME',
        'win98'              =>  'Windows 98',
        'win95'              =>  'Windows 95',
        'win16'              =>  'Windows 3.11',
        'macintosh|mac os x' =>  'Mac OS X',
        'mac_powerpc'        =>  'Mac OS 9',
        'linux'              =>  'Linux',
        'ubuntu'             =>  'Ubuntu',
        'iphone'             =>  'iPhone',
        'ipod'               =>  'iPod',
        'ipad'               =>  'iPad',
        'android'            =>  'Android',
        'blackberry'         =>  'BlackBerry',
        'webos'              =>  'Mobile'
    );

    foreach ($os_array as $regex => $value) {
        if (preg_match('/' . $regex . '/i', $user_agent)) {
            return $value;
        }
    }

    return 'Unknown OS Platform';
}
```

```
function getBrowser($array=false) {

    $user_agent = $_SERVER['HTTP_USER_AGENT'];

    $browser_array = array(
        'msie'       =>  'Internet Explorer',
        'firefox'    =>  'Firefox',
        'safari'     =>  'Safari',
        'chrome'     =>  'Chrome',
        'edge'       =>  'Edge',
        'opera'      =>  'Opera',
        'netscape'   =>  'Netscape',
        'maxthon'    =>  'Maxthon',
        'konqueror'  =>  'Konqueror',
        'mobile'     =>  'Handheld Browser'
    );

    if($array) return $browser_array;

    foreach ($browser_array as $regex => $value) {
        if (preg_match('/' . $regex . '/i', $user_agent)) {
            return $value;
        }
    }

    return 'Unknown Browser';
}

function get_client_ip() {
    $ipaddress = '';
    if (isset($_SERVER['HTTP_CLIENT_IP']))
        $ipaddress = $_SERVER['HTTP_CLIENT_IP'];
    else if(isset($_SERVER['HTTP_X_FORWARDED_FOR']))
        $ipaddress = $_SERVER['HTTP_X_FORWARDED_FOR'];
    else if(isset($_SERVER['HTTP_X_FORWARDED']))
        $ipaddress = $_SERVER['HTTP_X_FORWARDED'];
    else if(isset($_SERVER['HTTP_FORWARDED_FOR']))
        $ipaddress = $_SERVER['HTTP_FORWARDED_FOR'];
    else if(isset($_SERVER['HTTP_FORWARDED']))
        $ipaddress = $_SERVER['HTTP_FORWARDED'];
    else if(isset($_SERVER['REMOTE_ADDR']))
        $ipaddress = $_SERVER['REMOTE_ADDR'];
    else
        $ipaddress = 'UNKNOWN';

    return $ipaddress;
}

?>
```

b) Programa “Bloqueio.php”: captura as informações do dispositivo de acesso, endereço IP, navegador e sistema operacional, para realizar a validação com os atributos armazenados da conta de acesso.

Bloqueio.php

```
<?php
///Recupera a mensagem da URL
$message = (isset($_GET['msg'])) ? $_GET['msg'] : false;

?>

<!doctype html>
<html lang="pt-BR">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, user-scalable=no,
initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">

    <link  href="/css/bootstrap.css" rel="stylesheet" />
    <link rel="stylesheet"
href="https://use.fontawesome.com/releases/v5.8.1/css/all.css"
integrity="sha384-
50oBUHEmvpQ+1lW4y57PTFmhCaXp0ML5d60M1M7uH2+nqUivzIebhndOJK28anvf"
crossorigin="anonymous">

    <link  href="/css/custom.css" rel="stylesheet" />

    <title>SISTEMA DECOM DIGITAL</title>
</head>
<body class="text-center">

<div class="container text-center">

    <div class="row">

        <div class="col-md-12">
            <h3>SISTEMA DECOM DIGITAL</h3>
            <h4>Ministério da Economia</h4>

        </div>
        <div class="col-md-12">
            <h5>Sua máquina possui:</h5>
        </div>
        <div class="col-md-12">
            <strong>Sistema Operacional:</strong> <br>
            <?php echo getOS();?>
        </div>
        <div class="col-md-12">
            <strong>Navegador:</strong> <br><?php echo
$_SERVER['HTTP_USER_AGENT'];?>
        </div>
    </div>


    <?php if($message){?>
        <div class="row">
            <div class="col-md-12">
                <div class="alert alert-danger">
                    <?php echo $message; ?>
```

```
                </div>
            </div>
        </div>
    <?php }; ?>

    <a class="btn btn-success" href="index.php">Voltar ao Login</a>
</div>


</body>

<script src="/js/bootstrap.min.js" type="text/javascript"></script>
</html>


<?php

function getOS() {
    $user_agent = $_SERVER['HTTP_USER_AGENT'];

