UNIVERSIDADE FEDERAL DE MINAS GERAIS

FACULDADE DE CIÊNCIAS ECONÔMICAS
CENTRO DE PÓS-GRADUAÇÃO EM CONTABILIDADE E CONTROLADORIA

CURSO DE ESPECIALIZAÇÃO EM AUDITORIA INTERNA E EXTERNA

Geraldo Martins da Costa

Auditoria dos Controles Internos com Ênfase em Segurança da Informação: Um estudo de caso no Centro de Computação da Universidade Federal de Minas Gerais

Belo Horizonte – MG
2016

Geraldo Martins da Costa

Auditoria dos Controles Internos com Ênfase em Segurança da Informação: Um estudo de caso no Centro de Computação da Universidade Federal de Minas Gerais

Trabalho de Conclusão de Curso apresentado ao Centro de Pós-graduação em Contabilidade e Controladoria da Universidade Federal de Minas Gerais, como requisito parcial à obtenção do título de especialização em auditoria interna e externa.

Orientador: Prof. Dr. José Roberto de Souza Francisco

Belo Horizonte – MG
2016

Ata da Sessão Pública de Defesa de Trabalho Final de **GERALDO MARTINS DA COSTA, no. de registro 2015694573**, aluno do Curso de Especialização em Auditoria Externa e Interna da Faculdade de Ciências Econômicas da Universidade Federal de Minas Gerais. Aos dezessete dias do mês de junho do ano de dois mil e dezesseis, às dezessete horas na Faculdade de Ciências Econômicas da Universidade Federal de Minas Gerais, o presidente da Banca Examinadora Prof. José Roberto de Souza Francisco abriu a sessão pública de defesa de trabalho final de Geraldo Martins da Costa, intitulado **"Auditoria dos controles internos com ênfase em segurança da informação: Um estudo de caso no centro de computação da UFMG".** A Banca Examinadora, indicada pelo Colegiado do Curso em maio de 2016 foi constituída pelos professores, *José Roberto de Souza Francisco (orientador) e Carlos Maurício Vieira.* A defesa constou da apresentação de seminário versando sobre o assunto do trabalho, seguido de arguição do candidato pelos membros da banca. Posteriormente, a banca examinadora reuniu-se em sala fechada para o julgamento final, tendo sido considerado APROVADO com nota/conceito 92,1 A o trabalho final de Geraldo Martins da Costa. O resultado foi comunicado ao público presente pelo Prof. José Roberto de Souza Francisco, que, em seguida, declarou encerrada a sessão. Nada mais havendo a tratar, lavrou-se a presente Ata, que será assinada pelos membros da Banca Examinadora. Belo Horizonte, 16 de junho de 2016.**********

Prof. José Roberto de Souza Francisco _____
(Doutor)

Prof. Carlos Maurício Vieira _____
(Mestre)

AGRADECIMENTO

Agradeço primeiramente a Deus por estar sempre presente em minha vida.

Obrigado a minha esposa e filha que estiveram ao meu lado durante todo o curso.

Meu muito obrigado aos professores e aos funcionários da secretaria, os quais tive o privilégio de conhecer durante o curso, pela amizade e profissionalismo.

Um agradecimento especial ao professor José Roberto, meu orientador, por gentilmente ter me guiado no desenvolvimento do trabalho, estando sempre à disposição.

Agradeço também aos colegas do Centro de Computação-CECOM que se dispuseram de alguns minutos de seu tempo para responder o meu questionário.

Agradeço ao Carlos Alfeu, Diretor do CECOM, por ter autorizado a execução do trabalho e, também, a todos os funcionários do Centro de Computação.

Enfim, muito obrigado a todos os colegas de curso pela amizade, um grande abraço a todos.

LISTA DE SIGLAS

CECOM Centro de Computação

CEPCON Centro de Pós-graduação e Pesquisas em Contabilidade e Controladoria

CFC Conselho Federal de Contabilidade

CIA *Certified Internal Auditor*

COBIT® *Control Objectives for Information and related Technology*

ENIAC Calculador e Integrador Numérico Eletrônico

IIABrasil Instituto dos Auditores Internos do Brasil

ISACA *Information Systems Audit and Control Association*

ISO *International Organization for Standardization*

ITIL *Information Technology Infrastructure Library*

SMC *System Management Controller*

TCU Tribunal de Contas da União

TI Tecnologia da Informação

TIC Tecnologia da Informação e Comunicação

LISTA DE FIGURAS

LISTA DE GRÁFICOS

S U M Á R I O

1. CONTEXTUALIZAÇÃO

1.1. Introdução

Com o advento da globalização, as organizações passaram a investir em outros mercados distantes de suas sedes, visando o crescimento do negócio e, muitas vezes, como recurso para fugir de crises internas. Com a abertura dessas filiais, surge a necessidade de adaptar os controles para uma aplicação à distância.

Nesse contexto, os escritórios de contabilidade procuraram se adaptar para atender esses clientes, levando ao surgimento da figura do auditor. O auditor seguia as normas do país de origem das empresas, sem deixar de observar as normas internas aplicadas pela legislação do país em que estava instalada a filial.

Com o passar do tempo e com a evolução tecnológica, as formas de controle tiveram que se adaptar passando de um controle a base de papel para um controle baseado na tecnologia da informação.

A área de tecnologia da informação das organizações passou a ser de extrema importância. Entretanto, muitas vezes, essa importância é negligenciada e, ainda hoje, algumas empresas não enxergam a tecnologia da informação como parte do negócio da empresa o que pode acabar comprometendo os resultados.

O trabalho apresenta o título "Auditoria dos Controles Internos com Ênfase em Segurança da Informação: Um estudo de caso no Centro de Computação da Universidade Federal de Minas Gerais", no qual foi proposta uma avaliação dos mecanismos de controles internos e dos procedimentos de segurança da informação adotados no Centro de Computação (CECOM) da Universidade Federal de Minas Gerais.

A importância do trabalho está no fato de a gestão poder contar com informações de qualidade, no tempo certo e para quem de direito, contribuindo para planejamentos estratégicos e melhorando a eficácia dos processos gerências. Assim, a auditoria interna passa

a ser vista como um aliado precioso na garantia dessa qualidade, ajudando a desenvolver processos seguros e mitigando os riscos, atuando como colaborador.

1.2. Problema de Pesquisa

Com o advento da globalização e a necessidade das empresas em captar recursos financeiros, surge a necessidade de melhorar o sistema de controle, demonstrando maior transparência na aplicação dos recursos e evolução patrimonial das empresas, atendendo a possíveis investidores, fisco e os próprios administradores. Nesse sentido, espera-se que um controle interno efetivo contribua, significativamente, na tomada de decisões pelos gestores e ajude a organização a alcançar seus objetivos.

Nesse contexto, a tecnologia tornou-se uma aliada indispensável e, com o passar do tempo, passou de mero instrumento de trabalho para tornar-se parte do negócio das empresas. Por ser um componente de elevado custo, com exigência de pessoal treinado, podendo levar o comprometimento do bom funcionamento da empresa, a necessidade de avaliação do sistema de controle e de segurança é substancial para verificação e possíveis ajustes nos processos para o bom desempenho de uma empresa.

A auditoria dos controles e da segurança da informação ajudará a evidenciar a eficiência dos processos, podendo contribuir na gestão dos processos operacionais, na mitigação de riscos e, também, no planejamento estratégico do Centro de Computação (CECOM) da Universidade Federal de Minas Gerais. Assim, procurou-se responder à questão: “Qual a aderência dos mecanismos de auditoria de controle interno e de segurança da informação no Centro de Computação da Universidade Federal de Minas Gerais”?

A confirmação da aderência dos controles internos junto aos funcionários do Centro de Computação da UFMG irá contribuir na gestão dos processos operacionais, auxiliando na identificação de possíveis falhas de segurança da informação, na melhora de processos e mitigando possíveis riscos.

1.3. Objetivos

O trabalho visa avaliar objetivamente a gestão de TI da unidade alvo de estudo de caso, no que diz respeito à aderência dos controles internos e à salvaguarda das informações, procurando identificar cada ponto de controle e analisar a segurança dos dados gerados diariamente.

1.4. Objetivo Geral

O objetivo principal deste trabalho é avaliar a aderência dos mecanismos de controles internos e os procedimentos de segurança da informação dentro do Centro de Computação (CECOM) da Universidade Federal de Minas Gerais, levando-se em conta as normas de auditoria interna adotadas no Brasil. Este trabalho tem caráter meramente acadêmico, sem o propósito, a princípio, de aplicações práticas no setor estudado.

Uma instituição com a área de tecnologia alinhada ao seu negócio oferece maior segurança aos seus usuários, maior transparência na preparação do planejamento estratégico e maior eficiência no emprego de recursos.

1.5. Objetivos Específicos

Pretende-se propor a necessidade de se estabelecer processos formais de:

- ✓ Mapeamento dos controles interno e de segurança da informação;
- ✓ Analisar os riscos de TI, visando o gerenciamento da segurança da informação;
- ✓ Apresentar soluções viáveis para aperfeiçoamento do funcionamento do setor de tecnologia da informação.

1.6. Justificativa

Com o passar dos anos as empresas passaram a gerar um volume substancial de informações, deixaram de utilizar exclusivamente o papel em seus controles e passaram a usar computadores. Com o avanço tecnológico as empresas passaram a depender cada vez mais de

uma infraestrutura de tecnologia no seu dia a dia. Entretanto, com essa dependência surgiu também à necessidade de ampliar os controles com o intuito de diminuir os riscos.

Atualmente, as informações estão disponíveis em quase todos os lugares através de computadores cada vez mais rápidos, telefones inteligentes (*smartphones) dentre outros dispositivos moveis (tables*). Essas disponibilidades ao mesmo tempo em que facilitam a vida das pessoas, permitindo que gerenciem suas tarefas, também abrem uma porta para possíveis roubos de confidenciais.

Essa falta de confiança levou a necessidade de maior controle da qualidade da informação, de sua disponibilidade no tempo certo para o usuário solicitante. Portanto, uma organização não pode correr o risco de ter seus negócios comprometidos em virtude de uma informação incorreta ou por acessos maliciosos.

Na figura 1 temos uma noção dos potenciais riscos a que a informação pode estar sujeita dentro de uma organização.

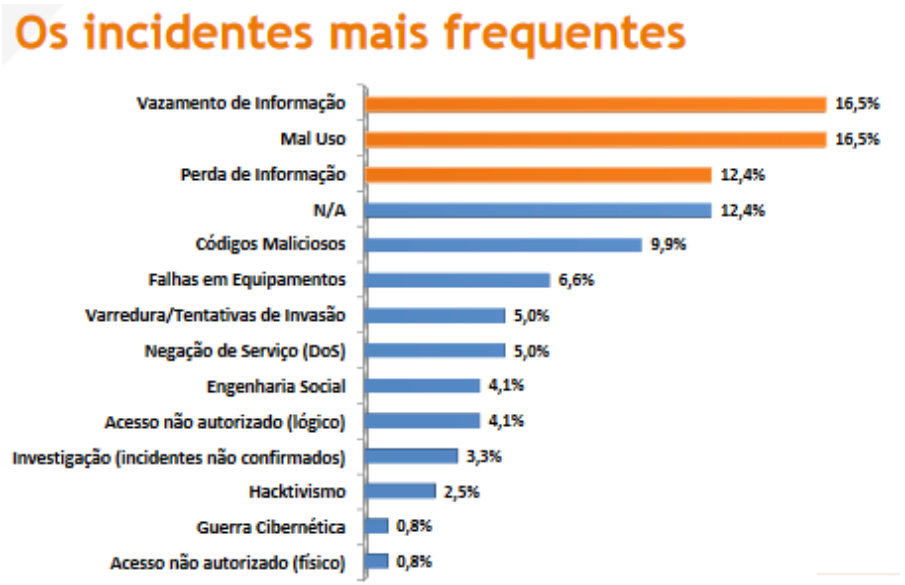


Figura 1. Principais ameaças às informações nas organizações.
Fonte: Pesq. Nacional sobre Segurança da Informação – *DARYUS-Strategic Risk Cosnulting* - (2014).

É nesse contexto que a auditoria se apresenta como aliado importante na obtenção de informações de qualidade, seguras e confiáveis, uma vez que atua na verificação se essa informação é gerada com as qualidades necessárias ao negócio, identificando pontos de falha

e propondo correções. Mas, para que se tenha um bom trabalho de auditoria é vital que as empresas invistam em melhores práticas de gestão do negócio e, nesse caso, em tecnologia da informação e, principalmente, em segurança da informação.

A experiência na área de tecnologia da informação demonstra a necessidade de um maior controle na qualidade das informações disponibilizadas. Muitas vezes as pessoas têm seus dados roubados e utilizados por simples falta de controle de acessos, levando a constrangimentos e prejuízos. Constantemente, ouvimos falar de pessoas que tiveram seu cartão de crédito clonado ou que não conseguiram efetuar um pagamento com o cartão por este estar bloqueado.

Assim, o controle da segurança da informação é crucial para a obtenção de informações seguras, de qualidade e no tempo certo aos usuários. A segurança da informação irá contribuir para a tomada de decisões dos gestores, possibilitando um trabalho de maior qualidade no desenvolvimento de planos estratégicos e contribuindo para a continuidade do negócio e redução de incertezas e para uma boa gestão da instituição. Para isso, a tecnologia da informação apresenta recursos tecnológicos e computacionais que facilitam a geração de informações precisas, contribuindo na redução de incertezas e para uma boa gestão de uma instituição.

Nesse contexto, a auditoria dos controles e da segurança da informação tende a identificar possíveis falhas de processos e de segurança, gerando informações úteis que irão permitir a tomada de decisões pelos gestores, contribuindo no planejamento estratégico, na integração e conhecimento das atividades da empresa, na redução de riscos.

1.7. Estrutura de Pesquisa

A pesquisa está estruturada em cinco partes, sendo:

1. - Contextualização, que traz a introdução, o problema tratado, os objetivos e justificativas;
2. - O referencial teórico em que se baseia a pesquisa, com informações sobre os princípios de auditoria e do sistema de informação, baseados em normas técnicas e literatura específica;

3. - A metodologia utilizada, onde se descrevem os processos utilizados na elaboração do trabalho, com a formulação de hipóteses, e a preparação e coleta de dados através de questionários.
4. - Análise dos dados, onde são apresentados os resultados obtidos com o tratamento dos dados e sua interpretação.
5. – Considerações finais, abordando as limitações e futuras linhas de investigação que o trabalho pode proporcionar.

2. REFERENCIAL TEÓRICO

2.1. Sistemas de Informação

Apresenta um breve histórico da evolução tecnológica e, posteriormente, como a tecnologia da informação passou a ser essencial no dia a dia de qualquer empresa seja ela pública ou privada, transformando a vida das pessoas.

O homem começou a usar auxílios mecânicos para executar contagens e cálculos por volta do ano 5000 a.c. Época notável se deu quando a inovação dos cartões perfurados (*punch cards*) por Herman Hollerith e a subsequente invenção do tubo a vácuo, a evolução para o "diodo", por Ambrose Fleming, em 1904, inovou reduzindo consideravelmente o tamanho dos equipamentos.

Durante a Segunda Guerra Mundial, foi à primeira vez em que um computador foi usado, conhecido por Calculador e Integrador Numérico Eletrônico – ENIAC. O equipamento pesava 30 toneladas e executava 5.000 cálculos por segundo, continha 18.000 tubos a vácuo que dissipavam 150 quilowatts de calor (ONOME, 2014).

