UNIVERSIDADE FEDERAL DO PARANÁ

CARLOS VINÍCIUS ORSI

# PRÁTICAS DE AUDITORIA INTERNA PARA IDENTIFICAÇÃO, AVALIAÇÃO E MONITORAMENTO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

**CURITIBA**

**2017**

UNIVERSIDADE FEDERAL DO PARANÁ

CARLOS VINÍCIUS ORSI

# PRÁTICAS DE AUDITORIA INTERNA PARA IDENTIFICAÇÃO, AVALIAÇÃO E MONITORAMENTO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Monografia apresentado ao Departamento de Ciências Contábeis, do Setor de Ciências Sociais Aplicadas, da Universidade Federal do Paraná, como pré-requisito para obtenção do título de Especialista em MBA – Auditoria Integral.

Orientador: Prof. Dr. Egon Walter Wildauer

**CURITIBA**

**2017**

Dedico mais essa conquista aos meus pais, Carlos e Célia, por me ensinarem valores incontestáveis como amor incondicional, honestidade, generosidade e ética, e que sempre me apoiaram na busca pelo conhecimento.

## AGRADECIMENTOS

Em primeiro lugar, a Deus; pela saúde, sabedoria e por ter constantemente me abençoado de várias formas.

À minha família, que de uma maneira ou de outra tem participação essencial em tudo que faço e sou na vida, pois sempre tive o apoio, confiança, encorajamento e compreensão de todos, mesmo à distância, para atingir meus objetivos profissionais e como Homem.

Agradeço especialmente à minha esposa, Taísa, pelo apoio incondicional, respeito e compreensão para a execução e conclusão deste projeto e nos demais momentos de muito trabalho.

Ao orientador e professores, sou grato por compartilharem o conhecimento, apoio na realização deste trabalho e serem mentores dessa evolução em minha carreira profissional.

Aos amigos e colegas de graduação, pós-graduação e de profissão que de alguma forma compartilharam suas experiências e contribuíram para o meu crescimento profissional como engenheiro de computação e auditor.

## RESUMO

As empresas estão operando em um ambiente competitivo e de muitas mudanças, consequentemente expostas à riscos que desafiam uma estratégia de sucesso, dentre eles os riscos de segurança de dados e confidencialidade são desafios relevantes para todas as organizações. A auditoria interna está sendo pressionada a evoluir para realizar a salvaguarda de informações valiosas em formatos digitais, e conhecer os diversos riscos emergentes inerentes nas organizações, para então conseguir agregar valor. Este trabalho refere-se à identificação das melhores práticas de auditoria interna para a identificação, avaliação e monitoramento de riscos de segurança da informação. Para isto, foi realizado um levantamento na literatura especializada da área e por meio de questionário, estruturado com questões objetivas e subjetivas, verificar as práticas adotas pelo Grupo dos Auditores Internos do Paraná (GAIP). A partir da análise dos resultados obtidos do questionário, verificou-se o perfil das organizações, dos profissionais, das auditorias internas e a percepção dos respondentes para com os riscos de segurança da informação e como a auditoria interna está abordando tais riscos. Foram comparadas as práticas levantadas na literatura e as adotadas pelo GAIP, verificando o nível de aderência deste com o mencionado na literatura. O resultado evidenciou que há normas e orientações práticas robustas que suportem o gerenciamento de riscos de segurança da informação durante todo o ciclo de vida de auditoria e quais os principais riscos de segurança da informação.



Palavras-chave: Auditoria Interna. Riscos. Segurança da Informação. Gerenciamento de Riscos. Tecnologia da Informação. Cibersegurança. Práticas de Auditoria. Grupo dos Auditores Internos do Paraná.

## ABSTRACT

Companies are operating in a competitive environment and many changes, therefore exposed to the risks that challenge a successful strategy, among them the risks of data security and confidentiality are challenges relevant to all organizations. Internal auditing is being pushed to evolve to safeguard valuable information in digital formats, and to know the various emerging risks inherent in organizations, in order to be able to add value. This work refers to the identification of best internal audit practices for the identification, evaluation and monitoring of information security risks. For this, a survey was carried out in the specialized literature of the area and through a questionnaire, structured with objective and subjective questions, to verify the practices adopted by the Group of Internal Auditors of Paraná (GAIP). From the analysis of the results obtained from the questionnaire, it was verified the profile of organizations, professionals, internal audits and the perception of respondents to the risks of information security and how internal auditing addresses these risks. It was compared the practices cited in the literature and those adopted by GAIP, verifying the level of adherence of this with that mentioned in the literature. The result showed that there are robust standards and practical guidelines that support the management of information security risks throughout the audit lifecycle and what are the main security risks of the information.



Key-words: Internal Audit. Risks. Information security. Risk management. Information Technology. Cyber security. Audit Practices. Group of Internal Auditors of Paraná.

## LISTA DE ILUSTRAÇÕES



## LISTA DE QUADROS



## LISTA DE TABELAS



## LISTA DE GRÁFICOS

# SUMÁRIO

# 1 INTRODUÇÃO

A auditoria interna, geralmente, é estabelecida em grandes organizações como um órgão de controle de um sistema de governança corporativa, a qual, de maneira independente, tem como funções primárias avaliar, monitorar e informar as atividades da organização aos *stakeholders*[1].

De acordo com o Instituto Brasileiro de Governança Corporativa,

> Governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas.
> As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico delongo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum. (IBGC, 2015, p.20).

A auditoria interna pode atuar em diversos tipos de ambientes organizacionais que variam de objetivos, complexidade, cultura, tamanhos, estruturas, processos, pessoas, riscos e tecnologias, contudo possui um papel desafiador de adicionar valor e melhorar a eficácia dos processos e operações organizacionais, que são inerentes ao dinamismo dos riscos corporativos e aos efeitos da evolução tecnológica constante.

As organizações PWC, Deloitte, KPMG e IIA realizaram pesquisas recentes para capturar qual **o papel da auditoria interna em um ambiente de negócios globalizado, dinâmico, com riscos complexos e de constante evolução tecnológica, assim como as habilidades necessárias para ela acompanhar essa evolução, agregar valor e contribuir de forma relevante para o negócio**.

No Estudo sobre a Prática Profissional de Auditoria Interna 2015 global, realizado pela PricewaterhouseCoopers Auditores Independentes (PWC, 2015, p. 5), constata que na opinião geral dos mais de 1.300 executivos de auditoria e membros da alta administração entrevistados, a auditoria interna precisa evoluir para acompanhar as necessidades dos negócios neste período de rápida transformação.

Ainda pare este mesmo estudo, Anton Van Wyk, presidente do *Global Institute of Internal Auditors*, África do Sul cita em entrevista que:

---

[1]Termo criado pelo filósofo Robert Edward Freeman, em português significa partes interessadas.

> Devido às mudanças no cenário global de riscos, os membros da alta administração são forçados a reavaliar os limitados recursos disponíveis para fornecer asseguração, além de apoio, à medida que suas atribuições mudam e as responsabilidades aumentam. Essa situação, associada à maior sensibilidade ao risco, levará as empresas a reconsiderar o papel e a importância da auditoria interna. Os auditores internos devem aproveitar essa oportunidade para ganhar a confiança do comitê de auditoria, da alta administração, do conselho e, em algumas circunstâncias, dos órgãos reguladores. (PWC, 2015, p. 6).

Todavia neste estudo, percebe-se que as empresas estão operando em um ambiente competitivo e de muitas mudanças, consequentemente expostas à riscos que desafiam uma estratégia de sucesso, dentre eles os riscos de segurança de dados e confidencialidade são desafios relevantes para 74% dos executivos. (PWC, 2015, p. 6).

No Brasil o número médio de incidentes de segurança aumentou em 274%, muito acima da média global que teve aumento de 38% e Dennis Chesley, líder global de Consultoria em Riscos da PWC, cita que muitos executivos apontam a questão cibernética como o risco que definirá a nossa geração. (PWC, 2016, p. 4)

Em 2016, a Deloitte e o IIA Brasil realizaram pesquisa de auditoria interna objetivando uma análise comparativa das práticas existentes no Brasil e no mundo, na qual verificaram que cerca de 80% dos respondentes, acreditam que nos próximos três a cinco anos a auditoria deverá passar por mudanças moderadas ou significativas para viabilizar o sucesso da organização diante do ambiente de incertezas e volatilidade da economia, mudanças tecnológicas e regulamentares que estão presentes de forma intensa no dia a dia das empresas. (Deloitte & IIA, 2016, p. 11).

De acordo com a publicação CBOK[2] de 2015 verifica-se que a auditoria interna está sendo pressionada a evoluir para realizar a salvaguarda de ativos, estes agora como informações valiosas e em formatos digitais, e conhecer os diversos riscos emergentes inerentes nas organizações, para então conseguir agregar valor.

> Em um momento em que o mundo tem acesso instantâneo à informação, os riscos capazes de destruir décadas de valor acumulado podem se materializar da noite para o dia e sem qualquer aviso prévio. Surpresas geopolíticas, macroeconômicas e ciberrelacionadas tornaram-se quase rotineiras. Raramente se passa um dia sem uma referência a uma nova ameaça global ou ciberataque.

[2]O Global Internal Audit Common Body of Knowledge (CBOK) é o maior estudo contínuo, no mundo todo, sobre a profissão da auditoria interna. Apoiado por institutos do IIA em todo o mundo, o CBOK inclui estudos abrangentes dos praticantes de auditoria interna e suas partes interessadas.

> [...] A volatilidade de tais riscos emergentes e em evolução está colocando uma pressão enorme sobre as funções de auditoria interna [...] (IIA, 2015 p. 4)

As organizações têm um volume de dados estruturados e não estruturados cada vez maior, presentes nesta era do *big data e internet das coisas*, além de que as estratégias e riscos estão mudando cada vez mais rápidos de tal forma que, conforme as pesquisas citadas anteriormente, a auditoria interna não tem conseguido realizar os trabalhos de maneira tempestiva, alinhada com os interesses e estratégia da alta administração e agregando valor efetivo à Companhia.

As organizações estão inseridas em um universo tecnológico que evolui rapidamente e as empresas que se adaptam mais facilmente a estes recursos obtém ganhos de competitividade no mercado. O volume de informações geradas, processadas e recebidas em cada empresa cresce constantemente, em função disso, muitos paradigmas da auditoria estão sendo revistos e novas ferramentas e soluções estão sendo empregadas.

Neste contexto surge o questionamento: “Quais as melhores práticas de abordagem da auditoria interna para identificar, avaliar e monitorar os principais riscos relacionados à segurança da informação diante de um ambiente tecnológico dinâmico?”.

Nesta hipótese, diante de um mercado altamente competitivo e tecnológico, a auditoria interna deve ser uma entidade não somente para a salva guarda de ativos e revisão de processos, mas atuando na identificação e avaliação de riscos e utilizando a tecnologia e dados disponíveis para análises robustas e mais precisas, agregando valor como parte estratégica para tomada de decisão.

Há pouco estudo para identificar as práticas de abordagem da auditoria interna em empresas com ambientes complexos de tecnologia e com riscos inerentes de segurança da informação, onde seja possível verificar quais metodologias e ferramentas têm sido adotadas para identificar e avaliar riscos de segurança da informação que são cada vez mais dinâmicos, realizar análises cada vez mais complexas de maneira tempestiva e a necessidade de auditores especialistas em TI.

Será de grande relevância para convergência de melhores práticas e contribuição para o desenvolvimento dos profissionais e estruturas de auditoria interna, observar as perspectivas dos executivos e abordagens já adotadas em auditorias baseadas em riscos pelas grandes empresas nacionais e multinacionais.

Neste sentido, este trabalho tem por objetivo elencar as melhores práticas de auditoria interna para identificar, avaliar e monitorar os riscos de segurança da informação recomendadas tanto pela literatura quanto as adotadas pelas auditorias inseridas no GAIP (Grupo dos Auditores Internos do Paraná).

Portanto este trabalho apresenta os seguintes objetivos específicos: (i) levantar informações das estruturas de auditorias internas atuantes nas empresas participantes do Grupo dos Auditores Internos do Paraná. (ii) verificar os principais riscos abordados por estas empresas em relação à segurança da informação. (iii) mapear os principais procedimentos e ferramentas, utilizados pelas auditorias durante a realização dos trabalhos, que auxiliam na identificação e avaliação de riscos de segurança da informação. (iv) elencar os principais práticas recomendados pela literatura como abordagem de auditoria interna em relação aos riscos de segurança da informação.

Esta monografia está estruturada com a seguinte abordagem: Referencial teórico, metodologia da pesquisa, consolidação das informações, análise e discussão e considerações finais.

## 2 REVISÃO DE LITERATURA

Neste capítulo, busca-se referencial teórico sobre os principais temas abordados neste trabalho, através de conceitos, origem e evolução da auditoria interna, normas e práticas internacionais, frameworks e legislação pertinente, para fundamentar quais são as melhores práticas que a auditoria interna baseada em riscos e inserida em um ambiente tecnológico dinâmico pode utilizar para identificar e monitorar os riscos específicos de segurança da informação.

### 2.1 Auditoria Interna

Conhecer a história e evolução da atividade de auditoria e especificamente da auditoria interna é essencial para compreender o conceito moderno de auditoria interna, suas práticas e objetivos e porque esta atividade precisa acompanhar os avanços tecnológicos das últimas décadas para continuar sendo eficaz e agregando valor à suas organizações e *stakeholders*.

### 2.1.1 Conceito e Aspectos Históricos da Auditoria Interna

A atividade de auditoria é bastante antiga, alguns pesquisadores citam sua existência há mais de 4.000 anos, na antiga Babilônia. (OLIVEIRA, 2008, p. 2). Apesar de historiadores também identificarem atividades de auditoria interna à milhares de anos, todavia segundo o Instituto dos Auditores Internos (IIA, 2016) o crescimento da profissão de auditoria interna ocorreu nos séculos XIX e XX com a expansão dos negócios corporativos.

A grande depressão econômica nos Estados Unidos e ruptura da bolsa de valores norte americana em 1929 foram decisivas para o desenvolvimento da auditoria independente. Pinho (2007, p. 6) comenta que “No início dos anos 30, é criado o famoso Comitê May, um grupo de trabalho instituído com a finalidade de estabelecer regras para as empresas que tivessem suas ações cotadas em bolsa, tornando obrigatória a Auditoria Contábil Independente nos demonstrativos contábeis dessas empresas”.

Franco e Marra (2000, p. 43), cita que “quanto ao efetivo exercício da atividade de Contador como profissional liberal, na qual se incluía a função de auditor independente, pouca coisa existia no Brasil antes de 1931, a não ser os escritórios estrangeiros de auditores, todos de origem inglesa”.

Como uma ramificação dessa auditoria externa, motivada pela necessidade de um acompanhamento mais aprofundado e permanente das operações da companhia além da possibilidade de redução de custos com a auditoria externa, alguns colaboradores da própria empresa começaram a realizar algumas atividades de auditoria internamente.

Segundo o IIA (2016) a gênese da auditoria interna moderna se deu com a criação do próprio instituto em 1941, quando Brink, Milne e Thurston em contato com outros profissionais de auditoria interna nos Estados Unidos resolveram formar uma organização independente para os auditores internos.

No Brasil, a fundação do Instituto dos Auditores Internos do Brasil ocorreu em 1960 e sua afiliação ao IIA Global foi no ano de 1999 (IIA BRASIL, 2016).

É notório que a auditoria, seja interna ou externa, se adaptou ao longo do século XX, devido aos inúmeros avanços tecnológicos e da expansão das

organizações, para cumprir com sua filosofia e objetivos. “A filosofia da auditoria consiste em avaliar a política de sistema da empresa, em termos da adequação, comunicação, aceitação, aplicação e controle, se é necessária na situação, se contribui para atingir os objetivos da empresa” (CREPALDI, 2002, p. 25).

O *International Professional Practices Framework* (IPPF) promovido por *The Institute of Internal Auditors* (IIA), define a auditoria interna como:

> A auditoria interna é uma atividade independente e objetiva de avaliação (*assurance*) e de consultoria, desenhada para adicionar valor e melhorar as operações empresariais.
> Ela auxilia uma organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança. (IIA, 2013)

Quanto ao conceito de auditoria interna, no Brasil o Conselho Federal de Contabilidade por meio da Norma Brasileira de Contabilidade NBC TI 01 define a atividade de Auditoria Interna como

> A Auditoria Interna compreende os exames, análises, avaliações, levantamentos e comprovações, metodologicamente estruturados para a avaliação da integridade, adequação, eficácia, eficiência e economicidade dos processos, dos sistemas de informações e de controles internos integrados ao ambiente, e de gerenciamento de riscos, com vistas a assistir à administração da entidade no cumprimento de seus objetivos. (CFC, 2012)

Para o IBGC, a auditoria interna é fundamentada como:

> Tem a responsabilidade de monitorar, avaliar e realizar recomendações visando a aperfeiçoar os controles internos e as normas e procedimentos estabelecidos pelos administradores. As organizações devem possuir uma função de auditoria interna, própria ou terceirizada. A diretoria e, particularmente, o diretor-presidente também são diretamente beneficiados pela melhoria do ambiente de controles decorrente de uma atuação ativa da auditoria interna. IBGC (2015, p. 90).

A auditoria interna, via de regra, atua como auditoria de processo avaliando a eficácia dos processos operacionais e do sistema de controles internos. Na análise dos processos operacionais, o trabalho do auditor é definido de forma mais ampla por DIAS como:

> Uma atividade de avaliação independente de assessoramento à alta gestão da empresa, que visa à avaliação dos sistemas de controle envolvidos e verificação dos procedimentos e das normas alocados no desenvolvimento do negócio exercido, atentando para o desempenho operacional e para a

> eficácia obtida por suas áreas produtivas, considerando planos de metas, macrobjetivos e políticas definidas pela organização. DIAS (2006, p. 1).

### 2.1.2 Melhores práticas de Estrutura e Procedimentos de Auditoria Interna

Quanto à estrutura da atividade ou uma área de auditoria interna, cada organização desenvolve um modelo dependendo da sua complexidade, estrutura hierárquica e suas respectivas relações.

O IIA (2013, p. 3) estabelece que assim como a definição de auditoria interna e o código de ética, as normas descritas no IPPF também devem ser reconhecidas no estatuto de auditoria interna. Dentre as normas o IIA não define exatamente uma estrutura ou modelo hierárquico conceitual e obrigatório, mas define na norma 1100 a independência e objetividade como “A atividade de auditoria interna deve ser independente e os auditores internos devem ser objetivos ao executar seus trabalhos.” IIA (2013, p. 3).

Para o IIA, a interpretação que deve ser considerada quanto à independência é:

> Independência é a imunidade quanto às condições que ameaçam a capacidade da atividade de auditoria interna de conduzir as responsabilidades de auditoria interna de maneira imparcial. Para atingir o grau de independência necessário para conduzir eficazmente as responsabilidades da atividade de auditoria interna, o executivo chefe de auditoria tem acesso direto e irrestrito à alta administração e ao conselho. Isto pode ser alcançado através de um relacionamento de duplo reporte. As ameaças à independência devem ser gerenciadas nos níveis do auditor individual, do trabalho de auditoria, funcional e organizacional. IIA (2013, p. 3).

Quanto à independência organizacional, é citada pelo IIA na norma 1110 como:

> O executivo chefe de auditoria deve reportar-se a um nível dentro da organização que permita à atividade de auditoria interna cumprir suas responsabilidades. O executivo chefe de auditoria deve confirmar junto ao conselho, pelo menos anualmente, a independência organizacional da atividade de auditoria interna. IIA (2013, p. 4)

O CPC (2012, p. 5), através da norma NBC TI 01, descreve que a auditoria interna está estruturada em procedimentos técnicos, sistemático e objetivo com a

finalidade de agregar valor à organização com melhoria dos processos, da gestão e dos controles internos.

As diferentes normas, entidades e autores relacionados com a atividade de auditoria interna abordam como principais processos, sendo:

a) Planejamento de Auditoria;
b) Programa de Trabalho;
c) Execução e Análises;
d) Comunicação dos Resultados;
e) Monitoramento.

#### *2.1.2.1 Planejamento de Auditoria*

Nas normas internacionais do IPPF, o IIA (2013, p. 9) define que o planejamento de auditoria interna deve ser baseado em uma avaliação de riscos, realizado em período mínimo de um ano, e que deve considerar informações pertinentes do conselho e alta administração da organização.

De acordo com a norma NBC TI 01, o planejamento "compreende os exames preliminares das áreas, atividades, produtos e processos, para definir a amplitude e a época do trabalho a ser realizado, de acordo com as diretrizes estabelecidas pela administração da entidade." CFC (2012, p. 6).

Essa mesma norma ainda vai além e descreve que o planejamento deve considerar como fatores relevantes na execução dos trabalhos:

> a) o conhecimento detalhado da política e dos instrumentos de gestão de riscos da entidade;
> b) o conhecimento detalhado das atividades operacionais e dos sistemas contábil e de controles internos e seu grau de confiabilidade da entidade;
> c) a natureza, a oportunidade e a extensão dos procedimentos de auditoria interna a serem aplicados, alinhados com a política de gestão de riscos da entidade;
> d) a existência de entidades associadas, filiais e partes relacionadas que estejam no âmbito dos trabalhos da Auditoria Interna;
> e) o uso do trabalho de especialistas;
> f) os riscos de auditoria, quer pelo volume ou pela complexidade das transações e operações;
> g) o conhecimento do resultado e das providências tomadas em relação a trabalhos anteriores, semelhantes ou relacionados;
> h) as orientações e as expectativas externadas pela administração aos auditores internos; e
> i) o conhecimento da missão e objetivos estratégicos da entidade. CFC (2012, p.6).

Segundo DIAS (2006, p. 15) os processos a serem auditados são definidos pela relevância para a execução do negócio-fim da empresa e cabe à área de auditoria definir o grau de risco envolvido em cada processo, para avaliação da relevância perante os riscos.

#### *2.1.2.2 Programa de Trabalho*

Para estabelecer um programa de trabalho de auditoria, é necessário definir o objetivo e escopo que este programa de trabalho deve abordar, para então definir quais procedimentos de teste serão necessários para atingir o escopo e objetivo deste programa.

De acordo com IIA (2013, p. 13), preliminarmente deve-se realizar uma análise dos riscos relevantes do processo a ser auditado, e considerar os resultados desta avaliação assim como a probabilidade de erros relevantes, fraudes e não conformidades aos objetivos da auditoria. Enquanto o escopo deve ser suficiente e considerar sistemas, registros, pessoal e propriedades físicas relevantes para atingir os objetivos definidos para o trabalho de auditoria.

O IPPF ainda descreve que é dever do auditor interno elaborar e documentar programas de trabalho que suportem os objetivos estabelecidos, além de que nestes programas devem ser incluídos os procedimentos de identificação, análise, avaliação e documentação das informações ao longo da auditoria.

Neste contexto, a norma brasileira é mais simplificada em sua definição de programas de trabalho, descrevendo que “devem ser estruturados de forma a servir como guia e meio de controle de execução do trabalho, devendo ser revisados e atualizados sempre que as circunstâncias o exigirem.” CFC (2012, p. 7)

#### *2.1.2.3 Execução e Análises*

Em um trabalho de auditoria, a etapa de execução e análises é o momento de executar e documentar o que foi planejado no programa de trabalho, por meio de testes, avaliações e análises para suportar as conclusões e resultados.

Segundo o IPPF, na etapa de execução “os auditores internos devem identificar, analisar, avaliar e documentar informações suficientes para cumprir os objetivos do trabalho de auditoria.” IIA (2013, p. 14)

Quanto à etapa de análise e avaliação, “Os auditores internos devem basear suas conclusões e resultados dos trabalhos de auditoria em análises e avaliações apropriadas.” IIA (2013, p.14)

O CPC (2012, p.7) fundamenta “Os procedimentos da Auditoria Interna constituem exames e investigações, incluindo testes de observância e testes substantivos, que permitem ao auditor interno obter subsídios suficientes para fundamentar suas conclusões e recomendações à administração da entidade.”.

A NBC TI 01 ainda determina que “No trabalho da Auditoria Interna, quando aplicável, deve ser examinada a observância dos Princípios Fundamentais de Contabilidade, das Normas Brasileiras de Contabilidade e da legislação tributária, trabalhista e societária, bem como o cumprimento das normas reguladoras a que estiver sujeita a entidade.” CPC (2012, p. 8).

#### *2.1.2.4 Comunicação dos Resultados*

As conclusões e resultados obtidos durante a fase de execução do trabalho de auditoria, assim como as recomendações expressas pelos auditores responsáveis devem ser comunicados às partes interessadas, e o meio comumente utilizado para esta comunicação é o relatório de auditoria.

Dentre as práticas internacionais do IPPF, o IIA (2013, p.15) determina a respeito da comunicação final dos resultados, que esta deve incluir os objetivos, escopo, conclusões, recomendações e planos de ação aplicáveis. Esta comunicação deve ser precisa, objetiva, clara, concisa, construtiva, completa e tempestiva.

De acordo com IPPF:

> Se não houver exigências legais, estatutárias ou regulatórias em contrário, antes de se divulgar os resultados para partes externas à organização, o executivo chefe de auditoria deve:
> • Avaliar o risco potencial à organização;
> • Consultar a alta administração e/ou advogado, conforme for apropriado; e
> • Controlar a disseminação através da restrição da utilização dos resultados.
> CPC (2012, p.16)

Na norma brasileira há entendimento que a comunicação do trabalho de auditoria também deve ser realizar por meio de relatório, a qual trata do conceito e a abordagem de um relatório.

> 12.3.1 – O relatório é o documento pelo qual a Auditoria Interna apresenta o resultado dos seus trabalhos, devendo ser redigido com objetividade e imparcialidade, de forma a expressar, claramente, suas conclusões, recomendações e providências a serem tomadas pela administração da entidade.
> 12.3.2 – O relatório da Auditoria Interna deve abordar, no mínimo, os seguintes aspectos:
> a) o objetivo e a extensão dos trabalhos;
> b) a metodologia adotada;
> c) os principais procedimentos de auditoria aplicados e sua extensão;
> d) eventuais limitações ao alcance dos procedimentos de auditoria;
> e) a descrição dos fatos constatados e as evidências encontradas;
> f) os riscos associados aos fatos constatados; e
> g) as conclusões e as recomendações resultantes dos fatos constatados. CFC (2012, p. 9)

#### *2.1.2.5 Monitoramento*

Como última fase dos processos de auditoria interna, o monitoramento, também conhecido como *follow up*, se faz necessário para a auditoria interna acompanhar se as ações planificadas pelas áreas de negócio estão de fato sendo implementadas.

O IIA (2013, p. 17), determina que “O executivo chefe de auditoria deve estabelecer um processo de acompanhamento para monitorar e assegurar que as ações da administração tenham sido efetivamente implantadas ou que a alta administração tenha aceitado o risco de não tomar nenhuma ação.”

O CPC não comenta na norma NBC TI 01 sobre o processo de monitoramento da auditoria interna.

## 2.2 Tecnologia da Informação

De acordo com IMONIANA:

> Em 1950, mudanças foram provocadas em todos os ambientes de negócios. As instituições e as empresas comerciais começaram a expandir-se rapidamente. [...] As complexidades das empresas aumentaram tão exponencialmente, que os métodos tradicionais de processamento de dados e de sistemas de controles internos não puderam conviver com a mesma situação por muito mais tempo, uma vez que os equipamentos que agilizavam

> ou auxiliavam nas operações começaram a ser aplicados nas atividades simples e de maior complexidade [...]. IMONIANA (2016, p.1).

Nas últimas décadas do século XX houve uma evolução tecnológica mais acentuada em todo o mundo, que disseminou o uso de sistemas informatizados e computadores interligados em redes nas organizações.

> Entretanto, os custos e o aumento de vulnerabilidade do sistema de processamento eletrônico de dados emanados do uso difundido de Tecnologia de Informação geraram a necessidade de os auditores internos e independentes possuírem habilidades em processamento eletrônico de dados, bem como a necessidade de aumentar as técnicas e ferramentas de avaliação de sistemas, assegurando os acionistas, investidores, órgãos governamentais e outros usuários das demonstrações contábeis de se defrontarem com situações embaraçosas ou incomuns. IMONIANA (2016, p.1)

Essa necessidade de conhecimento específico em Tecnologia de Informação para avaliação dos sistemas e seus dados, por parte dos auditores, desenvolveu uma especialidade ou segmento de auditoria conhecida como Auditoria de Sistemas e defina como "[..] é o ramo da auditoria que revisa e avalia os riscos de tecnologia da informação e os Controles Internos Informatizados, associados a Sistemas Aplicativos e os Ativos de TI da organização [...]". (IIA BRASIL, 2014, p.11).

A tecnologia continua evoluindo exponencialmente no século XXI, os dispositivos digitais e a internet se tornaram algo indispensável na vida das pessoas e nas organizações, não importando sua área de atuação ou faturamento. O grande volume de informações geradas, transmitidas e armazenadas a cada segundo pelas empresas é algo incrível e impossível a uma década atrás.

Atualmente a tecnologia de uma forma ou de outra é parte inerente aos negócios e por isso o conceito de governança transcendeu para a área de tecnologia. Segundo o IPPF (IIA, 2016) "Governança de TI consiste da liderança, estruturas organizacionais e processos que asseguram que a tecnologia da informação corporativa dá suporte às estratégias e aos objetivos da organização.".

Segundo ainda o COBIT® 5[3] (ISACA, 2012) o objetivo da Governança de TI é atender as diretrizes e necessidades dos *stakeholders* e criar valor ao negócio.

[3]COBIT® 5 é uma estrutura de governança e gerenciamento da TI corporativa mantido pela ISACA (Information Systems AuditandControlAssociation).

Atualmente as organizações e suas áreas de tecnologia estão enfrentando um novo desafio em seu processo de governança de TI e tomada de decisão, lidar diariamente com um volume muito grande de informação. Este volume gigantesco de dados, em todos os formatos digitais, é conhecido por *Big Data*.

Para MCKINSEY GLOBAL INSTITUTE (2011) "*Big Data* refere-se aos conjuntos de dados cujo tamanho está além da capacidade de ferramentas típicas de software de banco de dados para capturar, armazenar, gerenciar e analisar".

De maneira mais simplificada O'REILLY (2012) define *Big Data* como dados que excedem a capacidade de processamento dos sistemas de banco de dados convencionais.

O relatório de 2014, intitulado "O Universo Digital das Oportunidades: riquezas de dados e valor crescente da Internet das Coisas" da EMC sobre o universo digital com pesquisa e análise pela IDC, o único a quantificar e prever o volume de dados produzido anualmente no mundo, mostra que o volume de dados digitais está dobrando de tamanho a cada dois anos e vai se multiplicar por dez até o ano de 2020. O estudo também estima que dos 4,4 zettabytes (ou 4,4 trilhões de gigabytes) de informação em 2013, o universo digital alcançará 44 zettabytes de dados em 2020. (IDC, 2014).

Para o Brasil, o estudo da IDC estima que em 2013 o universo digital era 212 exabytes e será de 1.6 zettabytes em 2020, representando cerca de 4% do universo digital global. (IDC, 2014).

Pode-se entender que este universo digital citado pela pesquisa da IDC está intrínseco ao conceito de *Big Data* e Internet das Coisas, exemplos típicos da evolução tecnológica que desafiam as corporações, uma vez que "Em 2013, dois terços dos bits do universo digital foram criados ou capturados pelos consumidores e trabalhadores, mas as empresas tinham obrigação ou responsabilidade por 85% (cerca de 2.3 zettabytes) do universo digital" (IDC, 2014).

Quanto ao volume de dados úteis, em 2013, apenas cerca de 5% eram valiosos, mas em 2020 esse percentual deve estar acima de 10%, conforme as empresas aproveitarem novas tecnologias em *Big Data*, análises e fontes de dados, e utilizá-los melhor na organização. (IDC, 2014).

Quanto à segurança da informação "Em 2013, enquanto cerca de 40% da informação no universo digital requeria algum tipo de proteção de dados, menos de 20% do universo digital realmente tinha essas proteções." (IDC, 2014).

### 2.2.1 Segurança da Informação

A segurança da informação tem se tornado cada vez mais relevante dentro das organizações para alcançar seus objetivos e se manter competitiva no mercado.

De acordo com BEAL, qualquer dado ou informação relevante que represente um valor para o negócio é um ativo de informação.

> Dados, informações e conhecimento, pela sua alta capacidade de adicionar valor a processos, produtos e serviços, constituem recursos cada vez mais críticos para o alcance da missão e dos objetivos organizacionais. Como qualquer outro ativo valioso para as organizações, as informações críticas para o negócio precisam ser protegidas contra as ameaças que podem levar à sua destruição, indisponibilidade temporária, adulteração ou divulgação não autorizada. (BEAL, 2005, p. xi).