    $os_array = array(
        'windows nt 10'      =>  'Windows 10',
        'windows nt 6\.3'     =>  'Windows 8.1',
        'windows nt 6\.2'     =>  'Windows 8',
        'windows nt 6\.1'     =>  'Windows 7',
        'windows nt 6\.0'     =>  'Windows Vista',
        'windows nt 5\.2'     =>  'Windows Server 2003/XP x64',
        'windows nt 5\.1'     =>  'Windows XP',
        'windows xp'         =>  'Windows XP',
        'windows nt 5\.0'     =>  'Windows 2000',
        'windows me'         =>  'Windows ME',
        'win98'              =>  'Windows 98',
        'win95'              =>  'Windows 95',
        'win16'              =>  'Windows 3.11',
        'macintosh|mac os x' =>  'Mac OS X',
        'mac_powerpc'        =>  'Mac OS 9',
        'linux'              =>  'Linux',
        'ubuntu'             =>  'Ubuntu',
        'iphone'             =>  'iPhone',
        'ipod'               =>  'iPod',
        'ipad'               =>  'iPad',
        'android'            =>  'Android',
        'blackberry'         =>  'BlackBerry',
        'webos'              =>  'Mobile'
    );

    foreach ($os_array as $regex => $value) {
        if (preg_match('/' . $regex . '/i', $user_agent)) {
            return $value;
        }
    }

    return 'Unknown OS Platform';
}

function getBrowser($array=false) {

    $user_agent = $_SERVER['HTTP_USER_AGENT'];

    $browser_array = array(
        'msie'       =>  'Internet Explorer',
```

```
        'firefox'    =>  'Firefox',
        'safari'     =>  'Safari',
        'chrome'     =>  'Chrome',
        'edge'       =>  'Edge',
        'opera'      =>  'Opera',
        'netscape'   =>  'Netscape',
        'maxthon'    =>  'Maxthon',
        'konqueror'  =>  'Konqueror',
        'mobile'     =>  'Handheld Browser'
    );

    if($array) return $browser_array;

    foreach ($browser_array as $regex => $value) {
        if (preg_match('/' . $regex . '/i', $user_agent)) {
            return $value;
        }
    }

    return 'Unknown Browser';
}

function get_client_ip() {
    $ipaddress = '';
    if (isset($_SERVER['HTTP_CLIENT_IP']))
        $ipaddress = $_SERVER['HTTP_CLIENT_IP'];
    else if(isset($_SERVER['HTTP_X_FORWARDED_FOR']))
        $ipaddress = $_SERVER['HTTP_X_FORWARDED_FOR'];
    else if(isset($_SERVER['HTTP_X_FORWARDED']))
        $ipaddress = $_SERVER['HTTP_X_FORWARDED'];
    else if(isset($_SERVER['HTTP_FORWARDED_FOR']))
        $ipaddress = $_SERVER['HTTP_FORWARDED_FOR'];
    else if(isset($_SERVER['HTTP_FORWARDED']))
        $ipaddress = $_SERVER['HTTP_FORWARDED'];
    else if(isset($_SERVER['REMOTE_ADDR']))
        $ipaddress = $_SERVER['REMOTE_ADDR'];
    else
        $ipaddress = 'UNKNOWN';

    return $ipaddress;
}

?>
```

c) Programa “Index.php”: Realiza as chamadas das funções de outros programas e trata as mensagens da aplicação.

Index.php

```
<?php
///Recupera a mensagem da URL
$message = (isset($_GET['msg'])) ? $_GET['msg'] : false;

?>

<!doctype html>
<html lang="pt-BR">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, user-scalable=no,
initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">

    <link  href="/css/bootstrap.css" rel="stylesheet" />
    <link rel="stylesheet"
href="https://use.fontawesome.com/releases/v5.8.1/css/all.css"
integrity="sha384-
50oBUHEmvpQ+1lW4y57PTFmhCaXp0ML5d60M1M7uH2+nqUivzIebhndOJK28anvf"
crossorigin="anonymous">

    <link  href="/css/custom.css" rel="stylesheet" />

    <title>SISTEMA DECOM DIGITAL</title>
</head>
<body class="text-center">

<div class="container text-center">

    <div class="row">
        <div class="col-md-12">
            <h3>SISTEMA DECOM DIGITAL</h3>
            <h4>Ministério da Economia</h4>
            <h5>Sua máquina possui:</h5>
        </div>
        <div class="col-md-12">
            <strong>Sistema Operacional:</strong> <br>
            <?php echo getOS();?>
        </div>
        <div class="col-md-12">
            <strong>Navegador:</strong> <br><?php echo
$_SERVER['HTTP_USER_AGENT'];?>
        </div>
    </div>

    <?php if($message){?>
        <div class="row">
            <div class="col-md-12">
                <div class="alert alert-danger">
                    <?php echo $message; ?>
                </div>
            </div>
        </div>
    <?php }; ?>