No ano de 1950, ocorrem grandes mudanças em todos os ambientes de negócios. Houve uma expansão rápida de empresas que passaram a operar em vários pontos dentro e fora do país onde se encontrava a sede. O aumento da complexidade das empresas passou a exigir equipamentos que agilizassem ou auxiliassem nas operações. Assim, os equipamentos passaram por aprimoramentos para atender cada vez mais as necessidades das empresas, sejam públicas ou privadas (ONOME, 2014).

Com o advento da *internet*, foi criada uma rede mundial com mais de três bilhões de usuários, incluindo governo, organizações e pessoas em todo planeta. A figura 2 demonstra o crescimento dessa rede nos últimos dez anos (ITU, 2015).

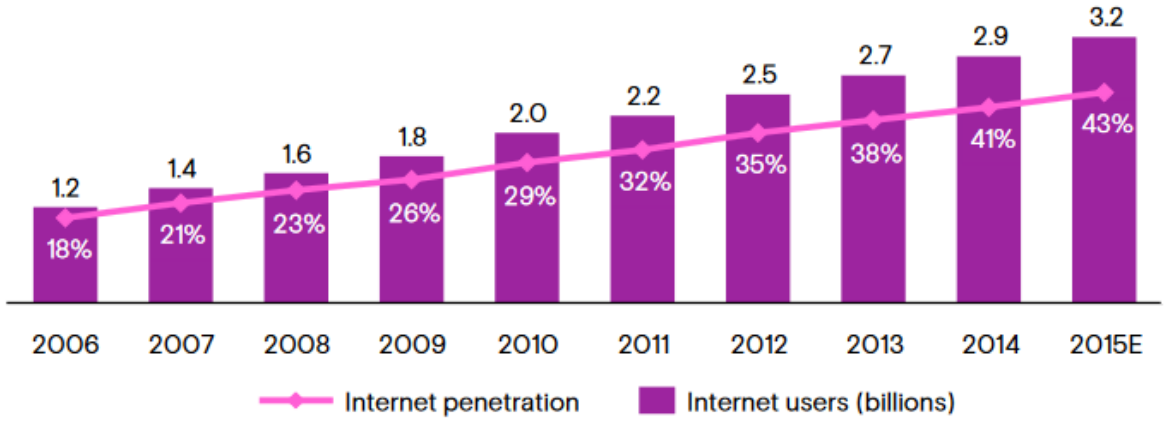


Figura: 2 Crescimento/Penetração do número de usuários da internet no mundo
Fonte: *ITU - International Telecommunication Union* - (2015)

Nesse contexto, com toda a evolução tecnológica, com computadores cada vez mais rápidos, telefones inteligentes (*smartphones*) e outros dispositivos móveis (*tablets*), a informação passou a ser disponibilizada em quase todos os lugares, cabendo às organizações se adaptarem para obter um desempenho melhor dos seus negócios. Entretanto, com essa facilidade de comunicação surgiu, também, a necessidade de controle da qualidade da informação (CUNHA, 2013).

Para Campos, (2007, p.16), "a utilização da informação alinhada à estratégia da organização representa benefícios à imagem da organização, facilitação para inovação, para diferenciação do produto e para a redução do custo e do risco do negócio, minimamente".

Assim, a expressão "sistema da informação" em processamento de dados abrange a captação e entrada de dados, o processamento por meio de aplicativos de computador e as saídas de informações para a devida utilização pelos usuários finais (ARIMA, 1994).

Um sistema de segurança da informação baseia-se em três princípios básicos (CAMPOS, 2007):

1. CONFIDENCIALIDADE, garantindo que somente pessoas explicitamente autorizadas podem ter acesso à informação. A ocorrência de acessos não autorizados à informação, seja por qualquer motivo, é considerado incidente de segurança da informação.

2. INTEGRIDADE, nesse caso é garantido que a informação está completa, sem alterações e, portanto, confiável.

3. DISPONIBILIDADE, este princípio garante que a informação está disponível à pessoa autorizada sempre que necessário.

Sempre que um dos princípios mencionados acima for violado ocorrerá um incidente de segurança da informação, podendo causar interrupções ou prejuízos aos processos do negócio.

Atualmente, verifica-se que as empresas estão cada vez mais dependentes da tecnologia para execução de seus processos. Podemos observar que a tecnologia tornou-se parte fundamental dos negócios de uma empresa, tornando-se meio para que essas possam atingir seus objetivos.

Portanto, a informação é essencial para geração do conhecimento, para a tomada de decisões, e que representa efetivamente o valor do negócio, dentro de cada um de seus processos, permeando toda a organização, apoiando seus processos de várias formas e em diversos meios (CAMPOS, 2007).

Na Administração Pública não é diferente, sendo notável a importância da tecnologia no desenvolvimento de uma boa gestão. Dentro da Universidade Federal de Minas Gerais observa-se uma dependência clara desses recursos tanto pelo corpo docente e discente quanto pelos funcionários técnicos administrativos.

São perceptíveis os problemas ocasionados quando, por algum motivo, os recursos tecnológicos ficam indisponíveis. Portanto, verificou-se qual a importância dos mecanismos de auditoria dos controles internos, utilizando como estudo de caso o Departamento de Computação (CECOM) da Universidade Federal de Minas Gerais.

Sendo assim, torna-se necessário a adoção de princípios, políticas e *frameworks* que atendem à tecnologia da informação. Os princípios, as políticas e os frameworks são dispositivos pelos

quais as decisões relativas à tecnologia da informação são institucionalizadas e, por essa razão, agem como elementos integradores entre o estabelecimento da direção e as atividades de gestão (TCU, 2014).

Os princípios, segundo ABNT (2009), "expressam o comportamento preferido para orientar a tomada de decisão e a sua aplicação deve ser exigida pelos dirigentes". Dessa forma, os funcionários da área de tecnologia da informação de uma organização deverão tomar decisões e executar ações com base nos princípios pré-estabelecidos.

As políticas são diretrizes que direciona a atuação da gestão de tecnologia da informação, representando um conjunto de instruções ou indicações para o alcance de um determinado objetivo, fixando parâmetros básicos de governança de TI para a organização (TCU, 2014).

No que diz respeito aos frameworks, esse devem promover estrutura, orientação e ferramentas que possibilitem a governança e o gerenciamento apropriados da tecnologia da informação dentro de uma organização. Atualmente, existem frameworks genéricos, ou seja, guias de melhores práticas, que podem apoiar uma organização na implementação de processos e práticas de governança de tecnologia da informação (TCU, 2014).

A auditoria operacional consiste em revisões metódicas de programas, organizações, atividades ou segmentos operacionais dos setores público e privado, com a finalidade de avaliar e comunicar se os recursos da organização estão sendo usados eficientemente e se estão sendo alcançados os objetivos operacionais (CREPALDI, 2013).

Assim, uma avaliação dos desempenhos dos controles internos, em confronto com as normas de auditoria adotadas no Brasil e com os *frameworks* de melhores práticas no ambiente de tecnologia da informação permitirá melhor visualização dos processos operacionais e uma possível mitigação dos riscos.

2.2. AUDITORIA

O surgimento da auditoria se deu devido à necessidade de confirmação dos registros contábeis que visava taxação de imposto sobre a renda de grandes empresas compostas por capitais de

muitas pessoas. O primeiro país a executar auditoria foi à Inglaterra que dominava a navegação e comércio mundial o que levou ao surgimento de grandes companhias de comércio e sendo precursora na instituição do imposto de renda sobre os lucros dessas empresas (CREPALDI, 2013).

Com a globalização e, consequentemente, a exportação de capitais através da abertura de filiais de grandes empresas em diversos países em desenvolvimento, as matrizes passaram a enviar a figura do auditor para verificação da correta aplicação dos capitais, aplicação dos lucros e retorno financeiro. Dessa forma, empresas de contabilidade passaram a atender esse mercado, abrindo filiais em outros países. Assim, houve o desenvolvimento da profissão de auditor independente com as características de contador. (CREPALDI, 2013).

Auditoria interna governamental, segundo Silva (2015, p.01), "...é o ápice da pirâmide do sistema de controle interno", uma vez que o controle interno é subordinado ao titular do órgão ou entidade por ser parte das atividades administrativas. Por outro lado, a auditoria interna governamental deve fiscalizar e avaliar o grau de confiabilidade, controlar a eficiência e a eficácia dos controles internos.

2.2.1. Auditoria Externa

A todo tempo, administradores, investidores e o fisco gostariam de saber se o capital aplicado em uma empresa, os recursos gerados e aplicados, o resultado operacional e a variação patrimonial correspondem ao que está sendo apresentado, se foi utilizado de forma eficiente de acordo com as normas de contabilidade adotadas no Brasil.

Nesse contexto, a auditoria independente mostra sua importância, uma vez que atua na avaliação da evolução patrimonial de uma empresa de forma autônoma, utilizando-se de normas e padrões de natureza técnica e ética evidentemente determinada. Portanto, a auditoria é um elemento relevante no sistema de informações, medição de desempenho e prestação de contas da administração (CREPALDI, 2013).

De acordo com a *Academy of Management Review*, o auditor externo independente deve possuir total independência na execução de seu trabalho, o que permitirá a apresentação de

um trabalho sem viés. Ao concluir seu trabalho, o auditor deve confirmar que os relatórios financeiros de seus clientes foram preparados de acordo com as exigências das normas técnicas brasileiras ou emitir um relatório substanciado com as divergências encontradas durante o processo de auditoria. Portanto, o auditor externo deve ser independente e imparcial, devendo obediência final para os credores e acionistas da empresa, bem como ao público investidor (MOORE et al., 2006).

A resolução do CFC - NBC PA 290 R1, 2014 -, traz a condição de independência como fator primordial no exercício da atividade de auditoria externa. Como segue:

> O cumprimento do princípio fundamental de objetividade requer ser independente dos clientes de asseguração. No caso em que o trabalho de asseguração é de interesse público e, portanto, requerido por esta Norma que os membros das equipes de asseguração e as firmas sejam independentes dos clientes de asseguração, e que sejam avaliadas quaisquer ameaças que a firma acredita que são criadas por interesses e relacionamentos de uma firma em rede. Além disso, quando a equipe de asseguração sabe ou acredita que uma relação ou circunstância envolvendo outra entidade relacionada do cliente de asseguração é relevante para a avaliação da independência da firma em relação ao cliente, a equipe de asseguração deve incluir essa entidade relacionada na identificação e avaliação de ameaças à independência e na aplicação das salvaguardas adequadas. (CFC, NBC PA 290 R1, 2014).

Na auditoria externa a independência deve ser tanto de pensamento quanto de aparência (CFC, NBC PA 290 R1, 2014).

A independência de pensamento é aquela em que o auditor tem liberdade total de expressar uma opinião sem ser afetado por influências que possam comprometer o seu julgamento profissional, permitindo que ele possa agir com integridade, objetividade e ceticismo profissional.

A aparência de independência é aquela em que o auditor procura evitar fatos e circunstâncias que possam ser significativos. Evitando que um terceiro com experiência, ou seja, com conhecimento e bom senso provavelmente concluiria, ponderando todos os fatos e circunstâncias específicas, que a integridade, a objetividade ou o ceticismo profissional da firma ou de membro da equipe de asseguração sejam comprometidos (CFC, NBC PA 290 R1, 2014).

2.2.2. Auditoria Interna

Com a expansão dos negócios e a necessidade cada vez maior de transparência na evolução patrimonial da empresa, visando atender normas específicas ou pelo simples fato de alguns proprietários não poderem supervisionar pessoalmente todas as atividades da empresa, tornou-se cada vez mais necessário a adoção de normas e procedimentos para regular os trabalhos.

Entretanto, de nada valia a implementação de normas e procedimentos internos se não houvesse um acompanhamento periódico para verificação se estavam sendo seguidas por todos empregados da empresa.

Com a globalização e a necessidade crescente de melhoramento dos resultados, as empresas estão buscando cada vez mais a identificação de oportunidades e estratégias para minimizar riscos aos seus negócios, aumentar a eficiência em suas operações e um nível adequado de controle e retorno aos seus investimentos (CREPALDI, 2013).

Segundo Morais (2008), em "*A importância da auditoria interna para a gestão: Caso das empresas portuguesas*" houve uma mudança de paradigma da visão da auditoria, que passou a ser vista não mais como uma tradicional função de controle financeiro/contabilístico, mas centrando-se na identificação de todos os riscos inerentes às diversas atividades da organização, procurando atingir objetivos de forma mais eficiente. A auditoria interna passou a ser um instrumento de apoio à gestão, ajudando a organização a alcançar seus objetivos servindo de assessor e consultor na identificação de riscos e propondo possíveis estratégias de ação (MORAIS, 2008).

Assim, surgiu a figura do auditor interno como uma ramificação da profissão do auditor externo e, consequentemente, do contador. A esses profissionais passou-se a exigir, além de experiências, uma vasta gama de conhecimentos em áreas como: Governança, Gerenciamento de Riscos, Estrutura Organizacional e Processo de Negócio, Comunicação, Liderança, Continuidade de TI do negócio, além de outros específicos ao tipo de negócio da organização em que trabalha (INSTITUTO DOS AUDITORES INTERNOS DO BRASIL, 2016).

Portanto, o auditor interno é um empregado da empresa e, dentro da organização, não deve estar subordinado àqueles cujos trabalhos irá examinar.

A Figura 3 apresenta um fluxograma em que é possível localizar o setor de auditoria interna dentro de uma empresa.

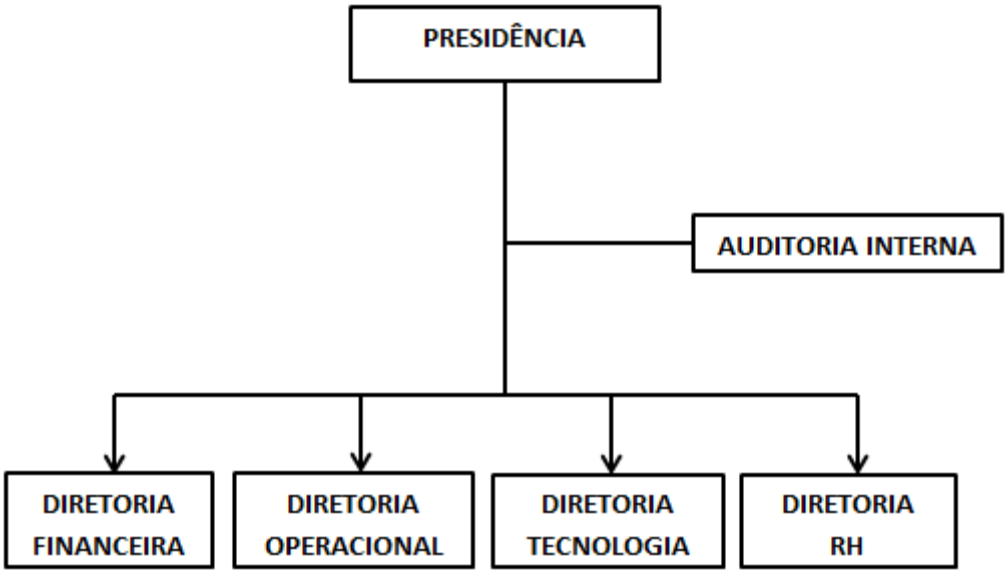


Figura 3 Localização do setor de auditoria interna dentro de uma empresa.
Fonte: ALMEIDA - (2012).

No entanto, essa posição estratégica muitas vezes acaba criando um pensamento deturpado do serviço do auditor interno, sendo necessária a desmistificação entre os funcionários da organização onde há uma equipe de auditoria interna. Procura-se deixar claro que a participação da equipe é no auxílio de desempenho das tarefas dentro da organização, visando sempre maior eficiência, e não apenas para apontar erros, e sim para tornar-se parceiro na busca de um melhor desempenho (MORAIS, 2008).

