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

PLANO DE GERENCIAMENTO DE RISCOS PARA A INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO COMUM AOS CAMPI DO INSTITUTO FEDERAL DE BRASÍLIA

Tiago Júnio Pires da Cunha

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

Orientador
Prof. Dr. Gladston Luiz da Silva

Brasília
2016

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

Cunha, Tiago Júnio Pires da
CR595p PLANO DE GERENCIAMENTO DE RISCOS PARA A INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO COMUM AOS CAMPI DO INSTITUTO FEDERAL DE BRASÍLIA / Tiago Júnio Pires da Cunha; orientador Gladston Luiz da Silva. - Brasília, 2016.
261 p.

Dissertação (Mestrado - Mestrado Profissional em Computação Aplicada) -- Universidade de Brasília, 2016.

1. Risco. 2. Infraestrutura de Tecnologia da Informação. 3. Instituição de Ensino. I. Silva, Gladston Luiz da, orient. II. Título.

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

PLANO DE GERENCIAMENTO DE RISCOS PARA A INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO COMUM AOS CAMPI DO INSTITUTO FEDERAL DE BRASÍLIA

Tiago Júnio Pires da Cunha

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

Prof. Dr. Gladston Luiz da Silva (Orientador)
CIC/UnB

Prof. Dr. Simone Borges Simão Monteiro
UnB

Prof. Dr. Leandro Vaguetti
IFB

Prof. Dr. Marcelo Ladeira
Coordenador do Programa de Pós-graduação em Computação Aplicada

Brasília, 16 de Dezembro de 2016

Dedicatória

Àqueles que fazem parte de nossas vidas, aos quais dirigimos as mais diversas emoções e o nosso mais profundo amor, com todo carinho dedico o esforço e realizações deste trabalho.

Agradecimentos

Agradeço a todos aqueles que tornaram este trabalho possível, a todos que apoiaram, incentivaram e torceram pelo sucesso desta empreitada, tornando-a possível, direta ou indiretamente.

Resumo

O Instituto Federal de Brasília é uma instituição de ensino composta por vários *campi*, tendo um importante papel na expansão do ensino básico, técnico e tecnológico e disseminação da tecnologia. Conta com uma infraestrutura de tecnologia da informação, comum em muitos pontos a seus vários *campi*, visando atender milhares de alunos. Esta infraestrutura está sujeita a riscos. A concretização destes riscos poderia trazer uma gama de efeitos negativos para a instituição, tornando-se institucionalmente interessante gerenciar estes riscos. Esta pesquisa objetivou realizar um diagnóstico, um levantamento inicial dos riscos aos quais esta infraestrutura comum aos *campi* estava sujeita. Foi uma pesquisa exploratória que adotou como método um estudo de caso, tendo uma abordagem qualitativa. Foram pesquisadas outras instituições de ensino com estrutura similar para importação de um possível processo de gestão de riscos, utilizando questionários, entrevistas e documentos das instituições. Com práticas propostas pela ISO 31000, pela ISO 31010 e pelo Plano de Gerenciamento de Riscos da Universidade da Virgínia foram realizadas pesquisas no Instituto Federal de Brasília para levantamento dos riscos. Obteve-se uma lista de riscos de acordo com a opinião da equipe de tecnologia da informação e a alta gestão dos *campi*, que foram então classificados pela equipe de tecnologia da informação. Os riscos foram validados por formadores de opinião dos respectivos *campi*, que também informaram o quanto a interrupção de cada serviço causada pela concretização dos riscos afetaria seu trabalho. As informações obtidas podem proporcionar as bases para um eventual plano de gerenciamento de riscos para a organização, tendo sido levadas para discussão no planejamento do Plano Diretor de Tecnologia da Informação do órgão para o biênio 2017-2018.