    <div class="row">
        <div class="col-md-4" style="margin: 0 auto">
```

```
            <form class="form-signin" method="post" action="validar.php">
                <input type="hidden" value="<?php echo
$_SERVER['HTTP_USER_AGENT'];?>" name="navegador">
                <input type="hidden" value="<?php echo getOS();?>"
name="os">
                <span style="font-size: 72px;">
                    <i class="fa fa-unlock" aria-hidden="true"></i>
                </span>

                <h1 class="h3 mb-3 font-weight-normal">Autenticação</h1>
                <label for="inputEmail">Login</label>
                <input type="text" id="inputEmail"  name="login"
class="form-control" placeholder="Login" required autofocus>
                <label for="inputPassword">Senha</label>
                <input type="password" id="inputPassword" class="form-
control" placeholder="Senha" name="senha" required>
                <label for="inputPassword">IP</label>
                <input type="text" class="form-control"
placeholder="Endereço de IP" name="ip" required value="186.235.87.241">
                <br>
                <button class="btn btn-lg btn-primary btn-block"
type="submit">Enviar</button>

                <h5>Bloqueio IPS</h5>
                <div class="checkbox">
                    <label>
                        <input type="radio" value="brasil" id=""
name="bloqueio">
                        <img src="img/bandeira-brasil.png" alt=""> Brasil
                    </label>

                    <label>
                        <input type="radio" value="china" id=""
name="bloqueio">
                        <img src="img/bandeira-china.png" alt=""> China
                    </label>

                    <h5>Validacao Especial</h5>

                    <label>
                        <input type="checkbox" value="sim" id=""
name="bloqueio_navegador">
                        Navegador
                    </label>
                    <label>
                        <input type="checkbox" value="sim" id=""
name="bloqueio_os">
                        Sistema Operacional
                    </label>
                </div>

            </form>
        </div>
    </div>
</div>


</body>

<script src="/js/bootstrap.min.js" type="text/javascript"></script>
</html>
```

```php
<?php

/**
 * @return mixed|string
 * Função para retornar o sistema operacional
 */
function getOS() {
    $user_agent = $_SERVER['HTTP_USER_AGENT'];

    $os_array = array(
        'windows nt 10'      =>  'Windows 10',
        'windows nt 6\.3'     =>  'Windows 8.1',
        'windows nt 6\.2'     =>  'Windows 8',
        'windows nt 6\.1'     =>  'Windows 7',
        'windows nt 6\.0'     =>  'Windows Vista',
        'windows nt 5\.2'     =>  'Windows Server 2003/XP x64',
        'windows nt 5\.1'     =>  'Windows XP',
        'windows xp'         =>  'Windows XP',
        'windows nt 5\.0'     =>  'Windows 2000',
        'windows me'         =>  'Windows ME',
        'win98'              =>  'Windows 98',
        'win95'              =>  'Windows 95',
        'win16'              =>  'Windows 3.11',
        'macintosh|mac os x' =>  'Mac OS X',
        'mac_powerpc'        =>  'Mac OS 9',
        'linux'              =>  'Linux',
        'ubuntu'             =>  'Ubuntu',
        'iphone'             =>  'iPhone',
        'ipod'               =>  'iPod',
        'ipad'               =>  'iPad',
        'android'            =>  'Android',
        'blackberry'         =>  'BlackBerry',
        'webos'              =>  'Mobile'
    );

    foreach ($os_array as $regex => $value) {
        if (preg_match('/' . $regex . '/i', $user_agent)) {
            return $value;
        }
    }

    return 'Unknown OS Platform';
}

/**
 * @param bool $array
 * @return array|mixed|string
 *
 * Função para retornar o browser
 */
function getBrowser($array=false) {

    $user_agent = $_SERVER['HTTP_USER_AGENT'];

    $browser_array = array(
        'msie'       =>  'Internet Explorer',
        'firefox'    =>  'Firefox',
        'safari'     =>  'Safari',
        'chrome'     =>  'Chrome',
```

```
        'edge'       =>  'Edge',
        'opera'      =>  'Opera',
        'netscape'   =>  'Netscape',
        'maxthon'    =>  'Maxthon',
        'konqueror'  =>  'Konqueror',
        'mobile'     =>  'Handheld Browser'
    );

    if($array) return $browser_array;

    foreach ($browser_array as $regex => $value) {
        if (preg_match('/' . $regex . '/i', $user_agent)) {
            return $value;
        }
    }