Dentro do processo de auditoria de gestão, podemos mencionar as principais características dentro de uma empresa:

- A Auditoria Interna participando de todos os processos empresariais - nesse caso, o responsável pela auditoria interna estaria participando de comitê de negócios, grupos de planejamento estratégico, reuniões da área de qualidade, procurando uma total

integração e conhecimento detalhado das atividades da empresa, principalmente daquelas vinculadas às tomadas de decisões.

- A "atividade de auditoria" deve buscar uma participação inovadora, criando ciclos de estudos internos na empresa sobre a "atividade de auditoria". Assim, a busca pelo conhecimento seria disseminada para todos os administradores da empresa, visando antecipar processos e procurando uma melhor forma de trabalho.

- A auditoria de gestão deve ser voltada a padrões de excelência, procurando visualizar não somente padrões monetários, mas avaliando todo o negócio empresarial. A auditoria de gestão visa à qualidade, focando no planejamento, execução e controle dos processos, mitigando riscos e procurando maior eficiência e eficácia.

2.2.3. Auditoria Governamental

A Auditoria Governamental é voltada ao atendimento de empresas da Administração Pública direta e indireta, abrangendo tanto o âmbito da auditoria externa como a auditoria interna e envolvendo diretamente o patrimônio e, também, o interesse público. Esse tipo de auditoria apresenta duas vertentes (PETER e MACHADO, 2007).

- Auditoria Tributária/fiscal: A qual é realizada pelo governo para controlar o patrimônio privado com o intuito de identificar e normalizar as atitudes contributivas, especialmente nas áreas de impostos, taxas e contribuições.

- Auditoria de Gestão Pública: Nesse caso é efetuada pelo estado, visando a autotutela e o controle de sua gestão. Devem ser observados além dos princípios de auditoria, os princípios da: moralidade, publicidade, impessoalidade, economicidade e eficiência (PETER e MACHADO, 2007).

A gestão pública deve prestar conta em relação à responsabilidade delegada, ou seja, quem tem por responsabilidade o dever de prestar conta de seu trabalho e como ele está sendo desenvolvido em relação à responsabilidade delegada. Esse processo é conhecido como *accountability* (PETER e MACHADO, 2007).

Segundo Silva (2014), quando um sistema de controle interno é inadequado, pode resultar na possibilidade de diversas irregularidades que podem permitir a ocorrência de anomalias, fraudes e atos de imprudência contra a empresa.

De acordo com Machado e Peter (2007), os tipos de Auditoria Governamental são:

- Auditoria de Gestão: tem como objetivo emitir opinião com vistas a certificar a regularidade das contas, verificar a execução de contratos, convênios, acordos ou ajustes, a probidade na aplicação dos dinheiros e na guarda ou administração de valores e outros bens da União ou a ela confiados, compreendendo, entre outros, os seguintes aspectos: exame das peças que instruem os processos de tomada ou prestação de contas; exame da documentação comprobatória dos atos e fatos administrativos; verificação da existência física de bens e outros valores; verificação da eficiência dos sistemas de controles administrativo e contábil; verificação do cumprimento da legislação pertinente.

- Auditoria de Programas: O objetivo é acompanhar, examinar e avaliar a execução de programas e projetos governamentais específicos, bem como a aplicação de recursos descentralizados, compreendendo, entre outros, os seguintes aspectos: análise da realização físico-financeira em face dos objetivos e metas estabelecidos; análises dos demonstrativos e dos relatórios de acompanhamento produzidos com vistas à avaliação dos resultados alcançados e à eficiência gerencial; verificação da documentação instrutiva e comprobatória, quanto à propriedade dos gastos realizados; análise da educação dos instrumentos de gestão – contratos, convênios, acordos, ajuste e outros congêneres – para consecução dos planos, programas, projetos e atividades desenvolvidas pelo gestor, inclusive quanto à legalidade e diretrizes estabelecidas.

- Auditoria Operacional: Irá atuar na avaliação das ações gerenciais e nos procedimentos relacionados ao processo operacional, ou parte dele, dos órgãos/entidade da Administração Pública, programas de governo, atividades, ou segmentos destes. Esse processo tem o objetivo de emissão de opinião sobre a gestão, avaliando a eficiência dos seus resultados em relação aos recursos materiais, humanos e tecnológicos disponíveis, bem como a economicidade e eficiência dos controles internos existentes para gestão dos recursos públicos.

- Auditoria Contábil: É utilizada no exame dos registros e documentos e na coleta de informações e confirmações, mediante procedimentos específicos, pertinentes ao controle do patrimônio de um órgão ou entidade. O objetivo é obter elementos comprobatórios suficientes que permitam opinar se os registros contábeis foram efetuados de acordo com os princípios fundamentais de contabilidade e se as demonstrações deles originárias refletem, adequadamente, a situação econômico-financeira, do patrimônio, os resultados do período administrativo examinado e as demais situações nelas demonstradas.

- Auditoria de Sistemas: Objetiva assegurar a adequação, privacidade dos dados e informações oriundas dos sistemas eletrônicos de processamento, observando as diretrizes estabelecidas e a legislação específica.

- Auditoria Especial: Tem como objetivo o exame de fatos ou situações consideradas relevantes, de natureza incomum ou extraordinária, sendo realizadas para atender a determinação do Presidente da República, de Ministros de Estado ou por solicitação de outras autoridades.

- Auditoria de Qualidade: Nesse caso, o objetivo é permitir a formação de uma opinião mais concreta sobre o desempenho gerencial dos administradores públicos, servindo como estímulo à adoção de uma cultura gerencial voltada para o atingimento de resultados dentro dos princípios da qualidade, identificando os pontos fortes e fracos da organização.

Por fim, para que o controle interno funcione corretamente, não basta apenas planejamento efetivo da empresa e da eficiência dos procedimentos e normas definidas, é necessário pessoal competente e envolvido para que sejam levados adiante os propósitos da empresa de forma adequada.

De modo geral, um bom sistema de controle interno deve prevenir e detectar todas as possíveis irregularidades.

2.2.4. Auditoria na Tecnologia de Informação

A crescente instabilidade e a forte concorrência com tecnologias sofisticadas e com a vida útil cada vez menor dos equipamentos, permitindo acesso à informação de modo generalizado,

leva ao crescimento exponencial dos riscos nas organizações. Nesse contexto surge, portanto, a necessidade de um controle que privilegie o desempenho e a competição, visando principalmente a utilização eficiente dos recursos e a eficácia das organizações, em contraste a um controle apenas financeiro adotado no passado (MORAIS, 2008).

Tendo a área de tecnologia como parte estratégica de uma empresa, seja ela pública ou privada, permitindo que a mesma avance ou se mantenha estagnada, tornou-se necessário um maior controle dos recursos de tecnologia da informação.

Em auditoria de tecnologia da informação, procura-se validar a confiabilidade do sistema de informação, gerenciamento de riscos e dos controles internos da área de tecnologia da informação. O auditor procura revisar e avaliar se os controles internos do sistema da informação são efetivos.

Para verificar a fidelidade da informação em relação ao dado, o auditor irá identificar se as saídas das informações de um determinado sistema computadorizado estão corretas, e se são provenientes dos dados de entrada. O controle interno avaliará todos os procedimentos operacionais, a segurança física e lógica (ARIMA, 1994).

Portanto, uma validação dos controles internos irá fornecer maior segurança na tomada de decisões por parte dos gestores de tecnologia, contribuindo na elaboração de planos estratégicos na área de tecnologia, demonstrando maior profissionalismo e controle do negócio.

O EX-MINISTRO do Tribunal de Contas da União, Augusto Sherman, deixa clara essa mudança de paradigma dentro da administração pública ao dizer:

> A tecnologia da informação é o coração da administração pública, podendo fazê-la parar ou avançar. (TRIBUNAL DE CONTAS DA UNIÃO, 2012).

Além do surgimento de diversos tipos de computadores, de pequenos e grandes portes, existem também, disponíveis no mercado, diversos softwares aplicativos atendendo às mais variadas necessidades. Esses recursos, conectados a rede local e/ou a redes de larga escala via telecomunicação, saíram do ambiente do escritório e residencial e passaram a ser

disponibilizados nos mais diversos pontos tais como: universidades, aeroportos, *shopping centers* e até mesmo em vias públicas, deixando sempre conectados os usuários, tornando-se uma extensão do ambiente de trabalho.

2.2.5. Controle Interno na Tecnologia da Informação

O avanço tecnológico nas últimas décadas levou a uma mudança no paradigma de como a área de tecnologia da informação era vista pelos administradores das empresas. A princípio, essa área era tratada como custo dentro de uma empresa e, atualmente, as empresas passaram a enxergá-la como investimento. Essa mudança ocorreu devido à dependência cada vez maior das empresas por recursos tecnológicos os quais passaram a fazer parte dos negócios, sendo essenciais para o bom desempenho de uma empresa.

Como não poderia deixar de ser, essa disponibilidade trouxe também um aumento da vulnerabilidade dos computadores e alguns casos comuns de fraudes, uma vez que negócios e consultas à base de dados podem ser efetuados de qualquer ponto remoto.

Assim, visando maior controle dos processos, tornou-se necessário o desenvolvimento de métodos e medidas para garantir a exatidão, veracidade e integridade dos dados processados, promovendo a eficiência operacional. Nesse contexto, o controle interno dos processos e a segurança tornaram-se peças chaves para a mitigação dos riscos.

A segurança em sistemas computadorizados muda de tempos em tempos, dependendo da evolução da tecnologia do computador, da necessidade de proteção física dos dados e da prevenção de ocorrências de incidentes fatais, que podem causar danos irreparáveis em documentos e programas (ONOME, 2014).

Além dos controles de segurança que reduzem as pequenas ameaças e frequentes acontecimentos operacionais, em detrimento do funcionamento normal do sistema, são previstos também o desenvolvimento de facilidade de *backup* com planos de contingenciamento e recuperação em caso de desastres.

Os controles de segurança de sistema apresentam algumas propriedades (ONOME, 2014):

- SIGILO: Fornecer privacidade ou situação estritamente confidencial dos dados, visando garantir que a informação esteja disponível apenas ao proprietário da mesma.
- INTEGRIDADE: Fornecer um requisito de informação completa, correta, válida e confiável.
- DISPONIBILIDADE: Os dados devem estar disponíveis a quem quer que seja autorizado a usá-los.
- CONTABILIDADE: Registro de todas as operações executadas, permitindo auditoria.
- AUDITORIABILIDADE: Os sistemas de segurança devem ser auditados, permitindo o acompanhamento pela gerência e facilitando a efetivação dos controles.

Nas ultimas décadas, houve significativa evolução no processo de gestão da tecnologia da informação (TI) dentro das empresas, e essa evolução demonstra que a TI passa de um mero provedor de serviços para um novo parceiro estratégico nos negócios, possibilitando novas oportunidades e agregando valor aos negócios. O ambiente atual de Tecnologia da Informação e Comunicação (TIC) é visto como um parceiro inseparável do negócio e como um investimento a ser gerenciado.

Na Figura 4, é mostrada a evolução temporal do processo de TIC.

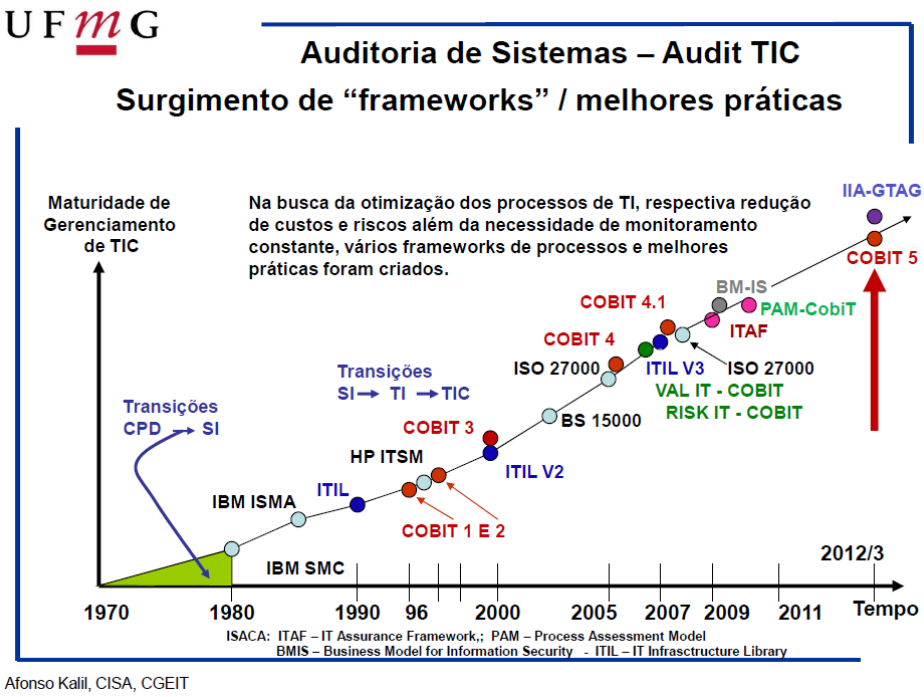


Figura 4. Evolução temporal do processo de TIC.
Fonte: Kalil (2015).

Os processos operacionais de TIC foram definidos em *frameworks* guias de melhores práticas da ISACA (*Information Systems Audit and Control Association*), ISO (*International Organization for Standardization)*, no COBIT (*Control Objectives for Information and related Technology*), no ITIL (*Information Technology Infrastructure Library*) e no SMC (*System Management Control*), e têm como objetivo fornecer serviços aos usuários dentro dos compromissos assumidos e assegurar a gestão correta dos recursos do ambiente tecnológico.

2.2.5.1. Normatizações aplicadas no Controle na Administração Pública

Com a TIC assumindo uma importância estratégica dentro das empresas, uso crescente na manipulação e armazenamento de dados, com os valores gastos nas aquisições relacionadas à tecnologia da informação e os recursos geridos por este meio sendo cada vez maior, tornou-se necessário o aprimoramento de leis já existentes e definições de como obter um ambiente tecnológico que esteja sempre disponível, íntegro e seguro.

A seguir, são descritos dispositivos legais que vieram amparar essa evolução e a necessidade de um maior controle interno dentro das organizações.

A Lei nº 4.320/64

A Lei nº 4.320/64 preconiza em seu art. 75:

> O controle da execução orçamentária compreenderá:
> I – a legalidade dos atos de que resultem a arrecadação da receita ou a realização da despesa, o nascimento ou a extinção de direitos e obrigações;
> II – a fidelidade funcional dos agentes da administração responsáveis por bens e valores públicos;
> III – o cumprimento do programa de trabalho expresso em termos monetários e em termos de realização de obras e prestação de serviços.

Constata-se, pelo texto da lei, a grande preocupação com o aspecto legal e com a formalidade e abrangência do controle, compreendendo a execução orçamentária-financeira e o cumprimento das propostas de melhorias ao bem-estar da sociedade, traduzidas nos programas de trabalho (PETER e a MACHADO, 2007).

A Lei nº 4320/64 nos artigos 76 a 82, ao determinar que o Poder Executivo exerça todas as formas definidas no art. 75, deixa claro que deve ser feito sem prejuízo das atribuições dos órgãos de controle, devendo ser prévia, concomitante e subsequente, deixando clara a existência dos controles internos e externos.

A Constituição Federal de 1988 reforça a necessidade do controle e define em seu art. 70 (BRASIL, 1988):

> A Fiscalização Contábil, financeira, orçamentária, operacional e patrimonial da União e das Entidades da Administração Direta e Indireta, quanto à legalidade, economicidade, aplicação das subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada poder.
>
> Parágrafo único: Prestará contas qualquer pessoa física ou entidade pública que utilize, arrecade, guarde, gerencie ou administre dinheiro, bens e valores públicos ou pelos quais a União responda, ou que, em nome desta, assuma obrigações de natureza pecuniária.