No entendimento de SÊMOLA (2014, p. 2), “Segredos de negócio, análise de mercado e concorrência, dados operacionais históricos e pesquisas são informações fundamentais e se revelam como importante diferencial competitivo ligado ao crescimento e à continuidade do negócio.”.

#### *2.2.1.1 Conceito e Normas*

O conceito de informação é amplo e com diversos significados de acordo com cada contexto, por isso não é objetivo deste trabalho definir o que é informação, mas considerar a informação como um ativo de valor, seja ela um conjunto de dados, uma instrução ou conhecimento sobre algo.

Também é importante ressaltar que há diversos fatores que podem agregar mais ou menos valor a esse ativo. Estes fatores também não serão tema de discussão desta dissertação, visto que trataremos dos ativos de valor, ou seja, as informações com algum grau de relevância para uma organização.

Segundo a norma ABNT NBR ISO 27002 que estabelece código de prática para a gestão de segurança da informação:

> 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 agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades. (ABNT, 2005, p. x)

Dessa maneira, todo ativo de valor necessita ser protegido para que seja preservado o valor do ativo para a organização que a possui.

O conceito de segurança da informação para BEAL (2005, p. 1) é “[...] o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade.”.

No contexto tecnológico e de negócios o conceito de segurança da informação está padronizado pela norma internacional ISO/IEC 27002:2005, a qual foi adotada na norma brasileira ABNT NBR ISO/IEC 27002 como “Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.” (ABNT, 2005, p. x)

A norma ABNT NBR ISO/IEC 27001 (2006, p.2) também define segurança da informação como “preservação da confidencialidade, integridade, e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem estar envolvidas”.

Em sua Política de Segurança da Informação a BM&FBovespa define o conceito de segurança da informação como:

> A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:
>  Confidencialidade: Garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário;
>  Disponibilidade: Garante que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessária;
>  Integridade: Garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida. (BM&FBOVESPA, 2016, p. 3)

#### *2.2.1.2 Ameaças e Vulnerabilidades*

Para que se entenda o que pode ser uma ameaça ou vulnerabilidade aos ativos de informação de uma organização é preciso conhecer os conceitos, classificação e exemplos de ameaças e vulnerabilidades do meio tecnológico.

A norma NBR ISO/IEC 27002 (2006, p.3) define ameaça em “causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou

organização”, enquanto a vulnerabilidade é considerada “fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças”.

Conceitualmente KIM & SOLOMON (2014, p. 5) definem “Uma ameaça é qualquer ação que possa danificar um bem. Sistemas de informação enfrentam ameaças naturais e induzidas por humanos. [...] Uma vulnerabilidade é um ponto fraco que permita que uma ameaça seja concretizada ou que tenha efeito sobre um bem.”.

No entendimento de BEAL (2005, p. 14) “Ameaça: expectativa de acontecimento acidental ou proposital, causado por um agente, que pode afetar um ambiente, sistema ou ativo de informação. Vulnerabilidade: fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque.”.

Neste contexto, BEAL (2005, p.14) ainda observa que ameaça é algo geralmente externo ao ativo, como por exemplo, um vírus ou fogo, enquanto a vulnerabilidade pode ser decorrente de diversos fatores e associada ao ativo como a falta de treinamento ou falha nos controles de acesso.

De maneira mais abrangente SÊMOLA (2014) define e classifica ameaças como:

> São agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, e, consequentemente, causando impactos aos negócios de uma organização.
> Classificando as ameaças quanto a sua intencionalidade, elas podem ser divididas nos seguintes grupos:
> **Naturais** – Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, [...].
> **Involuntárias** – Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia etc.
> **Voluntárias** – Ameaças propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários. (SÊMOLA, 2014, p. 45)

As vulnerabilidades também são definidas e exemplificadas por SÊMOLA (2014) como:

> São fragilidades presentes ou associadas a ativos que manipulam e/ou processam informações que, ao serem exploradas por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade. [...] Exemplos de vulnerabilidades:
> **Físicas** – Instalações prediais que não atendem as boas práticas ou as normas e regulamentações vigentes; [...] controle de acesso deficiente em locais contendo informações confidenciais ou sensíveis etc.

> **Naturais** – Ambientes com equipamentos eletrônicos próximos a locais suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades e outros, como falta de energia, [...]
> **Hardware** – Computadores são suscetíveis à poeira, umidade, sujeira e acesso indevido a recursos inadequadamente protegidos, podendo ainda sofrer com componentes deficientes ou mal configurados, [...]
> **Software** – Erros na codificação, instalação ou configuração de sistemas e aplicativos podem acarretar acessos indevidos, vazamento de informações, perda de dados e de trilhas de auditoria ou indisponibilidade do recurso quando necessário.
> **Mídias** – Discos, fitas, relatórios e impressos podem ser perdidos ou danificados; [...]
> **Comunicação** – A comunicação telefônica é vulnerável a escutas (acesso indevido) ou a problemas na infraestrutura física ou lógica que a impeçam de ser estabelecida.
> **Humanas** – Falta de treinamento ou conscientização das pessoas, falta de avaliação psicológica adequada ou de verificação de antecedentes (*background check*), [...] podem levar ao compartilhamento indevido de informações confidenciais, à não execução de rotinas de segurança ou a erros, omissões etc, que ponham em risco às informações. (SÊMOLA, 2014, p. 46)

#### *2.2.1.3 Práticas e Ferramentas para Segurança da Informação*

Há inúmeras ferramentas e soluções utilizadas para implementar um ambiente de informação mais seguro, mas o objetivo deste tópico é identificar e elencar as principais práticas, medidas e ferramentas citadas pela literatura.

A prática adotada pela ABNT NBR ISO/IEC 27001 (2006, p. v) é a implantação de um Sistema de Gestão da Segurança da Informação (SGSI) que enfatiza a importância para a organização que esta necessita entender os requisitos e estabelecer política e objetivos de segurança da informação, implementar controles para gerenciar os riscos de segurança da informação, monitorar e avaliar o desempenho e eficácia do SGSI, além de realizar melhoria contínua do SGSI. Para isso, a norma adota o modelo "*Plan-Do-Check-Act*" para as etapas dos processos do SGSI, considerando ainda o atendimento dos requisitos de segurança da informação e expectativas das partes interessadas.

| | |
|---|---|
| ***Plan* (planejar) (estabelecer o SGSI)** | Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização. |
| ***Do* (fazer) (implementar e operar o SGSI)** | Implementar e operar a política, controles, processos e procedimentos do SGSI. |
| ***Check* (checar) (monitorar e analisar criticamente o SGSI)** | Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção. |
| ***Act* (agir) (manter e melhorar o SGSI)** | Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI. |

**Tabela 1 - Modelo PDCA aplicado aos processos do SGSI**

De acordo ainda com a norma NBR ISO/IEC 27001 (2006, p. 3) o sistema de gestão de segurança da informação é definido como:

> A parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação. O sistema de gestão inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos. (ABNT, 2006, p. 3)

Para estabelecer um SGSI a NBR ISO/IEC 27001 (2006, p. 4) orienta os principais processos que a organização deve implementar, sendo:

> a) Definir o escopo e os limites do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo [...];
> b) Definir uma política do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia [...];
> c) Definir a abordagem de análise/avaliação de riscos da organização. [...];
> d) Identificar os riscos [...];
> e) Analisar e avaliar os riscos [...];
> f) Identificar e avaliar as opções para o tratamento de riscos [...];
> g) Selecionar objetivos de controle e controles para o tratamento de riscos [...];
> h) Obter aprovação da direção dos riscos residuais propostos;
> i) Obter autorização da direção para implementar e operar o SGSI;
> j) Preparar uma Declaração de Aplicabilidade. (ABNT, 2006, p. 4)

Observamos na norma 27001 que a identificação e gestão de riscos de segurança da informação, assim como a adequada definição de controles internos são processos ou práticas fundamentais para um SGSI.

Segundo BEAL (2005, p. 10), “Toda organização precisa adquirir uma visão sistêmica das suas necessidades de segurança, dos recursos a serem protegidos e

das ameaças às quais está sujeita, para então poder identificar as medidas de proteção mais adequadas, [...] para reduzir ou eliminar os principais riscos para o negócio.”.

Ainda, de acordo com BEAL (2005), as medidas de proteção são controles para eliminar ou reduzir o risco, e podem ser classificados como:

> - **Medidas preventivas:** controles que reduzem a probabilidade de uma ameaça se concretizar ou diminuem o grau de vulnerabilidade do ambiente/ativo/sistema, reduzindo assim a probabilidade de um ataque e/ou sua capacidade de gerar efeitos adversos na organização.
> - **Medidas corretivas ou reativas:** reduzem o impacto de um ataque/incidente. São medidas tomadas durante ou após a ocorrência do evento.
> - **Métodos detectivos:** expõem ataques/incidentes e disparam medidas reativas, tentando evitar a concretização do dano, reduzi-lo ou impedir que se repita. (BEAL, 2005, p. 26)

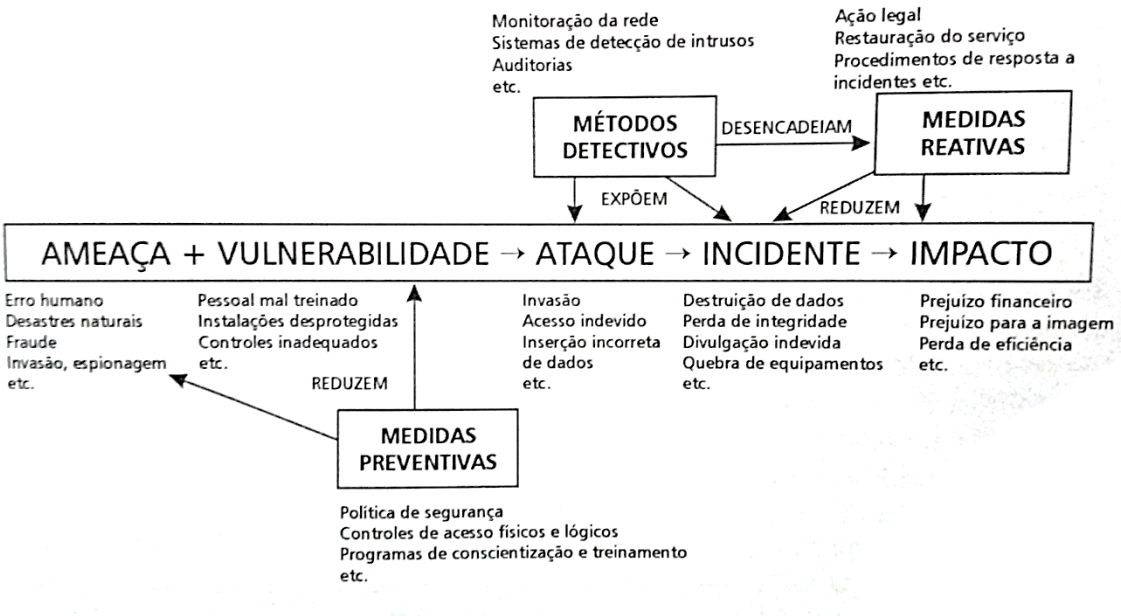



**Figura 1 - Componentes do risco e medidas de proteção usadas para reduzi-lo**

Com entendimento similar, SÊMOLA (2014, p. 47) descreve que medidas de segurança são controles que podem ser preventivos, detectivos e/ou corretivos. O primeiro, com objetivo de evitar a ocorrência de incidentes e garantir a segurança por meio de mecanismos que estabeleçam a conduta e a ética, como a política de segurança, procedimentos de trabalho e conscientização de usuários. Os detectivos objetivam identificar condições ou indivíduos causadores de ameaças e com possibilidade de evitar que as vulnerabilidades sejam exploradas, como exemplos

análise de riscos e alertas de segurança. Já os controles corretivos são ações para a correção de uma estrutura às condições estabelecidas pela organização ou para a redução dos impactos, como plano de continuidade e restauração de *backup*.

Segundo Kim & Solomon (2014, p. 12) independentemente do tamanho da empresa, uma estrutura típica de TI consiste em sete domínios, sendo eles os domínios de usuário, de estação de trabalho, de LAN, de LAN para WAN, de WAN, de acesso remoto e domínio de sistema/aplicativo, e cada um exige controles de segurança apropriados devendo atender a tríade de segurança da informação, Disponibilidade, Integridade e Confidencialidade. O autor ainda destaca que o domínio de usuário é o elo mais fraco em uma infraestrutura de TI e que o responsável por segurança precisa entender o que motiva uma pessoa a comprometer um sistema, aplicativos ou dados de uma organização.

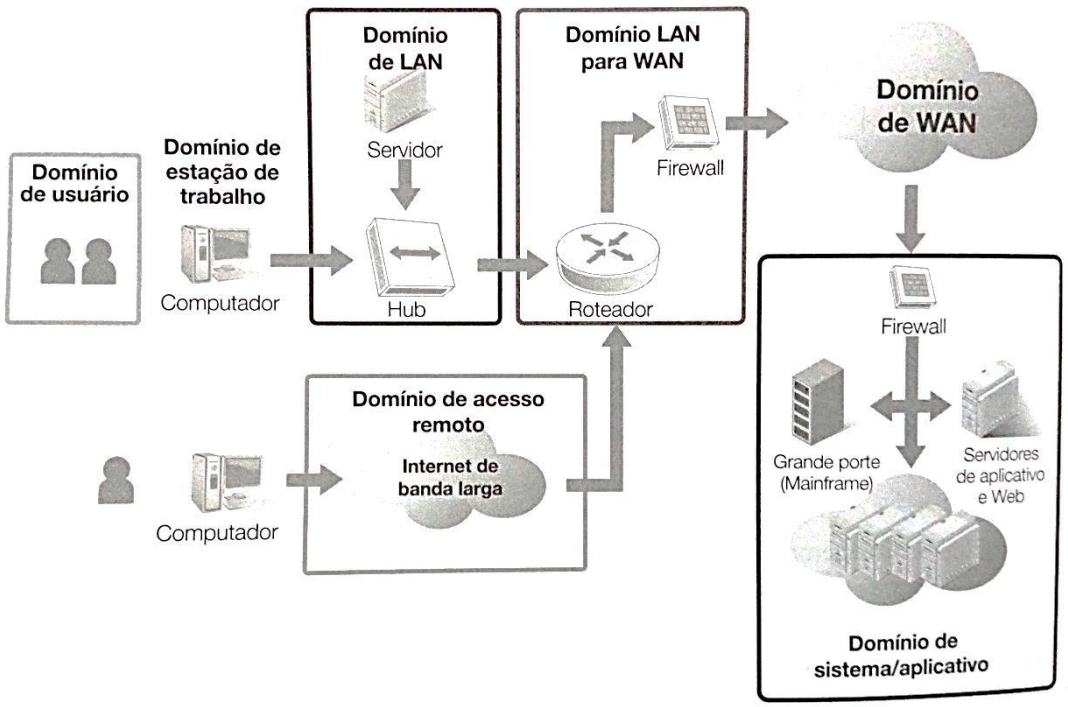



**Figura 2 - Os sete domínios de uma infraestrutura típica de TI**

Para o planejamento da segurança BEAL (2005) afirma que:

> A organização de planejar a implementação da segurança da informação começando do nível mais alto, de identificação dos processos críticos de negócios e dos fluxos de informação associados, antes de descer para o nível dos sistemas e serviços de informação que contribuem para esses processos e da infraestrutura de TI que dá suporte a tais sistemas e serviços. [...]

> Nesse caso, os requisitos de proteção da informação e dos ativos a ela associados são identificados com base em critérios objetivos, de acordo com o seu grau de importância para os processos de negócio e de sua sensibilidade em relação aos aspectos de confidencialidade, integridade e disponibilidade da informação. (BEAL, 2005, p. 38).

Na fase de planejamento da segurança, de acordo com a NBR ISO 27002 (2005, p. xi), é essencial que a organização identifique seus requisitos de segurança da informação e a norma relaciona três principais fontes para identificação destes requisitos. A primeira fonte é obtida a partir da avaliação de riscos, observando os objetivos e as estratégias da organização, para identificação das ameaças e vulnerabilidades, assim como uma estimativa da probabilidade de ocorrência e do impacto potencial associado. A segunda fonte é a legislação e regulamentação vigente, estatutos e cláusulas contratuais que a organização e todos seus parceiros de negócio devem estar em conformidade. A terceira fonte é um conjunto de princípios, objetivos e requisitos particulares do negócio para o processamento das informações pertinentes à operação da organização.

Para a etapa de implementação da segurança BEAL (2005, p. 39) descreve que todas as atividades necessárias devem ser executadas para atender aos requisitos de segurança que foram planejados, inclusive a divulgação da política de segurança, definição de normas e implantação dos controles físicos, lógicos, gerenciais e tecnológicos para tratamento do risco.

Segundo a norma NBR ISO 27002 (2005, p. xi), “a seleção de controles de segurança da informação depende das decisões da organização, baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado à organização, e convém que também esteja sujeito a todas as legislações e regulamentações [...]”

Esta norma também orienta como ponto de partida para a implementação da segurança da informação um certo número de controles baseados tanto em requisitos legais quanto nas melhores práticas utilizadas, sendo:

> Os controles considerados essenciais para uma organização, sob o ponto de vista legal, incluem, dependendo da legislação aplicável:
> a) proteção de dados e privacidade de informações pessoais;
> b) proteção de registros organizacionais;
> c) direitos de propriedade intelectual.
> Os controles considerados práticas para a segurança da informação incluem:
> a) documento da política de segurança da informação;
> b) atribuição de responsabilidades para a segurança da informação;
> c) conscientização, educação e treinamento em segurança da informação;

> d) processamento correto nas aplicações;
> e) gestão de vulnerabilidades técnicas;
> f) gestão da continuidade do negócio;
> g) gestão de incidentes de segurança da informação e melhorias.
> Esses controles se aplicam para a maioria das organizações e na maioria dos ambientes. (ABNT, 2005, p. xii)

Quanto à avaliação da segurança e ação corretiva, BEAL (2005, p. 39) ainda descreve que deve ser realizado testes de conformidade e de eficácia de controles, e revisão periódica dos resultados alcançados.

Ainda como prática de segurança da informação, BEAL (2005, p.40) e a norma ABNT NBR ISO 27002 (2005, p. 14) no item 6.1.8, entendem como controle relevante a análise crítica sobre a gestão de segurança da informação, de forma independente e periódica, necessária para assegurar que as práticas da organização permanecem adequadas e eficazes quanto aos riscos e controles existentes.

Há um aspecto interessante abordado especificamente por SÊMOLA (2014, p. 72) para o contexto de práticas e ferramentas de segurança da informação, não observado com esta mesma simplicidade e objetividade em outros autores, sobre a diferença norma versus metodologia, o qual cita que o fato de já existirem normas nacionais e internacionais que abordem o código de conduta para o gerenciamento da segurança da informação não soluciona os desafios das empresas, pois as normas indicam apenas O QUE fazer para o adequado gerenciamento, mas não como uma metodologia que explora o COMO deve ser realizadas as atividades.

Ainda neste contexto, SÊMOLA (2014) conclui que:

> Portanto, de nada adiantará estar ciente dos controles e aspectos apontados por uma norma se segurança se você não dispuser de uma metodologia condizente e consistente, capaz de orientar as atividades, transformando-as em resultados reais ligados à redução dos riscos. [...]
> Diante disso, adotar uma metodologia passou a ser fator crítico de sucesso para subsidiar o cada vez mais complexo plano de ação, ou melhor, o plano diretor de segurança.
> Exemplos de ferramentas metodológicas:
> - Formulário para mapeamento de vulnerabilidades
> - Formulário para mapeamento de processos de negócio críticos
> - Formulário para orientação na condução de entrevistas
> - Planilha para identificação de ativos físicos, tecnológicos e humanos
> - Planilha para estudo de sensibilidade à quebra de segurança
> - Instrumento para mapeamento topológico
> - Matriz de criticidade para priorização das ações
> - Matriz de tolerância à paralisação
>
> Diferentemente da norma que se propõe a orientar todos no sentido de construir uma base comum de conduta, não haverá uma única e recomendada metodologia. (SÊMOLA, 2014, p. 72).

Como observado, nenhuma norma, metodologia, controle ou outra prática por si só serão efetivos quanto à segurança da informação senão forem implementados na organização concomitantemente todas as práticas aplicáveis de avaliação de riscos, controles internos, sistema de gestão de segurança da informação, políticas e sistemas de proteção.

## 2.3 Riscos

O COSO (2013, p. 7) define risco como a possibilidade de que um evento ocorra e afete adversamente a realização dos objetivos da entidade.

“Costuma-se entender “risco” como possibilidade de “algo não dar certo”, mas seu conceito atual envolve a quantificação e qualificação da incerteza, tanto no que diz respeito às “perdas” como aos “ganhos”, com relação ao rumo dos acontecimentos planejados, seja por indivíduos, seja por organizações.” (IBGC, 2007, p.11)

A norma ABNT NBR ISO 31000 (2009, p.1) define risco como efeito da incerteza nos objetivos considerando que um efeito é um desvio em relação ao esperado seja ele de valor positivo ou negativo, enquanto que os objetivos podem ter diferentes aspectos e aplicados em diferentes níveis. A ISO considera ainda que o risco é muitas vezes caracterizado pela referência aos eventos potenciais e às consequências, ou uma combinação de ambos.

### 2.3.1 Riscos Corporativos

Negócios estão sujeitos a riscos e as organizações devem gerenciar estes riscos para prevenir perdas e contribuir para a tomada de decisão dos administradores. O processo de gerenciamento de riscos é abordado extensivamente na literatura com a visão estratégica de que agrega valor para a organização, melhora os padrões de governança, proporciona maior competitividade e promove a transparência aos *stakeholders*.

O IBGC (2007, 12) descreve que o modelo de gerenciamento de riscos corporativos é um instrumento de tomada de decisão da alta administração que visa melhor desempenho por meio de oportunidades de ganhos e de redução de probabilidade e/ou impacto de perdas [...].

Ainda, segundo o IBGC sobre a adoção de um modelo de Gerenciamento de Riscos Corporativos (GRCorp):

> [...] visa a permitir que a alta administração e demais gestores da organização lidem eficientemente com a incerteza, buscando um balanceamento ótimo entre desempenho, retorno e riscos associados.
> A implantação do GRCorp traz vários benefícios para a organização:
> a) Preserva e aumenta o valor da organização, mediante a redução da probabilidade e/ou impacto de eventos de perda, combinada com a diminuição de custos de capital que resulta da menor percepção de risco por parte de financiadores e seguradoras e do mercado em geral;
> b) Promove maior transparência, ao informar aos investidores e ao público em geral os riscos aos quais a organização está sujeita, as políticas adotadas para sua mitigação, bem como a eficácia das mesmas;
> c) Melhora os padrões de governança, mediante a explicitação do perfil de riscos adotado, em consonância com o posicionamento dos acionistas e a cultura da organização, além de introduzir uma uniformidade conceitual em todos os níveis da organização, seu conselho de administração e acionistas.
> Além dos benefícios listados acima, a implementação de um modelo de GRCorp eficaz apresenta ainda vários outros resultados positivos para a organização:
> d) Desenho de processos claros para identificar, monitorar e mitigar os riscos relevantes;
> e) Aprimoramento das ferramentas de controles internos (sistemas de controles) para medir, monitorar e gerir os riscos;
> f) Melhoria da comunicação entre as áreas da organização;
> g) Identificação e priorização dos riscos relevantes (exposição líquida, já considerando os impactos interrelacionados e integrados a diversos tipos de riscos);
> h) Definição de uma metodologia robusta para mensurar e priorizar riscos;
> i) Definição e implementação do modelo de governança para gerir a exposição (fóruns de decisão, políticas e processos e definição de alçadas);
> j) Identificação de competências para antecipar riscos relevantes e, se for o caso, mitigá-los após uma análise custo-benefício;
> k) Melhor entendimento do posicionamento competitivo da organização;
> l) Promoção de transparência para os stakeholders5, em relação aos fatores que possam valorizar ou prejudicar a organização. (IBGC, 2007, p. 12).

A norma ISO 31000 cita que uma organização para ter uma gestão de riscos eficaz atenda aos seguintes princípios:

> a) A gestão de riscos cria e protege valor.
> A gestão de riscos contribui para a realização demonstrável dos objetivos e para a melhoria do desempenho referente, por exemplo, à segurança e saúde das pessoas, à segurança, à conformidade legal e regulatória, à aceitação pública, à proteção do meio ambiente, à qualidade do produto, ao gerenciamento de projetos, à eficiência nas operações, à governança e à reputação.
> b) A gestão de riscos é parte integrante de todos os processos organizacionais.
> A gestão de riscos não é uma atividade autônoma separada das principais atividades e processos da organização. A gestão de riscos faz parte das responsabilidades da administração e é parte integrante de todos os processos organizacionais, incluindo o planejamento estratégico e todos os processos de gestão de projetos e gestão de mudanças.

> c) A gestão de riscos é parte da tomada de decisões.
> A gestão de riscos auxilia os tomadores de decisão a fazer escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação.
> d) A gestão de riscos aborda explicitamente a incerteza.
> A gestão de riscos explicitamente leva em consideração a incerteza, a natureza dessa incerteza, e como ela pode ser tratada.
> e) A gestão de riscos é sistemática, estruturada e oportuna.
> Uma abordagem sistemática, oportuna e estruturada para a gestão de riscos contribui para a eficiência e para os resultados consistentes, comparáveis e confiáveis.
> f) A gestão de riscos baseia-se nas melhores informações disponíveis.
> As entradas para o processo de gerenciar riscos são baseadas em fontes de informação, tais como dados históricos, experiências, retroalimentação das partes interessadas, observações, previsões, e opiniões de especialistas. Entretanto, convém que os tomadores de decisão se informem e levem em consideração quaisquer limitações dos dados ou modelagem utilizados, ou a possibilidade de divergências entre especialistas.
> g) A gestão de riscos é feita sob medida.
> A gestão de riscos está alinhada com o contexto interno e externo da organização e com o perfil do risco.
> h) A gestão de riscos considera fatores humanos e culturais.
> A gestão de riscos reconhece as capacidades, percepções e intenções do pessoal interno e externo que podem facilitar ou dificultar a realização dos objetivos da organização.
> i) A gestão de riscos é transparente e inclusiva.
> O envolvimento apropriado e oportuno de partes interessadas e, em particular, dos tomadores de decisão em todos os níveis da organização assegura que a gestão de riscos permaneça pertinente e atualizada. O envolvimento também permite que as partes interessadas sejam devidamente representadas e terem suas opiniões levadas em consideração na determinação dos critérios de risco.
> j) A gestão de riscos é dinâmica, iterativa e capaz de reagir a mudanças.
> A gestão de riscos continuamente percebe e reage às mudanças. Na medida em que acontecem eventos externos e internos, o contexto e o conhecimento modificam-se, o monitoramento e a análise crítica de riscos são realizados, novos riscos surgem, alguns se modificam e outros desaparecem.
> k) A gestão de riscos facilita a melhoria contínua da organização.
> Convém que as organizações desenvolvam e implementem estratégias para melhorar a sua maturidade na gestão de riscos juntamente com todos os demais aspectos da sua organização. (ABNT, 2009, p. 7)

Segundo estudo realizado pela Comissão de Valores Mobiliários sobre gerenciamento de riscos corporativos:

> O gerenciamento de riscos é mais holístico, ao inserir-se não só nos contornos das operações, mas também no direcionamento estratégico da organização, incorporando diferentes perspectivas, tais como o ambiente externo e a reputação da organização. Também, gerenciamento de riscos é mais amplo, incluindo o processo de identificação, mensuração (qualitativa ou quantitativa), avaliação de riscos, bem como a definição da atitude da organização perante estes riscos e os seus tratamentos (inclusive controle). (CVM, 2015, p. 14)

A implementação de um processo de gestão de riscos é constituída de várias atividades e etapas que são dinâmicas e iterativas devido às particularidades e objetivos de cada organização.

De acordo com a ISO 31000, o processo de gestão de riscos se dá pela “aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.” (ABNT, 2009, p. 7)

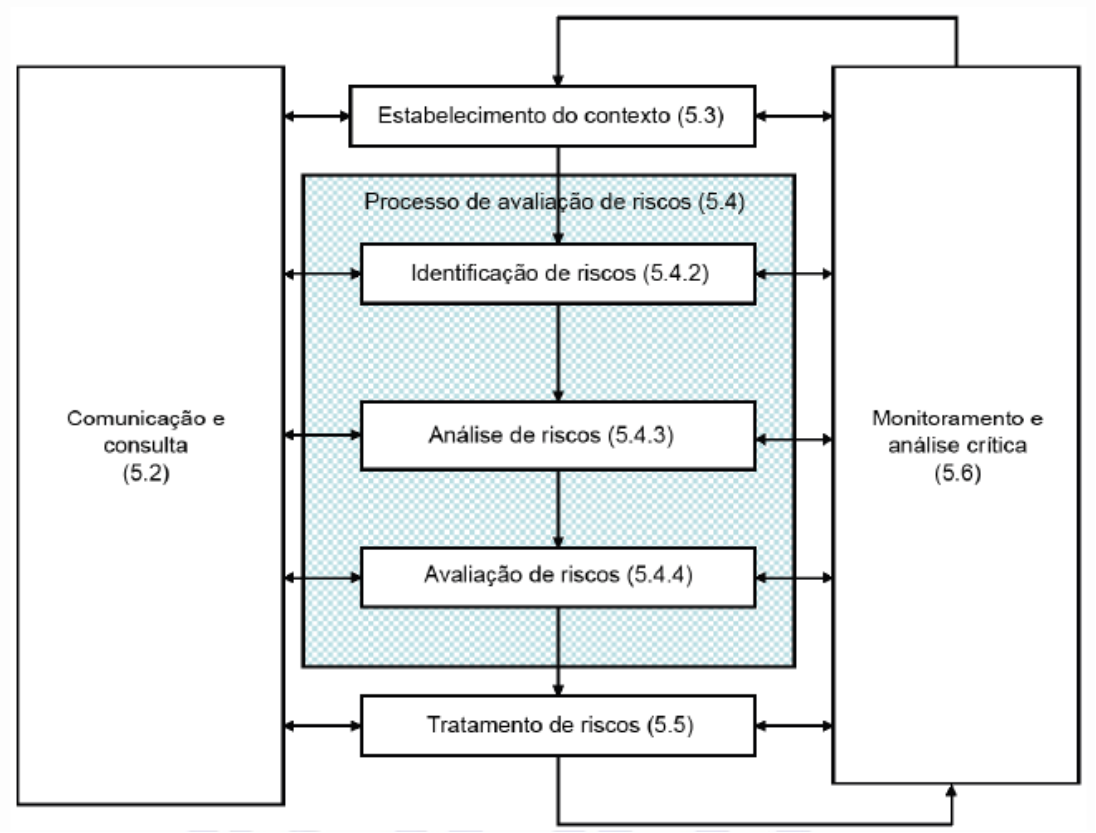



**Figura 3 - Processo de gestão de riscos (ABNT NBR ISO 31000)**

“A avaliação de riscos envolve um processo dinâmico e iterativo para identificar e avaliar os riscos à realização dos objetivos [...]. Dessa forma, a avaliação de riscos estabelece a base para determinar a maneira como os riscos serão gerenciados.” COSO (2013, p. 7).

Segundo o IBGC (2007, p. 16) durante a etapa de identificação de riscos deve-se definir os eventos, externos ou internos, que podem impactar os objetivos estratégicos da organização, inclusive os objetivos relacionados aos ativos

intangíveis[4]. Ressalta ainda que sempre haverá riscos desconhecidos pela organização, por isto o processo de identificação e análise de riscos deve ser continuamente monitorado e aprimorado.

Na identificação dos riscos convém classificá-los de acordo com as características de cada organização e particularidades do mercado em que atua, pois esta atividade irá beneficiar em uma análise mais eficaz quanto a qualidade da informação, mensuração, priorização e exposição de cada risco.

“Uma das formas de categorização dos riscos consiste em desenhar uma matriz que considere a origem dos eventos, a natureza dos riscos e uma tipificação dos mesmos” (IBGC, 2007, p. 17).

| | | Tipos | Natureza dos Riscos | | |
|---|---|---|---|---|---|
| | | | Estratégico | Operacional | Financeiro |
| origem dos eventos | Externo | Macroeconômico | | | |
| | | Ambiental | | | |
| | | Social | | | |
| | | Tecnológico | | | |
| | | Legal | | | |
| | Interno | Financeiro | | | |
| | | Ambiental | | | |
| | | Social | | | |
| | | Tecnológico | | | |
| | | Conformidade | | | |

**Figura 4 - Matriz de classificação de riscos**

A análise e avaliação dos riscos são fundamentais para a tomada de decisão quanto ao tratamento de cada risco, considerando grau de exposição, priorização de tratamento e controles internos mitigatórios a serem adotados.