    return 'Unknown Browser';
}

/**
 * @return string
 *
 * Função para retonar o IP do usuário
 */
function get_client_ip() {
    $ipaddress = '';
    if (isset($_SERVER['HTTP_CLIENT_IP']))
        $ipaddress = $_SERVER['HTTP_CLIENT_IP'];
    else if(isset($_SERVER['HTTP_X_FORWARDED_FOR']))
        $ipaddress = $_SERVER['HTTP_X_FORWARDED_FOR'];
    else if(isset($_SERVER['HTTP_X_FORWARDED']))
        $ipaddress = $_SERVER['HTTP_X_FORWARDED'];
    else if(isset($_SERVER['HTTP_FORWARDED_FOR']))
        $ipaddress = $_SERVER['HTTP_FORWARDED_FOR'];
    else if(isset($_SERVER['HTTP_FORWARDED']))
        $ipaddress = $_SERVER['HTTP_FORWARDED'];
    else if(isset($_SERVER['REMOTE_ADDR']))
        $ipaddress = $_SERVER['REMOTE_ADDR'];
    else
        $ipaddress = 'UNKNOWN';

    return $ipaddress;
}

?>
```

d) Programa “Perguntas.php”: Realiza o subsistema de desafio para o usuário, envia as mensagens e perguntas desse subsistema.

Perguntas.php

```
<?php

$message = (isset($_GET['msg'])) ? $_GET['msg'] : false;

?>

    <!doctype html>
    <html lang="pt-BR">
    <head>
        <meta charset="UTF-8">
        <meta name="viewport" content="width=device-width, user-
scalable=no, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0">
        <meta http-equiv="X-UA-Compatible" content="ie=edge">

        <link  href="/css/bootstrap.css" rel="stylesheet" />
        <link rel="stylesheet"
href="https://use.fontawesome.com/releases/v5.8.1/css/all.css"
integrity="sha384-
50oBUHEmvpQ+1lW4y57PTFmhCaXp0ML5d60M1M7uH2+nqUivzIebhndOJK28anvf"
crossorigin="anonymous">

        <link  href="/css/custom.css" rel="stylesheet" />

        <title>SISTEMA DECOM DIGITAL</title>
    </head>
    <body class="text-center">

    <div class="container text-center">

        <div class="row">
            <div class="col-md-12">
                <h3>SISTEMA DECOM DIGITAL</h3>
                <h4>Ministério da Economia</h4>
                <h5>Sua máquina possui:</h5>
            </div>
            <div class="col-md-12">
                <strong>Sistema Operacional:</strong> <br>
                <?php echo getOS();?>
            </div>
            <div class="col-md-12">
                <strong>Navegador:</strong> <br><?php echo
$_SERVER['HTTP_USER_AGENT'];?>
            </div>
        </div>

        <div class="row">
            <div class="col-md-12">
                <div class="alert alert-danger">
                    Por questões de segurança necessitamos de confirmações
para validação do seu acesso
                </div>
            </div>
        </div>

        <div class="row">
```

```
            <div class="col-md-6" style="margin: 0 auto">
                <form class="form-signin" method="post" action="validar-
pergunta.php">
                    <label>Informe seu CPF</label>
                    <input type="text" id="inputEmail"  name="CPF"
class="form-control" placeholder="Digite a Resposta" required autofocus>
                    <label>Nome da cidade que sua mãe nasceu</label>
                    <input type="text" id="inputEmail"  name="mae"
class="form-control" placeholder="Digite a Resposta" required autofocus>
                    <br>
                    <button class="btn btn-lg btn-primary btn-block"
type="submit">Enviar</button>
                </form>
            </div>
        </div>
    </div>


    </body>

    <script src="/js/bootstrap.min.js" type="text/javascript"></script>
    </html>


<?php

function getOS() {
    $user_agent = $_SERVER['HTTP_USER_AGENT'];

    $os_array = array(
        'windows nt 10'      =>  'Windows 10',
        'windows nt 6\.3'     =>  'Windows 8.1',
        'windows nt 6\.2'     =>  'Windows 8',
        'windows nt 6\.1'     =>  'Windows 7',
        'windows nt 6\.0'     =>  'Windows Vista',
        'windows nt 5\.2'     =>  'Windows Server 2003/XP x64',
        'windows nt 5\.1'     =>  'Windows XP',
        'windows xp'         =>  'Windows XP',
        'windows nt 5\.0'     =>  'Windows 2000',
        'windows me'         =>  'Windows ME',
        'win98'              =>  'Windows 98',
        'win95'              =>  'Windows 95',
        'win16'              =>  'Windows 3.11',
        'macintosh|mac os x' =>  'Mac OS X',
        'mac_powerpc'        =>  'Mac OS 9',
        'linux'              =>  'Linux',
        'ubuntu'             =>  'Ubuntu',
        'iphone'             =>  'iPhone',
        'ipod'               =>  'iPod',
        'ipad'               =>  'iPad',
        'android'            =>  'Android',
        'blackberry'         =>  'BlackBerry',
        'webos'              =>  'Mobile'
    );

    foreach ($os_array as $regex => $value) {
        if (preg_match('/' . $regex . '/i', $user_agent)) {
            return $value;
        }
    }
```

```
    return 'Unknown OS Platform';
}

function getBrowser($array=false) {

    $user_agent = $_SERVER['HTTP_USER_AGENT'];