Acórdão 2.094/2004-TCU-Plenário

> 9.3. determinar (...) que, no seu âmbito de atuação, exerça o controle efetivo dos contratos de terceirização de serviços de informática e de desenvolvimento de sistemas fazendo constar nas tomadas e prestações de contas das entidades que realizam tais contratações os exames realizados e os resultados obtidos;

O acórdão procura salientar a necessidade da administração em exercer o controle efetivo de contratos de serviços, bem como demonstrar esse controle em sua prestação de conta, evidenciando os pontos de controle e os resultados obtidos.

Acórdão 1603/2008-TCU-Plenário

> 9.3. recomendar à (...) que realize regularmente Auditorias de TI e/ou promova ações para estimular a realização dessas Auditorias nos órgãos/entidades da Administração Pública Federal;

Partindo do pressuposto da autotutela, o acórdão vem recomendar auditorias de TI periodicamente e, caso necessário, a promoção de ações para que visem o estimulo à realização de auditorias de TI na Administração Pública Federal.

Acórdão 381/2011-Plenário

> 9.1.11. em face da Resolução CNJ 90/2009, art. 10, promova ações para que a auditoria interna apoie a avaliação da TI, observando as orientações contidas na Norma Técnica – ITGI – Cobit 4.1, ME2 – Monitorar e avaliar os controles internos, conforme tratado no achado 18 – Auditoria interna não apoia avaliação da TI – do relatório de fiscalização;

O acórdão citado chama atenção para a necessidade da área de auditoria interna promover a avaliação da tecnologia da informação, levando-se em consideração a norma técnica tratada no Cobit 4.1, ME2 – Monitorar e avaliar. Essa norma descreve a necessidade de se estabelecer um programa de controle interno efetivo para a TI requerendo um processo de monitoração bem definido.

Esse controle interno tem como objetivo principal o monitoramento e fornecer segurança relacionada à eficiência e eficácia operacional, além de atentar para a conformidade com *compliance*, ou seja, a utilização de normas e regras adotadas no Brasil.

Acórdão 757/2011-Plenário

> 9.1.9. estabeleça processo de avaliação da gestão de TI, à semelhança do Cobit 4.1, itens ME1.4 – Avaliação de desempenho, ME1.5 – Relatórios gerenciais, ME1.6 – Ações corretivas e ME2 – Monitorar e avaliar os controles internos;
> 9.1.10. promova ações para que a auditoria interna apoie a avaliação da TI, à semelhança das orientações do Cobit 4.1, ME2 – Monitorar e avaliar os controles internos;

O acórdão 757/2011 não destoa dos mencionados anteriormente e discorre sobre a necessidade de se estabelecer processos de controle e avaliação da área de tecnologia da informação, utilizando como base um dos domínios do Cobit 4.1 em que trata da questão de monitoramento e avaliação do desempenho de TI. Nesse contexto, o administrador procura assegurar que os investimentos em TI estejam alinhados com as estratégias e com os objetivos empresarias.

Portanto, sem a intenção de exaurir o assunto, está absolutamente claro que dentro da administração pública federal deve ser adotado um maior controle da área de tecnologia da informação em virtude de sua real importância.

2.2.5.2. Ambiente de Controle

São espaços físicos onde acontecem os processos, o local de trabalho das pessoas e no local onde está o CPD, onde estão instalados os equipamentos de processamento (Servidores/Mainframe). Nesse local encontram-se os demais ativos de informação, podendo representar risco para o negócio da organização (CAMPOS, 2007).

As vulnerabilidades podem ser de diversas formas e, entre elas, temos invasões de sistemas desprotegidos por pessoas maliciosas, via servidor de e-mail, dispositivos móveis, dentre outros. Na figura 5 têm-se uma representação simplificada do fluxo das informações.

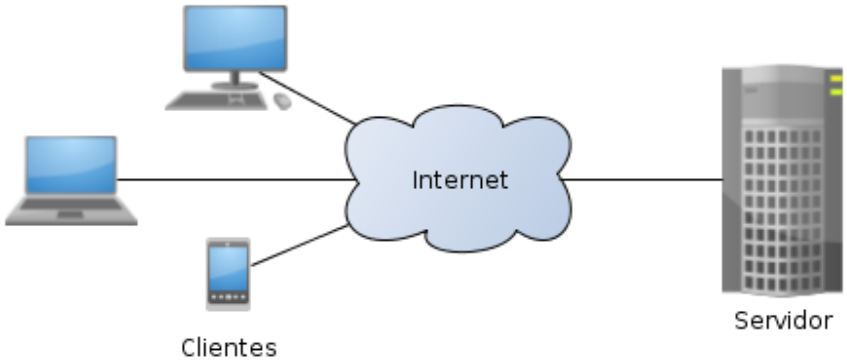


Figura 05. Exemplo de ativos tecnológicos.
Fonte: Wikipédia - (2016).

2.2.5.3. Avaliação de Risco

A crescente utilização de equipamentos tecnológicos e a facilidade de conexão aos negócios, aliado ao aumento constante da dependência dos recursos de sistemas da informação nas organizações, fortalece a importância da segurança da informação como um parceiro na governança coorporativa.

As ameaças à informação vão desde ataques de hackers, fraudes eletrônicas, espionagem e vandalismo; a falhas elétricas, invasões físicas, perdas de hardwares e softwares, entre outras, exigindo uma administração atenta aos possíveis riscos de modo a mitigar ou mesmo eliminá-los, garantindo a continuidade dos negócios (Alexandria).

Baseado no princípio de Pareto, em que diz que 20% das causas geram 80% das consequências, não seria necessário tratar 100% dos riscos, mas um percentual que responda pela diminuição de riscos desejada pela organização. Na figura 6 é mostrado um esquema para tratamento de risco (CAMPOS, 2007).

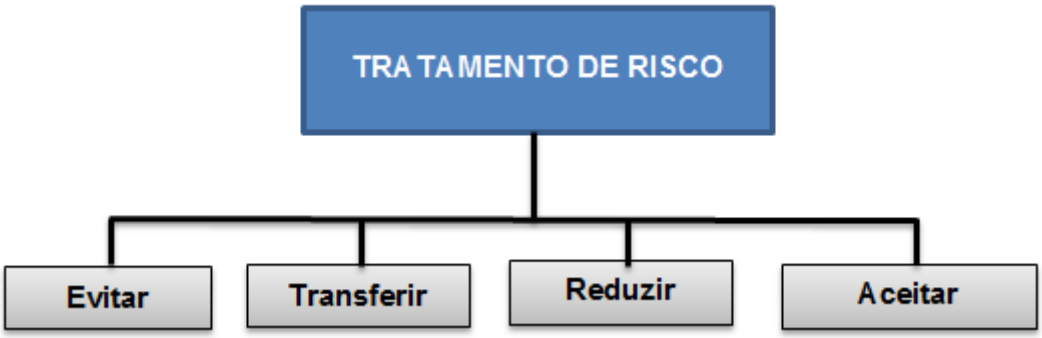


Figura 6. Operações para o tratamento de risco.
Fonte: Campos - (2007).

Portando, avaliação de risco é comparar a estimativa de risco contra os critérios de risco, determinando dessa forma os níveis de riscos de incidentes de segurança da informação, calculando o impacto e a probabilidade de ocorrência. Na figura 7, é ilustrada uma visualização da relação entre impacto, probabilidade e risco (CAMPOS, 2007).

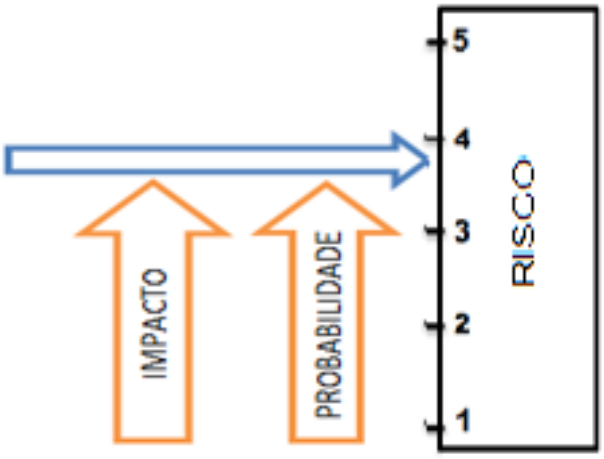


Figura 7. Relação entre Impacto, Probabilidade e Risco.
Fonte: Campos - (2007).

Assim, quanto maior o impacto e a probabilidade, maior será o risco. O impacto é a relevância do ativo, relevância do serviço e relevância do processo, enquanto a probabilidade é o produto do grau da ameaça e do grau da vulnerabilidade. Assim, temos:

Risco = I * P, ou seja:
Risco = ((Ga/5).(Gv/5)).((Ra/5).(Rs/5).(Rp/5)), onde:

- ✓ I: Impacto
- ✓ P: Probabilidade
- ✓ Ga: Grau da ameaça.
- ✓ Gv: Grau da vulnerabilidade.
- ✓ Ra: Relevância do ativo.
- ✓ Rs: Relevância do serviço.
- ✓ Rp: Relevância do processo.

Aplicando essa equação com seus devidos parâmetros, pode-se obter uma análise do risco.

2.2.5.4. Atividade de Controle

Sabemos que incidentes de segurança da informação são passiveis de ocorrer. No entanto, a questão é: Como evitar que ocorra um incidente de segurança?

Como vimos anteriormente, são dois fatores que constituem a probabilidade de que ocorra o incidente, sendo o grau de ameaça e o grau da vulnerabilidade. As ameaças são agentes externos sobre as quais, normalmente, não temos o controle. Por outro lado, a vulnerabilidade está nos ativos da organização que geralmente estão dentro de seu raio de ação. Partindo desse contexto, uma organização deve voltar seus esforços para diminuição das vulnerabilidades dos ativos de informação (CAMPOS, 2007).

Portanto, um controle é qualquer mecanismo voltado para reduzir as fraquezas ou a vulnerabilidade de um ativo, seja ele uma tecnologia, uma pessoa, um processo ou um ambiente de processamento de dados. Pode ser restrição de acesso na sala de servidores, senhas de acesso, política de segurança da informação, firewall, antivírus, dentre outros.

2.2.5.5. Informações e Comunicações

A informação é considerada um insumo fundamental dentro de qualquer ambiente, sob a pena de que sem sua presença todo o processo possa ser comprometido. A informação é necessária para viabilizar a tomada de decisões ou elaborar um planejamento sem o qual não há como viabilizar as demais etapas. A informação representa os dados trabalhados e processados, em que se pretende atingir determinado propósito (FERNANDES, 2011).

Comunicação é o processo de transmitir uma informação entre os agentes envolvidos. Comunicar de forma adequada significa perceber que o receptor da informação entendeu a mensagem com a mesma fidelidade que o emissor o fez quando essa foi gerada. Nesse contexto, a disciplina de Sistemas de Informação por apresentar uma necessidade de controle das informações entre as organizações e pessoas, procura garantir a qualidade, o tempo certo e para o receptor correto (FERNANDES, 2011).

2.2.5.6. Monitoramento

As condições de uma organização estão em constante movimento, por esse motivo não se pode realizar a identificação e análise de risco apenas uma vez. Faz-se necessário um acompanhamento constante, um monitoramento constante dos riscos e uma análise adicional sempre que forem encontrados problemas que possam comprometer o ambiente da empresa (KIM, 2012).

Os riscos devem ser reavaliados sempre que ocorrer um dos eventos abaixo (KIM, 2012):

- Verificação de evidência de que uma ameaça foi observada ou em via de ocorrer.
- Aprovação, pela organização, de uma solicitação de seu plano de resposta a riscos.
- Ocorrência de mudanças que possam levar a riscos de recursos.
- Aplicação de ações corretivas ou preventivas no ambiente.

Portanto, a empresa deverá garantir que o plano de gerenciamento de riscos corresponda ao ambiente atual, caso contrário, deverá ser reavaliado.

3. Metodologia da Pesquisa

Conforme Marconi e Lakatos (2003), "todas as ciências caracterizam-se pela utilização de métodos científicos; em contrapartida, nem todos os ramos de estudo que empregam estes métodos são ciências. Dessas afirmações pode-se concluir que a utilização de métodos científicos não é da alçada exclusiva da ciência, mas não há ciência sem o emprego de métodos científicos. Assim, o método é o conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo - conhecimentos válidos e verdadeiros -, traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista" (MARCONI E LAKATOS, 2003).

Assim, a pesquisa é um método de procedimento formal, com método de pensamento reflexivo, que requer um tratamento científico e se constitui no caminho para conhecer a realidade ou para descobrir verdades parciais (MARCONI e LAKATOS, 2003).

De acordo com o objetivo do trabalho, baseando-se na revisão bibliográfica, foi possível identificar algumas questões que evidenciam a importância da auditoria interna ao desenvolvimento de uma gestão eficaz dentro de um ambiente de tecnologia da informação, contribuindo para um modelo de gestão eficaz (MORAIS, 2008).

No desenvolvimento da pesquisa foi utilizado o método descritivo, onde foi feito um estudo de caso tendo como base o universo dos funcionários da área de tecnologia da informação do Centro de Computação (CECOM) da Universidade Federal de Minas Gerais, aplicando-se questionários aos funcionários para levantamento dos dados. O estudo de caso é uma técnica de pesquisa que consiste em analisar com maior detalhe uma unidade especifica com vistas em conhecer essa unidade confrontando com uma base teórica consistente (QUERINO et al., 2015).

Em uma população de, aproximadamente 115 funcionários foi aplicado um questionário via *internet* contemplando três áreas específicas, sendo:

1. O Controle de Processos e força de trabalho, onde se procurou avaliar a preocupação com as normas e regras da área da tecnologia da informação.

2. A Segurança Física, com avaliação da infraestrura do ambiente de tecnologia e, também, o conhecimento dos funcionários em relação à gestão dos riscos.
3. Segurança Lógica, onde foram avaliados os riscos envolvendo software e hardware, controle de senhas de acesso e utilização de recursos.

A utilização de questionários é viável por: envolver baixo custo e pela praticidade; apresentar as mesmas questões para todas as pessoas; garantir o anonimato e por poder conter itens para atender a finalidades específicas de uma pesquisa. Quando bem elaborado e aplicado com critérios, apresenta elevada confiabilidade nos resultados (QUERINO, 2015).

A princípio, foram aplicados questionários como teste e, posteriormente, após ajustes, os questionários foram disponibilizados via *e-mail* a cada funcionário para que pudesse responder. No processo de coleta de dados, foi deixada a opção de anonimato de forma a permitir maior liberdade.

De modo geral, não se tem o interesse em conhecer tudo sobre uma população, mas apenas algumas de suas características que são conhecidas como parâmetros. A amostragem e o objetivo da inferência estatística têm como finalidade ajuizar sobre parâmetros populacionais da base de estatística amostral. Esses juízos são tentativas de previsão com certo grau de segurança e podem ser de dois tipos (BRESSAN, 2015) :

De posse dos dados coletados foi feita uma consolidação desses e gerados gráficos através do Excel e Google formulário, utilizado para coleta dos dados, para melhor visualização do cenário estudado. Finalmente, procurou-se responder com base no estudo a seguinte questão:

"Qual a aderência dos mecanismos de auditoria de controle interno e de segurança da informação no Centro de Computação da Universidade Federal de Minas Gerais"?

Concluídas as questões citadas, os resultados serão apresentados ao Centro de Computação (CECOM) e na FACE como trabalho de conclusão do curso de Auditoria Interna e Externa.