Segundo a ISO 31000 (2009, p. 18) a fase de análise de riscos envolve analisar as causas e as fontes de risco, assim como a probabilidade de ocorrência e consequências positivas e negativas. Já a fase de avaliação de riscos é auxiliar na

[4] “Ativos intangíveis” podem ser entendidos como os ativos e métodos responsáveis pela diferença entre o market value (valor de mercado) e o book value (valor contábil) da organização. São direitos, sem representação física, que dão à organização uma posição exclusiva ou preferencial no mercado, ou seja, contribuem para o seu valor econômico.

tomada de decisões quanto ao tratamento e a prioridade para implementação do mesmo.

Sobre a avaliação de riscos o guia do IBGC (2007) cita que:

> Para se definir qual o tratamento que será dado a determinado risco, o primeiro passo 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 aspectos11: a probabilidade de ocorrência e o seu impacto (em geral medido pelo impacto no desempenho econômico-financeiro do período). Deve-se incorporar também o impacto "intangível" à análise. (IBGC, 2007, p. 20)

O IBGC (2007, p. 21) ainda recomenda como fundamental a elaboração de um Mapa de Avaliação dos Riscos para a priorização do gerenciamento de riscos e na definição de tratamento para cada risco identificado, conforme ilustração abaixo.

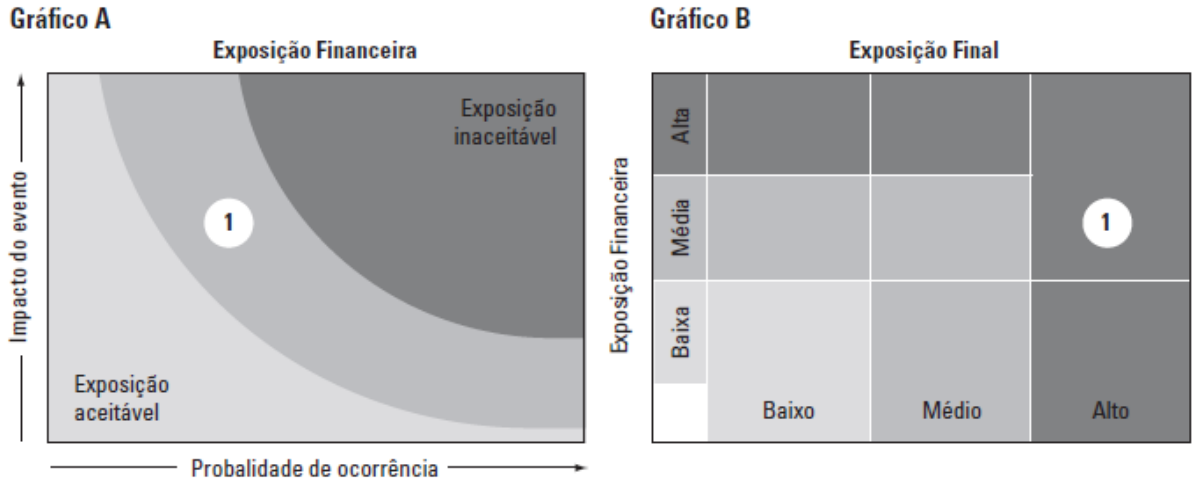



**Figura 5 - Mapa de Avaliação dos Riscos**

O Gráfico A, representa a avaliação de probabilidade e impacto de um risco (círculo com número 1) quanto à exposição financeira. Enquanto no gráfico B, representa a avaliação do risco com a exposição final (exposição financeira mensurada + impacto intangível).

### 2.3.2 Riscos de Tecnologia da Informação

Atualmente, qualquer empresa, independente do seu porte ou faturamento, utiliza de alguma maneira uma infraestrutura e/ou sistema de tecnologia para suas

operações, transações financeiras e relações comerciais. Os ambientes de TI das organizações diferem em tamanho, complexidade e riscos.

“Embora a tecnologia ofereça oportunidades de crescimento e desenvolvimento, representam também ameaças, como interrupções, enganos, roubos e fraudes.” (IIA, 2012, p. 4).

“O risco de TI sempre existe, seja ou não detectado ou reconhecido por uma empresa. Neste contexto, é importante identificar e gerenciar as questões de riscos de TI potencialmente significativas [...]” (ISACA, 2009, p. 11).

Segundo a ISACA (2009, p. 8), os riscos de negócio estão relacionados ao uso de TI. Essas conexões com os negócios são baseadas nos princípios efetivos da governança empresarial e gestão de riscos de TI, que são:

• Sempre se conecta aos objetivos de negócios;

• Alinha a gestão do risco de negócio relacionado à TI com o risco global da empresa (ERM) - se aplicável, isto é, se o ERM é implementado na empresa;

• Equilibra os custos e benefícios do gerenciamento de riscos de TI;

• Promove uma comunicação justa e aberta dos riscos de TI

• Estabelece o tom certo a partir do topo, definindo e aplicando responsabilização por operar dentro de níveis de tolerância aceitáveis e bem definidos;

• É um processo contínuo e parte das atividades diárias.

### 2.3.3 Riscos de Segurança da Informação

Para as organizações, os dados e informações são altamente valiosos, pois possibilitam tomadas de decisão mais precisas, vantagens tecnológicas e competitivas, conhecer o cliente e seus hábitos, ou até mesmo criar análises preditivas para gerar receitas futuras.

Neste contexto, a proteção das informações é de extrema importância para assegurar confidencialidade, integridade e disponibilidade. Sem a proteção adequada, as empresas ficam vulneráveis à várias ameaças inerentes à computação.

Riscos de segurança da informação são as possibilidades de uma ameaça explorar vulnerabilidades dos ativos, comprometendo a confidencialidade, integridade

e disponibilidade das informações de uma organização (ABNT NBR ISO/IEC 27005, 2008).

A norma ISO/IEC 27005 fornece diretrizes e descreve um processo genérico para a Gestão de Riscos de Segurança da Informação em uma organização, cabendo a cada organização avaliar os cenários e definir a melhor abordagem.

Segundo pesquisa realizada em 2015 pelo IIA e publicada no CBOK intitulado Navigating Technology's Top 10 Risks, o IIA identificou que o risco de segurança da informação é crítico e está em segundo lugar dentre os 10 top riscos de tecnologia, sendo precedido apenas pelo risco de cibersegurança, o qual é um assunto abordado dentro da perspectiva de segurança da informação. (CBOK, 2015, p. 7).

## 2.4 Auditoria Interna e Segurança da Informação

Nesta era tecnológica, a auditoria não pode se ater apenas aos sistemas e controles informatizados, por isso se adaptando mais uma vez, a auditoria de TI ampliou seu escopo e se especializou para avaliar também a eficácia dos processos de tecnologia e de governança em TI.

> Auditoria de TI é o ramo da auditoria que revisa e avalia os riscos de tecnologia da informação associados aos Processos de Tecnologia da Informação e aos Ativos de TI da organização, visando:
> - atender aos critérios da informação;
> - atingir eficaz e eficientemente os objetivos da organização;
> - promover a Governança Corporativa de TI. (IIA BRASIL, 2014, p.11).

Conforme a norma de desempenho 2110.A2 de Governança do IPPF (IIA, 2016) "A atividade de auditoria interna deve avaliar se a governança de tecnologia da informação da organização dá suporte às estratégias e objetivos da organização.".

O IPPF na Orientação Prática 2120-1: Avaliação da Adequação do Gerenciamento de Riscos cita o dever da auditoria avaliar riscos e contribuir com a melhoria do gerenciamento de riscos.

> 2120 – Gerenciamento de riscos: A atividade de auditoria interna deve avaliar a eficácia e contribuir para a melhoria dos processos de gerenciamento de riscos.
> Interpretação: Determinar se os processos de gerenciamento de riscos são eficazes é um julgamento que resulta da avaliação do auditor interno quanto a se:

> Os objetivos da organização dão suporte e estão alinhados com a missão da organização;
> Os riscos significativos são identificados e avaliados;
> Respostas apropriadas aos riscos são selecionadas de forma a alinhar os riscos com o apetite de risco da organização; e
> Informações de riscos relevantes são capturadas e comunicadas de forma oportuna através da organização, permitindo que colaboradores, administração e conselho cumpram com suas responsabilidades.
> A atividade de auditoria interna reúne informações para apoiar esta avaliação através de múltiplos trabalhos de auditoria. O resultado destes trabalhos, visto em conjunto, proporciona uma compreensão dos processos de gerenciamento de riscos das organizações e sua eficácia.
> Os processos de gerenciamento de riscos são monitorados através de atividades contínuas de gerenciamento, de avaliações específicas ou de ambos. (IPPF, 2013)

Na Orientação Prática 2120-3: Cobertura de Auditoria Interna para Riscos de Alcance dos Objetivos Estratégicos o IPPF determina que a auditoria interna também deve avaliar riscos relacionados à governança, operações e sistemas de informação.

> A atividade de auditoria interna deve avaliar as exposições a riscos relacionadas à governança, às operações e aos sistemas de informação da organização, em relação a:
> - Alcance dos objetivos estratégicos da organização;
> - Confiabilidade e integridade das informações financeiras e operacionais;
> - Eficácia e eficiência das operações e programas;
> - Salvaguarda dos ativos; e
> - Conformidade com leis, regulamentos, políticas, procedimentos e contratos. (IPPF, 2013)

Neste cenário de evolução constante da tecnologia, a auditoria interna deve avaliar também os riscos relacionados à segurança da informação, assim como avaliar como a empresa está manipulando seus dados e contribuir com a proteção da informação.

De acordo com IIA (2014), a auditoria interna deve avaliar se a organização está protegendo suas informações quanto à confidencialidade, integridade e disponibilidade.

> Os procedimentos de proteção das informações de uma organização são importantes para assegurar:
> - Confidencialidade: proteção de informações confidenciais para evitar a divulgação indevida.
> - Integridade: fidedignidade (que merece crédito) e totalidade da informação bem como sua validade de acordo os valores de negócios e expectativas
> - Disponibilidade: disponibilidade da informação quando exigida pelo processo de negócio hoje e no futuro. Também está ligada à

> salvaguarda dos recursos necessários e capacidades associadas. (IIA, 2014)

Segundo KIM & SOLOMON (2014) a auditoria de segurança deve assegurar que seus sistemas e controles funcionem conforme esperado e quando o auditor analisar seus sistemas deverá verificar se:

> **As políticas de segurança são sólidas e apropriadas para a empresa ou atividade?** A finalidade de segurança de informação é dar suporte à missão da empresa e protegê-la dos riscos que ela enfrenta. As políticas de sua organização e os documentos de suporte definem os riscos que a afetam. Os documentos incluem procedimentos, padrões e linhas de base de sua organização. Quando realiza uma auditoria, você está fazendo a seguinte pergunta: “Nossas políticas são seguidas e compreendidas? ” A auditoria em si não define novas políticas. Auditores, porém, podem fazer recomendações com base em experiência ou conhecimento de novas regulamentações.
> **Existem controles que apoiam suas políticas?** Os controles de segurança estão alinhados corretamente às estratégicas e à missão de sua organização? Eles apoiam suas políticas e sua cultura? Se você não puder justificar um controle com uma política, provavelmente deverá removê-lo. Sempre que um controle for explicado como “por segurança”, mas sem qualquer outra explicação, você deverá removê-lo. Segurança não é um centro de lucro e nunca deverá existir por conta própria. É um departamento de suporte cuja finalidade é proteger os ativos e o fluxo de receita da organização.
> **Existem implementação e manutenção efetivas de controles?** À medida que sua organização evolui e ameaças amadurecem, é importante garantir que os controles ainda façam frente aos riscos que você enfrenta hoje. (KIM & SOLOMON, 2014, p. 165).

No estudo CBOK (2015) intitulado Lidando com os 10 Principais Riscos Tecnológicos, o IIA, observa que “Os riscos tecnológicos primários e emergentes de sua organização estão sendo identificados e geridos apropriadamente? Essa é uma das perguntas fundamentais que os comitês de auditoria e conselhos de organizações em todos os lugares estão fazendo. ” (IIA, 2015, p.4).

A ordem de prioridade dos riscos pode variar dependendo do mercado de atuação de cada empresa, dessa maneira os 10 principais riscos tecnológicos abordados neste CBOK, são:

| | |
|---|---|
| 1 | CIBERSEGURANÇA |
| | • Roubo de dados sensíveis ou sigilosos |
| 2 | SEGURANÇA DA INFORMAÇÃO |
| | • Danos à confidencialidade, integridade e disponibilidade das informações críticas para a organização |
| 3 | PROJETOS DE DESENVOLVIMENTO DE SISTEMAS DE TI |
| | • Falhas e/ ou insucesso no desenvolvimento ou atualização de sistemas tecnológicos |
| 4 | GOVERNANÇA DE TI |
| | • Desalinhamento da TI com os processos de negócio e objetivos da organização |
| 5 | SERVIÇOS TERCEIRIZADOS DE TI |
| | • Processos tecnológicos essenciais executados por terceiros e/ou materialização de riscos não conhecidos pela contratante |
| 6 | USO DE MÍDIAS SOCIAIS |
| | • Violação de política de mídias sociais e postagem de mensagens prejudiciais |
| 7 | COMPUTAÇÃO MOBILE |
| | • Extravio de dados, descumprimento de procedimentos e leis, invasão de privacidade ou vulnerabilidades na rede |
| 8 | HABILIDADES DE TI ENTRE AUDITORES INTERNOS |
| | • Ausência de auditores de TI qualificados |
| 9 | TECNOLOGIAS EMERGENTES |
| | • Tecnologias que não estejam em uso e/ou não possuem diretrizes na organização atualmente, mas que podem ser empregadas no futuro próximo (exemplo: Big Dta e Internet das Coisas) |
| 10 | CONSCIENTIZAÇÃO TECNOLÓGICA DO COMITÊ E DO CONSELHO DE AUDITORIA |
| | • Nível de conhecimento/expertise de TI limitado no conselho e comitê de auditoria |

**Quadro 1 - Resumo dos 10 principais riscos de tecnológicos (CBOK 2015)**

Para cada risco o estudo CBOK (2015) traz a lista de perguntas fundamentais para os auditores internos fazerem sobre o risco e as atividades fundamentais para lidar com estes riscos tecnológicos. Destes 10 riscos, destaca-se conforme objetivos deste trabalho, as perguntas e atividades chaves recomendadas para a auditoria interna referentes aos 6 riscos diretamente relacionados à governança e segurança da informação.

Quanto ao risco 1 – Cibersegurança, o CBOK cita:

**PERGUNTAS CHAVE PARA A AUDITORIA INTERNA FAZER**

1. A organização é capaz de monitorar intrusões suspeitas na rede?
2. A organização é capaz de identificar se um ataque está ocorrendo?
3. A organização pode isolar o ataque e restringir danos potenciais?
4. A organização é capaz de saber se dados confidenciais estão saindo da organização?
5. Se houver um incidente, há um plano formal de gerenciamento de crises em prática, testado e alinhado ao risco organizacional?
6. Se houver um incidente, a organização tem acesso a habilidades forenses para auxiliar com o incidente?
7. A equipe de incidentes está a postos e sabe de seus papéis e responsabilidades?

**ATIVIDADES CHAVE PARA A AUDITORIA INTERNA CONDUZIR**

1. Conduzir um exame anual independente e um teste de penetração da rede externa.
2. Verificar que exercícios de simulação sejam realizados com relação ao plano de gerenciamento de crises da organização, para preparar a equipe de incidentes para o caso de um incidente real.
3. Conduzir uma auditoria da arquitetura de rede, para determinar a conformidade com as políticas e procedimentos de rede.
4. Conduzir uma auditoria de um incidente recente e determinar se as políticas, procedimentos e ferramentas foram aplicadas conforme planejado e se os especialistas forenses atuaram durante o incidente.

**Quadro 2 - Perguntas e atividades de auditoria para o risco de cibersegurança (CBOK 2015)**

Quanto ao risco 2 – Segurança da Informação, o CBOK (2015) destaca que “A auditoria interna tem um papel principal a desempenhar para garantir que o programa de segurança da informação de uma organização seja eficaz e eficiente.” e elenca as perguntas e atividades a seguir:

## PERGUNTAS CHAVE PARA A AUDITORIA INTERNA FAZER

1. Qual foi a última vez em que a política de segurança da informação foi revisada e atualizada?
2. Qual a taxa de sucesso do programa de treinamento de conscientização de segurança? O treinamento é obrigatório? Quais as repercussões para os que não completaram o treinamento ainda?
3. Qual foi a última vez em que uma avaliação de riscos foi feita? A avaliação de riscos é feita para todos os novos fornecedores terceirizados?
4. A organização simula incidentes para determinar sua prontidão?
5. Qual foi a última vez em que um teste de recuperação de desastres foi feito? Foi bem sucedido? Quais questões foram encontradas?
6. Quais requisitos de conformidade a organização tem? *Health Insurance Portability and Accountability Act* de 1996 (HIPAA)? Lei Sarbanes-Oxley de 2002 (SOX)? *PCI Security Standards Council*?
7. Um infrator externo pode penetrar o parâmetro físico usando engenharia social? (Um exemplo desse tipo de violação seria começar uma conversa casual com um funcionário do lado de fora do prédio e entrar com ele no prédio quando passar o crachá na entrada.
8. A organização registra e monitora as atividades de usuários privilegiados (aqueles com autoridade administrativa para gerir o ambiente de TI)?

## ATIVIDADES CHAVE PARA A AUDITORIA INTERNA CONDUZIR

1. Conduzir um exame de vulnerabilidade da rede interna.
2. Revisar o processo de controle de acesso. Os proprietários realmente revisam a lista de acesso ou a revisão é um exercício de conformidade, no qual os proprietários apenas "aprovam" sem realmente examiná-la?
3. Usar terceiros para conduzir um ataque simulado e auditar os resultados. Por exemplo, conduzir um exercício de e-mail de phishing, para determinar a eficácia do programa de treinamento de conscientização (organizações médias e grandes).
4. Auditar o backup das informações críticas e verificar que os backups sejam realizados rotineiramente.
5. Auditar a atividade de usuários privilegiados e verificar se apenas usuários autorizados têm capacidades privilegiadas. Além disso, verificar se usuários privilegiados são registrados e monitorados.
6. Auditar terceiros que tenham acesso aos ativos críticos da organização ou revisar os relatórios Nº 16 de *Statement on Standards for Attestation Engagements* (SSAE) (organizações de grande porte).

**Quadro 3 - Perguntas e atividades de auditoria para o risco de Segurança da Informação (CBOK 2015)**

Quanto ao risco 4 – Governança de TI, as perguntas e atividades chaves de auditoria são:

**PERGUNTAS CHAVE PARA A AUDITORIA INTERNA FAZER**

1. Quais atividades TI está conduzindo para se alinhar com o negócio? Com que frequência TI se reúne com o corporativo para entender suas necessidades?
2. Qual é a percepção corporativa das capacidades e desempenho da TI?
3. Como TI determina o valor que agrega ao negócio?
4. Como os executivos de TI determinam o número apropriado de recursos a serem empregados na TI?
5. A TI conduz uma avaliação de riscos de TI periodicamente?
6. A TI tem métricas chave de desempenho definidas, para mensurar seu desempenho?
7. A TI gerencia seu custo?

**ATIVIDADES CHAVE PARA A AUDITORIA INTERNA CONDUZIR**

1. Avaliar o "tom no topo" da organização de TI em relação à cultura corporativa, métricas/expectativas de desempenho definidas, *service-level agreements* (SLA), atendimento ao cliente e etc.
2. Periodicamente, conduzir uma auditoria para determinar se a função de TI está alinhada e entende as prioridades estratégicas da organização.
3. Revisar a eficácia da gestão de recursos e desempenho de TI.
4. Avaliar os riscos que possam prejudicar o ambiente de TI.
5. Auditar as métricas de custo em prática no ambiente de TI.
6. Examinar o negócio, para determinar a percepção dos líderes do negócio sobre as capacidades e desempenho de TI.
7. Comparar o programa de conformidade dentro da organização com estruturas estabelecidas, tais como *Control Objectives for Information and Related Technology* (COBIT), *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), *National Institute of Standards and Technology* (NIST) e *International Organization for Standardization* (ISO) 27001 e ISO 27002, conforme apropriado (grandes organizações).

**Quadro 4 - Perguntas e atividades de auditoria para o risco de Governança de TI (CBOK 2015)**

Para o risco 6 – Uso de Mídias Sociais, o estudo recomenda como práticas às organizações e auditoria interna que:

> Para abordar os riscos de mídias sociais, as organizações devem incorporar os passos a seguir como parte de seus procedimentos de mídias sociais:
>
> 1. Definir uma política de uso corporativo de mídias sociais.
> 2. Comunicar a política por meio de um programa de conscientização e treinamento de segurança.
> 3. Implementar a política por meio do emprego de softwares de "filtros de conteúdo" para tecnologias, tais como Web 2.0.
> 4. Monitorar os resultados, para garantir que a política esteja sendo seguida.
> 5. Aplicar a política àqueles que a violarem.
>
> Os auditores internos podem ter um papel chave no gerenciamento de riscos associados às mídias sociais. Eles podem atuar no papel de consultores, enquanto a organização implementa os passos acima. Além disso, a auditoria interna deve considerar a inclusão de uma auditoria de mídias sociais como parte de seu plano anual de auditoria. (IIA, 2015, p. 18)

Ainda para auditoria interna, as perguntas e atividades chaves são:

**PERGUNTAS CHAVE PARA A AUDITORIA INTERNA FAZER**

1. Como a organização usa as redes sociais para atingir seus clientes e consumidores?
2. Qual conteúdo é permitido para postagem em sites de redes sociais?
3. Há um grupo ou pessoa responsável pelo monitoramento dos conteúdos reais disponíveis em redes sociais (condução de varreduras de sites de mídias sociais)?
4. Qual conteúdo é monitorado pelo software de "filtro de conteúdo"? Quem monitora os alertas criados pelo software?
5. Quais são as consequências para um funcionário que viole a política de mídias sociais?

**ATIVIDADES CHAVE PARA A AUDITORIA INTERNA CONDUZIR**

1. Conduzir uma auditoria das políticas e procedimentos de mídias sociais.
2. Revisar a adequação do treinamento de conscientização, para garantir que o tópico das mídias sociais seja abordado.
3. Entender o uso do software de "filtro de conteúdo" e sua eficácia para monitorar a entrada e saída de conteúdo.
4. Conduzir uma varredura independente de sites de mídias sociais, para determinar o conteúdo organizacional disponível.

**Quadro 5 - Perguntas e atividades de auditoria para o risco de Uso de Mídias Sociais (CBOK 2015)**

A evolução da tecnologia e multiplicação de dispositivos móveis, faz com que o risco 7 – Computação Mobile desafie a abordagem tradicional de um departamento

de tecnologia quanto ao gerenciamento de riscos, pois há vários outros riscos associados como segurança, legal, conformidade, privacidade e gestão de serviços. Quanto ao papel da auditoria, CBOK recomenda as seguintes perguntas e atividades:

**PERGUNTAS CHAVE PARA A AUDITORIA INTERNA FAZER**

1. A organização tem um processo para inventário de todos os dispositivos de computação mobile?
2. Como a organização gerencia dispositivos de computação mobile roubados ou perdidos?
3. Como a organização gerencia BYODs?
4. Como a organização gerencia o conteúdo em dispositivos móveis quando um funcionário deixa a organização?
5. Os dispositivos móveis são criptografados?

**ATIVIDADES CHAVE PARA A AUDITORIA INTERNA CONDUZIR**

1. Conduzir uma auditoria do processo de inventário dos dispositivos de computação mobile.
2. Auditar como dispositivos perdidos ou roubados são geridos.
3. Entender a forma como uma organização decide sobre o tipo de informação que pode ser armazenada em dispositivos móveis.
4. Verificar que informações delicadas não estejam sendo armazenadas em dispositivos móveis ou que sejam criptografadas.

**Quadro 6 - Perguntas e atividades de auditoria para o risco de Computação Mobile (CBOK 2015)**

O último a ser destacado é o risco 9 – Tecnologias Emergentes, o qual é abordado no CBOK como tecnologias que serão adotadas pela companhia em um futuro próximo, como por exemplo Big Data, análise preditiva de dados, internet das coisas (IOT), robótica, etc...

O IIA (2015, p.23) observa que “O ritmo no qual a tecnologia está mudando e evoluindo é impressionante e pode rapidamente apresentar novos riscos à organização. [...] A tecnologia emergente pode significar coisas diferentes para diferentes organizações.”.

Ainda, no que se refere ao risco de Tecnologias Emergentes, o CBOK (2015) cita que a auditoria interna pode realizar uma função importante na implantação de tecnologias emergentes na organização, pois pode orientar quanto aos riscos

envolvidos e requisitos de controle necessários desde as fases iniciais dessa implantação; e ainda atuando com as perguntas e atividades chaves a seguir:

**PERGUNTAS CHAVE PARA A AUDITORIA INTERNA FAZER**

1. A organização tem uma equipe que avalie as tecnologias emergentes de TI?
2. A organização tem um processo formal de avaliação de tecnologias emergentes?
3. Como a organização identifica os riscos apresentados pelas tecnologias emergentes?
4. Quais projetos atuais estão em condução nos quais novas tecnologias serão empregadas no ambiente de produção?

**ATIVIDADES CHAVE PARA A AUDITORIA INTERNA CONDUZIR**

1. Obter um inventário das tecnologias atualmente em uso.
2. Entender os novos projetos nos quais tecnologias emergentes possam ser empregadas.
3. Auditar o processo de riscos para tecnologias emergentes (como o risco é identificado durante a avaliação da tecnologia emergente).
4. Comunicar-se com a equipe de tecnologia de TI, para entender sua estratégia de adoção de tecnologias emergentes.

**Quadro 7 - Perguntas e atividades de auditoria para o risco de Tecnologias Emergentes (CBOK 2015)**

O IIA (2015, p. 26) conclui neste estudo CBOK que “Embora seja impossível prever o futuro, podemos ter certeza de que o cenário tecnológico mudará. Os auditores internos devem estar preparados para adaptação.”.

## 3 METODOLOGIA DA PESQUISA

A metodologia de pesquisa descreve de maneira detalhada e exata as etapas a seguir em um trabalho de pesquisa, além de explicar o tipo e abordagem de pesquisa, o instrumental utilizado, cronograma previsto, coleta e análise dos dados.

## 3.1 Quanto à Abordagem do Problema

Um estudo pode ter uma abordagem qualitativa ou quantitativa. Entende-se que a metodologia de pesquisa deste estudo é de caráter qualitativo sobre a análise das revisões literárias e levantamento do cenário atual das empresas atuantes do Grupo dos Auditores Internos do Paraná.

Quanto ao objetivo da pesquisa, se desenvolve pelo método descritivo, pois segundo Beuren et al., (2012, p. 81) “a pesquisa descritiva configura-se como um estudo intermediário entre a pesquisa exploratória e a explicativa, ou seja, não é tão preliminar como a primeira nem tão aprofundada como a segunda. Nesse contexto, descrever significa identificar, relatar, comparar, entre outros aspectos”.

Este trabalho tem como objetivo elencar as melhores práticas de auditoria interna para a identificação e monitoramento de riscos de segurança da informação recomendadas pela literatura e verificar se as auditorias inseridas no GAIP (Grupo dos Auditores Internos do Paraná) estão aderentes à essas práticas.

De acordo com MARTINS (2007), a Pesquisa Bibliográfica é a “Explicação e discussão de um assunto com base em livros, enciclopédias, jornais, sites, Cds, anais etc...”. MARTINS (2007) também cita a estratégia de Levantamento (*survey*) como “Estratégias apropriadas para análise de fatos e discussões. Exige sistematização na coleta de dados”.

## 3.2 Universo da Pesquisa

O GAIP - Grupo dos Auditores Internos do Paraná, criado em 2012, tem mantido sua organização desde então pela plataforma LinkedIn©, com objetivo de divulgar os temas, agenda e local dos encontros presenciais a todos os profissionais participantes do grupo.

Até o momento dessa pesquisa, o GAIP possui 472 profissionais inscritos no LinkedIn©, sendo estes profissionais de auditoria interna, riscos, controles internos, compliance e demais profissionais interessados em temas de governança corporativa.

O universo a ser pesquisado compreende todos os inscritos no GAIP, porém vale ressaltar que para os últimos cinco encontros presenciais, quatro em 2016 e um em 2017, a média de participantes foi de 56 profissionais.

## 3.3 Quanto à Coleta de Dados

Este trabalho utilizou-se das técnicas de pesquisa bibliográfica e de levantamento de informações (survey), a primeira para levantamento de conceitos, métodos, práticas e sistemas utilizados em auditoria interna, tecnologia, riscos e segurança da informação; já a segunda foi realizada por meio de questionário e observação direta extensiva para identificar a aderência e maturidade das empresas inseridas no GAIP quanto às melhores práticas citadas neste trabalho.

O questionário pretende captar a estrutura de governança das organizações inseridas no GAIP através da percepção de seus colaboradores quanto aos departamentos e estruturas de auditoria interna, gestão de riscos, controles internos, avaliação de riscos de segurança da informação e práticas utilizadas por estas entidades.

Para tanto, este questionário foi elaborado com 39 perguntas e subdividido em 4 categorias: Perfil Profissional, com objetivo de identificar o perfil e posição de atuação do colaborador dentro da empresa; Perfil da Organização, busca entender a complexidade da estrutura e governança de cada entidade e mercado de atuação; Perfil da Auditoria Interna, aborda a estrutura e equipe, atividades/responsabilidades, práticas e abordagem à riscos de segurança da informação; Visão do Profissional, para captar qual a percepção do colaborador sobre a segurança da informação e sua relevância para a organização, auditoria interna e para o próprio profissional.

O questionário foi elaborado e disponibilizados por meio digital utilizando a plataforma Google Formulários, com questões objetivas de múltiplas escolhas. O *link* para acesso ao questionário foi divulgado aos integrantes do GAIP através do seu grupo no site LinkedIn© e por email.

As perguntas do questionário e suas respectivas opções de resposta estão disponíveis no APÊNDICE 1 – QUESTIONÁRIO.

## 3.4 Quanto ao Cronograma

Este trabalho, desde a elaboração do projeto até sua entrega final, se desenvolveu conforme o cronograma abaixo**:**

| Meses / Atividades | Jul /16 | Ago /16 | Set /16 | Out /16 | Nov /16 | Dez /16 | Jan /17 | Fev /17 | Mar /17 | Abr /17 | Mai /17 | Jun /17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Aula Inicial** | **X** | | | | | | | | | | | |
| **Apresentação do Pré-projeto - Ideia** | | **X** | | | | | | | | | | |
| **Devolução do Pré-projeto- Revisão** | | | **X** | | | | | | | | | |
| **Retorno para alunos** | | | | **X** | | | | | | | | |
| **Revisão dos Pré-projeto pelos alunos - Encontro** | | | | **X** | | | | | | | | |
| **Recebimento e revisão pela Coordenação** | | | | | **X** | | | | | | | |
| **Devolução para os Alunos do Pré-projeto** | | | | | **X** | | | | | | | |
| **Revisão Bibliográfica – apresentação seminário** | | | | | | **X 03/12** | | | | | | |
| **Início da execução do projeto – TCC- Cronograma** | | | | | | **X** | **X** | | | | | |
| **Aprofunda-mento da Revisão Bibliográfica** | | | | | | **X** | **X** | **X** | | | | |
| **Período de Resposta ao Questionário** | | | | | | | | | **X 21/03** | **X** | **X 08/05** | |
| **Análise dos Resultados** | | | | | | | | | | | **X** | **X** |
| **Continuação do TCC – Cronograma de Orientação** | | | | | | **X** | **X** | **X** | **X** | **X** | **X** | **X** |
| **Entrega do TCC** | | | | | | | | | | | | **X 30/06** |

O questionário ficou disponível para resposta entre os dias 21 de março a 08 de maio de 2017.