    $browser_array = array(
        'msie'       =>  'Internet Explorer',
        'firefox'    =>  'Firefox',
        'safari'     =>  'Safari',
        'chrome'     =>  'Chrome',
        'edge'       =>  'Edge',
        'opera'      =>  'Opera',
        'netscape'   =>  'Netscape',
        'maxthon'    =>  'Maxthon',
        'konqueror'  =>  'Konqueror',
        'mobile'     =>  'Handheld Browser'
    );

    if($array) return $browser_array;

    foreach ($browser_array as $regex => $value) {
        if (preg_match('/' . $regex . '/i', $user_agent)) {
            return $value;
        }
    }

    return 'Unknown Browser';
}

function get_client_ip() {
    $ipaddress = '';
    if (isset($_SERVER['HTTP_CLIENT_IP']))
        $ipaddress = $_SERVER['HTTP_CLIENT_IP'];
    else if(isset($_SERVER['HTTP_X_FORWARDED_FOR']))
        $ipaddress = $_SERVER['HTTP_X_FORWARDED_FOR'];
    else if(isset($_SERVER['HTTP_X_FORWARDED']))
        $ipaddress = $_SERVER['HTTP_X_FORWARDED'];
    else if(isset($_SERVER['HTTP_FORWARDED_FOR']))
        $ipaddress = $_SERVER['HTTP_FORWARDED_FOR'];
    else if(isset($_SERVER['HTTP_FORWARDED']))
        $ipaddress = $_SERVER['HTTP_FORWARDED'];
    else if(isset($_SERVER['REMOTE_ADDR']))
        $ipaddress = $_SERVER['REMOTE_ADDR'];
    else
        $ipaddress = 'UNKNOWN';

    return $ipaddress;
}

?>
```

e) Programa “Validar.php”: Recebe o retorno das funções de outros programas e realiza a validação das funcionalidades do protótipo.

Validar.php

```
<?php


///Seta os dados padrões do sistema como navegador e sistema operacional
$navegador = 'Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36';
$os = 'Windows 8.1';

///Determina o números de tentativas para 0
$tentativas = 0;

/// Verifica se existe login e senha
if(isset($_POST['login']) && isset($_POST['senha'])){

    /// Verifica o conteudo da variavel Login e Senha, caso errado
redireciona para a página de login com a mensagem
    if($_POST['login'] != 'claudio' || $_POST['senha'] != '123456'){
        salvarLog('FALHA','Login ou Senha Inválido');
        redirect('index.php',$_POST['login'].' Login ou Senha Inválido');
    }

    /// Verificar se vai fazer o teste de bloqueio por navegador
    if(isset($_POST['bloqueio_navegador'])){
        if(trim($_POST['navegador']) != trim($navegador)){
            salvarLog('FALHA',$_POST['login'].' Navegador Inválido');
            $tentativas++;
        }
    }

    /// Verificar se vai fazer o teste de bloqueio por sistema operacional
    if(isset($_POST['bloqueio_os'])){
        if(trim($_POST['os']) != trim($os)){
            salvarLog('FALHA',$_POST['login'].' Sistema Operacional
Inválido');
            $tentativas++;
        }
    }

    //// Verifica se existe validação de bloqueio por pais
    if(isset($_POST['bloqueio'])){
        if($_POST['bloqueio'] == 'china' || $_POST['bloqueio'] ==
'brasil'){
            $regiao = ipDetails($_POST['ip']);
            if($_POST['bloqueio'] == 'brasil' && $regiao == 'Brazil'){
                salvarLog('FALHA',$_POST['login'].' Range de IP encontrado
no Bloqueio');
                $tentativas++;
            }

            if($_POST['bloqueio'] == 'china' && $regiao == 'China'){
                salvarLog('FALHA',$_POST['login'].' Range de IP encontrado
no Bloqueio');
                $tentativas++;
            }
        }
```

```
    }

    ///Verifica se o numero de falhas foi igual a 1 para redirecionar para
as perguntas
    if($tentativas){
        if($tentativas == 1){
            redirect('perguntas.php');
        }

        /// Caso o número de tentativas seja maior que o usuário é
redirecionado para o bloqueio;
        redirect('bloqueio.php','Por questões de segurança seu acesso foi
negado, favor entrar em contato com o gestor do sistema');
    }

}else{
 ///Rediciona em caso de inesistencia de login e senha
 redirect('index.php','Login/Senha Inválido');
}

/// Rediciona para a a tela de login
salvarLog('SUCESSO','Usuário efetou o login com sucesso');
redirect('acesso.php');


/**
 * @param $url
 * @param string $msg
 *
 * Função para redirecionamento, em caso de mensagem no parametro, adiciona
a URL
 */
function redirect($url,$msg=''){
    if($msg) $url .= '?msg='.$msg;
    header('Location: '.$url);
    die;
}