4. Análise dos Dados

Conforme mencionado anteriormente, foi aplicado aos funcionários do Centro de Computação, CECOM, o questionário contendo questões relativas a três áreas específicas sendo a primeira voltada aos controles físicos, a segunda apresentando questões relativas aos controles lógicos e, por fim, a terceira, referente a questões relativas à força de trabalho utilizado.

O CECOM abriga um total de aproximadamente 115 funcionários, incluindo terceirizados e estagiários. No total, foram respondidos 26 questionários, o que se demonstrou o suficiente para a análise por se tratar de uma amostra não probabilística, ou seja, não apresentam fundamentação matemática ou estatística, dependendo unicamente de critérios do pesquisador (BRESSAN, 2015).

A taxa de resposta pode variar consideravelmente de acordo com uma série de fatores tais como: a relação do pesquisador com o público alvo, o tamanho e a complexidade do questionário e, em alguns casos, o assunto do questionário. Assim, um índice de retorno de 26% pode ser considerado um número suficiente, levando em conta que questionários que são enviados para os entrevistados alcançam em média 25% de devolução (VIEIRA, 2010).

No Gráfico 8, é apresentado um resumo dos cargos das pessoas que responderam ao questionário.

Gráfico 8. Resumo de cargos.
Fonte: Gerado pelo autor.

Na análise das respostas, foi feita uma média para cada uma das três áreas estudas, ou seja, para o controle físico foram somados os valores de cada resposta dada e este valor foi divido pelo número de questões de cada área. Assim, para a soma dos percentuais encontrados para situações de "Não se aplica", a mesma foi dividida pelo número total de questões. Tem-se, então, o valor representativo de percentual de situações "Não se aplica" ao controle físico e, sucessivamente, a mesma metodologia foi aplicada para as outras opções.

No Gráfico 9, é apresentada uma análise do controle físico.

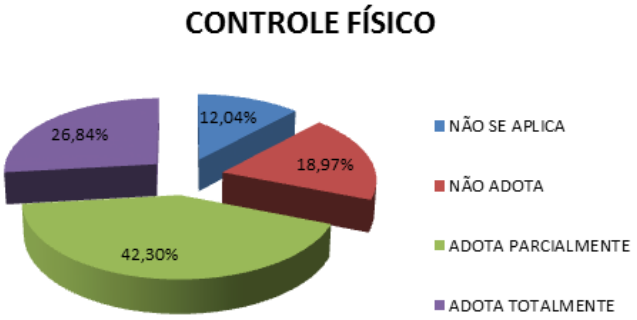


Gráfico 9. Média das respostas relativas ao controle físico.
Fonte: Gerado pelo autor.

Portanto, segundo informações obtidas através do questionário aplicado, para os funcionários, o CECOM adota totalmente o controle físico em 26,84% dos casos e parcialmente em 42,30%.

No Gráfico 10, é apresentada uma análise do controle lógico adotado e, nesse caso, segundo informações obtidas, o CECOM adota totalmente o controle lógico em 15,82% dos casos e parcialmente em 57,01%.

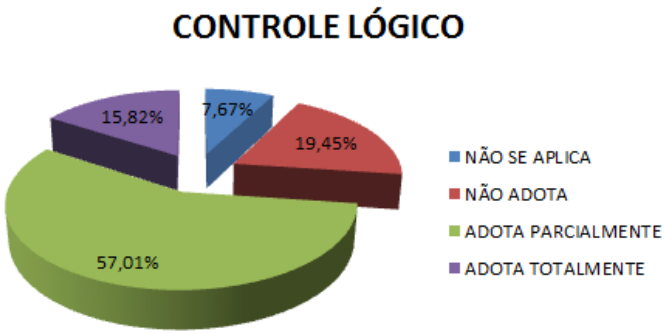


Gráfico 10. Média das respostas relativas ao controle lógico.
Fonte: Gerado pelo autor.

No Gráfico 11, é apresentada uma análise das respostas em relação à força de trabalho utilizada. Nesse caso, segundo informações obtidas, no CECOM, os pontos levantados nas questões atendem totalmente em 19,23% dos casos e parcialmente em 51,93%.

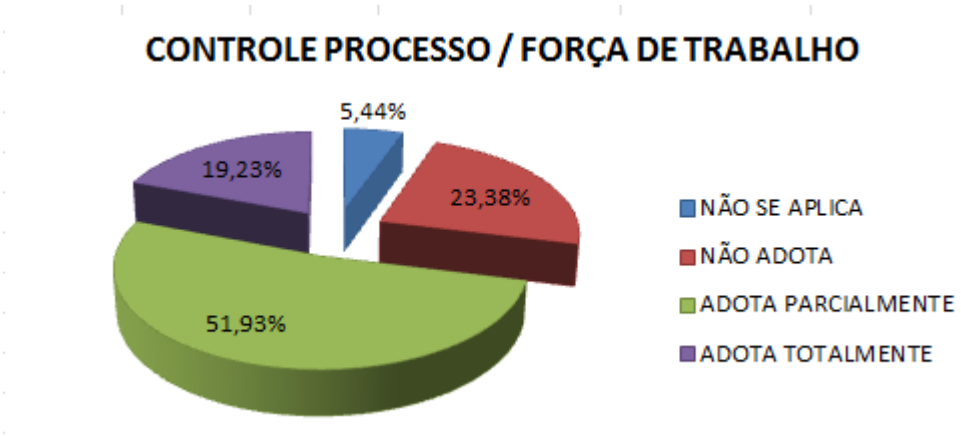


Gráfico 11. Média das respostas relativas ao controle de processo / força de trabalho.
Fonte: Gerado pelo autor.

As respostas obtidas, pelo questionário aplicado, em sua grande maioria, apresentaram certa insegurança quando se tem um índice de "adota parcialmente" elevado. Nos Gráficos 12 e 13, têm-se exemplos. Nos Anexos, são apresentados os questionários aplicados e, juntamente, a estatística para todas as questões.

Gráfico 12. Questão sobre controle físico.
Fonte: Gerado pelo autor.

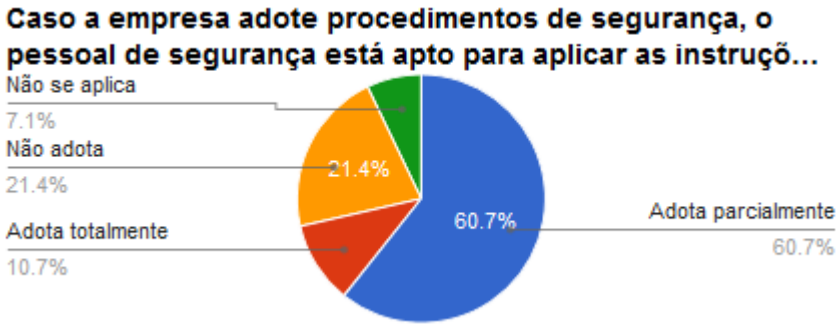


Gráfico 13. Questão sobre controle físico.
Fonte: Gerado pelo autor.

5. Considerações Finais

Atualmente, o cenário tecnológico e o volume de informações trocadas diariamente exigem que as organizações públicas ou privadas mantenham controles efetivos que possam assegurar aos usuários, colaboradores e possíveis investidores a transparência e eficiência no uso de recursos disponíveis dentro de uma organização. A tecnologia da informação apresenta-se como um suporte à gestão de processos e da informação, sendo inevitável sua utilização dentro de uma empresa atualmente.

Dessa forma, a tecnologia da informação não pode ser considerada apenas como um instrumento de trabalho e, sim, como um meio para que a empresa possa atender a suas demandas de forma segura e com qualidade, satisfazendo as necessidades dos usuários e contribuindo no processo de gestão.

Uma organização nunca estará segura totalmente, uma vez que novos métodos de ações surgem a cada dia. Entretanto, devem-se adotar ações para mitigar esses riscos. O fato de atender parcialmente contribui para uma falsa impressão de segurança quando, na realidade, o que se tem é uma abertura de portas para possíveis problemas. Recentemente, ouviu-se falar bastante sobre o problema ocorrido na cidade de Bento Rodrigues, distrito de Mariana, onde uma barragem de depósito de rejeitos de minério utilizada pela empresa Samarco rompeu. Certamente a empresa Samarco possuía procedimentos de segurança, mas que provavelmente atendiam parcialmente o que levou a uma perda irreparável.

No caso do CECOM, podemos observar pelas respostas obtidas e por se tratar de um órgão federal, que os controles existem e, em alguns casos, o que ocorre é falta de conhecimento

sobre o assunto. O funcionário público federal é regido pela lei 8.112/91 que estabelece normas de comportamento e penalidades em caso de falta.

Portanto, pelas respostas obtidas, foi possível concluir que há aderência dos controles internos e de segurança da informação junto aos funcionários. Entretanto, percebe-se a necessidade de melhora nos controles internos.

Nesse contexto, a auditoria interna é de grande importância no auxílio de desenvolvimento de processos mais seguros. Quanto mais a auditoria interna puder fornecer informações que sejam úteis e oportunas à gestão, mais contribuirá na redução de imprevisibilidade.

Como sugestões de melhoramentos:

- ✓ Criação e distribuição de manual com princípios básicos a ser seguindo dentro do CECOM;
- ✓ Adoção de um sistema de rotação de função visando equalizar o conhecimento dentro das áreas;
- ✓ Criar planos de contingências para recuperação de aplicativos/hardwares essenciais;
- ✓ Adotar plano de backup de base de dados, aplicativos e hardware que possam ser colocados em produção em pouco tempo em caso de falha do principal.

Portanto, há uma possibilidade de futuras investigações, como:

- ✓ Ampliação do questionário junto à comunidade universitária.
- ✓ Verificação da importância que pequenas e médias empresas dão à questão da segurança da informação.

Por fim, há grande possibilidade de desenvolvimento de pesquisas que possam contribuir para a redução de incertezas dentro das organizações e a auditoria interna certamente irá contribuir para esse objetivo. Pesquisas voltadas para melhoramento de controles de processos é essencial no crescimento de um país. O investimento em pesquisas é o ápice que toda nação deveria buscar para atender aos anseios de uma sociedade.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEXANDRIA, C. S. João. Gestão da Segurança da Informação: Uma Proposta para Potencializar a Efetividade da Segurança da Informação em Ambiente de Pesquisa Científica, IPEN, São Paulo, 2009.

ALMEIDA, C. Marcelo. Auditoria: Um Curso Moderno e Completo, 8ª ed., São Paulo, Ed. Atlas, 2012.

ARIMA, H. Carlos. Metodologia de Auditoria de Sistemas, 1ª Ed., São Paulo: Ed. Erica, 1994.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001: Sistemas de gestão de segurança da informação, Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: Código de prática para a gestão da segurança da informação, Rio de Janeiro, 2005.

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

BARROCA, M. Marialice. Diretrizes para Normalização dos Trabalhos Acadêmicos, FACE/UFMG, 2012.

BAZZOTTI, Cristiane e GARCIA, Elias. A Importância do Sistema de Informação Gerencial para Tomada de Decisões. Vol. 6, No 11 2006. Disponível em: http://e-revista.unioeste.br/index.php/csaemrevista/article/view/368. Acesso em: 15 mai. 2016.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil, Brasília: Senado Federal, Centro Gráfico, 1988.

BRESSAN, F. G. Valéria. Apostila de Estatística Descritiva, CEPCON, 2015.

CAMPOS, André. Sistemas de Segurança da Informação: Controlando os Riscos, 2ª ed., Florianópolis, Ed. Visual Books, 2007.

COBIT 4.1. Manual de Boas Práticas: *Framework for IT Governance and Contro*l, IGI, 2007. Disponível em: www.tjdft.jus.br/institucional/controle-interno/**boas-praticas/cobit**/at_download/file. Acesso em: 15 mai. 2016.

CONSELHO FEDERAL DE CONTABILIDADE, NBC PA 290 R1, 2005.

CREPALDI, A. Silvio. Auditoria Contábil: Teoria e Prática, 9ª ed., São Paulo: Ed. Atlas, 2013.

CUNHA, Dalvan e FENATO, A. Marcos. A Segurança da Informação e a sua Importância para Auditoria de Sistemas, 2013. Disponível em: http://semanaacademica.com.br/artigo/seguranca-da-informacao-e-sua-importancia-para-auditoria-de-sistemas. Acesso em: 15 mai. 2016

FERNANDES, C. Francisco e A, Rodrigo. As Teorias da Informação e da Comunicação e sua relação com as Disciplinas de Contabilidade, Administração e Sistemas de Informação. III Encontro de Pesquisa em Administração e Contabilidade. João Pessoa, nov. 2011. Disponível em: http://www.anpad.org.br/diversos/trabalhos/EnEPQ/enepq_2011/ENEPQ114.pdf. Acesso em: 31 mai. 2016.

GOMES, D. Eliane e et al., Auditoria: Alguns Aspectos a Respeito de sua Origem. FAEG/FAEFF. São Paulo: Ed FAEF, 2009. Disponível em http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/xza6N0w4fqVM1H2_2013-4-24-11-13-58.pdf. Acesso em: 31 mai. 2016.

GONÇALVES, Eduardo, F. Nicole e V. Talyta. Tragédia em Maria: Para que não se repita. Veja.com, 2015. Disponível em: http://veja.abril.com.br/complemento/brasil/para-que-nao-se-repita/. Acesso em: 13 jun. 2016.

INSTITUTO DOS AUDITORES INTERNOS DO BRASIL. *Cirtified Internal Auditor* (Cia): Dispõe sobre as exigências para obtenção do certificado de auditor interno, 2016. Disponível em: http://www.iiabrasil.org.br/new/cia.htmll. Acesso em: 25 abr. 2016.

KIM, David e S. G, Michael. Manual de Auditoria Governamental, 1ª Ed., São Paulo: Ed. Atlas, 2007.

LAUREANO, A. P. Marcos. Apostila de Gestão de Segurança da Informação, 2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. Acesso em: 15 mai. 2016.

Manual de Boas Práticas ITIL - (*Information Technology Infrastructure Library).*
MARCONI, A. Marina; LAKATOS M. Eva. Fundamentos de Metodologia Científica, 5ª ED., São Paulo: Ed. Atlas, 2003.

MOORE, A. Don e at al., *Conflicts of interest and the case of auditor independence: Moral Seduction and Strategicissue Cycling. USA, Academy of Management Review*, Vol 31,n. 1, p. 10-29, jan. 2006.

MORAES, A. D. Giseli e et al., A Tecnologia da Informação como Suporte à Gestão Estratégica da Informação na Pequena Empresa, 2005. Disponível em http://www.teses.usp.br/teses/disponiveis/18/18140/tde-15102005-111036/pt-br.php. Acesso em: 15 mai. 2016.

MORAIS, G. Maria. A importância da auditoria interna para a gestão: Caso das empresas portuguesas. Anais dos Trabalhos Científicos, 18º Congresso Brasileiro de Contabilidade. Gramado, 24 a 28 ago. 2008. Disponível em: http://www.ccontabeis.com.br/18cbc/570.pdf. Acesso em: 15 mar. 2016.

ONOME, I. Joshua. Auditoria de Sistemas de Informação, 2ª Ed., São Paulo: Ed. Atlas, 2014.

PACHECO, F. L., Furtado. Auditoria Interna na Área de Auditoria da Informação, Brasília, 2011.

PALACIO DO PLANALTO. Decreto nº 3.505/2000. Institui Política de Segurança da Informação na administração Federal, 13 de jun. 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm. Acesso em: 15 mar. 2016.

PETER, G. A. Maria; MACHADO, V. V. Marcus. Manual de Auditoria Governamental, 1ª Ed., São Paulo: Ed. Atlas, 2007.

QUERINO, F. M. Magda e at al., Apostila de Metodologia da Pesquisa e da Produção Científica. Brasília. agos. 2015.