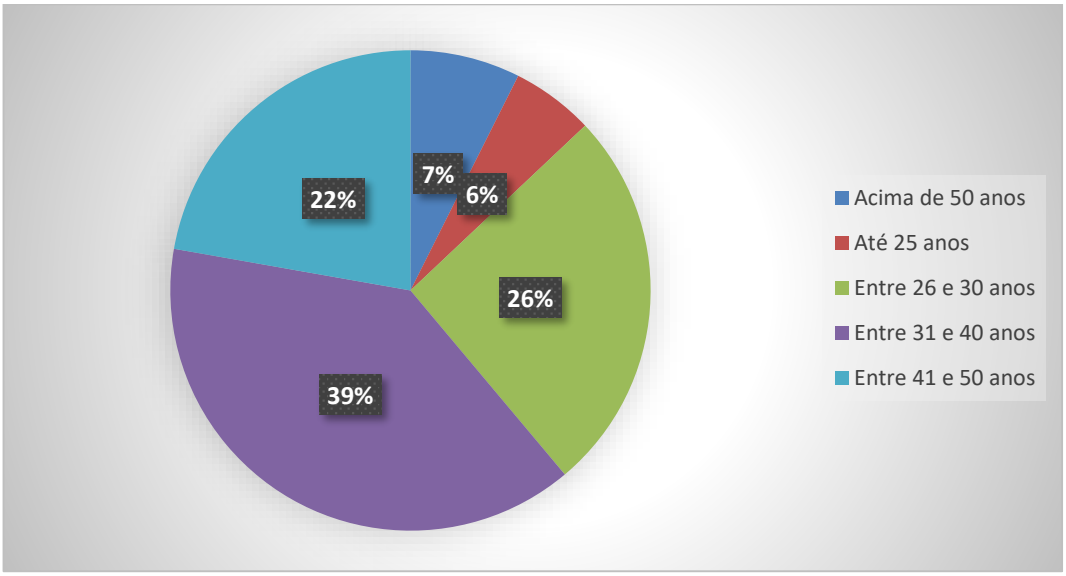
# 4 RESULTADOS E DISCUSSÃO

Os resultados obtidos e a interpretação dos dados coletados é apresentada em três partes: a primeira refere-se ao perfil dos profissionais entrevistados, a segunda ao perfil das organizações e estrutura de governança, a terceira parte trata da estrutura de auditoria interna e se a auditoria interna das empresas e profissionais participantes do GAIP estão seguindo as melhores práticas para atuar com os principais riscos de segurança da informação na era de tecnologias emergentes.

## 4.1 Perfil dos Profissionais

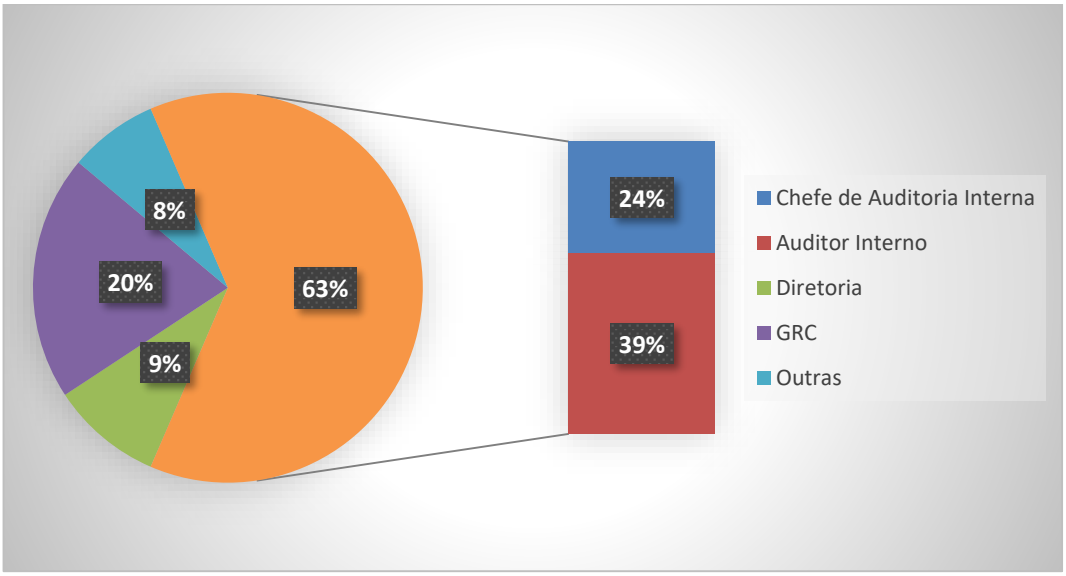
As faixas etárias predominantes dos profissionais do GAIP correspondem às idades entre 26-30 anos (26%), 31-40 anos (39%) e 41-50 anos (22%), perfazendo 87% dos respondentes, conforme ilustrado no (GRÁFICO 1).

**GRÁFICO 1 - FAIXA ETÁRIA DOS PROFISSIONAIS**



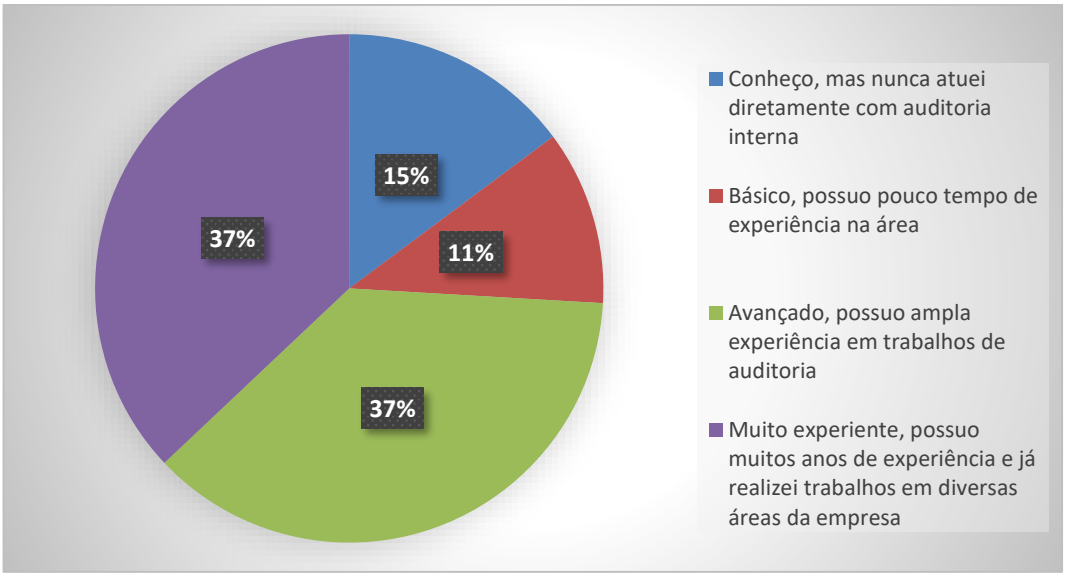

Verificou-se que 63% dos respondentes são profissionais com cargos de auditoria interna, os quais 24% exercem uma posição de chefia na auditoria interna de suas empresas, conforme ilustrado no (GRÁFICO 2).

**GRÁFICO 2 - POSIÇÃO ATUAL DOS PROFISSIONAIS**




A questão “Como você avalia seu conhecimento em auditoria interna?” teve como objetivo verificar de maneira geral o nível de experiência dos respondentes com atividades de auditoria interna e também de maneira simplista o nível de maturidade atual do GAIP. Verificou-se que o nível Avançado (37%) e Muito Experiente (37%) correspondem a 74% dos entrevistados, representando um elevado nível de experiência dos integrantes do GAIP e maturidade suficiente para discussão de qualquer tema relacionado a auditoria interna, conforme ilustrado no (GRÁFICO 3).

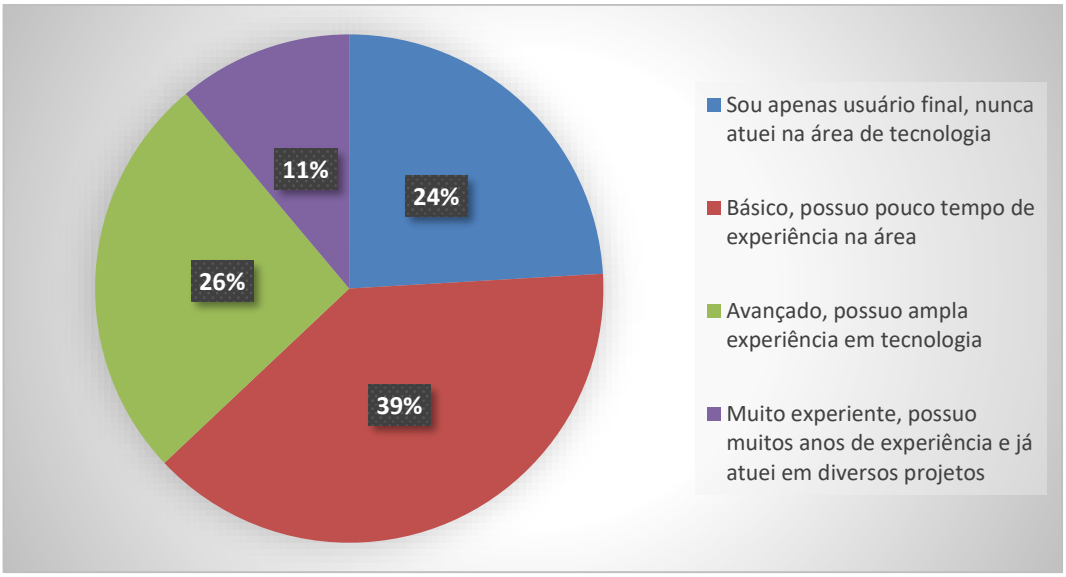
**GRÁFICO 3 - NÍVEL DE EXPERIÊNCIA EM AUDITORIA INTERNA**



De maneira geral, a questão “Como você avalia seu conhecimento em tecnologia?” visou captar se os auditores internos e demais profissionais do GAIP possuem experiência em tecnologia da informação ou apenas conhecimento limitado de usuário, com baixo nível de conhecimento em atividades de TI, pois entende-se que um usuário não precisa conhecer requisitos, riscos e controles de TI ou de segurança da informação para utilizar uma tecnologia.

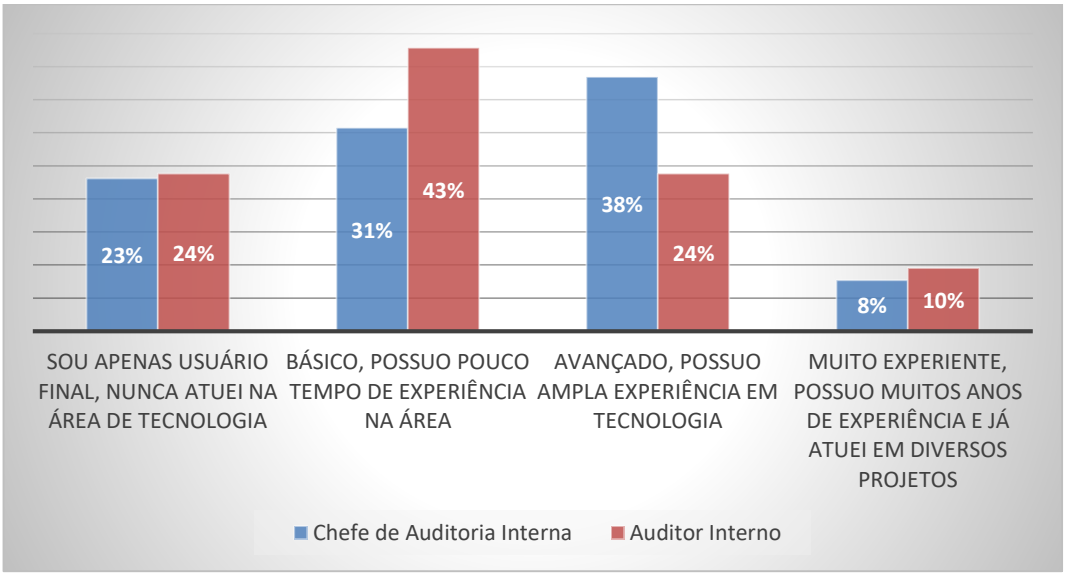
Conforme visualizado no (GRÁFICO 4), o nível de conhecimento em TI desses profissionais é considerado básico (39%) ou limitado/usuário (24%) para um total de 63% dos respondentes.

**GRÁFICO 4 - NÍVEL DE CONHECIMENTO EM TECNOLOGIA**




Quando analisado este nível de conhecimento em TI especificamente para os que exercem atividades de auditoria interna, observa-se uma possível defasagem em auditores com habilidades e/ou preparados para atuar com riscos, controles e/ou auditorias em tecnologia e segurança da informação, pois apenas 34% dos auditores internos e 46% dos chefes de auditoria possuem conhecimento mais aprofundado em tecnologia (GRÁFICO 5).

**GRÁFICO 5 - NÍVEL DE CONHECIMENTO EM TECNOLOGIA DOS AUDITORES**

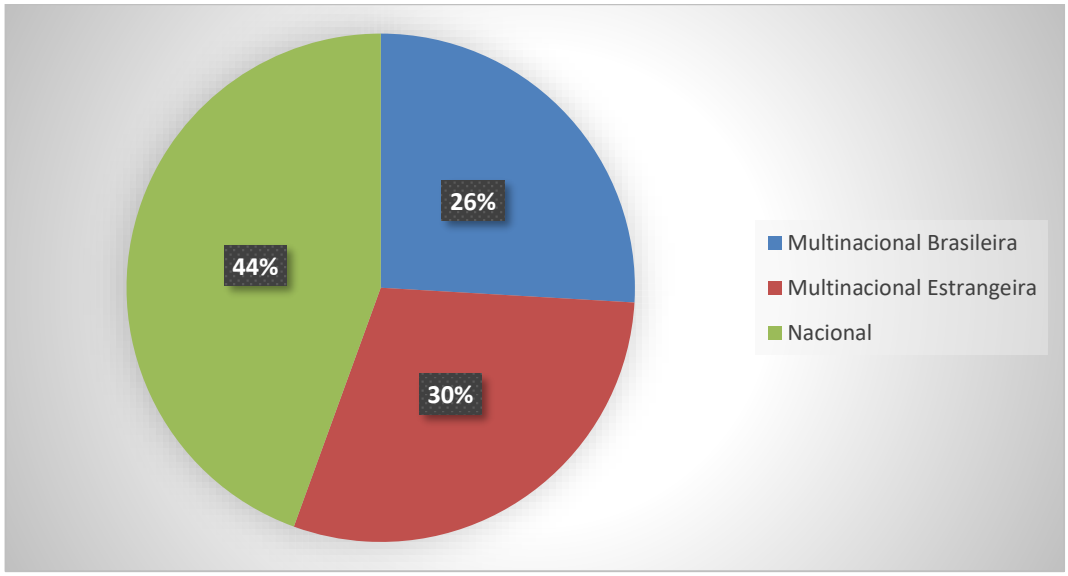



## 4.2 Perfil das Organizações

A análise do perfil das empresas com integrantes no GAIP torna-se relevante, pois estas entidades possuem origem, culturas e cenários econômico-financeiros distintos entre elas, os quais impactam no nível de governança corporativo estabelecido. As questões elaboradas referentes ao perfil das organizações tiveram o objetivo de elencar as principais características e qual o impacto destas na estrutura e práticas de auditoria interna.

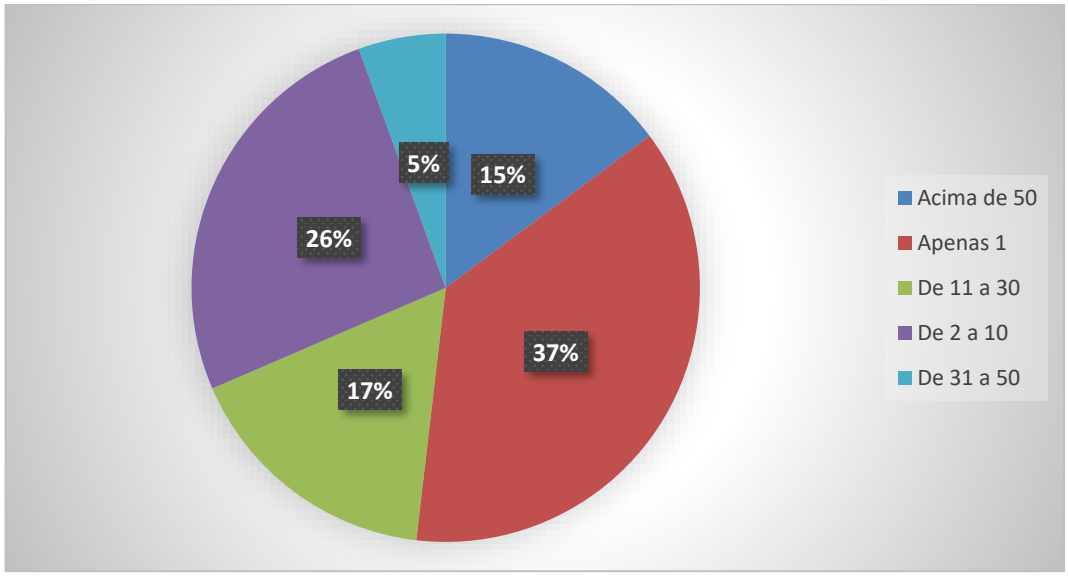
Verificou-se que 70% das empresas dos respondentes do GAIP são brasileiras, com atuação totalmente nacional (44%) e com filiais em outros países (26%), conforme apresentado no (GRÁFICO 6).

**GRÁFICO 6 - PRESENÇA DA ORGANIZAÇÃO**



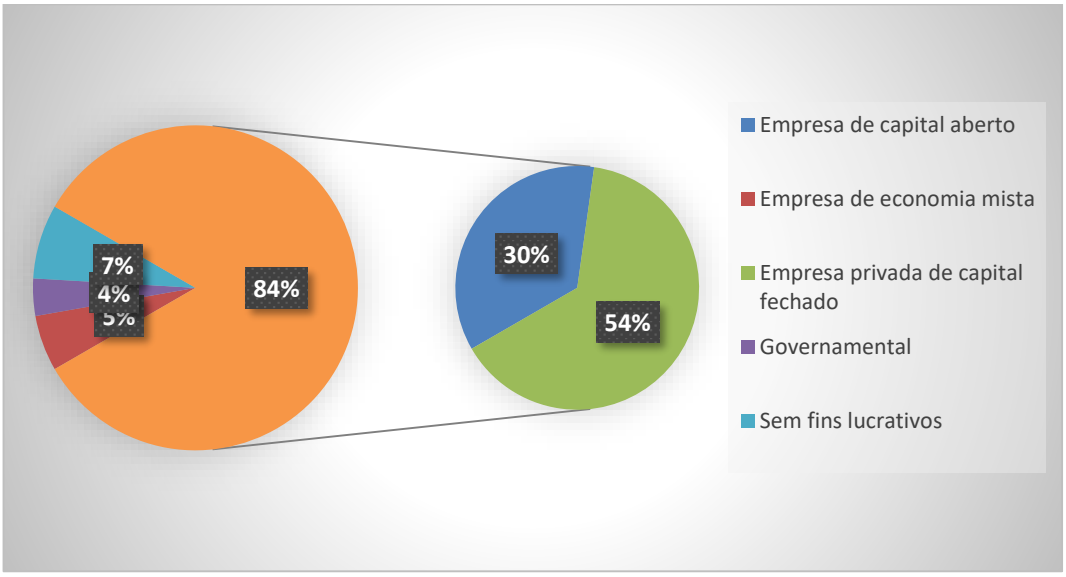

Observou-se que apenas 37% das empresas do GAIP atuam somente no Brasil e que 15% estão presentes em mais de 50 países, demonstrando um nível elevado de globalização e legislações pertinentes (GRÁFICO 7). Isto, sem dúvida, é um grande desafio para gestão de riscos, tecnologia, segurança da informação, *compliance* e auditoria, uma vez que em cada país há legislações, recursos e necessidades distintas para viabilizar a operação e venda de produtos ou serviços.

**GRÁFICO 7 - QUANTIDADE DE PAÍSES EM QUE A ORGANIZAÇÃO ESTÁ PRESENTE**



Quanto ao tipo de sociedade econômica das organizações, 84% das empresas dos respondentes do GAIP são privadas, e para estas empresas uma estrutura mínima de governança é obrigatória, seja por legislação e órgãos reguladores ou por determinação de acionistas que querem assegurar que seus investimentos não estão sendo utilizados de maneira inadequada. (GRÁFICO 8).

**GRÁFICO 8 - PERCENTUAL DE EMPRESAS POR TIPO DE SOCIEDADE ECONÔMICA**




Quanto ao setor de atuação, verificou-se uma composição heterogênea e diversificada das empresas (GRÁFICO 9), o mesmo foi observado quanto ao tamanho dessas organizações, mensurado pelo número de colaboradores e receita operacional bruta anual (APÊNDICE 2).

Provavelmente, devido a esta heterogeneidade observada, os cenários de negócios e riscos para estas empresas também devem ser distintos, e consequentemente a estrutura de governança estabelecida em cada empresa. Conforme (GRÁFICOS 10 e 11) a maioria das empresas (91%) possuem uma área específica de auditoria interna, mas apenas 44% apresentam uma área de gerenciamento de riscos e somente 43% possuem um comitê de auditoria interna.

**GRÁFICO 9 - SETORES DE ATUAÇÃO DAS EMPRESAS DO GAIP**

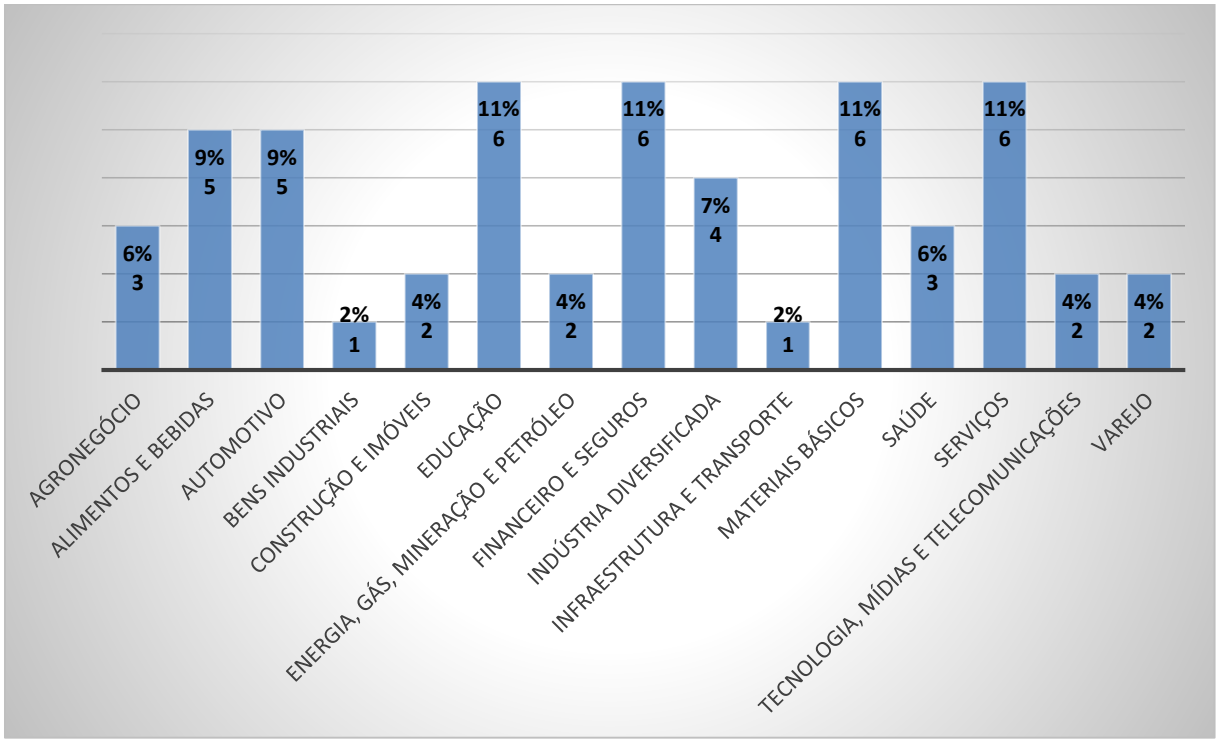



**GRÁFICO 10 - EMPRESAS QUE POSSUEM UMA ÁREA ESPECÍFICA DE AUDITORIA INTERNA**

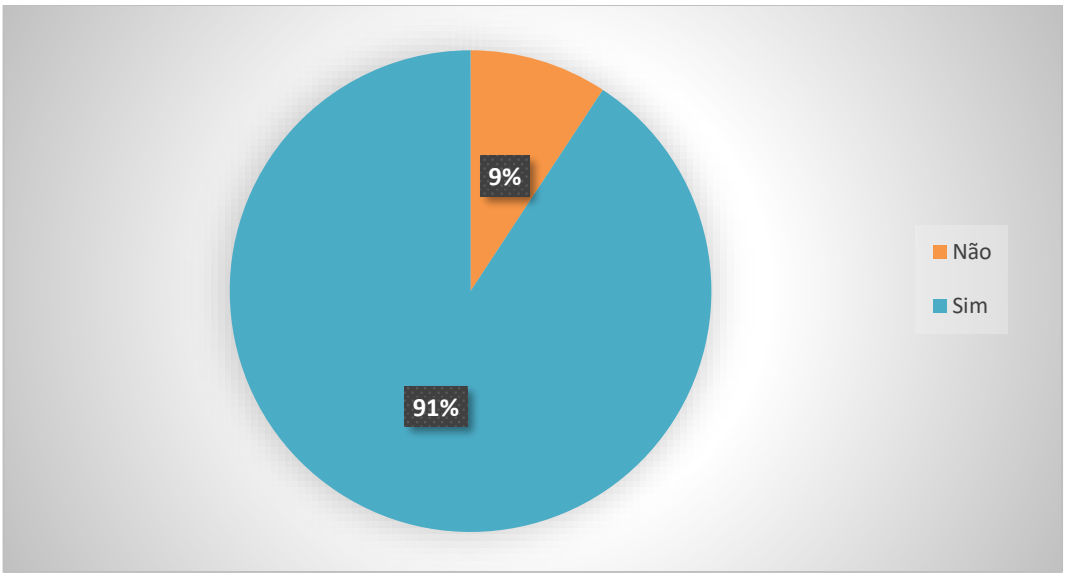
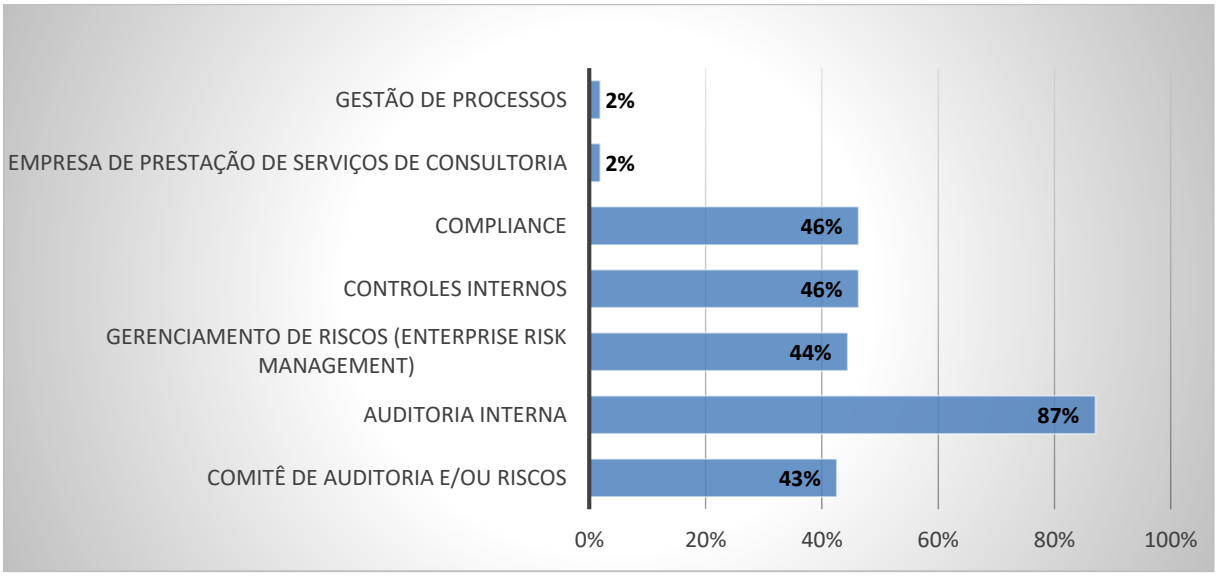


**GRÁFICO 11 - ÁREAS/DEPARTAMENTOS DE GOVERNANÇA ESTABELECIDAS POR EMPRESA**




Por fim, como requisitos fundamentais para segurança da informação dentro de uma organização, foi avaliado se as empresas dispõem ao menos de uma política com as diretrizes de segurança da informação e colaboradores especializados para tratar assuntos relacionados à segurança da informação, e o resultado encontrado demonstra que há ainda uma parcela significativa de empresas sem estes requisitos, 35% não possuem profissionais especializados neste tema (GRÁFICO 12) e 26% não possuem políticas (GRÁFICOS 13).

**GRÁFICO 12 - EMPRESA COM ESPECIALISTAS EM SEGURANÇA DA INFORMAÇÃO**

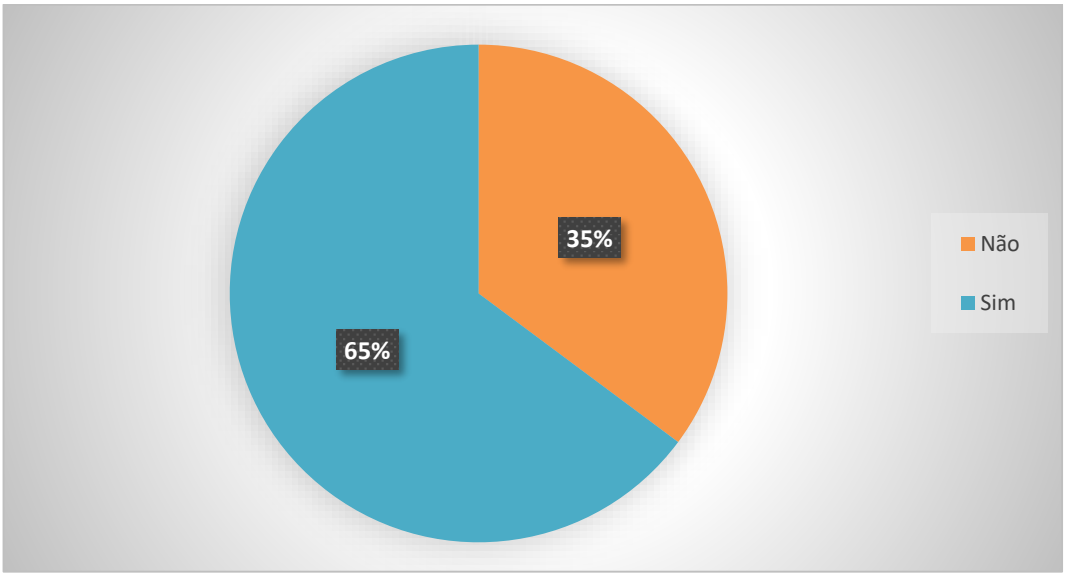
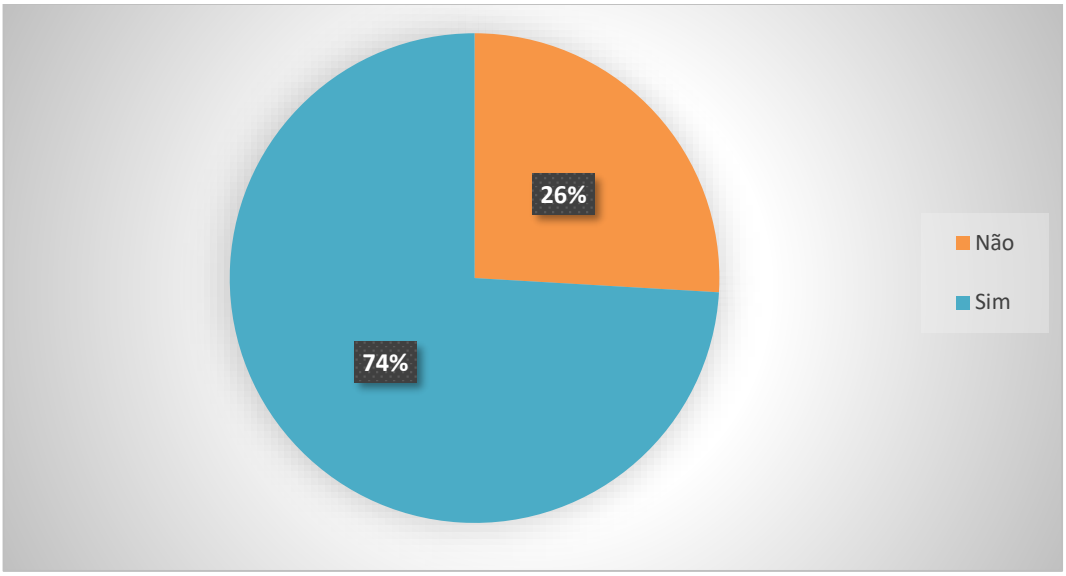
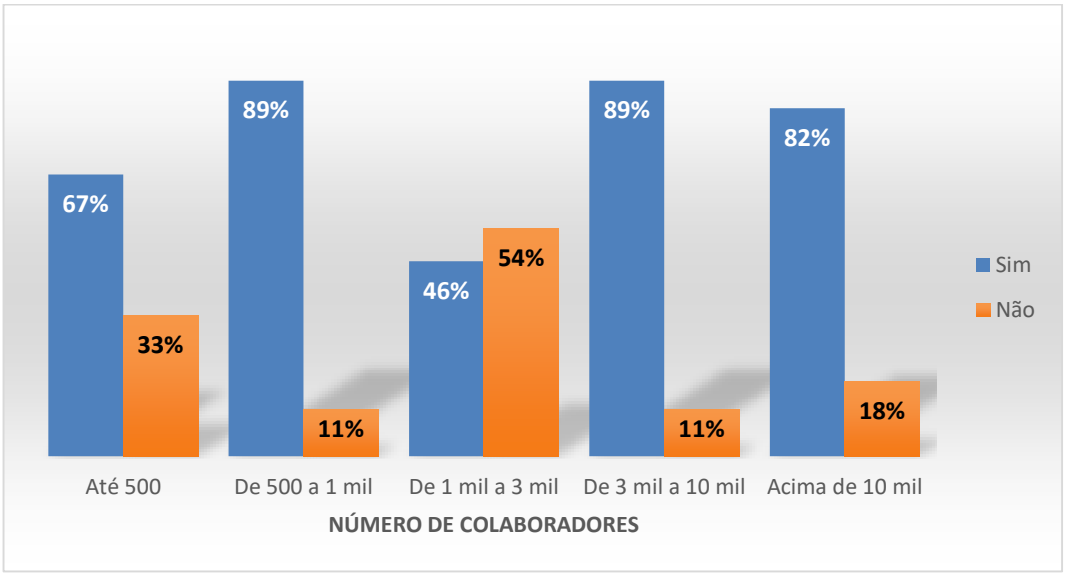


**GRÁFICO 13 - EMPRESAS COM POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO FORMALIZADAS E DIVULGADAS**




Quando analisado pelo tamanho da empresa, observa-se que não são apenas as menores empresas que não possuem uma política de segurança da informação, pois 54% das empresas de 1-3 mil e 18% das organizações acima de 10 mil colaboradores se enquadram nessa situação (GRÁFICO 14).