Palavras-chave: Risco, Infraestrutura de Tecnologia da Informação, Instituição de Ensino

Abstract

The Brasilia Federal Institute is an educational institution with various campi, playing an important role in the expansion of the basic, technical and technological education as well as dissemination of technology. To support this role, the institution possesses its own information technology infrastructure, with similar assets in each campus, serving thousands of students per year. This infrastructure is subject to risks. If they occur, they could negatively affect the organization, showing that it is relevant to manage them. This research intended to realize a diagnostic, an initial risk assessment of the IT infrastructure common to the various campi of the organization. It was an exploratory research, taking the form of a case study with a qualitative approach. Similar educational institutions were researched to import a possible risk management process. Using ISO 31000, ISO 31010 and the University of Virginia Information Technology Security Risk Management Program as references, research was performed to assess the risks of the organization. A list of risks elicited by the IT staff and the upper management of the campi was obtained, prioritized by the IT staff and validated by people with opinion leadership in these campi, that also indicated how much a service interruption caused by risks would affect their job. The obtained information can be used as basis for a risk management plan to the organization and was brought to discussion to its Information Technology Master Plan draft for 2017-2018.

Keywords: Risk, Information Technology Infrastructure, Educational Institution

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

CEFETs Centros Federais de Educação Tecnológica.

DF Distrito Federal.

ENISA European Union Agency for Network and Information Security.

IFB Instituto Federal de Brasília.

IFs Institutos Federais de Educação, Ciência e Tecnologia.

NTIC Núcleo de Tecnologia da Informação e Comunicação.

OECD Organisation for Economic Co-operation and Development.

PDTIC Plano Diretor de Tecnologia da Informação.

TI Tecnologia da Informação.

UFPE Universidade Federal de Pernambuco.

UnB Universidade de Brasília.

Capítulo 1

Introdução

Este capítulo apresenta uma contextualização geral da pesquisa, a justificativa, os objetivos e a estrutura do trabalho.

1.1 Breve Histórico da Rede Federal de Educação Profissional

A educação profissionalizante no Brasil remonta as primeiras décadas da república, tendo início em 1909 com a criação de 19 Escolas de Aprendizes Artífices, focadas em uma formação profissional básica e com uma função mais voltada para a inclusão social [10]. Em 1937 estas escolas passaram a se chamar liceus industriais, acompanhando a expansão da indústria [17][55]. Em 1941 o ensino profissional passou a ser considerado de nível médio e em 1942 os liceus foram denominados escolas técnicas industriais. Em 1959 passaram a se chamar escolas técnicas federais, ganhando a condição de autarquias [18].

Em 1978, escolas técnicas federais foram transformadas em Centros Federais de Educação Tecnológica (CEFETs), sendo seguidas por várias escolas técnicas e agrotécnicas federais na década de 90 [55]. Os CEFETs tinham reconhecimento equivalente aos centros universitários. Em 1998 o crescimento das escolas federais foi estagnado por políticas federais. Em 2004 houve uma re-orientação das políticas federais para a educação tecnológica, culminando com uma ampliação da rede federal de ensino [10][15][17][55].

A rede federal de ensino foi ampliada pela lei 11.892 de 29 de dezembro de 2008, que instituiu a Rede Federal de Educação Profissional, Científica e Tecnológica e criou os Institutos Federais de Educação, Ciência e Tecnologia (IFs). Os IFs são instituições de ensino voltadas para o ensino básico, técnico e tecnológico [8], visando, portanto, a formação de alunos em níveis diferentes.

Foram criados 38 Institutos Federais através da lei de 2008, sendo que no Distrito Federal (DF) foi criado o Instituto Federal de Brasília (IFB). Fundado em 2008, o IFB contava em 2009 com apenas 60 funcionários e cerca de 300 estudantes, atualmente possui milhares de alunos [19] e 10 *campi*.