SILVA, A. G., Antônio. Auditoria Governamental: Ápice da Pirâmide do Sistema de Controle Interno. Sobral, 2014. Disponível em: http://www.arcos.org.br/artigos/auditoria-governamental-apice-da-piramide-do-sistema-de-controle-interno/. Acesso em: 09 mar. 2016.

SUPERIOR TRIBUNAL DE JUSTICA. Cartilha: Segurança da Informação. Disponível em: http://www.stj.jus.br/portal_stj/arquivos/cartilha.pdf. Acesso em: 21 mar. 2016.

TRIBUNAL DE CONTAS DA UNIÃO. Manual de Boas Práticas em Segurança da Informação, 2012. Disponível em: http://portal2.tcu.gov.br/portal/pls/portal/docs/2188952.PDF. Acesso em: 24 abr. 2016.

TRIBUNAL DE CONTAS DA UNIÃO. Nota Técnica 7/2014. Disponível em: http://portal.**tcu**.gov.br/lumis/portal/file/fileDownload.jsp?fileId..1. Acesso em: 17 mai. 2016.

UNIÃO INTERNACIONAL DAS TELECOMUNICAÇÕES. *Statistic Global internet users and internet penetration.* Disponível em: *http://www.itu.int/en/ITU-D/Pages/default.aspx*. Acesso em: 16 mai. 2016.

VIEIRA, C. Henrique, E. C. Aline e S. J. Vitor. O uso de questionários via e-mail em pesquisas acadêmicas sob a ótica dos respondentes. XIII SemeAD, Santa Catarina, set. 2010. Disponível em: http://www.pucrs.br/famat/viali/recursos/inquiries/O%20uso%20de%20question%C3%A1rios%20via%20e-mail%20em%20pesquisas%20acad%C3%AAmicas%20sob%20a%20%C3%B3tica%20dos.pdf. Acesso em: 07 jun. 2016.

UFMG - CENTRO DE COMPUTAÇÃO - CECOM

VERIFICAÇÃO DOS CONTROLES INTERNOS

*Obrigatório

1. **Nome (Opcional):**

_____

2. **Função:**

_____

3. **Tempo de Trabalho na Área:**

_____

EM RELAÇÃO AO CONTROLE FÍSICO

Nessa seção você irá responder perguntas sobre o controle físico, onde deverá marcar apenas um nível de adoção da prática.

4. **Existe procedimentos de segurança definido para acesso ao ambiente de tecnologia?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

5. **Caso a empresa adote procedimentos de segurança, o pessoal de segurança está apto para aplicar as instruções em caso de emergência?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

6. **Existem regulamentos escritos e estabelecimento de penalidades contra violação concernentes a importantes medidas de segurança e práticas de proteção?** *
Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

7. **Caso a resposta anterior seja "adota parcialmente" ou "adota totalmente". Os funcionários possuem acesso a esses regulamentos?** *
Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

8. **Existe uma revisão formal e periódica por parte da Gerência, quanto às políticas, procedimentos e programas de segurança?** *
Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

9. **As instalações e os equipamentos de processamento eletrônico de dados estão cobertos por seguro?** *
Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

10. **Há um plano de contingência detalhado para a correção e restauração do CPD, em termos de "hardware" e "softwares"?** *
Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

11. **Caso a resposta anterior seja "adota parcialmente" ou "adota totalmente". O plano de contingência é revisto/testado regularmente?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

12. **Existe procedimento de backup definido?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

13. **Caso a resposta anterior seja "adota parcialmente" ou "adota totalmente". O backup é armazenado em local distinto do ambiente de produção?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

14. **O ambiente onde é armazenado o backup possui acesso restrito a pessoal autorizado?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

15. **Em caso de perda crítica a área de tecnologia tem condições de atuar para solucionar o problema no devido tempo?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

16. **Existe sistema alternativo de alimentação de energia elétrica (Nobreak, gerador)?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

17. **Caso a resposta anterior seja "adota parcialmente" ou "adota totalmente". Estes sistemas são testados regularmente?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

18. **São adequadas as medidas de segurança e proteção relativas ao controle e limitação de acesso às pessoas no CPD?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

EM RELAÇÃO AO CONTROLE LÓGICO

Nessa seção você irá responder perguntas sobre o controle Lógico, onde deverá marcar apenas um nível de adoção da prática.

19. **Há rotinas e procedimentos definidos para elaboração de especificações, visando dar suporte a projetos de novos sistemas ou mudanças nos sistemas existentes?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

20. **As mudanças previstas são comunicadas previamente aos usuários?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

21. **É de conhecimento de todos a importância da documentação e planejamento de mudanças?** *
Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

22. **Existe treinamento especifico na contratação de estagiários/funcionários terceirizados?** *
Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

23. **Existem rotinas e procedimentos estabelecidos para o envolvimento de usuários no planejamento de mudanças/atualizações?** *
Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

24. **Existem procedimentos especificos com relação a identificação e eliminação da senha de acesso de pessoas desligadas da empresa?** *
Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

25. **Existe um plano de teste dos backups?** *
Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

26. **Caso a resposta anterior seja "adota parcialmente" ou "adota totalmente". O plano de backup está coordenado com o plano de contingências?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

27. **Existem normas proibindo a utilização de cópias "não autorizadas" de softwares?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

28. **Caso a resposta anterior seja "adota parcialmente" ou "adota totalmente". As normas mencionadas na questão anterior são divulgas aos usuários?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

29. **Existem procedimentos para identificação e eliminação de cópias "não autorizadas" de softwares?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

30. **Existem controles e ferramentas (FIREWALL/ANTIVÍRUS) adequadas para a detecção e eliminação de vírus do computador?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

31. **Existe planejamento para implementação de mudanças, visando períodos de pouca ou nenhuma atividade para minimizar o potencial de erros nos sistemas em operação.** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

32. **As resoluções de problemas são documentadas e passadas ao responsável pela área?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

33. **Existem rotinas e procedimentos estabelecidos para atribuição ou modificação do nível de acesso?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

34. **Atualizações e trocas de aplicativos são documentados?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

35. **Existe sistema de detecção de usuários inativos, com linhas abertas?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

Ir para a pergunta 36.

EM RELAÇÃO A FORÇA DE TRABALHO DE TI

Nessa seção você irá responder perguntas sobre a força de trabalho utilizada na área de Tecnologia da Informação, onde deverá marcar apenas um nível de adoção da prática.

36. **Existe separação de atividades dentro da área de trabalho?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

37. **Existe um esquema rotativo de tarefas e treinamento de pessoal para evitar dependências da execução de atividades?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

38. **Existe programa de conscientização de segurança aplicado regularmente junto aos funcionários da área de tecnologia?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

39. **O pessoal foi treinado e está preparado para agir em caso de emergência?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

40. **Há programa de treinamento continuo aos funcionários da área de tecnologia da informação?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

41. **É possível interromper o trabalho, ou seja, impedir o acesso aos softwares utilizados, dos funcionários imediatamente após a decisão de dispensá-los?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

42. **A auditoria interna avalia a gestão de riscos de TI?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

43. **O trabalho de auditoria interna é aproveitado no aprimoramento dos processos de trabalho?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

44. **A execução do orçamento de TI é divulgado e de fácil acesso?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

45. **A direção define critérios para avaliação e atendimento dos pedidos de capacitação?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

46. **O quantitativo da força de trabalho de TI é suficiente?** *

Marcar apenas uma oval.

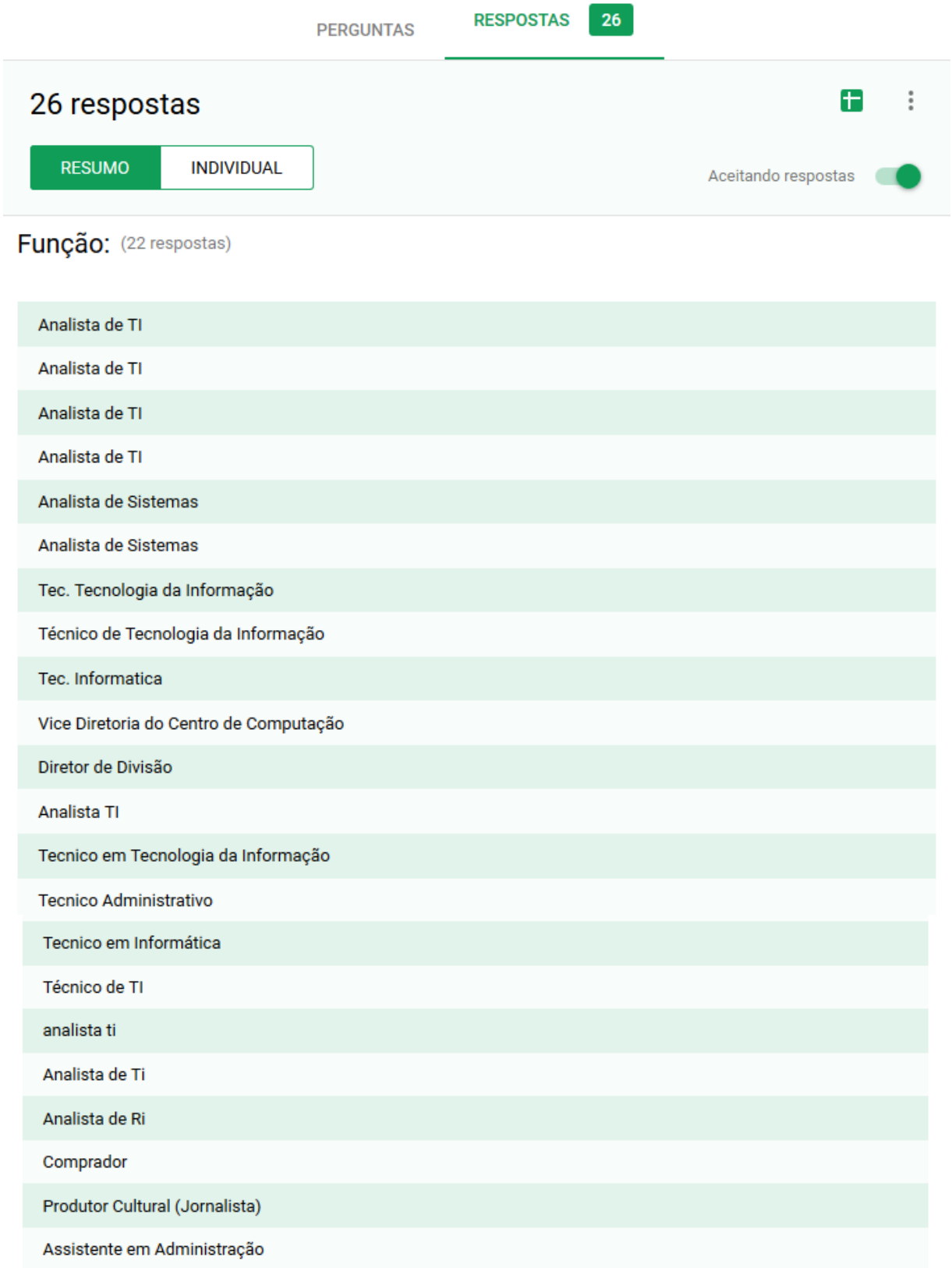
- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

47. **São definidas metas de desempenho para o pessoal de TI?** *

Marcar apenas uma oval.

- ◯ Não se aplica
- ◯ Não adota
- ◯ Adota parcialmente
- ◯ Adota totalmente

OBRIGADO !!!


PERGUNTAS
RESPOSTAS 26
26 respostas
RESUMO
INDIVIDUAL
Aceitando respostas
Função: (22 respostas)
Analista de TI
Analista de TI
Analista de TI
Analista de TI
Analista de Sistemas
Analista de Sistemas
Tec. Tecnologia da Informação
Técnico de Tecnologia da Informação
Tec. Informatica
Vice Diretoria do Centro de Computação
Diretor de Divisão
Analista TI
Tecnico em Tecnologia da Informação
Tecnico Administrativo
Tecnico em Informática
Técnico de TI
analista ti
Analista de Ti
Analista de Ri
Comprador
Produtor Cultural (Jornalista)
Assistente em Administração

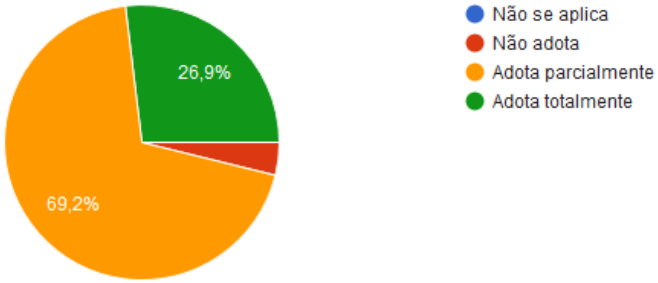
Tempo de Trabalho na Área: (22 respostas)

7 anos
7 anos
10 Anos
10 Anos
8 anos
8 anos
5 anos
5 anos
20 anos
02 anos
5 meses
36
23 anos
2 Anos
6 Anos
38 anos
29
3 meses
12 anos
1 ano e 7 meses
12 Anos
43

EM RELAÇÃO AO CONTROLE FÍSICO

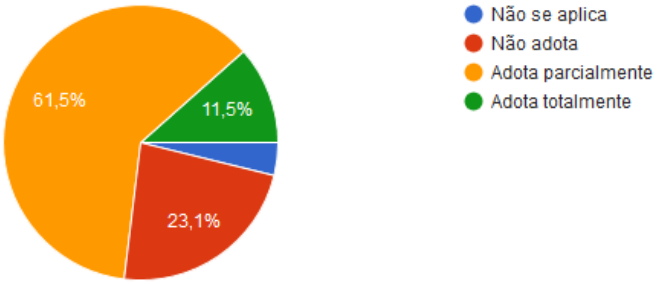
Existe procedimentos de segurança definido para acesso ao ambiente de tecnologia?

(26 respostas)



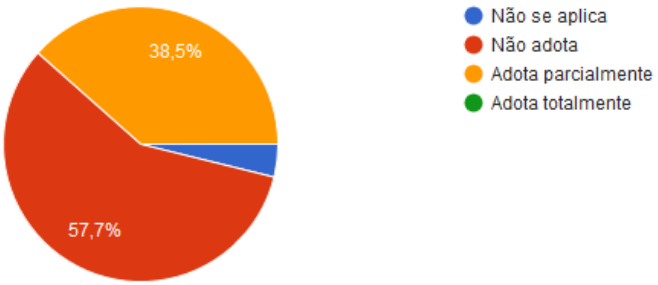
Caso a empresa adote procedimentos de segurança, o pessoal de segurança está apto para aplicar as instruções em caso de emergência?

(26 respostas)



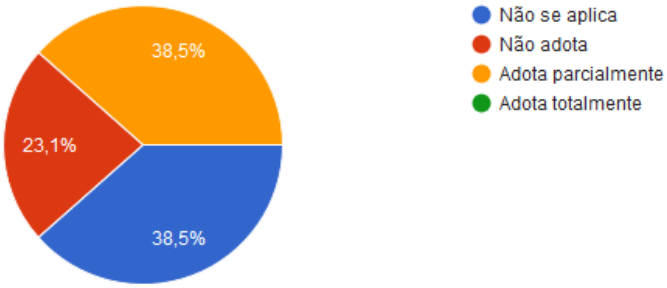
Existem regulamentos escritos e estabelecimento de penalidades contra violação concernentes a importantes medidas de segurança e práticas de proteção?