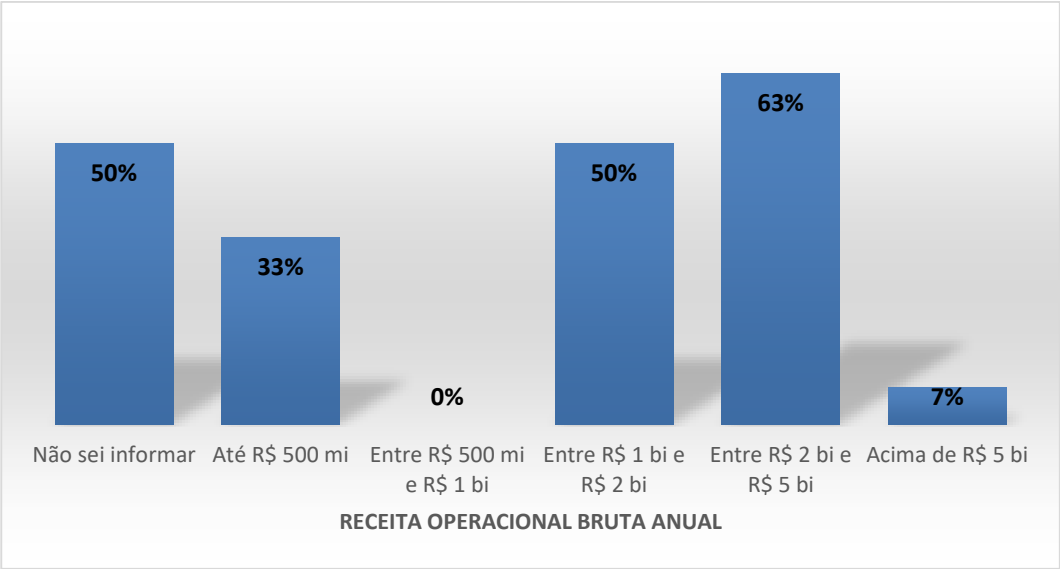
**GRÁFICO 14 - ANÁLISE DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO IMPLEMENTADAS POR TAMANHO DE EMPRESAS (NÚMERO DE COLABORADORES)**




O mesmo pode-se observar na análise de porte das empresas por faixas de receita operacional bruta anual, das quais empresas com receitas superiores à R$ 1

bilhão de reais ainda não possuem política de segurança da informação, com as faixas entre R$ 1-2 bi (50%), R$ 2-5 bi (63%) e com receitas acima de R$ 5 bilhões (7%).

**GRÁFICO 15 - ANÁLISE DE EMPRESAS POR FAIXA DE RECEITA QUE NÃO POSSUEM POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO (RECEITA OPERACIONAL BRUTA ANUAL)**




Segundo SÊMOLA (2014, p. 47), a política de segurança da informação é um controle preventivo e a NBR ISO 27002 (2005, p. xi) cita a política de segurança da informação como uma melhor prática de controle, com isso as empresas que não adotam essas práticas possuem maior probabilidade de incidente de segurança da informação.

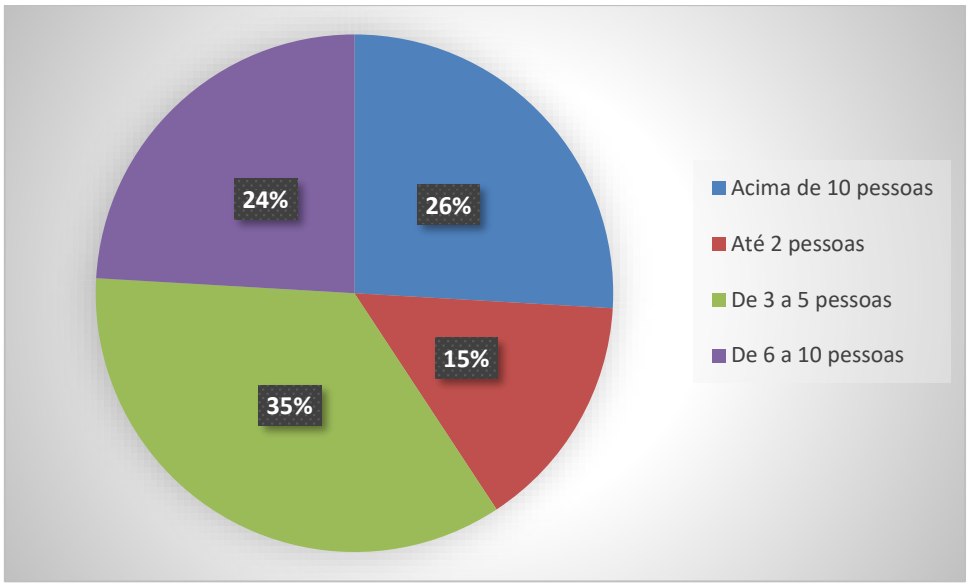
## 4.3 Perfil das Auditorias Internas e Práticas Adotadas para Riscos de Segurança da Informação

De maneira geral, a análise da estrutura das auditorias internas das empresas do GAIP e práticas adotadas por estas, possibilita identificar possíveis causas que as levam ter maior ou menor aderência às melhores práticas para atendimento dos objetivos de negócio com mudanças constantes em riscos de segurança da informação.

Para tal, primeiramente verificou-se os recursos disponíveis em pessoas, qualificação e orçamento para a estrutura de auditoria interna. Como ilustrado no

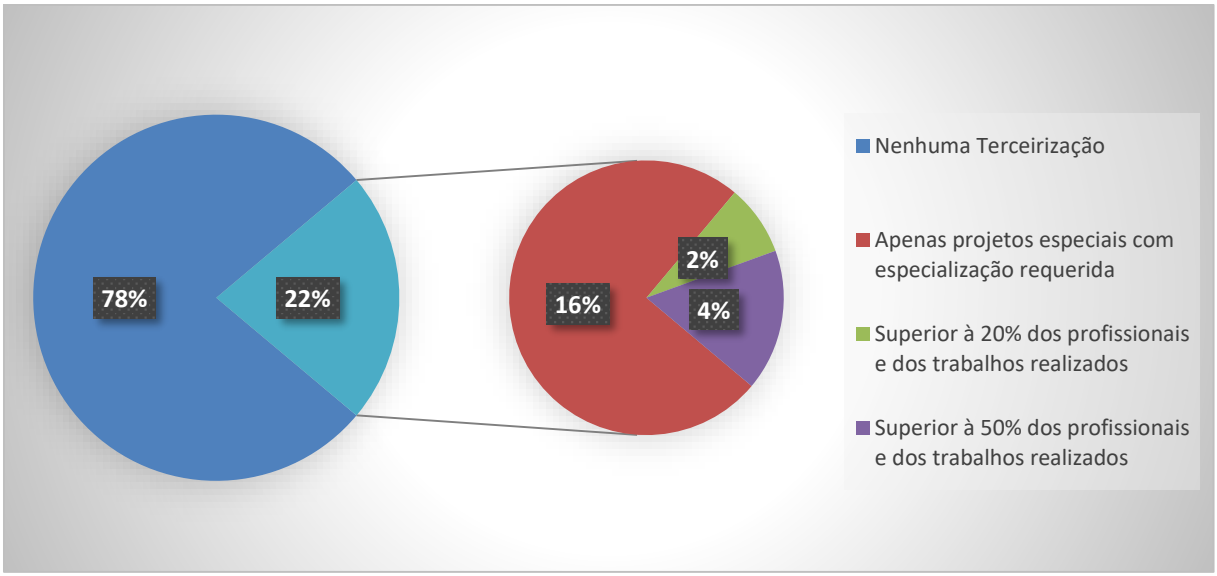
(GRÁFICO 16), 50% das estruturas de auditoria interna do GAIP possuem até 5 pessoas, mas vale destacar que também há empresas com departamentos de auditoria interna mais robustos com mais de 10 auditores em 26% dos casos.

**GRÁFICO 16 - PERCENTUAL DE EMPRESAS POR QUANTIDADE DE AUDITORES**



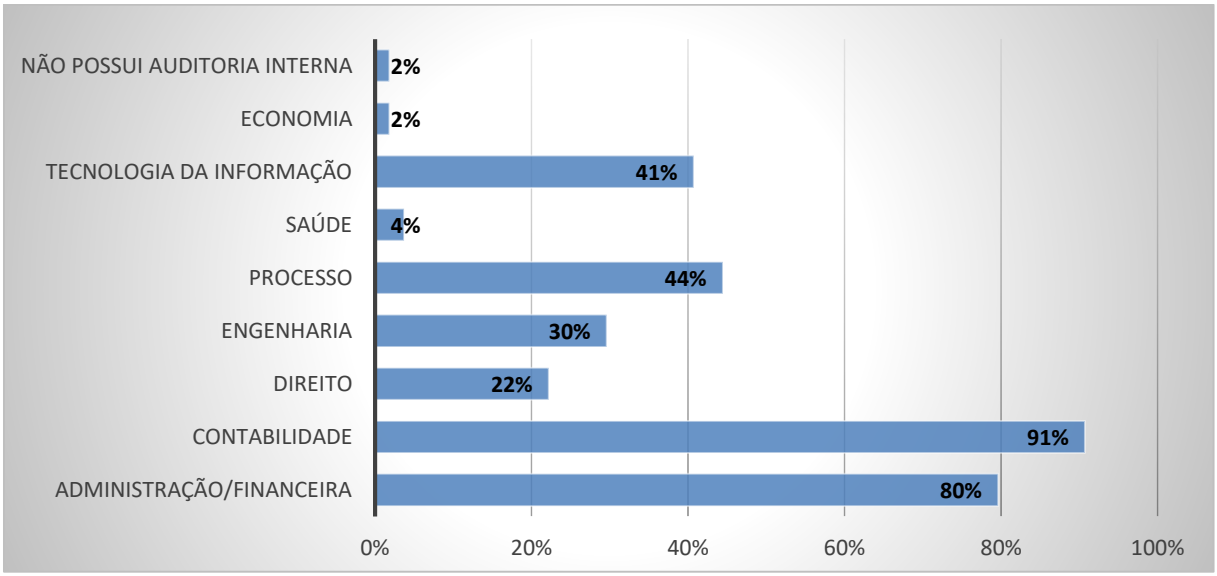

Além desta estrutura fixa de auditoria interna, 22% das empresas utilizam-se de serviços de auditoria interna prestados por terceiros, os quais 16% são apenas em projetos específicos que demandam profissionais com especialização apropriada para execução da auditoria, conforme (GRÁFICO 17).

**GRÁFICO 17 - PERCENTUAL DE TERCEIRIZAÇÃO**



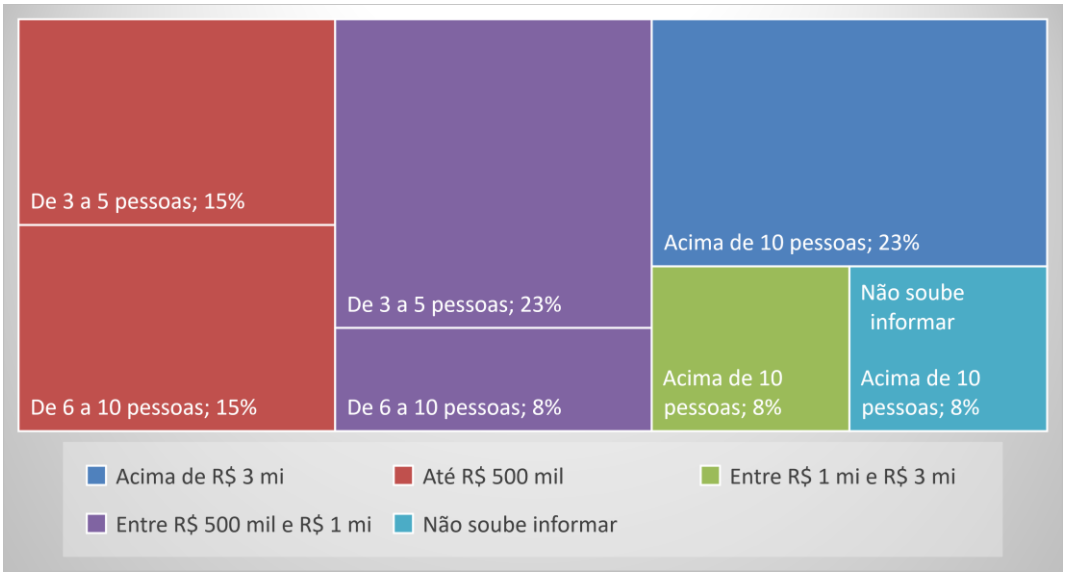
Das qualificações observadas, na quarta posição, apenas 41% dos profissionais possuem formação na área de Tecnologia da Informação, frente ao avanços tecnológicos e grande volume de dados operacionalizados pelas empresas, não ter auditores com conhecimentos em TI pode ser um risco para a área de auditoria interna e consequentemente para a organização, conforme apontado pelo CBOK (2015) como risco a ausência de auditores de TI qualificados.

**GRÁFICO 18 - ANÁLISE DAS QUALIFICAÇÕES PRESENTES NAS ÁREAS DE AUDITORIA INTERNA EM EMPRESAS DO GAIP**



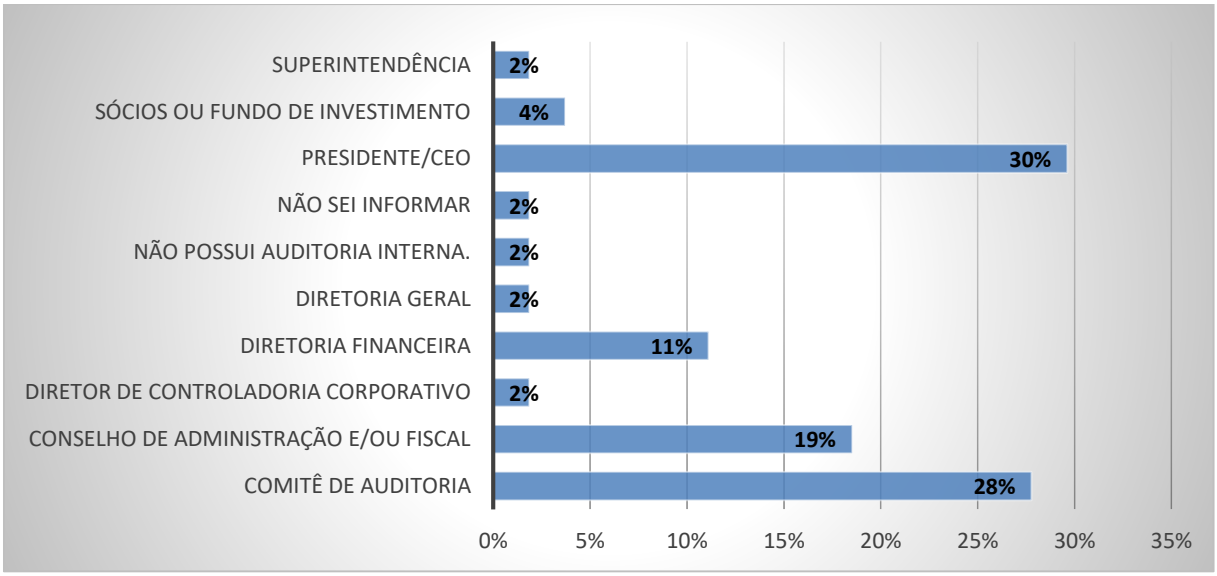

Em relação ao orçamento anual para a auditoria interna, foi considerado para análise apenas as respostas dos chefes de auditoria (24% da população), pois geralmente são estes os gestores do orçamento da área. Entende-se que o orçamento disponível está diretamente ligado à quantidade de auditores disponíveis para execução dos trabalhos, portanto no (GRÁFICO 19) observa-se que 61% das empresas possuem orçamento até R$ 1 milhão de reais, sendo compostas por equipes de 3-5 pessoas (38%) e de 6-10 pessoas (23%).

**GRÁFICO 19 - ANÁLISE ORÇAMENTO VERSUS TAMANHO DA EQUIPE DE AUDITORIA**




A linha de reporte e realizar atividades de competência de outras áreas podem ser indicadores para avaliação se a auditoria interna está com o nível de independência adequado. Dessa maneira, observamos (GRÁFICO 20) que apenas 28% das auditorias reportam para um comitê de auditoria e 19% com reporte ao conselho de administração, totalizando 47% dos respondentes.

**GRÁFICO 20 - NÍVEL DE REPORTE DA AUDITORIA INTERNA**

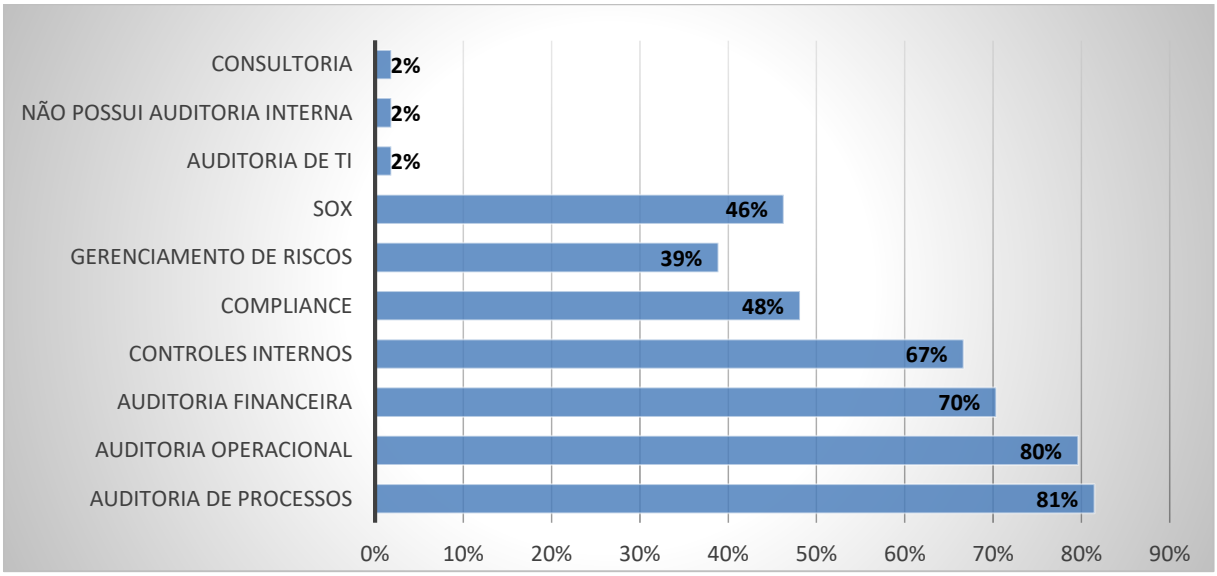



As empresas que não reportam diretamente a um comitê de auditoria ou conselho, podem ter um impacto significante para manter a independência, conforme

cita o IIA (2013, p. 3). “Para atingir o grau de independência necessário para conduzir eficazmente as responsabilidades da atividade de auditoria interna, o executivo chefe de auditoria tem acesso direto e irrestrito à alta administração e ao conselho”.

Quanto às atividades desempenhadas pelas áreas de auditoria interna do GAIP, verifica-se um acúmulo de funções pertinentes de atividades de gestão de riscos e controles, que por questões orçamentárias ou menor nível de maturidade em governança, estão sendo executadas pela área de auditoria interna. Destaca-se do (GRÁFICO 21) as atividades referentes à controles internos (67%) e SOX (46%), não recomendadas pelas melhores práticas de independência e objetividade abordados no modelo das Três Linhas de Defesa.

**GRÁFICO 21 - ANÁLISE DAS RESPONSABILIDADES E ATIVIDADES DAS AUDITORIAS INTERNAS (GAIP)**




De acordo com a Declaração de Posicionamento do IIA, As Três Linhas de Defesa no Gerenciamento de Riscos e Controle Eficazes (FIGURA 6), propõe:

> “A administração é a principal responsável pelos processos de monitoramento e controle e é a primeira linha de defesa do gerenciamento de riscos.
> A segunda linha de defesa consiste das funções de supervisão, estabelecidas separadamente, de risco, controle e conformidade, que garantem que processos e controles apropriadamente desenvolvidos estejam em prática na primeira linha de defesa e operando com eficácia. A natureza e tipos dessas funções dependem de muitos fatores, incluindo a maturidade da indústria e da organização.
> Funções como a auditoria interna, que prestam avaliação independente sobre os processos e controles, são consideradas a terceira linha de defesa. [...]

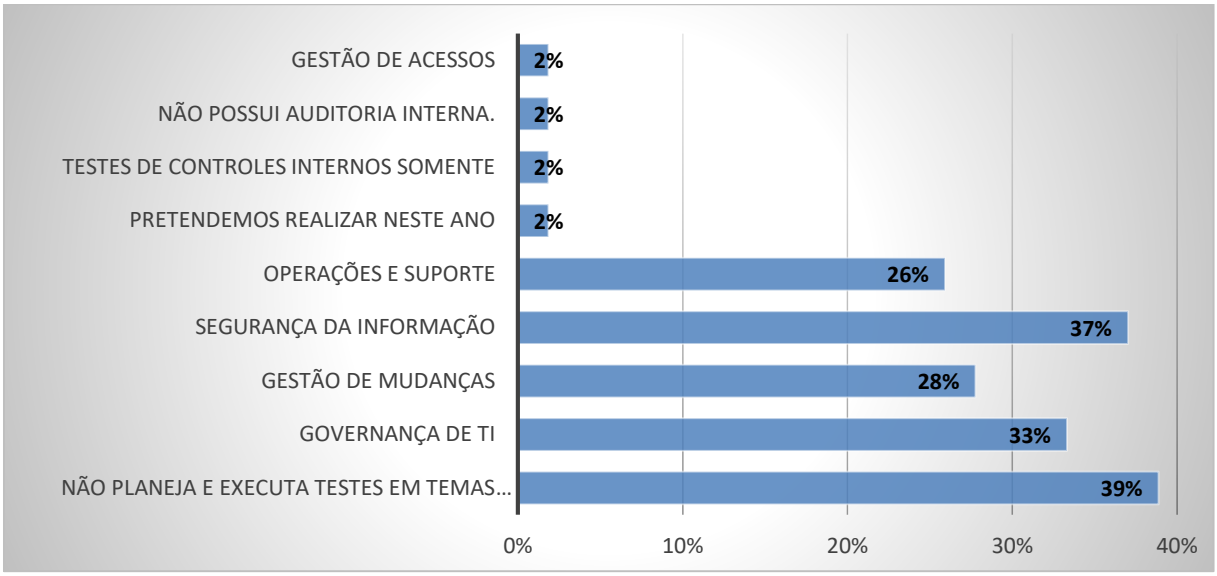
> A segunda e terceira linhas de defesa atuam na supervisão e/ou avaliação do gerenciamento de riscos. As diferenças principais entre a segunda e terceira linhas de defesa são os conceitos de independência e objetividade.” IIA (2016, p. 8)


**Figura 6 - As Três Linhas de Defesa no Gerenciamento de Riscos e Controle Eficazes**

Em relação às práticas de auditoria interna específicas para avaliação independente sobre os processos de governança, gerenciamento de riscos e controles de TI, inclusive segurança da informação, o questionário proposto teve como objetivo identificar a abordagem e práticas utilizadas pelas auditorias internas participantes do GAIP para monitoramento e avaliação de riscos de segurança da informação em suas respectivas organizações.

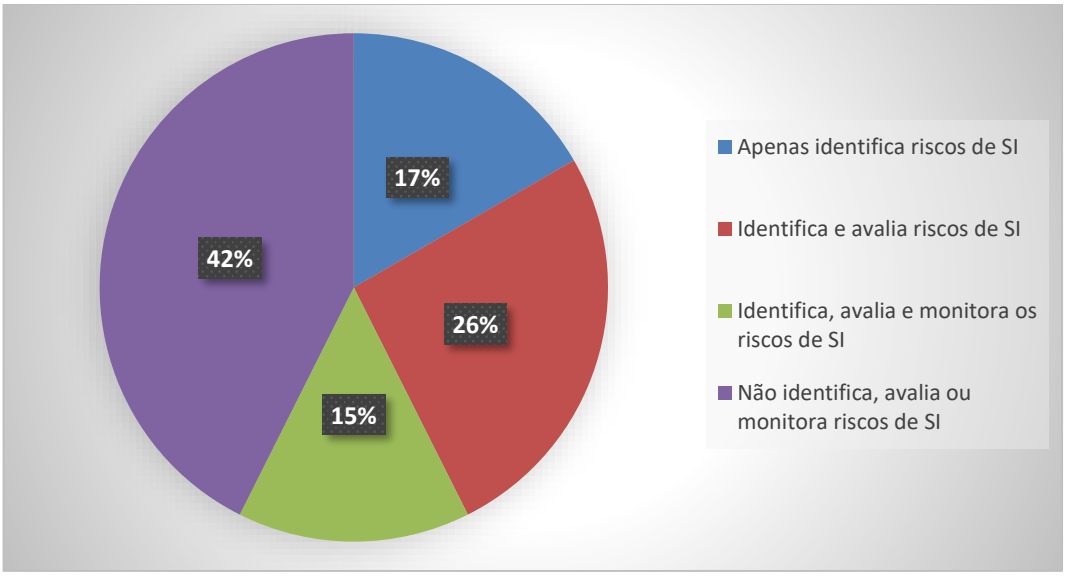
Segundo define o IIA BRASIL (2014, p.11) a Auditoria de TI revisa e avalia os riscos de tecnologia da informação associados aos processos e ativos de TI da organização e conforme a norma de desempenho 2110.A2 de Governança do IPPF (IIA, 2016) “A atividade de auditoria interna deve avaliar se a governança de tecnologia da informação da organização dá suporte às estratégias e objetivos da organização.”, porém não é este o resultado em 39% das auditorias que não planeja e executa testes em temas relacionados à tecnologia e 2% que ainda não realizou testes em TI, mas tem a pretensão de realizar testes na área de TI em 2017, ou seja, um total de 41% ainda não realizaram trabalhos de auditoria em TI (GRÁFICO 22).

**GRÁFICO 22 – AUDITORIAS QUE PLANEJAM E EXECUTAM TESTES NA ÁREA DE TI**



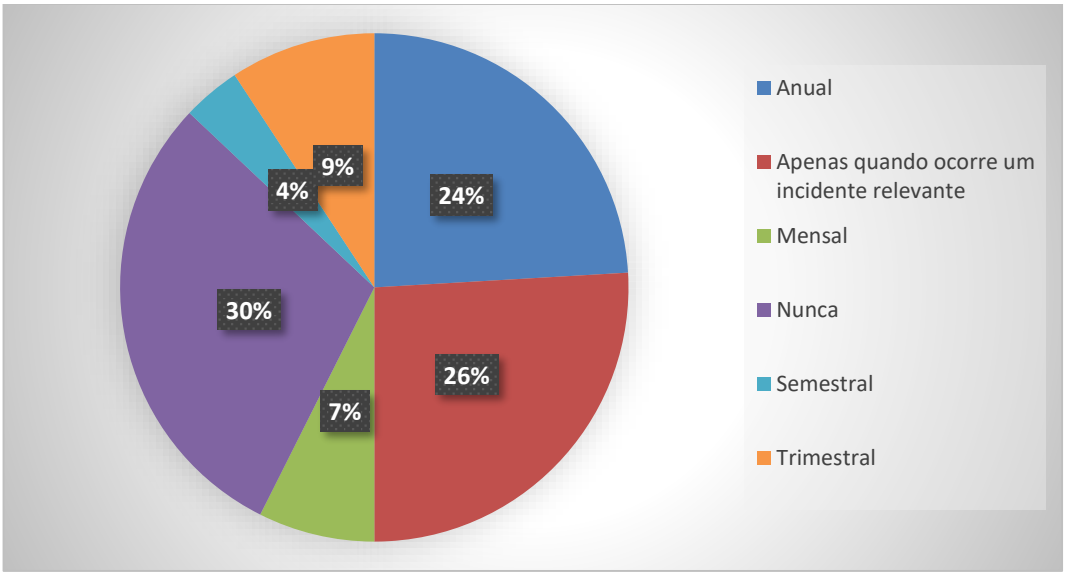

Verificou-se que 42% das auditorias ainda não identificam, avaliam ou monitoram riscos de segurança da informação (GRÁFICO 23), conforme orientam as melhores práticas, como citada na Orientação Prática 2120-3 onde o IPPF (2013) determina que a auditoria interna também deve avaliar riscos relacionados à governança, operações e sistemas de informação. Ainda, de acordo com IIA (2014), a auditoria interna deve avaliar se a organização está protegendo suas informações quanto à confidencialidade, integridade e disponibilidade. Segundo KIM & SOLOMON (2014) a auditoria de segurança deve assegurar que seus sistemas e controles funcionem conforme esperado.

**GRÁFICO 23 – PERCENTUAL DE AUDITORIAS QUE IDENTIFICAM, AVALIAM E MONITORAM RISCOS DE SEGURANÇA DA INFORMAÇÃO**




Conforme (GRÁFICO 24), 30% dos respondentes afirmam que a auditoria interna nunca realizou avaliação ou monitoramento de riscos de segurança da informação e que 26% só realizam tal atividade quando ocorre um incidente relevante, ou seja, 56% não atuam de maneira preventiva e periódica conforme citam , BEAL (2005, p.40) e a norma ABNT NBR ISO 27002 (2005, p. 14), como controle relevante a análise crítica sobre a gestão de segurança da informação, de forma independente e periódica, necessária para assegurar que as práticas da organização permanecem adequadas e eficazes quanto aos riscos e controles existentes.

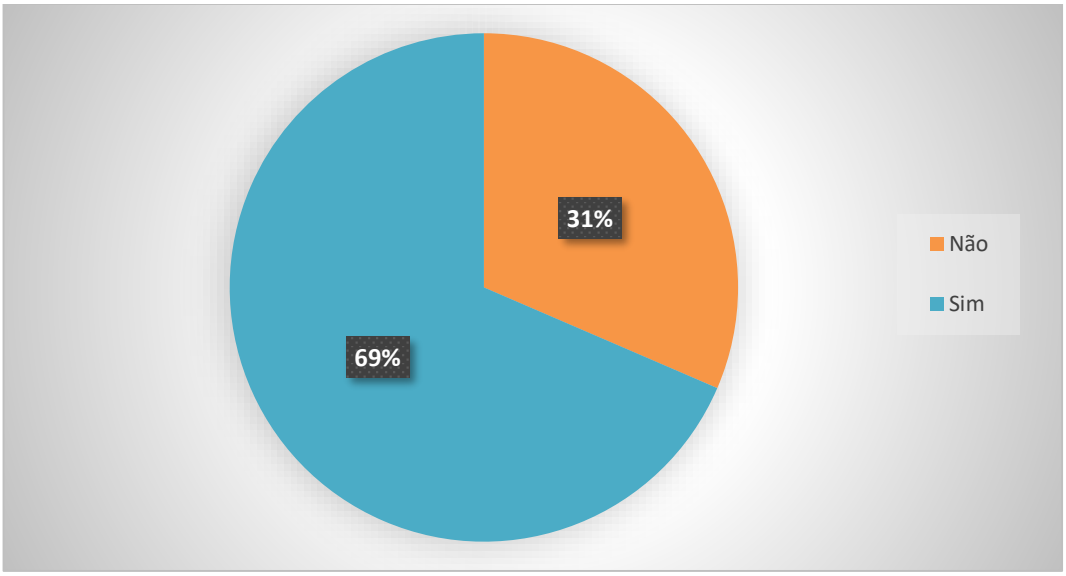
**GRÁFICO 24 - PERIODICIDADE QUE AUDITORIA AVALIA E MONITORA RISCOS DE SEGURANÇA DA INFORMAÇÃO**




Há um volume gigantesco e crescente de dados criados e utilizados pelas organizações gerando informações de valor à companhia, e praticamente toda informação gerada é de formato digital, com isso é indispensável que a auditoria interna utilize práticas e ferramentas avançadas para extração e análise de dados que seja possível processar toda essa informação em um espaço de tempo cada vez menor.