/**
 * @param $ip
 * @return mixed
 *
 * Função que captura as informações do pais pelo IP
 */
function ipDetails($ip){
    $url =
'http://api.ipapi.com/api/'.$ip.'?access_key=4e05f3abbc60e497db1734b3010f99
eb';
    $content = json_decode(file_get_contents($url), true);
    return $content['country_name'];
}

/**
 * @param $tipo
 * @param $msg
 *
 * Função que armazena as informações no log de acesso, arquivo gerado
diariamente
 */
function salvarLog($tipo,$msg){
    /// Seta o nome do arquivo de log
```

```
    $file = './logs/'.date('Y-m-d').'.csv';

    /// se o arquivo não existir ele cria com o cabeçalho do csv
    if(!file_exists($file)){
        $content = 'Hora;Tipo;Mensagem'.PHP_EOL;
        file_put_contents($file,$content);
    }

    /// Insere as informações no log
    file_put_contents($file,date('H:i:s').';'.$tipo.';'.$msg.PHP_EOL,
FILE_APPEND);
}
```

f) Programa "Validar-pergunta.php": Valida o retorno do desafio e insere as informações no arquivo de log.

Validar-pergunta.php

```
<?php

///Seta os dados padrões do sistema como CPF e Cidade em que a mãe nasceu
$cpf = '59903660510';
$cidade = 'Itapetinga';

/// Verifica se existe os campos CPF e nome da cidade da mãe prenchidos
if(isset($_POST['CPF']) && isset($_POST['mae'])){
    if($_POST['CPF'] != $cpf || $_POST['mae'] != $cidade){
        redirect('bloqueio.php','Seu acesso foi negado, por favor contacte
o administrador do sistema!');
    }
}else{
 ///Rediciona em caso de inesistencia de login e senha
 redirect('index.php','Seu acesso foi negado, por favor contacte o
administrador do sistema!');
}

/// Rediciona para a a tela de login
salvarLog('SUCESSO','Usuário efetou o login com sucesso');
redirect('acesso.php');


/**
 * @param $url
 * @param string $msg
 *
 * Função para redirecionamento, em caso de mensagem no parametro, adiciona
a URL
 */
function redirect($url,$msg=''){
    if($msg) $url .= '?msg='.$msg;
    header('Location: '.$url);
    die;
}

/**
 * @param $ip
 * @return mixed
```

```
 *
 * Função que captura as informações do pais pelo IP
 */
function ipDetails($ip){
    $url =
'http://api.ipapi.com/api/'.$ip.'?access_key=4e05f3abbc60e497db1734b3010f99
eb';
    $content = json_decode(file_get_contents($url), true);
    return $content['country_name'];
}

/**
 * @param $tipo
 * @param $msg
 *
 * Função que armazena as informações no log de acesso, arquivo gerado
diariamente
 */
function salvarLog($tipo,$msg){
    /// Seta o nome do arquivo de log
    $file = './logs/'.date('Y-m-d').'.csv';

    /// se o arquivo não existir ele cria com o cabeçalho do csv
    if(!file_exists($file)){
        $content = 'Hora;Tipo;Mensagem'.PHP_EOL;
        file_put_contents($file,$content);
    }