(26 respostas)



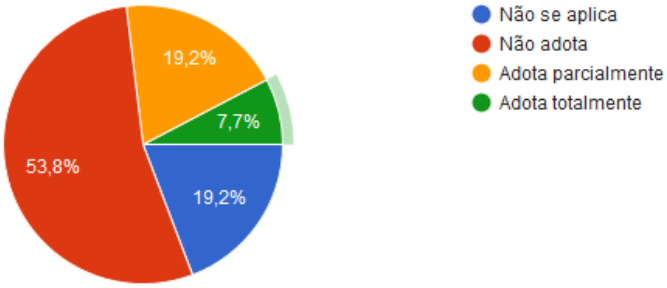
Caso a resposta anterior seja "adota parcialmente" ou "adota totalmente". Os funcionários possuem acesso a esses regulamentos?

(26 respostas)



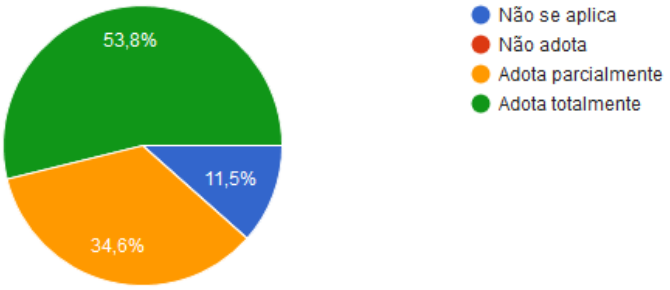
Existe uma revisão formal e periódica por parte da Gerência, quanto às políticas, procedimentos e programas de segurança?

(26 respostas)



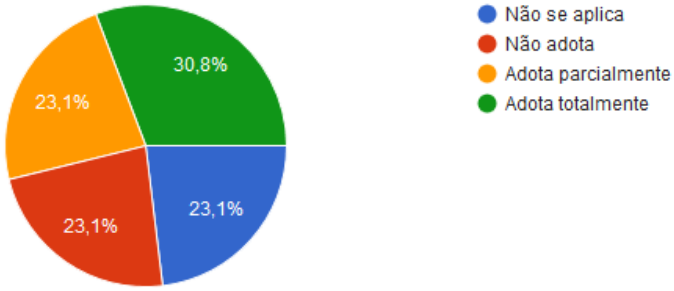
O ambiente onde é armazenado o backup possui acesso restrito a pessoal autorizado?

(26 respostas)



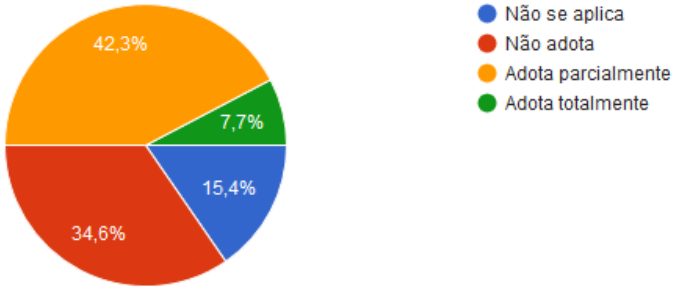
As instalações e os equipamentos de processamento eletrônico de dados estão cobertos por seguro?

(26 respostas)



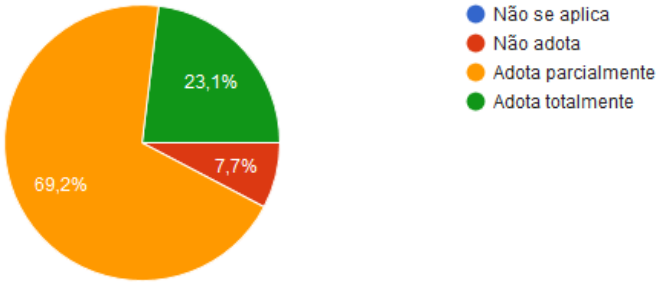
Há um plano de contingência detalhado para a correção e restauração do CPD, em termos de “hardware” e “softwares”?

(26 respostas)



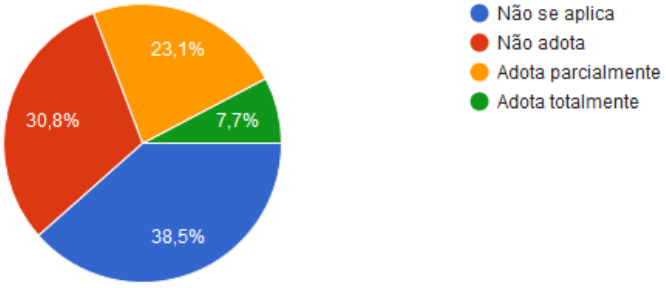
Em caso de perda crítica a área de tecnologia tem condições de atuar para solucionar o problema no devido tempo?

(26 respostas)

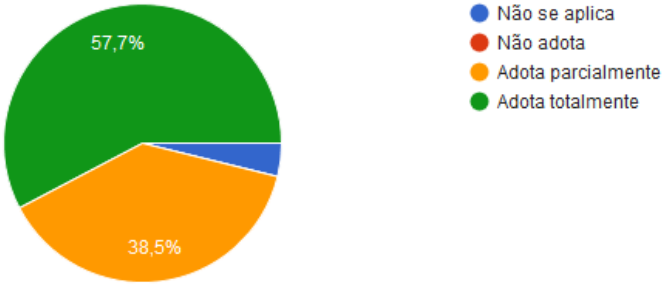


Caso a resposta anterior seja "adota parcialmente" ou "adota totalmente". O plano de contingência é revisto/testado regularmente?

(26 respostas)

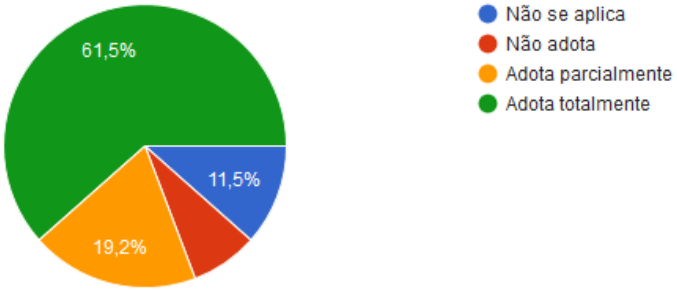


Existe procedimento de backup definido? (26 respostas)



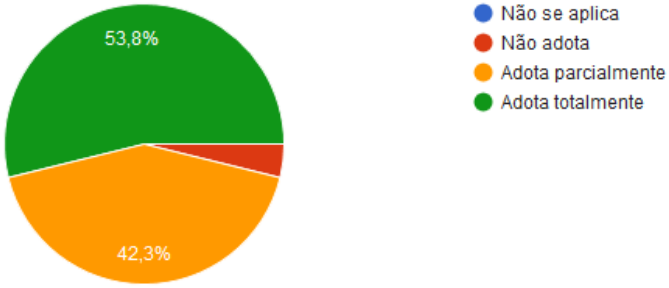
Caso a resposta anterior seja "adota parcialmente" ou "adota totalmente". O backup é armazenado em local distinto do ambiente de produção?

(26 respostas)



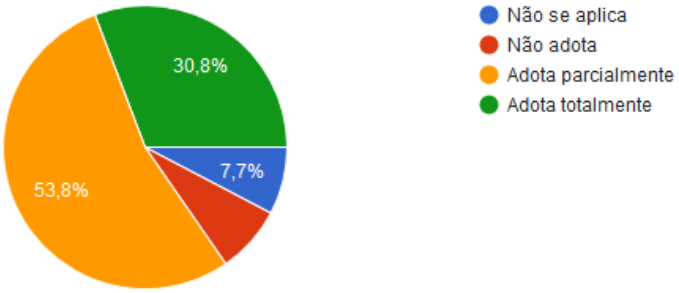
Existe sistema alternativo de alimentação de energia elétrica (Nobreak, gerador)?

(26 respostas)



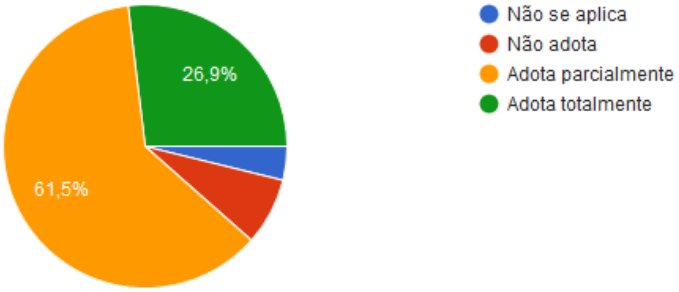
Caso a resposta anterior seja "adota parcialmente" ou "adota totalmente". Estes sistemas são testados regularmente?

(26 respostas)



São adequadas as medidas de segurança e proteção relativas ao controle e limitação de acesso às pessoas no CPD?

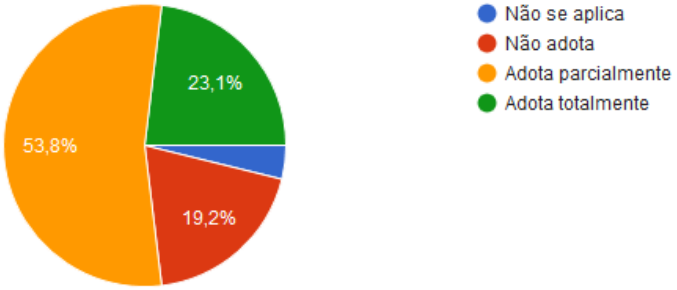
(26 respostas)



EM RELAÇÃO AO CONTROLE LÓGICO

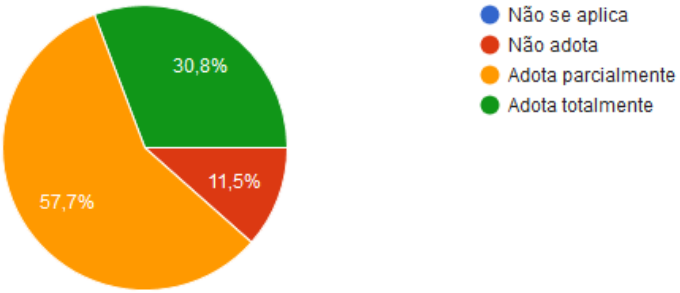
Há rotinas e procedimentos definidos para elaboração de especificações, visando dar suporte a projetos de novos sistemas ou mudanças nos sistemas existentes?

(26 respostas)



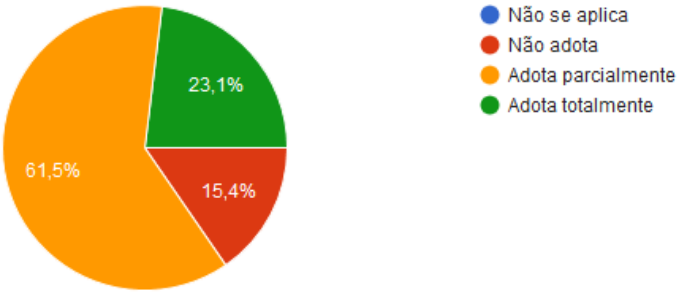
As mudanças previstas são comunicadas previamente aos usuários?

(26 respostas)



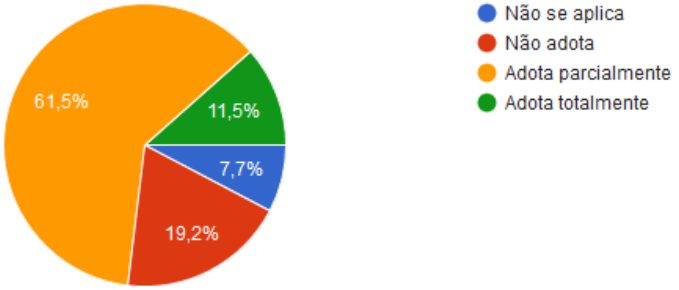
É de conhecimento de todos a importância da documentação e planejamento de mudanças?

(26 respostas)



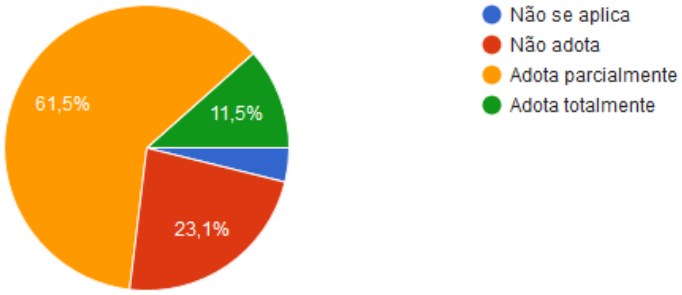
Existe treinamento específico na contratação de estagiários/funcionários terceirizados?

(26 respostas)



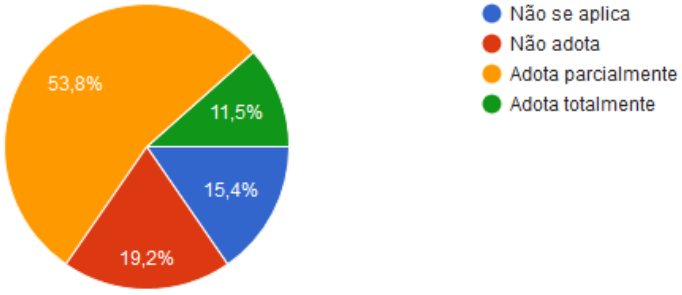
Existem rotinas e procedimentos estabelecidos para o envolvimento de usuários no planejamento de mudanças/atualizações?

(26 respostas)

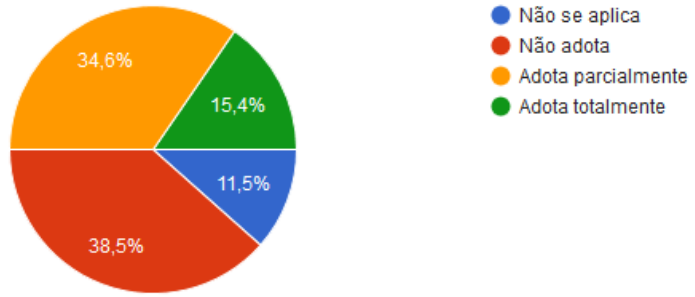


Existem procedimentos específicos com relação a identificação e eliminação da senha de acesso de pessoas desligadas da empresa?

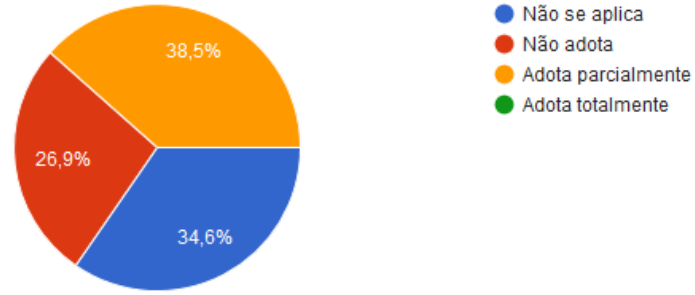
(26 respostas)



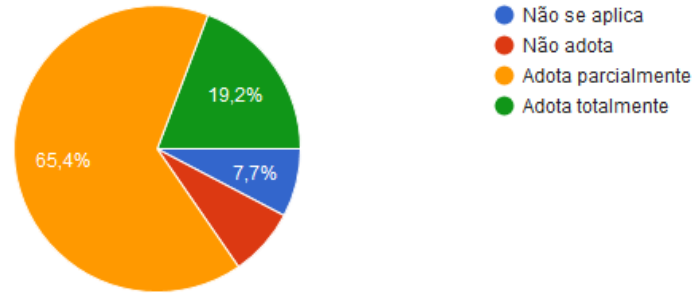
Existe um plano de teste dos backups? (26 respostas)



Caso a resposta anterior seja "adota parcialmente" ou "adota totalmente". O plano de backup está coordenado com o plano de contingências?
(26 respostas)

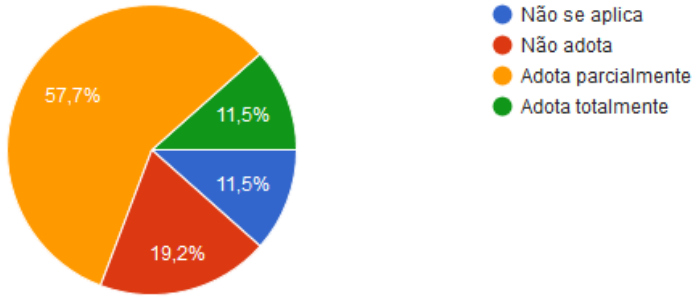


Existem normas proibindo a utilização de cópias “não autorizadas” de softwares?
(26 respostas)



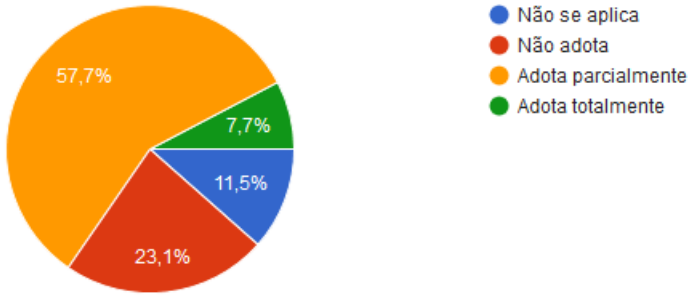
Caso a resposta anterior seja "adota parcialmente" ou "adota totalmente". As normas mencionadas na questão anterior são divulgas aos usuários?