Segundo pesquisas da PWC (2017), 40% das funções de auditoria interna aumentaram seus investimentos em análise de dados nos últimos três anos e 65% dos líderes de auditoria interna afirmam ter competências referentes à análise de dados em suas equipes ou por meio de terceiros, porém 31% dos respondentes participantes do GAIP afirmam que a auditoria interna ainda não possui ferramentas ou sistemas para extração e análise de dados (GRÁFICO 25).

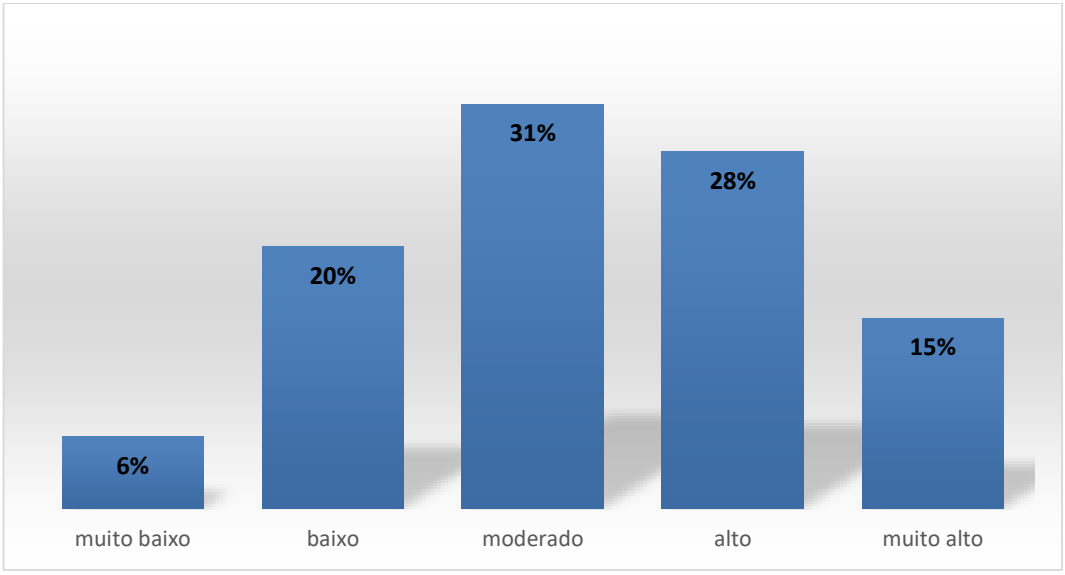
**GRÁFICO 25 - AUDITORIA INTERNA UTILIZA FERRAMENTAS OU SISTEMAS PARA EXTRAÇÃO E ANÁLISE DE DADOS**




No questionário, foi elaborado questões subjetivas referentes à segurança da informação e auditoria interna com o propósito de observar o senso crítico e cultura organizacional relacionadas ao compromisso da organização com segurança da informação e o engajamento da auditoria interna com estes riscos de segurança da informação.

Na percepção dos respondentes, o engajamento da diretoria em patrocinar, divulgar e monitorar assuntos relacionados à segurança da informação é de moderado à alto em 59% dos casos (GRÁFICO 26), porém 26% acredita que o apoio da diretoria para estes assuntos ainda é de muito baixo a baixo.

**GRÁFICO 26 - APOIO DA DIRETORIA PARA PATROCINAR, DIVULGAR E MONITORAR A SEGURANÇA DA INFORMAÇÃO**




De maneira geral, a maior parte (53%) dos entrevistados acreditam que os atuais riscos de segurança da informação em suas organizações são altos ou muitos altos (GRÁFICO 27), assim como metade dos entrevistados entende que são altos ou muito altos os níveis atuais de proteção às informações da companhia (GRÁFICO 28).

**GRÁFICO 27 - NÍVEL DOS RISCOS DE SEGURANÇA DA INFORMAÇÃO SEGUNDO PERCEPÇÃO DOS ENTREVISTADOS**

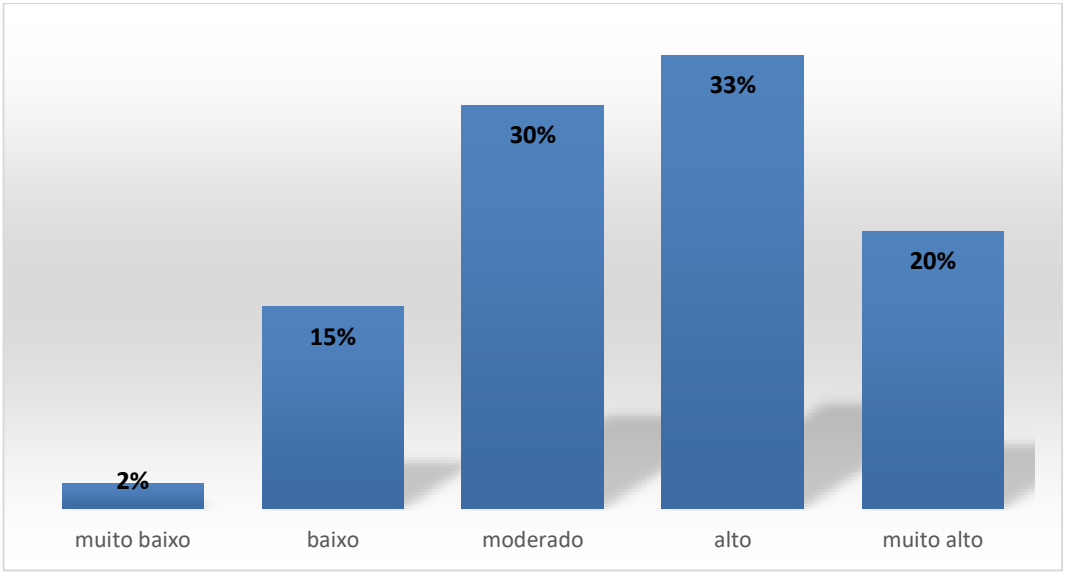
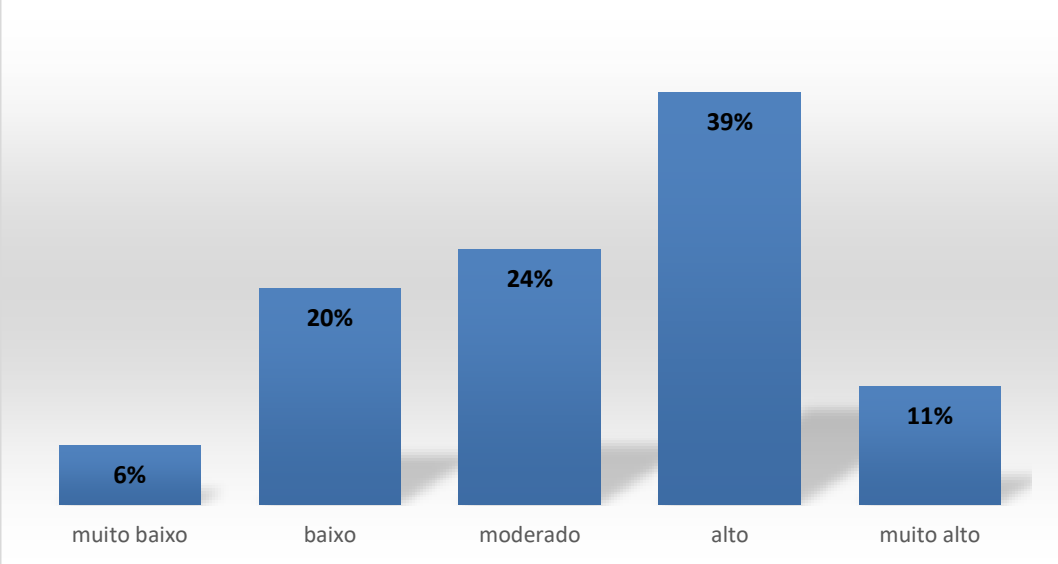


**GRÁFICO 28 - NÍVEIS DE SEGURANÇA DAS INFORMAÇÕES NAS ORGANIZAÇÕES NA PERCEPÇÃO DOS ENTREVISTADOS**




Neste contexto, a percepção quanto aos riscos de segurança serem altos parece adequada, mas em relação aos níveis de proteção serem altos há incertezas, pois conforme a PWC (2016) apontou em sua Pesquisa Global de Segurança da Informação, no Brasil o número médio de incidentes de segurança aumentou em 274%, muito acima da média global que teve aumento de 38%

Neste mesmo estudo a PWC (2016) cita que:

> Os números são estarrecedores. Ano após ano, os ataques cibernéticos seguem crescendo em frequência, gravidade e impacto. Os métodos de prevenção e detecção mostraram-se muito ineficazes contra investidas cada vez mais sofisticadas. Muitas organizações não sabem o que fazer, ou não têm os recursos necessários para combater criminosos cibernéticos altamente qualificados e agressivos.
> AO mesmo tempo, as mudanças tecnológicas continuam a transformar a maneira como as organizações competem e criam valor, muitas vezes alterando seus modelos operacionais. Algumas das tendências de negócios mais importantes atualmente — a explosão da análise de dados, a digitalização das funções de negócios e a combinação das ofertas de serviços de diferentes indústrias, expandem o uso de tecnologias e dados, o que cria riscos em uma quantidade jamais vista. [...]
> Muitos executivos afirmam que a questão cibernética representa o risco que definirá a nossa geração. (PWC, 2016, p. 4)

Os participantes do GAIP responderam quais os recursos e/ou ferramentas utilizados pela empresa para mitigar os riscos de segurança da informação (GRÁFICO 29), dos quais vale destacar que caso um incidente de segurança de maior gravidade ocorra, somente metade (50%) dos representantes do GAIP

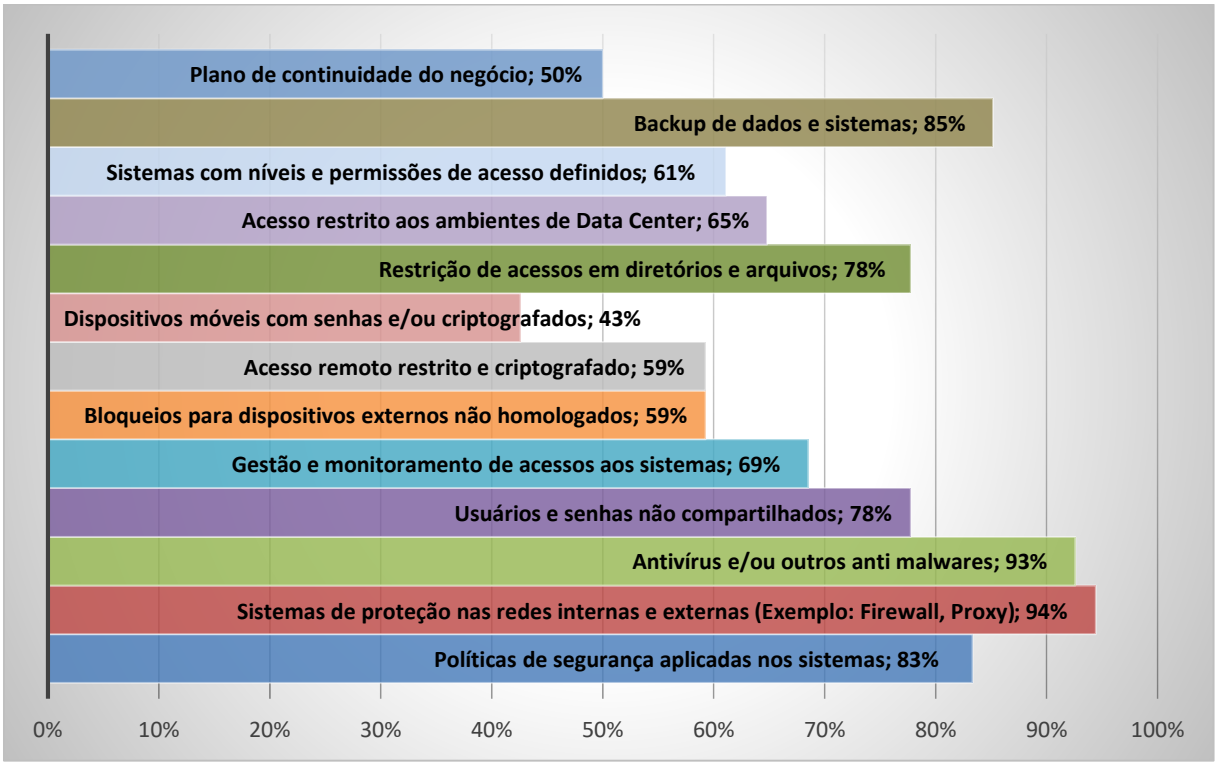
possuem um plano de continuidade para o negócio, ou seja, metade das organizações respondentes podem sofrer com a interrupção total de sua operação.

Outro resultado que deve ser destacado é que apenas 43% utilizam senhas e/ou criptografias nos dispositivos móveis; e conforme afirma o CBOK (2015) a computação mobile é um dos principais riscos, pois as informações contidas em dispositivos móveis podem incluir todos os tipos de dados e podem ser expostos se o dispositivo for perdido ou roubado, se o usuário que tem a posse do dispositivo deixar a organização sem deletar os dados, ou se os controles de segurança não estiverem adequados.

De acordo com CBOK (2015), Alejandro Rembado Mendizábal (Chefe Executivo de Auditoria da Telefonica Argentina) afirma que:

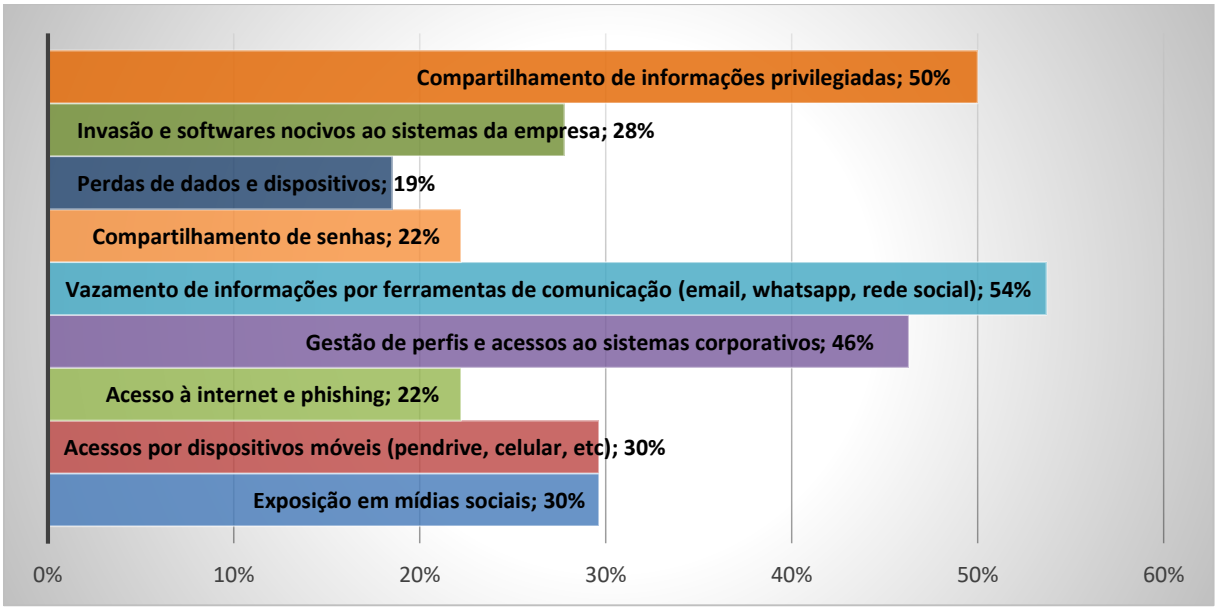
> "A informação viaja com seus usuários, portanto dados de segurança devem ser tão robustos em dispositivos móveis quanto o são na sede da empresa. Tablets, computadores pessoais, celulares, relógios smart, etc são pequenos data centers nos quais a maioria das informações estratégicas da empresa é guardada (ou dados suficientes para atacar os servidores centrais). A quantidade de equipamentos roubados e/ou perdidos agrava a situação." (CBOK, 2015, p. 19)

**GRÁFICO 29 - RECURSOS UTILIZADOS PELAS EMPRESAS PARA MITIGAR OS RISCOS DE SEGURANÇA DA INFORMAÇÃO**



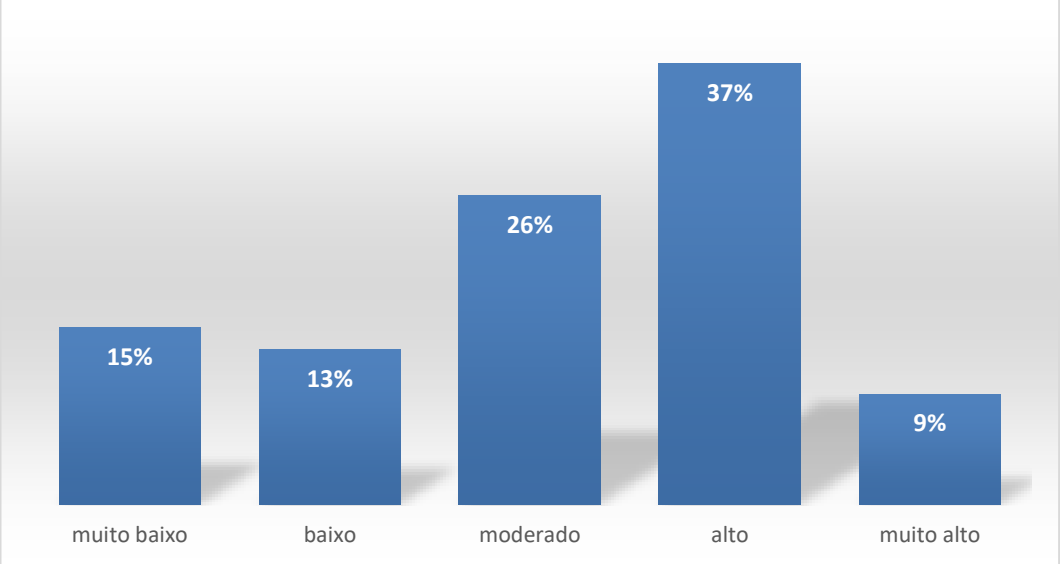
Os participantes do GAIP acreditam que os principais desafios/riscos de suas empresas é conter o vazamento de informações através de ferramentas de comunicação (54%), o compartilhamento de informações privilegiadas (50%) e gerenciar os acessos aos sistemas corporativos (46%), conforme demonstrado no (GRÁFICO 30).

**GRÁFICO 30 - OS PRINCIPAIS DESAFIOS DAS EMPRESAS EM SEGURANÇA DA INFORMAÇÃO**




Em relação à percepção do papel da auditoria interna, os entrevistados do GAIP entendem que o comprometimento da área de auditoria interna em identificar, avaliar e monitorar os riscos de segurança da informação é de moderado à alto em 63% dos casos. (GRÁFICO 31).

**GRÁFICO 31 - COMPROMENTIMENTO DA AUDITORIA INTERNA EM IDENTIFICAR, AVALIAR E MONITORAR RISCOS DE SEGURANÇA DA INFORMAÇÃO**



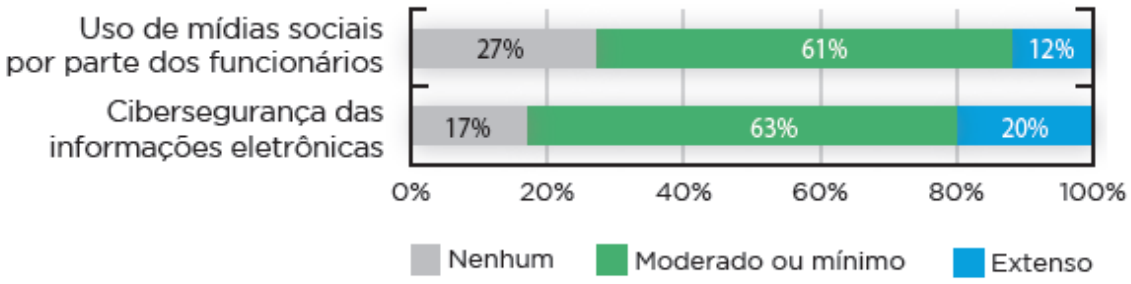

Segundo a pesquisa CBOK 2015 do IIA:

> Riscos tecnológicos são extremamente difíceis de gerenciar, porque estão em evolução constante. Os auditores internos precisam reagir proativamente, ajudando suas organizações a identificar, monitorar e lidar com tais riscos emergentes de TI e orientando seus conselhos sobre a melhor forma de fazê-lo.
> O risco de TI está entre os cinco principais riscos nos quais os auditores internos estão concentrando seu maior nível de atenção em 2015. (IIA, 2015, p. 15)

O estudo também demonstra (FIGURA 7) que o envolvimento da auditoria interna com relação à cibersegurança e mídias sociais é moderado ou mínimo em 63% e 61%, respectivamente; e destaca que este comprometimento da auditoria com estes dois riscos aumentará dentro dos próximos 2 a 3 anos em 74% para cibersegurança e em 54% em relação a mídias sociais.

Comparativamente, pela percepção dos participantes do GAIP e o apontado pelo estudo do IIA em 2015, de maneira geral o nível de comprometimento das auditorias internas do GAIP em relação aos riscos de segurança da informação está de acordo com as previsões de aumento do comprometimento destacadas pelo IIA.

**Documento 11** **Envolvimento da Atividade de Auditoria Interna com Relação à Cibersegurança e Mídias Sociais**



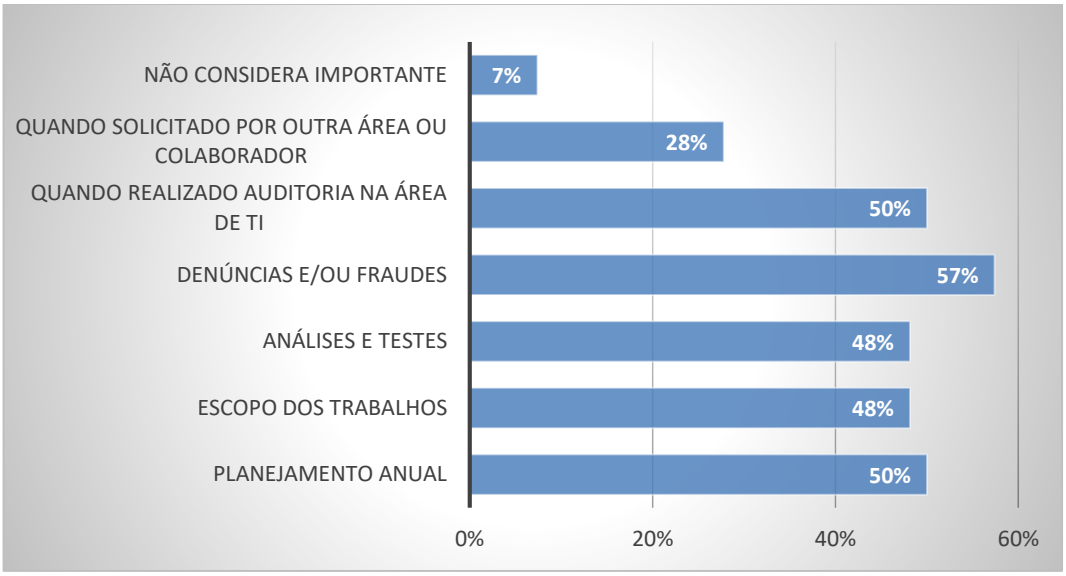

Observação: Q92: Para a segurança da tecnologia da informação (TI), especificamente, qual o envolvimento do departamento de auditoria interna em relação às áreas a seguir: uso de mídias sociais por parte dos funcionários e cibersegurança das informações eletrônicas?
9.941 participantes para cibersegurança; 9.747 participantes para mídias sociais.

**Figura 7 - Envolvimento da Auditoria Interna com Riscos de Cibersegurança e Mídias Sociais**

Quanto às melhores práticas levantadas neste trabalho, uma auditoria interna quando baseada em riscos, deve prever em seu planejamento trabalhos de auditoria direcionados aos principais riscos da organização. Dessa maneira procurou-se observar se as auditorias internas do GAIP estão seguindo esta prática e incluindo em seu planejamento trabalhos relacionados à TI e segurança da informação.

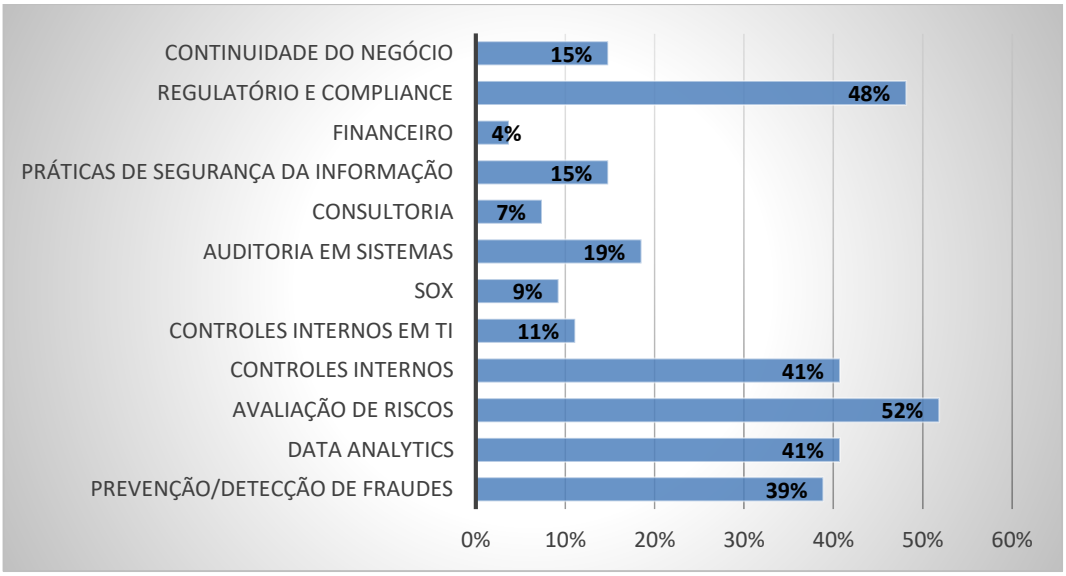
Identificou-se (GRÁFICO 32) que apenas metade (50%) dos entrevistados consideram em seus planejamentos anuais auditorias relacionadas à segurança da informação e que 7% ainda não consideram importante auditoria realizar trabalhos referentes a segurança, demonstrando não alinhamento às melhores práticas e necessidade de repensar sobre os riscos de segurança da informação e como a auditoria interna pode agregar valor e ajudar a companhia na proteção de suas informações.

**GRÁFICO 32 - EM QUAIS MOMENTOS A AUDITORIA INTERNA CONSIDERA RELEVANTE A SEGURANÇA DA INFORMAÇÃO**




Por fim, na percepção dos entrevistados, as quatro qualificações mais importantes para o sucesso da auditoria interna nos próximos três a cinco anos são avaliação de riscos (52%), regulatório e compliance (48%), controles internos (41%) e data analytics (41%).

**GRÁFICO 33 - QUALIFICAÇÕES IMPORTANTES PARA A AUDITORIA INTERNA NOS PRÓXIMOS 3 A 5 ANOS APONTADAS PELOS PARTICIPANTES DO GAIP**



As qualificações relacionadas às práticas de segurança da informação e auditoria em sistemas aparecem apenas com 15% e 19% respectivamente, mostrando uma opinião divergente da pesquisa de auditoria interna no Brasil (Deloitte & IIA, 2016), a qual identificou que as qualificações em tecnologia da informação especializada e segurança de dados são importantes para a auditoria interna nos próximos três a cinco anos para 54% dos respondentes no Brasil e respectivamente 52% e 37% para o global (FIGURA 8).

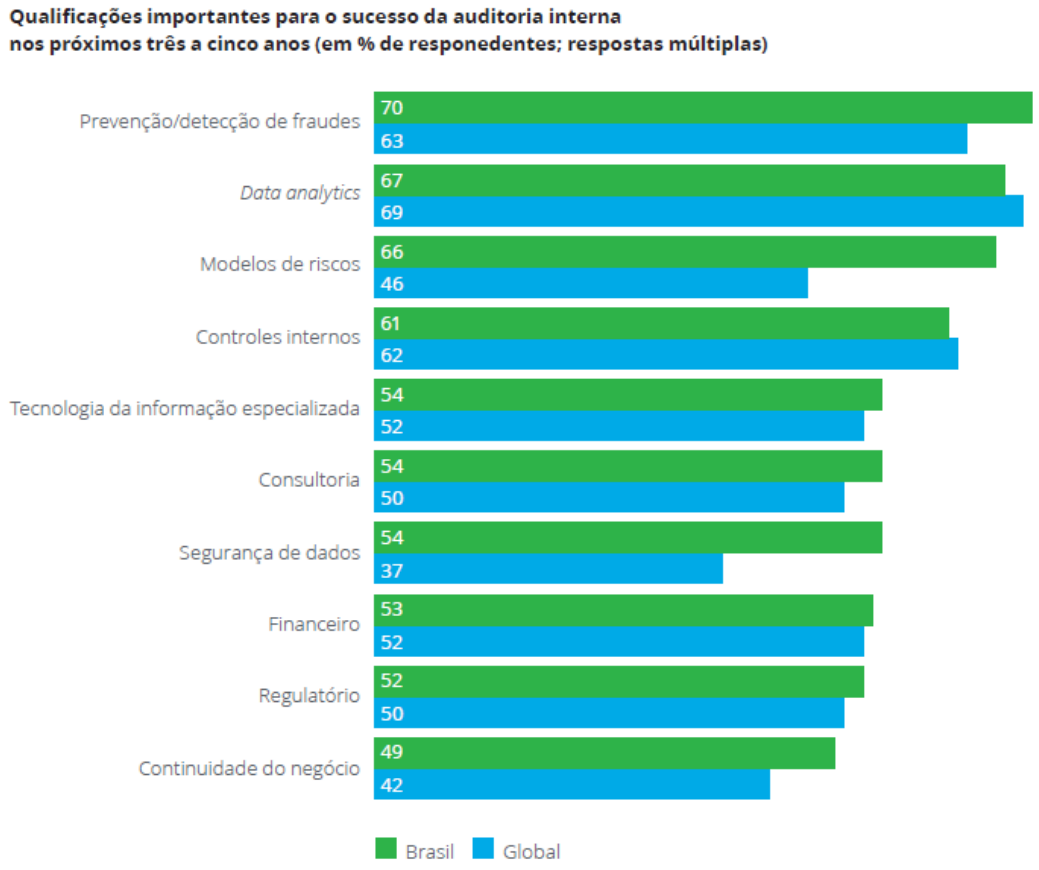



**Figura 8 - Qualificações importantes para o sucesso da auditoria interna apontadas pela Deloitte em 2016**

# 5 CONCLUSÃO

Estamos em uma era de ambientes de negócio cada vez mais competitivos e tecnológicos, em todos os setores, com mudanças rápidas e significativas proporcionadas principalmente pelas tecnologias emergentes. Esse dinamismo e evolução da tecnologia expõem as organizações à novos riscos, sendo estes cada vez mais complexos.

Identificar, avaliar e monitorar bem os riscos, principalmente os novos riscos de TI e segurança da informação (SI), se tornou um dos grandes desafios e ao mesmo tempo vantagem competitiva para as organizações.

Nesse contexto, a auditoria interna no âmbito de suas funções e objetivos, possui o papel de terceira linha de defesa, mas com o objetivo de acompanhar esse dinamismo de mercado e grandes avanços da tecnologia, a auditoria interna deve compreender as mudanças e se adaptar rapidamente de forma a apoiar e entregar valor à organização e *stakeholders*.

O propósito do GAIP é a troca de experiências entre auditores internos e demais profissionais das áreas de governança, riscos e Compliance, sobre metodologias, práticas, ferramentas e assuntos relacionados à governança e TI. Este trabalho também pode agregar ao GAIP, com a coleta de informações para entender melhor sobre as estruturas de empresas, auditorias internas e visão dos profissionais participantes do grupo, além de ser um referencial teórico das melhores práticas de auditoria interna em avaliação de riscos e SI.