1.2 O Problema

O IFB, como os outros IFs, tem um grande eixo de abrangência em questão de ensino. Diferentemente das universidades, cujo foco está no ensino superior [9], diferentemente das escolas de ensino técnico, cujo foco está no ensino técnico, o IFB é uma instituição mista, fazendo parte dos seus objetivos a oferta dos cursos técnicos e também de cursos de ensino superior. Pode oferecer desde o ensino médio-técnico até a pós-graduação *stricto sensu*, bem como a oferta de cursos de formação inicial e continuada de trabalhadores, entre outros [8]. Além disso, como define a lei 11.892 de 29 de dezembro de 2008, o IFB possui natureza jurídica de autarquia, detendo autonomia administrativa, patrimonial, financeira, didático-pedagógica e disciplinar. Ele necessita de uma infraestrutura de tecnologia da informação para apoiar suas atividades administrativas e de ensino, sendo que parte desta infraestrutura ainda está sendo implantada.

O IFB conta com a reitoria e 10 *campi*, implantados ou em implantação. Cada *campus* tem sua infraestrutura de Tecnologia da Informação (TI) para atender às demandas administrativas e de ensino, tendo estruturas bastante similares entre si.

Existe uma infraestrutura considerável de tecnologia para apoiar suas necessidades organizacionais, a instituição está sujeita a problemas advindos desta infraestrutura, incluindo falhas técnicas, produtos e serviços obsoletos ou precários, falhas de segurança, despreparo técnico, entre outros. A interrupção na continuidade da entrega da tecnologia poderá gerar perdas grandes à imagem da instituição, além das dificuldades advindas da falta do serviço para a continuidade do negócio. Esta interrupção também poderá ter um impacto negativo junto aos interessados, que podem entendê-la como ineficiência na gestão dos recursos públicos.

Faz-se necessário, portanto, que sejam elaboradas as bases para um plano de gerenciamento de riscos aplicável às áreas de infraestrutura de tecnologia da informação, consideradas comuns aos *campi* do IFB, beneficiando a organização que está dispersa geograficamente.

1.3 Justificativa

A governança de tecnologia da informação pode ser considerada estratégica para o IFB. Entretanto, a organização possui um eixo bastante grande de atuação, um parque tecnológico considerável e está dispersa fisicamente, surgem riscos inerentes à aplicação da tecnologia da informação e sua continuidade para os objetivos do negócio.

Como a concretização do risco pode trazer uma gama de efeitos negativos sobre os objetivos da organização, torna-se interessante do ponto de vista organizacional gerenciá-los. A gestão de riscos aliada aos processos organizacionais de gerência de tecnologia da informação se mostra uma arma poderosa para administrar recursos e melhorar os processos organizacionais.

Para o IFB, que é relativamente novo e ainda encontra-se implantando e desenvolvendo parte de sua estrutura física, tecnológica e organizacional, fica evidente a importância da gestão de riscos de tecnologia da informação como ferramenta facilitadora da gestão de recursos públicos.

1.4 Contribuição Esperada

Esta pesquisa intenciona fornecer à alta gestão do IFB e de seus *campi* elementos-base para o desenvolvimento de um plano de gerenciamento de riscos voltado à infraestrutura comum, de forma que estas informações possam ser usadas como facilitador para estudos posteriores e aplicações práticas.

1.5 Objetivo Geral

O objetivo geral desta pesquisa é realizar um diagnóstico da infraestrutura de tecnologia da informação, levantando riscos de tecnologia da informação aos quais a infraestrutura comum aos *campi* do IFB está sujeita, proporcionando as bases, um ponto de partida, para um plano de gerenciamento de riscos.

1.5.1 Objetivos Específicos

Os seguintes objetivos específicos apoiarão a execução do objetivo geral:

a) Analisar a gestão de riscos em outras instituições de ensino;

b) Entender o contexto organizacional da instituição;

c) Analisar seu estado atual de gestão de riscos;

d) Identificar os principais riscos associados à infraestrutura de tecnologia da informação comum aos *campi* da instituição;

e) Avaliar os principais riscos associados à infraestrutura de tecnologia da informação comum aos *campi* da instituição;

f) Propor uma validação para os riscos identificados na pesquisa.