(26 respostas)



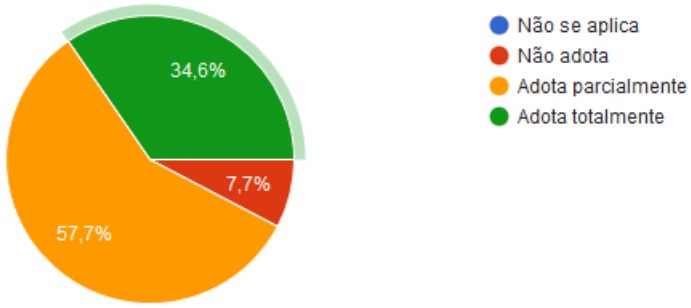
Existem procedimentos para identificação e eliminação de cópias “não autorizadas” de softwares?

(26 respostas)



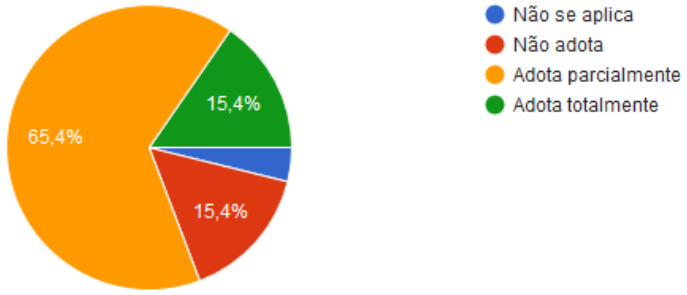
Existem controles e ferramentas (FIREWALL/ANTIVÍRUS) adequadas para a detecção e eliminação de vírus do computador?

(26 respostas)



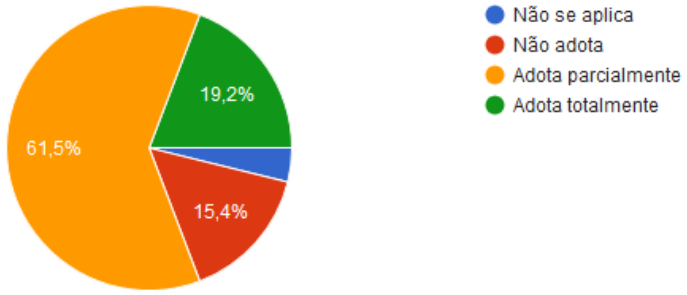
Existe planejamento para implementação de mudanças, visando períodos de pouca ou nenhuma atividade para minimizar o potencial de erros nos sistemas em operação.

(26 respostas)



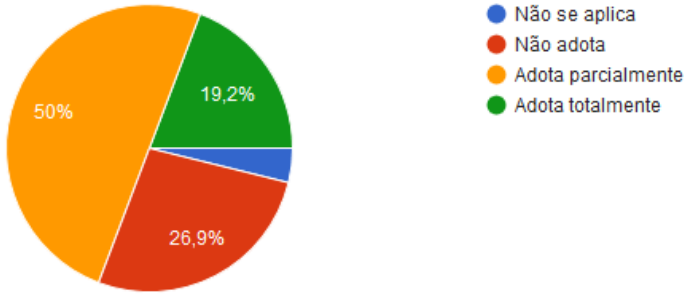
As resoluções de problemas são documentadas e passadas ao responsável pela área?

(26 respostas)

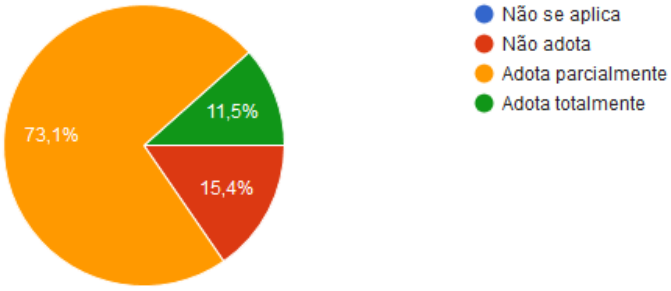


Existem rotinas e procedimentos estabelecidos para atribuição ou modificação do nível de acesso?

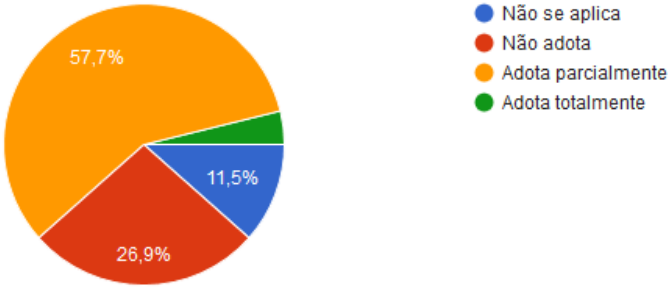
(26 respostas)



Atualizações e trocas de aplicativos são documentados? (26 respostas)

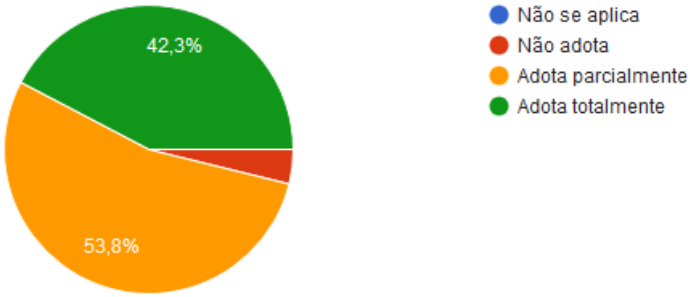


Existe sistema de detecção de usuários inativos, com linhas abertas?
(26 respostas)



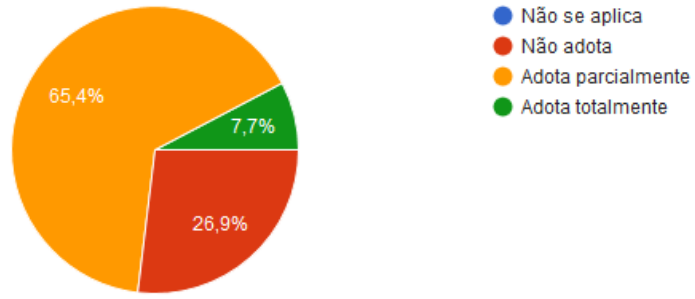
EM RELAÇÃO A FORÇA DE TRABALHO DE TI

Existe separação de atividades dentro da área de trabalho? (26 respostas)



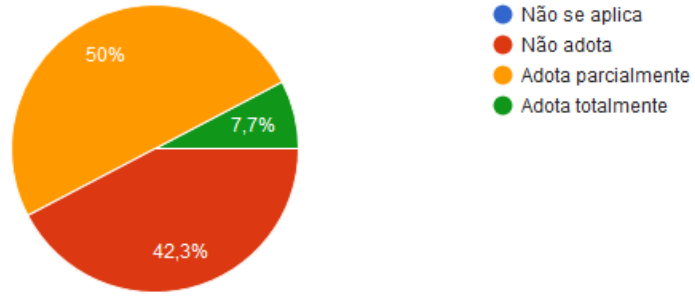
Existe um esquema rotativo de tarefas e treinamento de pessoal para evitar dependências da execução de atividades?

(26 respostas)



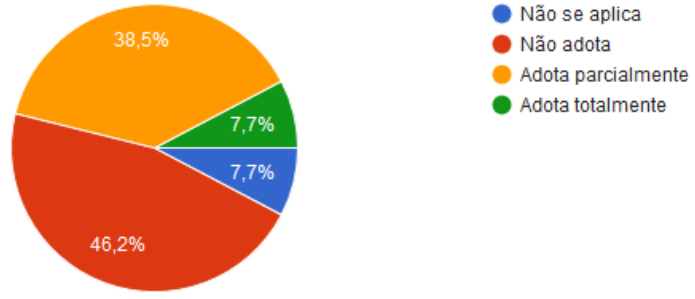
Existe programa de conscientização de segurança aplicado regularmente junto aos funcionários da área de tecnologia?

(26 respostas)

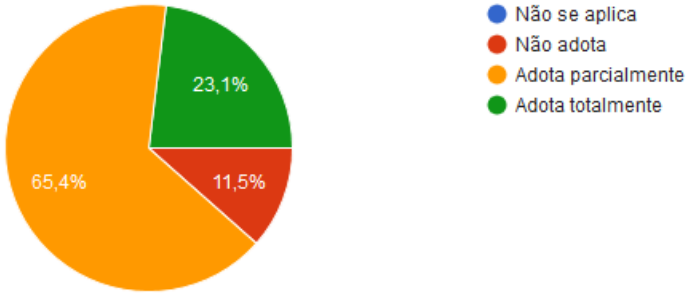


O pessoal foi treinado e está preparado para agir em caso de emergência?

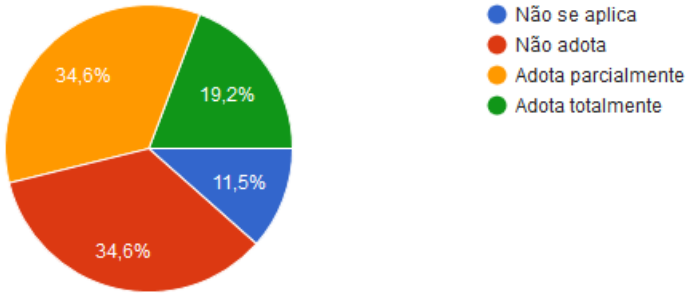
(26 respostas)



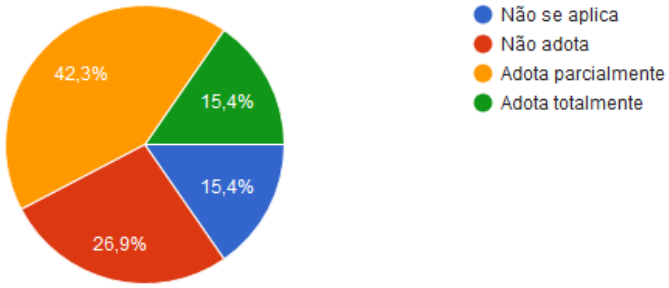
Há programa de treinamento contínuo aos funcionários da área de tecnologia da informação?
(26 respostas)



É possível interromper o trabalho, ou seja, impedir o acesso aos softwares utilizados, dos funcionários imediatamente após a decisão de dispensá-los?
(26 respostas)

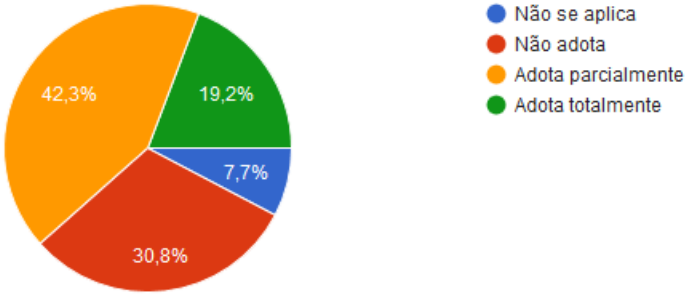


A auditoria interna avalia a gestão de riscos de TI? (26 respostas)

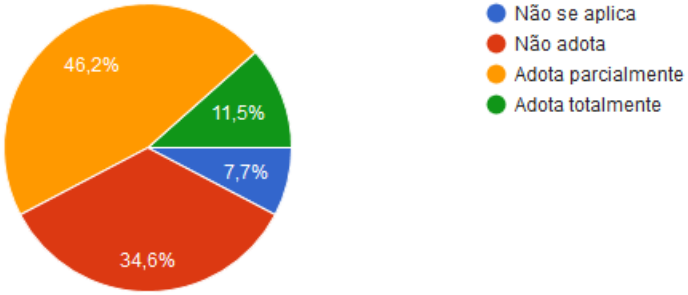


O trabalho de auditoria interna é aproveitado no aprimoramento dos processos de trabalho?

(26 respostas)

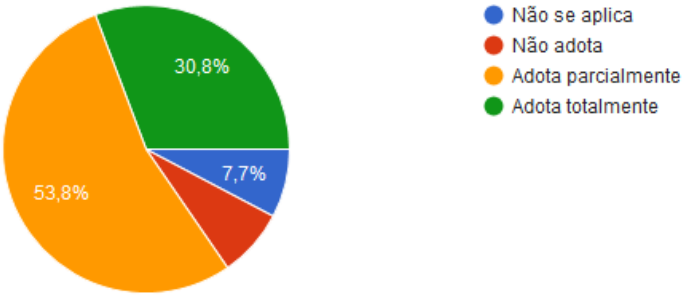


A execução do orçamento de TI é divulgado e de fácil acesso? (26 respostas)

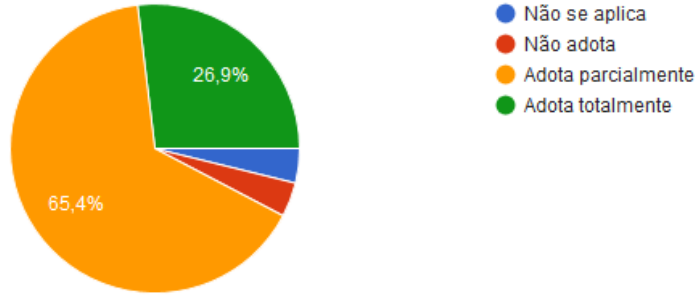


A direção define critérios para avaliação e atendimento dos pedidos de capacitação?

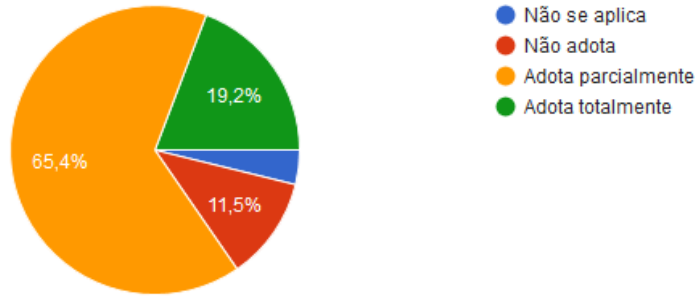
(26 respostas)



O quantitativo da força de trabalho de TI é suficiente? (26 respostas)



São definidas metas de desempenho para o pessoal de TI? (26 respostas)



OBRIGADO !!!