    /// Insere as informações no log
    file_put_contents($file,date('H:i:s').';'.$tipo.';'.$msg.PHP_EOL);
}
```

# Anexo I

# Arquitetura do Sistema DECOM Digital

O sistema DECOM possui um módulo que tem como requisito o envio (*upload*) de arquivos para o servidor *web* através de um componente *Applet*. O sistema utiliza o protocolo SFTP para o envio dos arquivos. O sistema foi implantado em um ambiente clusterizado, em cima de containers Docker, para que a carga dos servidores seja dividida e sua capacidade de processamento possa ser redimensionada conforme a demanda, simplesmente adicionando e removendo nós ao *cluster*.

A arquitetura atual do DECOM é composta de:

- *Balancer* - contém o container do docker dedicado ao serviço de balanceamento de carga, executando o *HAProxy* 1.5.4;
- App01 e app02 - cada um contém o *container* (*mdic-server*) do *docker* responsável pela aplicação *web* (Apache 2.2.15 e PHP 5.5.25), e o container (*mdic-sftp-server*) responsável pelo serviço SFTP (*Openssh* 5.3);
- App03 - contém a rotina responsável por gravar os arquivos XML resultantes das transações de envio no banco de dados. Este nó executa apenas o *container mdic-server*;
- NFS - é o servidor que apenas disponibiliza, através do serviço NFS, um local comum para o armazenamento dos arquivos compartilhados entre os servidores de aplicação (*NFS Utils* 1.2.3);
- Banco de Dados - os servidores de banco de dados utilizados pela aplicação nos ambientes de homologação e produção são, respectivamente, R1FP18 (192.168.0.180) e C1SB12 (192.168.0.112), que executam o *Oracle 11gr2*.

A arquitetura da aplicação está representada na imagem a seguir.

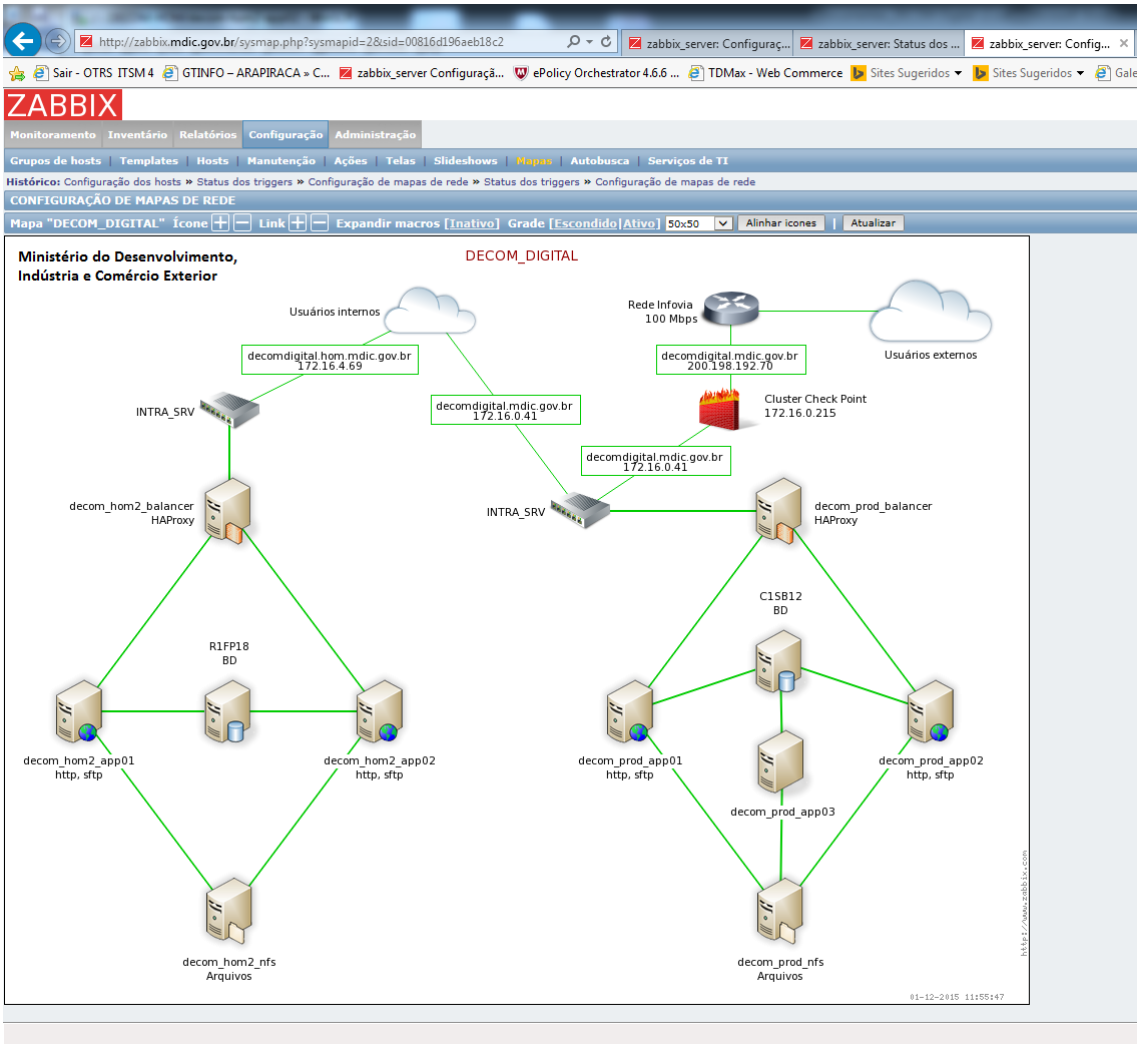


Figura I.1: Arquitetura do Sistema Decom Digital.