1.5.2 Limitações da Pesquisa

Esta pesquisa não objetiva elaborar, estabelecer ou executar todo um plano de gerenciamento de riscos no IFB, se limitando a alguns dos passos iniciais necessários para o estabelecimento deste processo, a saber: o estabelecimento de contexto e levantamento inicial dos riscos, bem como sua priorização. A Figura 1.1 mostra as áreas de confluência entre o escopo da pesquisa e o processo de gestão de riscos definido na ISO 31000.

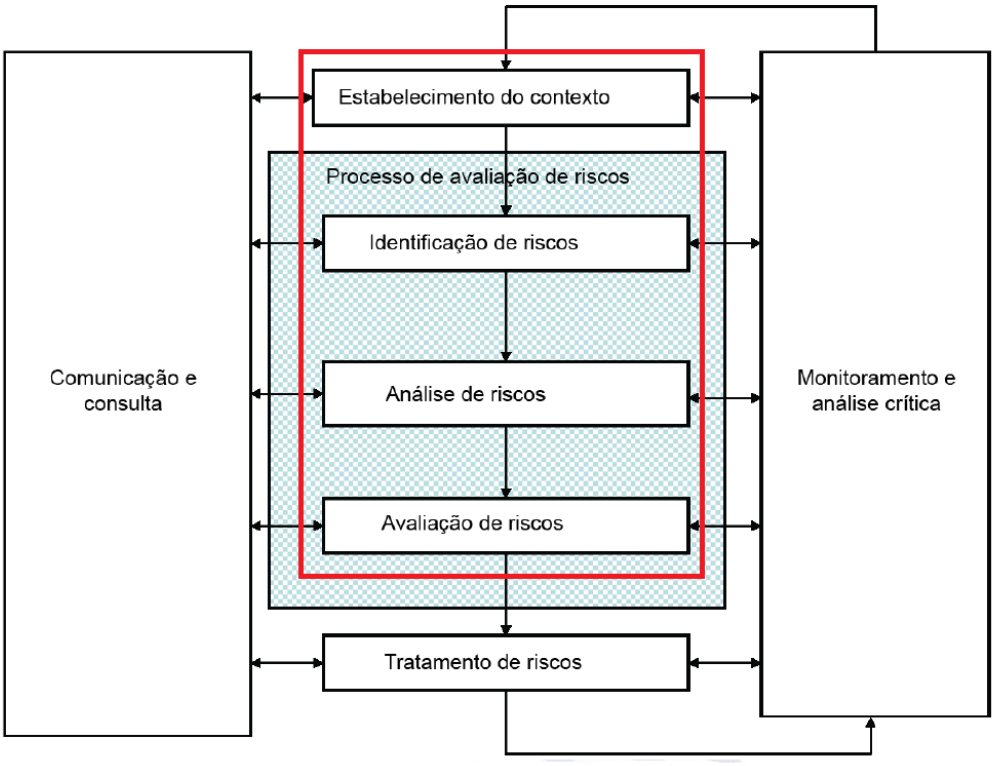


Figura 1.1: Limitação da Pesquisa de Acordo com o Processo de Gestão de Riscos definido na ISO 31000
Adaptado de: [59]

Visando estabelecer um ponto de partida através do levantamento de riscos, a pesquisa não se destina a realizar o tratamento ou estudar a fundo as causas dos mesmos, sendo que uma vez levantados, têm-se o ponto de partida esperado.

O foco da pesquisa é na infraestrutura presente nos *campi* e seus serviços principais que funcionam como ponte de acesso a outros serviços. Portanto estarão excluídos os riscos que não se encaixam nesta categoria, como desenvolvimento de *software*.