Ao analisar as informações obtidas por meio de revisão de normas, orientações práticas e pesquisas de diversos autores e compará-las às respostas do questionário submetido ao GAIP, observou-se para as auditorias do GAIP que, seja por questões econômicas ou possivelmente culturais, a maioria das empresas não possuem o nível de governança adequado para oferecer plena independência para as áreas de auditoria interna executarem e reportarem suas atividades, e as auditorias estão acumulando outras funções de GRC além das recomendadas pelas melhores práticas.

Verificou-se também que as auditorias internas não têm apoiado as organizações na implantação de Políticas de Segurança da Informação como controle preventivo; ainda é baixo o percentual de auditorias com profissionais

especializados em tecnologia e percentual significativamente alto de auditorias que não possuem ferramentas especializadas para análise de dados.

Apesar dos profissionais apontarem que os riscos de segurança da informação sejam altos e a auditoria interna possuir um moderado à alto comprometimento em identificar, avaliar e monitorar tais riscos, metade das auditorias internas não consideram os riscos de SI em seu planejamento anual e a maioria não está aderente às pesquisas recentes da Deloitte e IIA, que demonstram serem necessárias qualificações em TI na auditoria interna para os próximos anos.

Diante do exposto, parece haver confiança excessiva das auditorias nos controles e níveis de segurança utilizados para proteção à informação, entretanto existem 3 fatores que apontam em outra direção: a) atualmente os riscos de SI estão entre os mais importantes de uma organização; b) pesquisas apontam que o número de ameaças e incidentes com impacto elevado estão aumentando; e c) os riscos de cibersegurança e de tecnologias emergentes serão ainda mais desafiadores nos próximos anos.

As auditorias internas devem utilizar-se das orientações práticas, normas e frameworks para identificação, avaliação e monitoramento dos riscos de TI, principalmente os de segurança da informação que são mais dinâmicos e complexos, pois somente com o gerenciamento de riscos a auditoria poderá atuar de maneira preventiva, tempestiva e eficiente, com isso agregando maior valor à organização.

## REFERÊNCIAS


ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 27001 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação.** 1. Ed. Rio de Janeiro: ABNT, 2006.

_____. **ABNT NBR ISO 27002 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação.** 1. Ed. Rio de Janeiro: ABNT, 2005.

_____. **ABNT NBR ISO 27005 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação.** 1. Ed. Rio de Janeiro: ABNT, 2011.

_____. **ABNT NBR ISO 31000 – Gestão de riscos – Princípios e diretrizes.** Rio de Janeiro: ABNT, 2009.

BEAL, Adriana. **Segurança da Informação: Princípios e Melhores Práticas para a proteção dos Ativos de Informação nas Organizações**. São Paulo: Atlas, 2005.

BEUREN, I. M.; LONGARAY, A. A.; RAUPP, F. M.; SOUSA, M. A. B.; PORTON, R. A. B. **Como elaborar trabalhos monográficos em contabilidade - teoria e prática**. 3 ed. São Paulo: Atlas, 2012.

BM&FBOVESPA. **Política de Segurança da Informação.** 4 versão. São Paulo: BM&FBOVESPA, 2016. Disponível em: <http://ri.bmfbovespa.com.br/fck_temp/26_107/file/Pol%C3%ADtica%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o%2020160513.pdf>. Acesso em 10/05/2017.

CFC, CONSELHO FEDERAL DE CONTABILIDADE. **Normas brasileiras de contabilidade: auditoria interna: NBC TI 01 e NBC PI.** Brasília. Conselho Federal de Contabilidade, 2012

COSO, COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **Controle Interno - Estrutura Integrada – Sumário Executivo.** IIA Brasil, 2013.

CREPALDI, Silvio Aparecido. **Auditoria contábil: teoria e prática**. 2. ed. São Paulo: Atlas, 2002.

Deloitte, Deloitte Touche Tohmatsu Limited.e IIA, Instituto dos Auditres Internos do Brasil - **Auditoria Interna no Brasil - Análise comparativa das tendências globais para uma função em transformação - Pesquisa 2016**. Deloitte, 2016.

DIAS, Sergio Vidal dos Santos. **Auditoria de Processos Organizacionais: teoria, finalidade, metodologia de trabalho e resultados esperados.** São Paulo: Atlas, 2006.

FRANCO, Hilário e MARRA, Ernesto. **Auditoria Contábil**. 3 ed. São Paulo: Atlas, 2000.

IBGC, INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. 5.ed. São Paulo: IBGC, 2015.

_____. **Guia de orientação para o gerenciamento de riscos corporativos.** São Paulo: IBGC, 2007 (Série de Cadernos de Governança Corporativa, 3)

IDC, **The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things**, 2014. Disponível em: <http://brazil.emc.com/leadership/digital-universe/2014iview/index.htm>. Acesso em 15/09/2016.

IIA, THE INSTITUTE OF INTERNAL AUDITORS. **International Professional Practices Framework (IPPF).** Altamonte Springs, USA: IIA, 2013.

_____. **Lidando com os 10 Principaisa Riscos Tecnológicos – O Papel da Auditoria Interna – CBOK**. Altamonte Springs, USA: IIA, 2015.

_____. **Promovendo o Sucesso em um Mundo em Mudança – 10 Imperativos para a Auditoria Interna – CBOK** . Altamonte Springs, USA: IIA, 2015.

_____. **Global Technology Audit Guide (GTAG®) 1 - Information Technology Risk and Controls.** 2. ed. IIA, 2012.

_____. **Orientação Suplementar – Guia Prático – A Auditoria Interna e a Segunda Linha de Defesa.** IIA, 2016.

_____.**THE INSTITUTE OF INTERNAL AUDITORS.** Disponível em: <https://na.theiia.org/about-us/Pages/About-The-Institute-of-Internal-Auditors.aspx>. Acesso em 10/09/2016.

_____. **Pulso Global da Auditoria Interna 2015 - Aproveitando Oportunidades em um Ambiente Dinâmico.** Disponível em: <https://global.theiia.org/translations/PublicDocuments/2015-Global-Pulse-of-Internal-Audit-Report-Portuguese.pdf>. Acesso em 26/08/2016.

IIA BRASIL, **Audi TI – Auditoria de Tecnologia da Informação**. São Paulo: IIA Brasil, 2014.

_____.**INSTITUTO DOS AUDITORES INTERNOS DO BRASIL**. Disponível em:<http://www.iiabrasil.org.br/new/quemsomos.html>. Acesso em 10/09/2016.

IMONIANA, Joshua Onome. **Auditoria de Sistemas de Informação.** 3. ed. São Paulo: Atlas, 2016.

ISACA. **COBIT 5® - Modelo Corporativo para Governança e Gestão de TI da Organização.** USA: ISACA, 2012.

_____. **The Risk It Framework.** USA: ISACA, 2009.

KIM, David e SOLOMON, Michael G.. Tradução Daniel Vieira. **Fundamentos de Segurança de Sistemas de Informação.** 1.ed. Rio de Janeiro: LTC, 2014.

MARTINS, G. A.; THEOPHILO, C. R. **Metodologias da Investigação Cientifica para Ciência Sociais Aplicadas**. São Paulo. Atlas, 2007.

OLIVEIRA, Luís Martins [et al]. **Curso básico de auditoria**. 2.ed. São Paulo: Atlas, 2008.

O'REILLY. **Whatis big data? An introduction to the big data landscape**, 2012 Disponível em: <https://www.oreilly.com/ideas/what-is-big-data>. Acesso em 15/09/2016.

PINHO, Ruth Carvalho de Santana. **Fundamento de Auditoria**. São Paulo: Atlas, 2007.

PWC. **Estudo sobre a Prática Profissional de Auditoria Interna 2015 – Como encontrar o Norte Verdadeiro em um período de rápidas transformações**. Disponível em: <http://www.pwc.com.br/pt/publicacoes/servicos/auditoria/2015/pwc-estudo-pratica-profissional-auditoria-interna-2015.html>. Acesso em 30/08/2016.

_____. **Inovando e Transformando em Segurança Cibernética – Principais conclusões da Pesquisa Global de Segurança da Informação**, 2016. Disponível em: <http://www.pwc.com.br/pt/publicacoes/servicos/assets/consultoria-negocios/2016/tl-gsiss16-pt.pdf>. Acesso em 28/06/2017.

_____. **Superando Momentos Críticos – O papel da análise de dados na transformação da Auditoria Interna**, 2017. Disponível em: <http://www.pwc.com.br/pt/estudos/servicos/auditoria/2017/superando-momentos-criticos-17.pdf>

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma Visão Executiva.** 2.ed. Rio de Janeiro: Elsevier, 2014.

The McKinsey Global Institute, **Big data: The next frontier for innovation, competition, and productivity**, 2011. Disponível em: <http://www.mckinsey.com/business-functions/business-technology/our-insights/big-data-the-next-frontier-for-innovation>. Acesso em 15/09/2016.

## APÊNDICE 1 – QUESTIONÁRIO

# PESQUISA DE AUDITORIA INTERNA (GAIP)

**Pesquisa para monografia do curso MBA em Auditoria Integral - UFPR *Obrigatório**

## Perfil Profissional

---

**Nesta seção responda as perguntas de perfil profissional.**

1. **Qual a sua idade? * Marcar apenas uma oval.**

   - ◯ **Até 25 anos**
   - ◯ **Entre 26 e 30 anos**
   - ◯ **Entre 31 e 40 anos**
   - ◯ **Entre 41 e 50 anos**
   - ◯ **Acima de 50 anos**

2. **Qual sua posição atual na companhia? * Marcar apenas uma oval.**

   - ◯ **Membro do Conselho de Administração ou Fiscal**
   - ◯ **Membro de Comitê de Auditoria e/ou Riscos**
   - ◯ **Diretor**
   - ◯ **Gestor de Auditoria**
   - ◯ **Auditor Interno**
   - ◯ **Analista/Especialista em Riscos ou Controles Internos**
   - ◯ **Analista/Especialista em Tecnologia**
   - ◯ **Outro:** _____

3. **Como você avalia seu conhecimento em auditoria interna? * Marcar apenas uma oval.**

- ◯ **Conheço, mas nunca atuei diretamente com auditoria interna**
- ◯ **Básico, possuo pouco tempo de experiência na área**
- ◯ **Avançado, possuo ampla experiência em trabalhos de auditoria**
- ◯ **Muito experiente, possuo muitos anos de experiência e já realizei trabalhos em diversas áreas da empresa**

4. **Como você avalia seu conhecimento em tecnologia? * Marcar apenas uma oval.**

- ◯ **Sou apenas usuário final, nunca atuei na área de tecnologia**
- ◯ **Básico, possuo pouco tempo de experiência na área**
- ◯ **Avançado, possuo ampla experiência em tecnologia**
- ◯ **Muito experiente, possuo muitos anos de experiência e já atuei em diversos projetos**

## Perfil da Organização

**Nesta seção responda as perguntas relacionadas à empresa em que você trabalha.**

5. **A Companhia em que você trabalha é uma entidade: * Marcar apenas uma oval.**

- ◯ **Nacional**
- ◯ **Multinacional Brasileira**
- ◯ **Multinacional Estrangeira**

6. **A entidade controladora de sua organização está em qual região? * Marcar apenas uma oval.**

- ◯ **América do Sul**
- ◯ **América do Norte**

- Ásia
- Europa
- Outro:

---

**7. A organização que você trabalha está presente em quantos países?** * Marcar apenas uma oval.

- Apenas 1
- De 2 a 10
- De 11 a 30
- De 31 a 50
- Acima de 50

**8. Em qual tipo de organização a empresa que você trabalha se enquadra?** * Marcar apenas uma oval.

- Empresa de capital aberto
- Empresa privada de capital fechado
- Empresa de economia mista
- Governamental
- Sem fins lucrativos
- Outro:

---

**9. Qual setor de atuação sua empresa está inserida?** * Marcar apenas uma oval.

- Agronegócio
- Alimentos e Bebidas
- Automotivo

- Bens Industriais
- Construção e Imóveis
- Educação
- Energia, Gás, Mineração e Petróleo
- Financeiro e Seguros
- Gestão Pública
- Indústria Diversificada
- Infraestrutura e Transporte
- Materiais Básicos
- Saúde
- Serviços
- Tecnologia, Mídias e Telecomunicações
- Varejo

**10. Qual a quantidade de colaboradores diretos na sua empresa? * Marcar apenas uma oval.**

- Até 500
- De 500 a 1 mil
- De 1 mil a 3 mil
- De 3 mil a 10 mil
- Acima de 10 mil

**11. Qual é o tamanho da empresa em que trabalha atualmente (Receita Operacional Bruta Anual em R$)?** * Marcar apenas uma oval.

- Até R$ 500 mi
- Entre R$ 500 mi e R$ 1 bi
- Entre R$ 1 bi e R$ 2 bi
- Entre R$ 2 bi e R$ 5 bi
- Acima de R$ 5 bi
- Não sei informar

**12. Quais áreas/departamentos de governança estão presentes na estrutura da Companhia?** * Marque todas que se aplicam.

- [ ] Comitê de Auditoria e/ou Riscos
- [ ] Auditoria Interna
- [ ] Gerenciamento de Riscos (Enterprise Risk Management)
- [ ] Controles Internos
- [ ] Compliance
- [ ] Outro: _____

**13. A sua empresa possui uma área específica de auditoria interna?** * Marcar apenas uma oval.

- Sim
- Não

**14. Em sua organização há política com as diretrizes de segurança da informação formalizada e divulgada à todos os colaboradores?** * Marcar apenas uma oval.

- Sim
- Não

**15. A empresa possui especialistas, internos e/ou externos, em segurança da informação?** * Marcar apenas uma oval.

- Sim
- Não

## Perfil da Auditoria Interna

**Nesta seção responda as perguntas sobre o perfil e funções da auditoria interna ou considere área com funções semelhantes na sua organização.**

**16. Quais são as atividades/responsabilidades da Auditoria Interna atualmente?** * Marque todas que se aplicam.

- [ ] Auditoria de Processos
- [ ] Auditoria Operacional
- [ ] Auditoria Financeira
- [ ] Controles Internos
- [ ] Compliance
- [ ] Gerenciamento de Riscos
- [ ] SOX
- [ ] Outro:

**17. Qual é a estrutura (quantidade total) de pessoas na área de Auditoria Interna?** * Marcar apenas uma oval.

- Até 2 pessoas
- De 3 a 5 pessoas
- De 6 a 10 pessoas

- Acima de 10 pessoas

**18. Qual o orçamento anual aproximado da área de Auditoria Interna?** * Considere como orçamento total, incluindo remunerações dos colaboradores, despesas de viagens, treinamentos e demais despesas da área durante o período de 1 ano. Marcar apenas uma oval.

- Até R$ 500 mil
- Entre R$ 500 mil e R$ 1 mi
- Entre R$ 1 mi e R$ 3 mi
- Acima de R$ 3 mi
- Não tenho conhecimento

**19. Sua empresa realiza algum tipo de terceirização das funções de Auditoria Interna?** * Marcar apenas uma oval.

- Sim
- Não

**20. Qual é o percentual de terceirização da auditoria interna?** * Marcar apenas uma oval.

- Nenhuma
- 100% dos profissionais e dos trabalhos realizados
- Superior à 50% dos profissionais e dos trabalhos realizados
- Superior à 20% dos profissionais e dos trabalhos realizados
- Apenas projetos especiais com especialização requerida

**21. Auditoria Interna possui profissionais com qualificações em quais áreas?** * Marque todas que se aplicam.

- [ ] Administração/Financeira
- [ ] Contabilidade
- [ ] Direito

- [ ] **Engenharia**
- [ ] **Processo**
- [ ] **Saúde**
- [ ] **Tecnologia da Informação**
- [ ] **Outro:**

**22. À quem a Auditoria Interna se reporta? * Marcar apenas uma oval.**

- ◯ **Conselho de Administração e/ou Fiscal**
- ◯ **Sócios ou Fundo de Investimento**
- ◯ **Comitê de Auditoria**
- ◯ **Presidente/CEO**
- ◯ **Diretoria Financeira**
- ◯ **Outro:**

**23. A Auditoria Interna utiliza ferramentas/softwares para extração e análise de dados? * Marcar apenas uma oval.**

- ◯ **Sim**
- ◯ **Não**

**24. Quais tipos de ferramentas CAAT (Computer Assisted Audit Techniques) a auditoria utiliza? * Marque todas que se aplicam.**

- [ ] **Ferramentas Generalistas (Ex: ACL ou IDEA)**
- [ ] **Ferramentas Especializadas (Ex: ferramenta desenvolvida internamente)**
- [ ] **Ferramentas de Utilidade Geral (Ex: Excel, QlikView, Tableau)**
- [ ] **Ferramentas de Segurança da Informação (Ex: Gestão de acessos, gerenciamento de dispositivos, redes e comunicações)**

Outro:

**25. Auditoria Interna planeja e executa testes de controles e/ou testes subjetivos na área de TI em:** * Marque todas que se aplicam.

- Não planeja e executa testes em temas relacionados à tecnologia
- Governança de TI
- Gestão de Mudanças
- Segurança da Informação
- Operações e suporte
- Outro:

**26. Qual a periodicidade de trabalhos específicos conduzidos pela auditoria interna na área de TI ou em sistemas da Companhia?** * Marcar apenas uma oval.

- Nunca
- Apenas 1 trabalho por ano
- De 2 a 5 trabalhos por ano
- Acima de 5 trabalhos por ano
- Apenas a cada 2 anos ou mais são realizados trabalhos na área de TI

**27. Auditoria interna identifica, avalia e/ou monitora os riscos de Segurança da Informação (SI)?** * Marcar apenas uma oval.

- Não identifica, avalia ou monitora riscos de SI
- Apenas identifica riscos de SI
- Identifica e avalia riscos de SI
- Identifica, avalia e monitora os riscos de SI

**28. A auditoria interna possui indicadores (KRI) para monitoramento dos riscos de Segurança da Informação?** * Marcar apenas uma oval.

- Sim, monitora com KRIs definidos pela auditoria
- Sim, monitora com KRIs definidos por outras áreas
- Não

**29. Qual a periodicidade de avaliação e monitoramento dos riscos de Segurança da Informação (SI) pela auditoria interna?** * Marcar apenas uma oval.

- Nunca
- Mensal
- Trimestral
- Semestral
- Anual
- Apenas quando ocorre um incidente relevante

## Visão do Profissional

**Nesta seção responda as perguntas de acordo com sua visão profissional sobre o cenário atual da auditoria interna, segurança da informação e sua organização.**

**30. Em sua visão, a auditoria interna considera importante a segurança da informação em quais momentos?** * Marque todas que se aplicam.

- [ ] Planejamento anual
- [ ] Escopo dos trabalhos
- [ ] Análises e Testes
- [ ] Denúncias e/ou fraudes

- [ ] **Quando realizado auditoria na área de TI**
- [ ] **Quando solicitado por outra área ou colaborador**
- [ ] **Não considera importante**

**31. Em sua percepção, quais recursos são utilizados pela sua empresa para mitigar os riscos de segurança da informação? * Marque todas que se aplicam.**

- [ ] **Políticas de segurança aplicadas nos sistemas**
- [ ] **Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy)**
- [ ] **Antivírus e/ou outros anti malwares**
- [ ] **Usuários e senhas não compartilhados**
- [ ] **Gestão e monitoramento de acessos aos sistemas**
- [ ] **Bloqueios para dispositivos externos não homologados/autorizados**
- [ ] **Acesso remoto restrito e criptografado**
- [ ] **Dispositivos móveis com senhas e/ou criptografados**
- [ ] **Restrição de acessos em diretórios e arquivos**
- [ ] **Acesso restrito aos ambientes de Data Center**
- [ ] **Sistemas com níveis e permissões de acesso definidos**
- [ ] **Backup de dados e sistemas**
- [ ] **Plano de continuidade do negócio**

**32. Em sua visão, quais são as 3 qualificações mais importantes para o sucesso da auditoria interna nos próximos três a cinco anos? * Marque todas que se aplicam.**

- [ ] **Prevenção/detecção de fraudes**
- [ ] **Data Analytics**

- [ ] **Avaliação de Riscos**
- [ ] **Controles Internos**
- [ ] **Controles internos em TI**
- [ ] **SOX**
- [ ] **Auditorias em sistemas**
- [ ] **Consultoria**
- [ ] **Práticas de Segurança da Informação**
- [ ] **Financeiro**
- [ ] **Regulatório e Compliance**
- [ ] **Continuidade do Negócio**

**33. Em sua visão, qual o engajamento da diretoria em patrocinar, divulgar e monitorar as questões relacionadas à segurança da informação dentro da organização?** * **Responda em uma escala de 1 à 5, considerando que 1 significa muito baixo e 5 é muito alto. Marcar apenas uma oval.**

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Muito baixo | ◯ | ◯ | ◯ | ◯ | ◯ | Muito alto |

**34. Em sua percepção, qual é o nível de segurança das informações da organização?** * **Responda em uma escala de 1 à 5, considerando que 1 significa muito baixo e 5 é muito alto. Marcar apenas uma oval.**

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Muito baixo | ◯ | ◯ | ◯ | ◯ | ◯ | Muito alto |

**35. Pensando na cultura organizacional, qual é o atual nível de relevância da segurança da informação para a empresa e seus colaboradores?** * Responda em uma escala de 1 à 5, considerando que 1 significa muito baixo e 5 é muito alto. Marcar apenas uma oval.

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Muito baixo | ◯ | ◯ | ◯ | ◯ | ◯ | Muito alto |

**36. Em sua visão, de maneira geral, os atuais riscos de segurança da informação da organização são?** * Responda em uma escala de 1 à 5, considerando que 1 significa muito baixo e 5 é muito alto. Marcar apenas uma oval.

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Muito baixo | ◯ | ◯ | ◯ | ◯ | ◯ | Muito alto |

**37. Em sua visão, qual é o engajamento da auditoria interna em identificar, avaliar e monitorar riscos relacionadas à segurança da informação dentro da organização?** * Responda em uma escala de 1 à 5, considerando que 1 significa muito baixo e 5 é muito alto. Marcar apenas uma oval.

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Muito baixo | ◯ | ◯ | ◯ | ◯ | ◯ | Muito alto |

**38. Em sua visão, selecione os 3 principais desafios da sua organização quanto à segurança da informação.** *Marque todas que se aplicam.

- ☐ Exposição em mídias sociais
- ☐ Acessos por dispositivos móveis (pendrive, celular, etc)
- ☐ Acesso à internet e phishing
- ☐ Gestão de perfis e acessos ao sistemas corporativos
- ☐ Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc)
- ☐ Compartilhamento de senhas
- ☐ Perdas de dados e dispositivos
- ☐ Invasão e softwares nocivos ao sistemas da empresa

- [ ] **Compartilhamento de informações privilegiadas**

**39. Em sua visão, selecione as 3 principais práticas que sua organização está utilizando ou poderá utilizar para aculturamento e melhoria da segurança da informação.** * **Marque todas que se aplicam.**

- [ ] **Revisão periódica e divulgação da política de segurança da informação**
- [ ] **Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos**
- [ ] **Revisão periódica dos perfis e acessos aos sistemas**
- [ ] **Ferramentas de bloqueios para restrição de acesso e cópia de dados em dispositivos móveis**
- [ ] **Monitoramento dos acessos e compartilhamento de senhas Criptografia de dados**
- [ ] **Bloqueio de email pessoal e ferramentas de comunicação não homologadas pela empresa**
- [ ] **Níveis/Perfis de acesso de acordo com a classificação da informação (público, privado e confidencial)**

## APÊNDICE 2 – RESPOSTAS DO QUESTIONÁRIO

# Perfil Profissional

| 1- Qual a sua idade? | Quantidade de Respostas |
|---|---|
| Acima de 50 anos | 4 |
| Até 25 anos | 3 |
| Entre 26 e 30 anos | 14 |
| Entre 31 e 40 anos | 21 |
| Entre 41 e 50 anos | 12 |
| **Total Geral** | **54** |

| 2 - Qual sua posição atual na companhia? | Quantidade de Respostas |
|---|---|
| Analista/Especialista em Riscos ou Controles Internos | 9 |
| Auditor Interno | 21 |
| Consultor | 1 |
| Consultoria | 1 |
| Contador | 1 |
| Controle Interno | 1 |
| Coordenador de Riscos | 1 |
| Diretor | 4 |
| GERENTE DE AUDITORIA APOSENTADO | 1 |
| Gerente de Projetos | 1 |
| Gestor de Auditoria | 12 |
| Superintendente Administrativo | 1 |
| **Total Geral** | **54** |

| 3 - Como você avalia seu conhecimento em auditoria interna? | Quantidade de Respostas |
|---|---|
| Avançado, possuo ampla experiência em trabalhos de auditoria | 20 |
| Básico, possuo pouco tempo de experiência na área | 6 |
| Conheço, mas nunca atuei diretamente com auditoria interna | 8 |
| Muito experiente, possuo muitos anos de experiência e já realizei trabalhos em diversas áreas da empresa | 20 |
| **Total Geral** | **54** |

| 4 - Como você avalia seu conhecimento em tecnologia? | Quantidade de Respostas |
|---|---|
| Avançado, possuo ampla experiência em tecnologia | 14 |
| Básico, possuo pouco tempo de experiência na área | 21 |
| Muito experiente, possuo muitos anos de experiência e já atuei em diversos projetos | 6 |
| Sou apenas usuário final, nunca atuei na área de tecnologia | 13 |
| **Total Geral** | **54** |

# Perfil da Organização

| 5 - A Companhia em que você trabalha é uma entidade: | Quantidade de Respostas |
|---|---|
| Multinacional Brasileira | 14 |
| Multinacional Estrangeira | 16 |
| Nacional | 24 |
| **Total Geral** | **54** |

| 6 - A entidade controladora de sua organização está em qual região? | Quantidade de Respostas |
|---|---|
| América do Norte | 4 |
| América do Sul | 42 |
| Ásia | 4 |
| Europa | 4 |
| **Total Geral** | **54** |

| 7 - A organização que você trabalha está presente em quantos países? | Quantidade de Respostas |
|---|---|
| Acima de 50 | 8 |
| Apenas 1 | 20 |
| De 11 a 30 | 9 |
| De 2 a 10 | 14 |
| De 31 a 50 | 3 |
| **Total Geral** | **54** |

| 8 - Em qual tipo de organização a empresa que você trabalha se enquadra? | Quantidade de Respostas |
|---|---|
| Empresa de capital aberto | 16 |
| Empresa de economia mista | 3 |
| Empresa privada de capital fechado | 29 |
| Governamental | 2 |
| Sem fins lucrativos | 4 |
| **Total Geral** | **54** |

| 9 - Qual setor de atuação sua empresa está inserida? | Quantidade de Respostas |
|---|---|
| Agronegócio | 3 |
| Alimentos e Bebidas | 5 |
| Automotivo | 5 |
| Bens Industriais | 1 |
| Construção e Imóveis | 2 |
| Educação | 6 |
| Energia, Gás, Mineração e Petróleo | 2 |
| Financeiro e Seguros | 6 |
| Indústria Diversificada | 4 |
| Infraestrutura e Transporte | 1 |
| Materiais Básicos | 6 |

| | |
|---|---|
| Saúde | 3 |
| Serviços | 6 |
| Tecnologia, Mídias e Telecomunicações | 2 |
| Varejo | 2 |
| **Total Geral** | **54** |

| **10 - Qual a quantidade de colaboradores diretos na sua empresa?** | **Quantidade de Respostas** |
|---|---|
| Acima de 10 mil | 17 |
| Até 500 | 6 |
| De 1 mil a 3 mil | 13 |
| De 3 mil a 10 mil | 9 |
| De 500 a 1 mil | 9 |
| **Total Geral** | **54** |

| **11 - Qual é o tamanho da empresa em que trabalha atualmente (Receita Operacional Bruta Anual em R$)?** | **Quantidade de Respostas** |
|---|---|
| Acima de R$ 5 bi | 15 |
| Até R$ 500 mi | 9 |
| Entre R$ 1 bi e R$ 2 bi | 6 |
| Entre R$ 2 bi e R$ 5 bi | 8 |
| Entre R$ 500 mi e R$ 1 bi | 12 |
| Não sei informar | 4 |
| **Total Geral** | **54** |

| **12 - Quais áreas/departamentos de governança estão presentes na estrutura da Companhia?** | **Quantidade de Respostas** |
|---|---|
| Auditoria Interna | 10 |
| Auditoria Interna, Compliance | 5 |
| Auditoria Interna, Controles Internos | 2 |
| Auditoria Interna, Gerenciamento de Riscos (Enterprise Risk Management) | 2 |
| Auditoria Interna, Gerenciamento de Riscos (Enterprise Risk Management), Compliance | 3 |
| Auditoria Interna, Gerenciamento de Riscos (Enterprise Risk Management), Controles Internos | 1 |
| Auditoria Interna, Gerenciamento de Riscos (Enterprise Risk Management), Controles Internos, Compliance | 1 |
| Auditoria Interna, Gestão de Processos | 1 |
| Comitê de Auditoria e/ou Riscos, Auditoria Interna | 2 |
| Comitê de Auditoria e/ou Riscos, Auditoria Interna, Compliance | 1 |
| Comitê de Auditoria e/ou Riscos, Auditoria Interna, Controles Internos | 3 |
| Comitê de Auditoria e/ou Riscos, Auditoria Interna, Gerenciamento de Riscos (Enterprise Risk Management) | 1 |
| Comitê de Auditoria e/ou Riscos, Auditoria Interna, Gerenciamento de Riscos (Enterprise Risk Management), Compliance | 1 |
| Comitê de Auditoria e/ou Riscos, Auditoria Interna, Gerenciamento de Riscos (Enterprise Risk Management), Controles Internos | 3 |
| Comitê de Auditoria e/ou Riscos, Auditoria Interna, Gerenciamento de Riscos (Enterprise Risk Management), Controles Internos, Compliance | 11 |
| Comitê de Auditoria e/ou Riscos, Controles Internos, Compliance | 1 |
| Compliance | 1 |
| Controles Internos | 2 |

| | |
|---|---|
| Controles Internos, Compliance | 1 |
| Empresa de prestação de serviços de consultoria | 1 |
| Gerenciamento de Riscos (Enterprise Risk Management) | 1 |
| **Total Geral** | **54** |

| 13 - A sua empresa possui uma área específica de auditoria interna? | Quantidade de Respostas |
|---|---|
| Não | 5 |
| Sim | 49 |
| **Total Geral** | **54** |

| 14 - Em sua organização há política com as diretrizes de segurança da informação formalizada e divulgada à todos os colaboradores? | Quantidade de Respostas |
|---|---|
| Não | 14 |
| Sim | 40 |
| **Total Geral** | **54** |

| 15 - A empresa possui especialistas, internos e/ou externos, em segurança da informação? | Quantidade de Respostas |
|---|---|
| Não | 19 |
| Sim | 35 |
| **Total Geral** | **54** |