Arquivos e pastas importantes

A seguir, são apresentados alguns locais e arquivos importantes para o diagnóstico de problemas.

1. Lista de diretórios no sistema de arquivos do servidor de aplicação e sua respectiva montagem no container *docker*:

   - /opt/decom/webapp/decom - montado em - /var/www/html/decom
   - /opt/decom/webapp/decom/applet - link simbólico para: /opt/decom/sftp/
   - /opt/decom/webapp/cprod - montado em - /var/www/html/cprod
   - /opt/decom/webconf - montado em - /etc/httpd/conf.d/webconf

- /opt/decom/certificados - montado em - /var/www/certificados
- /opt/decom/sftp - montado em /opt/decom/sftp (container mdic-server)
- /opt/decom/sftp - montado em /opt/data (container mdic-sftp-server)

2. Arquivos de configuração do *apache*:

   - /opt/decom/webconf/decom-prod.conf
   - /opt/decom/webconf/ssl-decom-prod.conf

3. Arquivo de configuração da conexão com o banco de dados e do envio de *e-mail* através de relay SNMP.

   - /opt/decom/webapp/decom/app/config/parameters.php

4. Local dos arquivos XML gerados a partir dos arquivos carregados com sucesso pelos usuários. Este arquivo é armazenado no banco de dados através de uma rotina executada de 1 em 1 minuto. O nome dos arquivos é formado por: código do usuário no banco + número da transação + timestamp do arquivo + sequencial do arquivo.

   - /opt/decom/webapp/decom/applet/transacao

5. Diretório onde são mantidos os arquivos carregados pelos usuários do sistema, ao final do processo de upload.

   - /opt/decom/sftp

6. Diretório onde são gravados os logs gerados pela aplicação.

   - /opt/decom/webapp/decom/app/logs

# Anexo II

# Documentação do Sistema PEAD

Documento de Implantação do PEAD

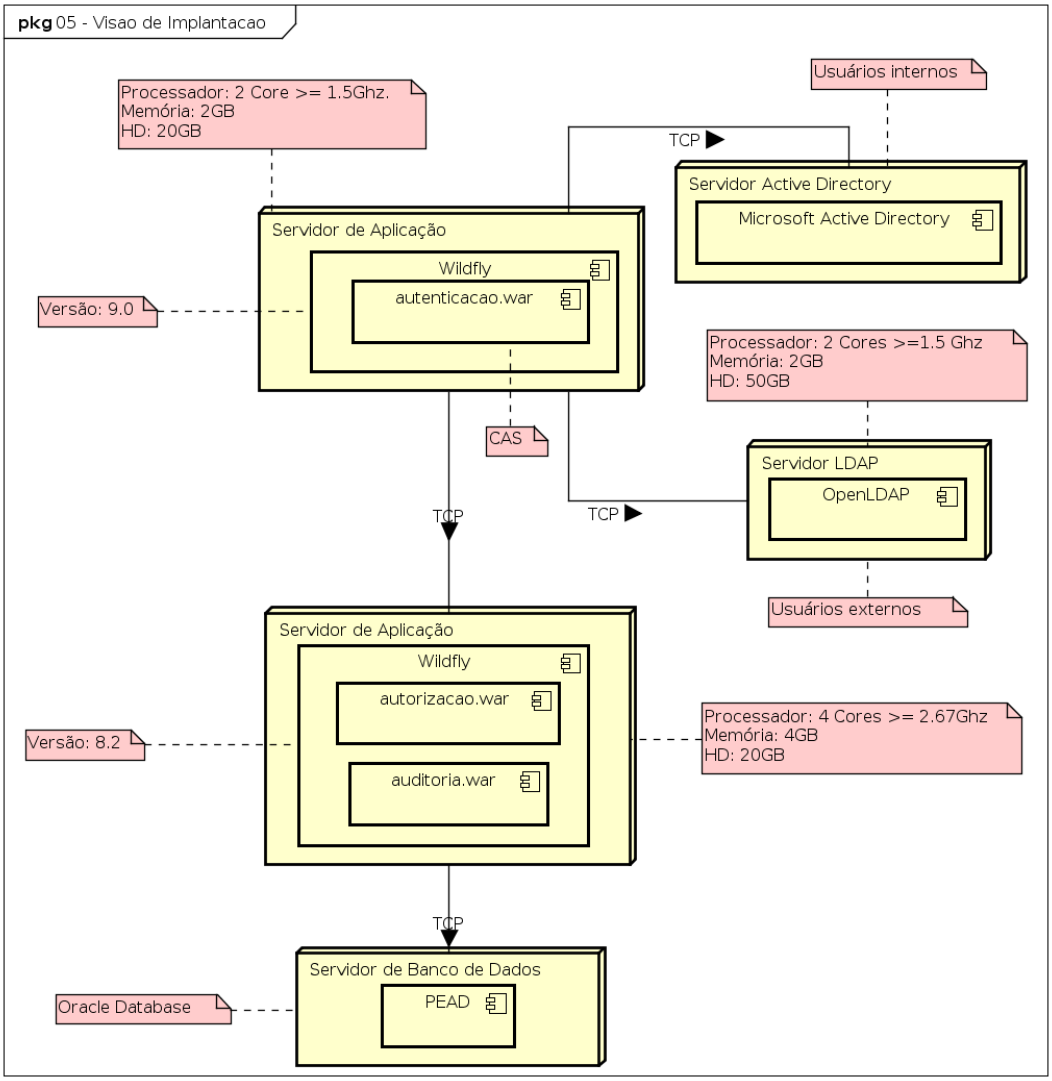


Figura II.1: Diagrama de Implantação do PEAD.