Onde aplicável, informações podem estar presentes apenas parcialmente para preservar a identidade dos entrevistados. O mesmo pode ocorrer para cumprir requisitos de segurança da informação, incluindo mas não limitado a nomes, modelos ou versões de *softwares* e equipamentos.

1.6 Estrutura da Dissertação

Esta seção apresenta a estrutura da dissertação, transpondo a forma como a pesquisa está estruturada e como seus resultados estão compilados.

O Capítulo 1 consiste de uma introdução geral à pesquisa, apresentando o problema, justificativa, objetivos e resultados esperados.

O Capítulo 2 consiste de uma revisão de literatura, apresentando o estado da arte nos temas abordados, definindo e explicando conceitos que serão apresentados no decorrer da pesquisa ou que serão fundamentais para o seu entendimento.

O Capítulo 3 apresenta a metodologia da pesquisa, detalhando os métodos utilizados e sua estrutura.

O Capítulo 4 analisa outras instituições de ensino no tocante à gestão de riscos.

O Capítulo 5 apresenta a organização e seu contexto interno e externo, sua estrutura e funcionamento bem como sua missão e valores.

O capítulo 6 apresenta a avaliação de riscos nos *campi* do IFB de acordo com a equipe técnica, bem como proposta de validação dos mesmos junto aos usuários.

Por fim, são apresentadas conclusões da pesquisa, bem como sugestões para trabalhos futuros e outras considerações.

Capítulo 2

Revisão da Literatura

Este capítulo revisa conceitos que foram usados no decorrer desta pesquisa ou necessários para o seu entendimento. Seu objetivo é esclarecer dúvidas e servir de introdução a elementos que aparecem no decorrer da pesquisa ou que necessitem de referencial para entendimento, conforme a Figura 2.1.