## Perfil da Auditoria Interna

| 16 - Quais são as atividades/responsabilidades da Auditoria Interna atualmente? | Quantidade de Respostas |
|---|---|
| Auditoria de Processos, Auditoria Financeira, Controles Internos, Compliance, Gerenciamento de Riscos | 1 |
| Auditoria de Processos, Auditoria Financeira, Controles Internos, Compliance, Gerenciamento de Riscos, SOX | 1 |
| Auditoria de Processos, Auditoria Operacional | 4 |
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira | 5 |
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira, Compliance, SOX | 1 |
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira, Controles Internos | 2 |
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira, Controles Internos, Compliance | 1 |
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira, Controles Internos, Compliance, Gerenciamento de Riscos | 2 |
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira, Controles Internos, Compliance, Gerenciamento de Riscos, SOX | 11 |
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira, Controles Internos, Compliance, Gerenciamento de Riscos, SOX, Auditoria de TI | 1 |
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira, Controles Internos, Compliance, SOX | 1 |
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira, Controles Internos, Consultoria | 1 |

| | |
|---|---|
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira, Controles Internos, Gerenciamento de Riscos | 2 |
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira, Controles Internos, Gerenciamento de Riscos, SOX | 1 |
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira, Controles Internos, SOX | 1 |
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira, Gerenciamento de Riscos, SOX | 1 |
| Auditoria de Processos, Auditoria Operacional, Auditoria Financeira, SOX | 1 |
| Auditoria de Processos, Auditoria Operacional, Compliance, SOX | 1 |
| Auditoria de Processos, Auditoria Operacional, Controles Internos | 2 |
| Auditoria de Processos, Auditoria Operacional, Controles Internos, Compliance, SOX | 1 |
| Auditoria de Processos, Compliance | 1 |
| Auditoria de Processos, Controles Internos, SOX | 2 |
| Auditoria Financeira, Compliance, SOX | 1 |
| Auditoria Operacional, Auditoria Financeira | 1 |
| Auditoria Operacional, Auditoria Financeira, Controles Internos | 1 |
| Auditoria Operacional, Auditoria Financeira, Controles Internos, Compliance | 1 |
| Auditoria Operacional, Auditoria Financeira, Controles Internos, Compliance, Gerenciamento de Riscos | 1 |
| Compliance | 1 |
| Controles Internos | 2 |
| Controles Internos, SOX | 1 |
| Não possui auditoria interna. | 1 |
| **Total Geral** | **54** |

| **17 - Qual é a estrutura (quantidade total) de pessoas na área de Auditoria Interna?** | **Quantidade de Respostas** |
|---|---|
| Acima de 10 pessoas | 14 |
| Até 2 pessoas | 8 |
| De 3 a 5 pessoas | 19 |
| De 6 a 10 pessoas | 13 |
| **Total Geral** | **54** |

| **18 - Qual o orçamento anual aproximado da área de Auditoria Interna?** | **Quantidade de Respostas** |
|---|---|
| Acima de R$ 3 mi | 8 |
| Até R$ 500 mil | 16 |
| Entre R$ 1 mi e R$ 3 mi | 3 |
| Entre R$ 500 mil e R$ 1 mi | 8 |
| Não tenho conhecimento | 19 |
| **Total Geral** | **54** |

| **19 - Sua empresa realiza algum tipo de terceirização das funções de Auditoria Interna?** | **Quantidade de Respostas** |
|---|---|
| Não | 42 |
| Sim | 12 |
| **Total Geral** | **54** |

| **20 - Qual é o percentual de terceirização da auditoria interna?** | **Quantidade de Respostas** |
|---|---|
| Apenas projetos especiais com especialização requerida | 9 |

| | |
|---|---|
| Nenhuma | 42 |
| Superior à 20% dos profissionais e dos trabalhos realizados | 1 |
| Superior à 50% dos profissionais e dos trabalhos realizados | 2 |
| **Total Geral** | **54** |

| **21 - Auditoria Interna possui profissionais com qualificações em quais áreas?** | **Quantidade de Respostas** |
|---|---|
| Administração/Financeira | 1 |
| Administração/Financeira, Contabilidade | 7 |
| Administração/Financeira, Contabilidade, Direito | 3 |
| Administração/Financeira, Contabilidade, Direito, Engenharia, Processo, Saúde | 1 |
| Administração/Financeira, Contabilidade, Direito, Engenharia, Processo, Saúde, Tecnologia da Informação | 1 |
| Administração/Financeira, Contabilidade, Direito, Engenharia, Processo, Tecnologia da Informação | 2 |
| Administração/Financeira, Contabilidade, Direito, Processo, Tecnologia da Informação | 1 |
| Administração/Financeira, Contabilidade, Direito, Tecnologia da Informação | 1 |
| Administração/Financeira, Contabilidade, Engenharia, Processo, Tecnologia da Informação | 6 |
| Administração/Financeira, Contabilidade, Engenharia, Tecnologia da Informação | 4 |
| Administração/Financeira, Contabilidade, Processo | 7 |
| Administração/Financeira, Contabilidade, Processo, Tecnologia da Informação | 3 |
| Administração/Financeira, Contabilidade, Tecnologia da Informação | 4 |
| Administração/Financeira, Direito, Economia | 1 |
| Administração/Financeira, Processo | 1 |
| Contabilidade | 5 |
| Contabilidade, Direito | 1 |
| Contabilidade, Direito, Engenharia | 1 |
| Contabilidade, Engenharia | 1 |
| Contabilidade, Processo | 1 |
| Não possui auditoria interna. | 1 |
| Processo | 1 |
| **Total Geral** | **54** |

| **22 - À quem a Auditoria Interna se reporta?** | **Quantidade de Respostas** |
|---|---|
| Comitê de Auditoria | 15 |
| Conselho de Administração e/ou Fiscal | 10 |
| Diretor de Controladoria Corporativo | 1 |
| Diretoria Financeira | 6 |
| Diretoria Geral | 1 |
| Não possui auditoria interna. | 1 |
| Não sei informar | 1 |
| Presidente/CEO | 16 |
| Sócios ou Fundo de Investimento | 2 |
| Superintendência | 1 |
| **Total Geral** | **54** |

| 23 - A Auditoria Interna utiliza ferramentas/softwares para extração e análise de dados? | Quantidade de Respostas |
|---|---|
| Não | 17 |
| Sim | 37 |
| **Total Geral** | **54** |

| 24 - Quais tipos de ferramentas CAAT (Computer Assisted Audit Techniques) a auditoria utiliza? | Quantidade de Respostas |
|---|---|
| Ferramentas de Segurança da Informação (Ex: Gestão de acessos, gerenciamento de dispositivos, redes e comunicações) | 1 |
| Ferramentas de Utilidade Geral (Ex: Excel, QlikView, Tableau) | 18 |
| Ferramentas de Utilidade Geral (Ex: Excel, QlikView, Tableau), Alteryx | 1 |
| Ferramentas Especializadas (Ex: ferramenta desenvolvida internamente) | 1 |
| Ferramentas Especializadas (Ex: ferramenta desenvolvida internamente), Ferramentas de Utilidade Geral (Ex: Excel, QlikView, Tableau) | 3 |
| Ferramentas Especializadas (Ex: ferramenta desenvolvida internamente), Ferramentas de Utilidade Geral (Ex: Excel, QlikView, Tableau), Ferramentas de Segurança da Informação (Ex: Gestão de acessos, gerenciamento de dispositivos, redes e comunicações) | 1 |
| Ferramentas Generalistas (Ex: ACL ou IDEA) | 4 |
| Ferramentas Generalistas (Ex: ACL ou IDEA), Ferramentas de Utilidade Geral (Ex: Excel, QlikView, Tableau) | 11 |
| Ferramentas Generalistas (Ex: ACL ou IDEA), Ferramentas de Utilidade Geral (Ex: Excel, QlikView, Tableau), Ferramentas de Segurança da Informação (Ex: Gestão de acessos, gerenciamento de dispositivos, redes e comunicações) | 9 |
| Ferramentas Generalistas (Ex: ACL ou IDEA), Ferramentas Especializadas (Ex: ferramenta desenvolvida internamente) | 1 |
| Ferramentas Generalistas (Ex: ACL ou IDEA), Ferramentas Especializadas (Ex: ferramenta desenvolvida internamente), Ferramentas de Utilidade Geral (Ex: Excel, QlikView, Tableau), Ferramentas de Segurança da Informação (Ex: Gestão de acessos, gerenciamento de dispositivos, redes e comunicações) | 3 |
| Não possui auditoria interna. | 1 |
| **Total Geral** | **54** |

| 25 - Auditoria Interna planeja e executa testes de controles e/ou testes subjetivos na área de TI em: | Quantidade de Respostas |
|---|---|
| Gestão de acessos | 1 |
| Gestão de Mudanças | 1 |
| Gestão de Mudanças, Operações e suporte, Testes de controles internos somente | 1 |
| Gestão de Mudanças, Segurança da Informação | 2 |
| Gestão de Mudanças, Segurança da Informação, Operações e suporte | 1 |
| Governança de TI | 4 |
| Governança de TI, Gestão de Mudanças, Segurança da Informação | 4 |
| Governança de TI, Gestão de Mudanças, Segurança da Informação, Operações e suporte | 5 |
| Governança de TI, Segurança da Informação | 3 |
| Governança de TI, Segurança da Informação, Operações e suporte | 2 |
| Não planeja e executa testes em temas relacionados à tecnologia | 20 |
| Não planeja e executa testes em temas relacionados à tecnologia, Gestão de Mudanças | 1 |
| Não possui auditoria interna. | 1 |
| Operações e suporte | 4 |

| | |
|---|---|
| Pretendemos realizar neste ano | 1 |
| Segurança da Informação | 2 |
| Segurança da Informação, Operações e suporte | 1 |
| **Total Geral** | **54** |

| **26 - Qual a periodicidade de trabalhos específicos conduzidos pela auditoria interna na área de TI ou em sistemas da Companhia?** | **Quantidade de Respostas** |
|---|---|
| Acima de 5 trabalhos por ano | 7 |
| Apenas 1 trabalho por ano | 15 |
| Apenas a cada 2 anos ou mais são realizados trabalhos na área de TI | 3 |
| De 2 a 5 trabalhos por ano | 13 |
| Nunca | 16 |
| **Total Geral** | **54** |

| **27 - Auditoria interna identifica, avalia e/ou monitora os riscos de Segurança da Informação (SI)?** | **Quantidade de Respostas** |
|---|---|
| Apenas identifica riscos de SI | 9 |
| Identifica e avalia riscos de SI | 14 |
| Identifica, avalia e monitora os riscos de SI | 8 |
| Não identifica, avalia ou monitora riscos de SI | 23 |
| **Total Geral** | **54** |

| **28 - A auditoria interna possui indicadores (KRI) para monitoramento dos riscos de Segurança da Informação?** | **Quantidade de Respostas** |
|---|---|
| Não | 45 |
| Sim, monitora com KRIs definidos pela auditoria | 8 |
| Sim, monitora com KRIs definidos por outras áreas | 1 |
| **Total Geral** | **54** |

| **29 - Qual a periodicidade de avaliação e monitoramento dos riscos de Segurança da Informação (SI) pela auditoria interna?** | **Quantidade de Respostas** |
|---|---|
| Anual | 13 |
| Apenas quando ocorre um incidente relevante | 14 |
| Mensal | 4 |
| Nunca | 16 |
| Semestral | 2 |
| Trimestral | 5 |
| **Total Geral** | **54** |

# Visão do Profissional

| 30 - Em sua visão, a auditoria interna considera importante a segurança da informação em quais momentos? | Quantidade de Respostas |
|---|---|
| Análises e Testes | 4 |
| Análises e Testes, Denúncias e/ou fraudes, Quando realizado auditoria na área de TI | 1 |
| Denúncias e/ou fraudes | 3 |
| Denúncias e/ou fraudes, Quando realizado auditoria na área de TI | 4 |
| Denúncias e/ou fraudes, Quando solicitado por outra área ou colaborador | 1 |
| Escopo dos trabalhos | 3 |
| Escopo dos trabalhos, Análises e Testes, Denúncias e/ou fraudes, Quando realizado auditoria na área de TI | 1 |
| Escopo dos trabalhos, Análises e Testes, Denúncias e/ou fraudes, Quando realizado auditoria na área de TI, Quando solicitado por outra área ou colaborador | 1 |
| Escopo dos trabalhos, Denúncias e/ou fraudes, Quando realizado auditoria na área de TI, Quando solicitado por outra área ou colaborador | 1 |
| Escopo dos trabalhos, Quando solicitado por outra área ou colaborador | 1 |
| Não considera importante | 4 |
| Planejamento anual | 2 |
| Planejamento anual, Análises e Testes, Denúncias e/ou fraudes, Quando realizado auditoria na área de TI | 2 |
| Planejamento anual, Denúncias e/ou fraudes | 1 |
| Planejamento anual, Denúncias e/ou fraudes, Quando realizado auditoria na área de TI | 2 |
| Planejamento anual, Escopo dos trabalhos | 1 |
| Planejamento anual, Escopo dos trabalhos, Análises e Testes | 2 |
| Planejamento anual, Escopo dos trabalhos, Análises e Testes, Denúncias e/ou fraudes | 2 |
| Planejamento anual, Escopo dos trabalhos, Análises e Testes, Denúncias e/ou fraudes, Quando realizado auditoria na área de TI | 4 |
| Planejamento anual, Escopo dos trabalhos, Análises e Testes, Denúncias e/ou fraudes, Quando realizado auditoria na área de TI, Quando solicitado por outra área ou colaborador | 7 |
| Planejamento anual, Escopo dos trabalhos, Análises e Testes, Denúncias e/ou fraudes, Quando solicitado por outra área ou colaborador | 1 |
| Planejamento anual, Escopo dos trabalhos, Análises e Testes, Quando realizado auditoria na área de TI | 1 |
| Planejamento anual, Escopo dos trabalhos, Quando realizado auditoria na área de TI | 1 |
| Planejamento anual, Quando realizado auditoria na área de TI, Quando solicitado por outra área ou colaborador | 1 |
| Quando realizado auditoria na área de TI | 1 |
| Quando solicitado por outra área ou colaborador | 2 |
| **Total Geral** | **54** |

| 31 - Em sua percepção, quais recursos são utilizados pela sua empresa para mitigar os riscos de segurança da informação? | Quantidade de Respostas |
|---|---|
| Antivírus e/ou outros anti malwares | 1 |
| Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas, Plano de continuidade do negócio | 1 |
| Políticas de segurança aplicadas nos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Backup de dados e sistemas | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Acesso remoto restrito e criptografado, Dispositivos móveis com senhas e/ou criptografados, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Backup de dados e sistemas | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Backup de dados e sistemas | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Dispositivos móveis com senhas e/ou criptografados, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Backup de dados e sistemas | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Gestão e monitoramento de acessos aos sistemas, Acesso remoto restrito e criptografado, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas, Plano de continuidade do negócio | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Gestão e monitoramento de acessos aos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Acesso remoto restrito e criptografado, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas, Plano de continuidade do negócio | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Gestão e monitoramento de acessos aos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Backup de dados e sistemas | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Acesso remoto restrito e criptografado, Dispositivos móveis com senhas e/ou criptografados, Restrição de acessos em diretórios e arquivos, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas, Plano de continuidade do negócio | 1 |

| | |
|---|---|
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Acesso restrito aos ambientes de Data Center, Plano de continuidade do negócio | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Bloqueios para dispositivos externos não homologados/autorizados, Acesso remoto restrito e criptografado, Backup de dados e sistemas, Plano de continuidade do negócio | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Bloqueios para dispositivos externos não homologados/autorizados, Dispositivos móveis com senhas e/ou criptografados, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Acesso remoto restrito e criptografado, Dispositivos móveis com senhas e/ou criptografados, Acesso restrito aos ambientes de Data Center, Backup de dados e sistemas, Plano de continuidade do negócio | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Acesso remoto restrito e criptografado, Dispositivos móveis com senhas e/ou criptografados, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Plano de continuidade do negócio | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Acesso remoto restrito e criptografado, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Acesso remoto restrito e criptografado, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas, Plano de continuidade do negócio | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Acesso remoto restrito e criptografado, Restrição de acessos em diretórios e arquivos, Backup de dados e sistemas | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Acesso remoto restrito e criptografado, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas | 1 |

| | |
|---|---|
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Acesso remoto restrito e criptografado, Dispositivos móveis com senhas e/ou criptografados, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas | 2 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Acesso remoto restrito e criptografado, Dispositivos móveis com senhas e/ou criptografados, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas, Plano de continuidade do negócio | 13 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Acesso remoto restrito e criptografado, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Acesso remoto restrito e criptografado, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas | 2 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Acesso remoto restrito e criptografado, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas, Plano de continuidade do negócio | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Restrição de acessos em diretórios e arquivos, Backup de dados e sistemas, Plano de continuidade do negócio | 1 |

| | |
|---|---|
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Dispositivos móveis com senhas e/ou criptografados, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas, Plano de continuidade do negócio | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Restrição de acessos em diretórios e arquivos, Plano de continuidade do negócio | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Restrição de acessos em diretórios e arquivos | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Backup de dados e sistemas | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Restrição de acessos em diretórios e arquivos, Backup de dados e sistemas | 1 |
| Políticas de segurança aplicadas nos sistemas, Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Acesso remoto restrito e criptografado, Restrição de acessos em diretórios e arquivos, Backup de dados e sistemas | 1 |
| Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy) | 2 |
| Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Bloqueios para dispositivos externos não homologados/autorizados, Dispositivos móveis com senhas e/ou criptografados, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Backup de dados e sistemas, Plano de continuidade do negócio | 1 |
| Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Acesso remoto restrito e criptografado, Restrição de acessos em diretórios e arquivos, Acesso restrito aos ambientes de Data Center, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas | 1 |
| Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Bloqueios para dispositivos externos não homologados/autorizados, Restrição de acessos em diretórios e arquivos, Sistemas com níveis e permissões de acesso definidos, Backup de dados e sistemas | 2 |
| Sistemas de proteção nas redes internas e externas (Exemplo: Firewall, Proxy), Antivírus e/ou outros anti malwares, Usuários e senhas não compartilhados, Gestão e monitoramento de acessos aos sistemas, Restrição de acessos em diretórios e arquivos, Backup de dados e sistemas | 1 |
| **Total Geral** | **54** |

| 32 - Em sua visão, quais são as 3 qualificações mais importantes para o sucesso da auditoria interna nos próximos três a cinco anos? | Quantidade de Respostas |
|---|---|
| Auditorias em sistemas, Financeiro, Regulatório e Compliance | 1 |
| Auditorias em sistemas, Práticas de Segurança da Informação, Regulatório e Compliance | 1 |
| Avaliação de Riscos, Auditorias em sistemas, Regulatório e Compliance | 1 |
| Avaliação de Riscos, Controles Internos, Auditorias em sistemas | 1 |
| Avaliação de Riscos, Controles Internos, Consultoria | 1 |
| Avaliação de Riscos, Controles Internos, Controles internos em TI | 1 |
| Avaliação de Riscos, Controles Internos, Regulatório e Compliance | 1 |
| Avaliação de Riscos, Práticas de Segurança da Informação, Regulatório e Compliance | 2 |
| Avaliação de Riscos, Regulatório e Compliance, Continuidade do Negócio | 3 |
| Controles Internos, Controles internos em TI, Regulatório e Compliance | 2 |
| Data Analytics, Avaliação de Riscos, Auditorias em sistemas | 1 |
| Data Analytics, Avaliação de Riscos, Consultoria | 1 |
| Data Analytics, Avaliação de Riscos, Controles Internos | 1 |
| Data Analytics, Avaliação de Riscos, Práticas de Segurança da Informação | 2 |
| Data Analytics, Avaliação de Riscos, Regulatório e Compliance | 3 |
| Data Analytics, Controles Internos, Auditorias em sistemas | 2 |
| Data Analytics, Controles Internos, Controles internos em TI | 1 |
| Data Analytics, Controles Internos, Regulatório e Compliance | 2 |
| Data Analytics, Financeiro, Regulatório e Compliance | 1 |
| Data Analytics, Práticas de Segurança da Informação, Regulatório e Compliance | 1 |
| Data Analytics, Regulatório e Compliance, Continuidade do Negócio | 2 |
| Data Analytics, SOX, Continuidade do Negócio | 1 |
| Data Analytics, SOX, Regulatório e Compliance | 1 |
| Prevenção/detecção de fraudes, Avaliação de Riscos, Consultoria | 1 |
| Prevenção/detecção de fraudes, Avaliação de Riscos, Controles Internos | 5 |
| Prevenção/detecção de fraudes, Avaliação de Riscos, Práticas de Segurança da Informação | 1 |
| Prevenção/detecção de fraudes, Avaliação de Riscos, Regulatório e Compliance | 2 |
| Prevenção/detecção de fraudes, Avaliação de Riscos, SOX | 1 |
| Prevenção/detecção de fraudes, Controles internos em TI, SOX | 1 |
| Prevenção/detecção de fraudes, Controles Internos, Auditorias em sistemas | 2 |
| Prevenção/detecção de fraudes, Controles Internos, Continuidade do Negócio | 1 |
| Prevenção/detecção de fraudes, Controles Internos, Controles internos em TI | 1 |
| Prevenção/detecção de fraudes, Controles Internos, Regulatório e Compliance | 1 |
| Prevenção/detecção de fraudes, Data Analytics, Auditorias em sistemas | 1 |
| Prevenção/detecção de fraudes, Data Analytics, Consultoria | 1 |
| Prevenção/detecção de fraudes, Data Analytics, SOX | 1 |
| Prevenção/detecção de fraudes, Práticas de Segurança da Informação, Regulatório e Compliance | 1 |
| Prevenção/detecção de fraudes, Regulatório e Compliance, Continuidade do Negócio | 1 |
| **Total Geral** | **54** |

| 33 - Em sua visão, qual o engajamento da diretoria em patrocinar, divulgar e monitorar as questões relacionadas à segurança da informação dentro da organização? | Quantidade de Respostas |
|---|---|
| 1 Muito baixo | 3 |
| 2 | 11 |
| 3 | 17 |
| 4 | 15 |
| 5 Muito alto | 8 |
| **Total Geral** | **54** |

| 34 - Em sua percepção, qual é o nível de segurança das informações da organização? | Quantidade de Respostas |
|---|---|
| 1 Muito baixo | 3 |
| 2 | 11 |
| 3 | 13 |
| 4 | 21 |
| 5 Muito alto | 6 |
| **Total Geral** | **54** |

| 35 - Pensando na cultura organizacional, qual é o atual nível de relevância da segurança da informação para a empresa e seus colaboradores? | Quantidade de Respostas |
|---|---|
| 1 Muito baixo | 4 |
| 2 | 12 |
| 3 | 19 |
| 4 | 10 |
| 5 Muito alto | 9 |
| **Total Geral** | **54** |

| 36 - Em sua visão, de maneira geral, os atuais riscos de segurança da informação da organização são? | Quantidade de Respostas |
|---|---|
| 1 Muito baixo | 1 |
| 2 | 8 |
| 3 | 16 |
| 4 | 18 |
| 5 Muito alto | 11 |
| **Total Geral** | **54** |

| 37 - Em sua visão, qual é o engajamento da auditoria interna em identificar, avaliar e monitorar riscos relacionadas à segurança da informação dentro da organização? | Quantidade de Respostas |
|---|---|
| 1 Muito baixo | 8 |
| 2 | 7 |
| 3 | 14 |
| 4 | 20 |
| 5 Muito alto | 5 |
| **Total Geral** | **54** |

| 38 - Em sua visão, selecione os 3 principais desafios da sua organização quanto à segurança da informação. | Quantidade de Respostas |
|---|---|
| Acesso à internet e phishing, Gestão de perfis e acessos ao sistemas corporativos, Compartilhamento de informações privilegiadas | 1 |
| Acesso à internet e phishing, Gestão de perfis e acessos ao sistemas corporativos, Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc) | 1 |
| Acesso à internet e phishing, Invasão e softwares nocivos ao sistemas da empresa, Compartilhamento de informações privilegiadas | 1 |
| Acesso à internet e phishing, Perdas de dados e dispositivos, Invasão e softwares nocivos ao sistemas da empresa | 1 |
| Acesso à internet e phishing, Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc), Compartilhamento de informações privilegiadas | 1 |
| Acesso à internet e phishing, Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc), Compartilhamento de senhas | 1 |
| Acesso à internet e phishing, Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc), Perdas de dados e dispositivos | 1 |
| Acessos por dispositivos móveis (pendrive, celular, etc), Acesso à internet e phishing, Compartilhamento de informações privilegiadas | 1 |
| Acessos por dispositivos móveis (pendrive, celular, etc), Acesso à internet e phishing, Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc) | 1 |
| Acessos por dispositivos móveis (pendrive, celular, etc), Gestão de perfis e acessos ao sistemas corporativos, Compartilhamento de informações privilegiadas | 1 |
| Acessos por dispositivos móveis (pendrive, celular, etc), Gestão de perfis e acessos ao sistemas corporativos, Compartilhamento de senhas | 1 |
| Acessos por dispositivos móveis (pendrive, celular, etc), Gestão de perfis e acessos ao sistemas corporativos, Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc) | 2 |
| Acessos por dispositivos móveis (pendrive, celular, etc), Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc), Compartilhamento de informações privilegiadas | 1 |
| Acessos por dispositivos móveis (pendrive, celular, etc), Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc), Compartilhamento de senhas | 1 |
| Acessos por dispositivos móveis (pendrive, celular, etc), Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc), Invasão e softwares nocivos ao sistemas da empresa | 3 |
| Exposição em mídias sociais, Acesso à internet e phishing, Compartilhamento de senhas | 2 |
| Exposição em mídias sociais, Acessos por dispositivos móveis (pendrive, celular, etc), Acesso à internet e phishing | 1 |
| Exposição em mídias sociais, Acessos por dispositivos móveis (pendrive, celular, etc), Gestão de perfis e acessos ao sistemas corporativos | 1 |

| | |
|---|---|
| Exposição em mídias sociais, Acessos por dispositivos móveis (pendrive, celular, etc), Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc) | 3 |
| Exposição em mídias sociais, Compartilhamento de senhas, Compartilhamento de informações privilegiadas | 1 |
| Exposição em mídias sociais, Compartilhamento de senhas, Perdas de dados e dispositivos | 1 |
| Exposição em mídias sociais, Gestão de perfis e acessos ao sistemas corporativos, Compartilhamento de informações privilegiadas | 2 |
| Exposição em mídias sociais, Gestão de perfis e acessos ao sistemas corporativos, Compartilhamento de senhas | 1 |
| Exposição em mídias sociais, Gestão de perfis e acessos ao sistemas corporativos, Invasão e softwares nocivos ao sistemas da empresa | 1 |
| Exposição em mídias sociais, Gestão de perfis e acessos ao sistemas corporativos, Perdas de dados e dispositivos | 1 |
| Exposição em mídias sociais, Invasão e softwares nocivos ao sistemas da empresa, Compartilhamento de informações privilegiadas | 1 |
| Exposição em mídias sociais, Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc), Invasão e softwares nocivos ao sistemas da empresa | 1 |
| Gestão de perfis e acessos ao sistemas corporativos, Compartilhamento de senhas, Compartilhamento de informações privilegiadas | 2 |
| Gestão de perfis e acessos ao sistemas corporativos, Invasão e softwares nocivos ao sistemas da empresa, Compartilhamento de informações privilegiadas | 1 |
| Gestão de perfis e acessos ao sistemas corporativos, Perdas de dados e dispositivos, Compartilhamento de informações privilegiadas | 3 |
| Gestão de perfis e acessos ao sistemas corporativos, Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc), Compartilhamento de informações privilegiadas | 6 |
| Gestão de perfis e acessos ao sistemas corporativos, Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc), Compartilhamento de senhas | 1 |
| Perdas de dados e dispositivos, Invasão e softwares nocivos ao sistemas da empresa, Compartilhamento de informações privilegiadas | 1 |
| Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc), Compartilhamento de senhas, Compartilhamento de informações privilegiadas | 1 |
| Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc), Invasão e softwares nocivos ao sistemas da empresa, Compartilhamento de informações privilegiadas | 3 |
| Vazamento de informações por ferramentas de comunicação (email, whatsapp, rede social, fotos, etc), Perdas de dados e dispositivos, Invasão e softwares nocivos ao sistemas da empresa | 2 |
| **Total Geral** | **54** |

| **39 - Em sua visão, selecione as 3 principais práticas que sua organização está utilizando ou poderá utilizar para aculturamento e melhoria da segurança da informação.** | **Quantidade de Respostas** |
|---|---|
| Ferramentas de bloqueios para restrição de acesso e cópia de dados em dispositivos móveis, Bloqueio de email pessoal e ferramentas de comunicação não homologadas pela empresa, Níveis/Perfis de acesso de acordo com a classificação da informação (público, privado e confidencial) | 1 |
| Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos, Ferramentas de bloqueios para restrição de acesso e cópia de dados em dispositivos móveis, Criptografia de dados em dispositivos | 1 |

| | |
|---|---|
| Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos, Revisão periódica dos perfis e acessos aos sistemas, Bloqueio de email pessoal e ferramentas de comunicação não homologadas pela empresa | 2 |
| Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos, Revisão periódica dos perfis e acessos aos sistemas, Criptografia de dados em dispositivos | 1 |
| Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos, Revisão periódica dos perfis e acessos aos sistemas, Ferramentas de bloqueios para restrição de acesso e cópia de dados em dispositivos móveis | 2 |
| Monitoramento dos acessos e compartilhamento de senhas, Bloqueio de email pessoal e ferramentas de comunicação não homologadas pela empresa, Níveis/Perfis de acesso de acordo com a classificação da informação (público, privado e confidencial) | 1 |
| Revisão periódica dos perfis e acessos aos sistemas, Bloqueio de email pessoal e ferramentas de comunicação não homologadas pela empresa, Níveis/Perfis de acesso de acordo com a classificação da informação (público, privado e confidencial) | 1 |
| Revisão periódica dos perfis e acessos aos sistemas, Ferramentas de bloqueios para restrição de acesso e cópia de dados em dispositivos móveis, Bloqueio de email pessoal e ferramentas de comunicação não homologadas pela empresa | 1 |
| Revisão periódica dos perfis e acessos aos sistemas, Monitoramento dos acessos e compartilhamento de senhas, Criptografia de dados em dispositivos | 1 |
| Revisão periódica dos perfis e acessos aos sistemas, Monitoramento dos acessos e compartilhamento de senhas, Níveis/Perfis de acesso de acordo com a classificação da informação (público, privado e confidencial) | 2 |
| Revisão periódica e divulgação da política de segurança da informação, Criptografia de dados em dispositivos, Níveis/Perfis de acesso de acordo com a classificação da informação (público, privado e confidencial) | 2 |
| Revisão periódica e divulgação da política de segurança da informação, Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos, Bloqueio de email pessoal e ferramentas de comunicação não homologadas pela empresa | 2 |
| Revisão periódica e divulgação da política de segurança da informação, Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos, Criptografia de dados em dispositivos | 4 |
| Revisão periódica e divulgação da política de segurança da informação, Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos, Ferramentas de bloqueios para restrição de acesso e cópia de dados em dispositivos móveis | 1 |
| Revisão periódica e divulgação da política de segurança da informação, Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos, Monitoramento dos acessos e compartilhamento de senhas | 2 |
| Revisão periódica e divulgação da política de segurança da informação, Implantação de ferramentas de proteção à rede e sistemas contra invasões e | 2 |

| | |
|---|---|
| softwares nocivos, Níveis/Perfis de acesso de acordo com a classificação da informação (público, privado e confidencial) | |
| Revisão periódica e divulgação da política de segurança da informação, Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos, Revisão periódica dos perfis e acessos aos sistemas | 3 |
| Revisão periódica e divulgação da política de segurança da informação, Revisão periódica dos perfis e acessos aos sistemas, Criptografia de dados em dispositivos | 1 |
| Revisão periódica e divulgação da política de segurança da informação, Revisão periódica dos perfis e acessos aos sistemas, Ferramentas de bloqueios para restrição de acesso e cópia de dados em dispositivos móveis | 1 |
| Revisão periódica e divulgação da política de segurança da informação, Revisão periódica dos perfis e acessos aos sistemas, Monitoramento dos acessos e compartilhamento de senhas | 5 |
| Revisão periódica e divulgação da política de segurança da informação, Treinamentos específicos para profissionais de TI e demais colaboradores, Bloqueio de email pessoal e ferramentas de comunicação não homologadas pela empresa | 1 |
| Revisão periódica e divulgação da política de segurança da informação, Treinamentos específicos para profissionais de TI e demais colaboradores, Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos | 4 |
| Revisão periódica e divulgação da política de segurança da informação, Treinamentos específicos para profissionais de TI e demais colaboradores, Níveis/Perfis de acesso de acordo com a classificação da informação (público, privado e confidencial) | 1 |
| Revisão periódica e divulgação da política de segurança da informação, Treinamentos específicos para profissionais de TI e demais colaboradores, Revisão periódica dos perfis e acessos aos sistemas | 3 |
| Treinamentos específicos para profissionais de TI e demais colaboradores, Criptografia de dados em dispositivos, Bloqueio de email pessoal e ferramentas de comunicação não homologadas pela empresa | 1 |
| Treinamentos específicos para profissionais de TI e demais colaboradores, Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos, Ferramentas de bloqueios para restrição de acesso e cópia de dados em dispositivos móveis | 1 |
| Treinamentos específicos para profissionais de TI e demais colaboradores, Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos, Monitoramento dos acessos e compartilhamento de senhas | 1 |
| Treinamentos específicos para profissionais de TI e demais colaboradores, Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos, Níveis/Perfis de acesso de acordo com a classificação da informação (público, privado e confidencial) | 1 |
| Treinamentos específicos para profissionais de TI e demais colaboradores, Implantação de ferramentas de proteção à rede e sistemas contra invasões e softwares nocivos, Revisão periódica dos perfis e acessos aos sistemas | 1 |

| | |
|---|---|
| Treinamentos específicos para profissionais de TI e demais colaboradores, Monitoramento dos acessos e compartilhamento de senhas, Criptografia de dados em dispositivos | 1 |
| Treinamentos específicos para profissionais de TI e demais colaboradores, Monitoramento dos acessos e compartilhamento de senhas, Níveis/Perfis de acesso de acordo com a classificação da informação (público, privado e confidencial) | 1 |
| Treinamentos específicos para profissionais de TI e demais colaboradores, Revisão periódica dos perfis e acessos aos sistemas, Ferramentas de bloqueios para restrição de acesso e cópia de dados em dispositivos móveis | 1 |
| Treinamentos específicos para profissionais de TI e demais colaboradores, Revisão periódica dos perfis e acessos aos sistemas, Monitoramento dos acessos e compartilhamento de senhas | 1 |
| **Total Geral** | **54** |