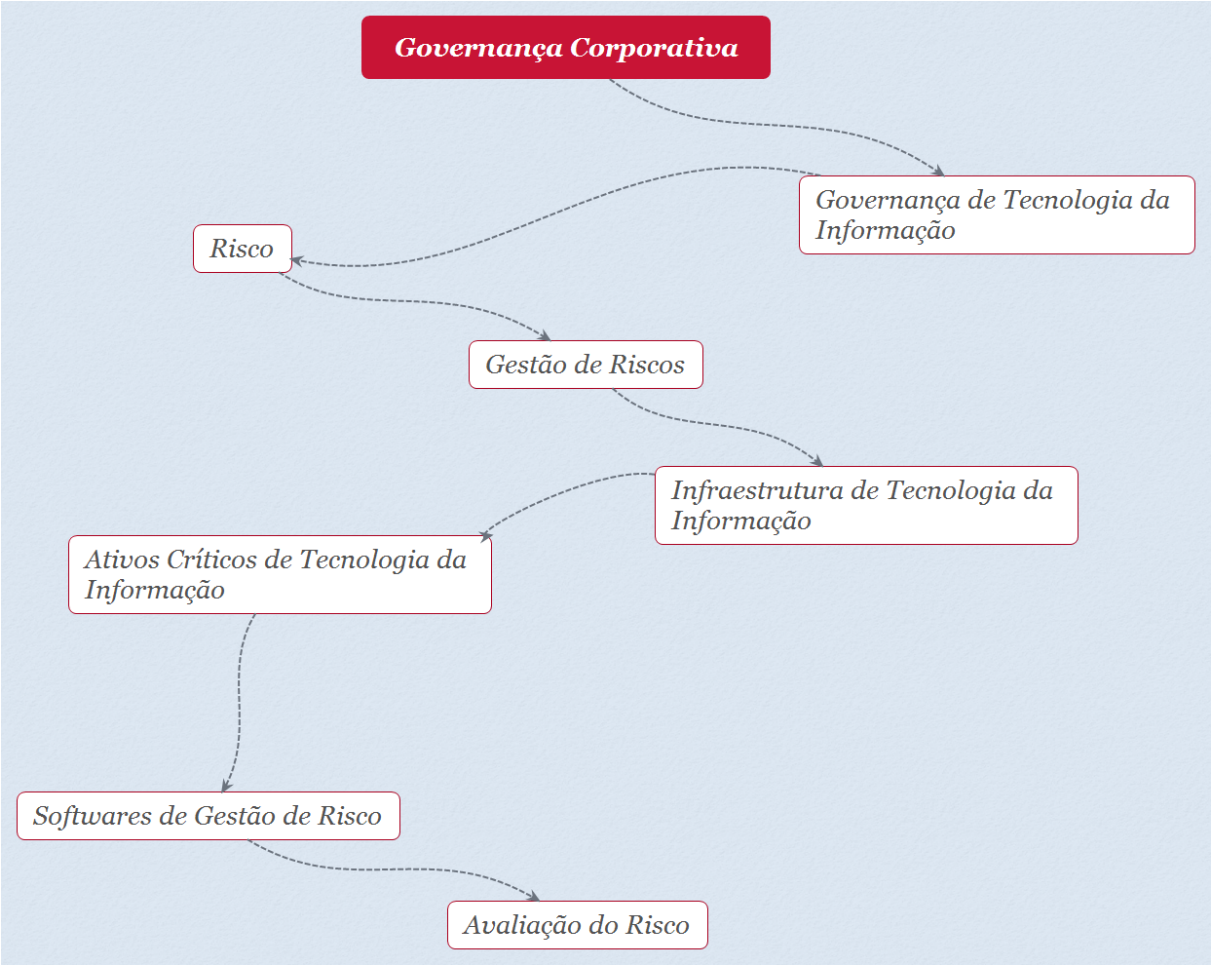


Figura 2.1: Elementos da Revisão de Literatura

2.1 Governança Corporativa

A evolução das organizações trouxe a separação entre a propriedade e controle, isentando os proprietários de administrar diretamente o negócio e delegando esta tarefa para terceiros. Naturalmente por existir conflito de interesse, se tornou relevante desenvolver mecanismos de controle para garantir o cumprimento da missão e o correto funcionamento da organização, culminando no que pode ser chamado de governança.

O termo governança corporativa surgiu nos últimos 20 anos [63] e diz respeito às relações entre a direção e os interessados de uma organização, fornecendo a estrutura pela qual os objetivos da organização são definidos e os meios para alcançar esses objetivos, bem como a monitoração e o desempenho são determinados [48].

A governança não é exclusiva da iniciativa privada. A administração de um país é executada através de um emaranhado composto por diversas organizações, sendo que tais organizações possuem seus objetivos, estrutura, pessoal, orçamento, entre outros. Assim a governança pode ser aplicável também a essas organizações. Segundo a Organisation for Economic Co-operation and Development (OECD) [29], governança pública pode ser entendida como o conjunto dos mecanismos destinados à avaliação, direção e monitoramento de organizações públicas.

Considerando o crescimento da tecnologia da informação nas organizações, uma porção da governança específica para a área de tecnologia ganhou força, a governança de tecnologia da informação.

2.2 Governança de Tecnologia da Informação

A governança de tecnologia da informação inclui os mecanismos para controle e monitoramento da área tecnológica das organizações. É uma das responsabilidades da alta direção e parte integral da governança corporativa, constituindo a liderança, estrutura organizacional e processos para garantir que a tecnologia da informação da organização suporte e estenda os objetivos e estratégias da organização [38].

A governança de tecnologia da informação pode ser considerada estratégica para as organizações que dependem de tecnologia de forma considerável, o que, no século XXI, inclui grande parte das organizações privadas e públicas. A presença de governança não é um fator que garanta sucesso na organização, mas é um fator relevante na redução dos riscos aos quais a organização está sujeita.

2.3 Risco

O estudo do risco pode ser associado inicialmente à área financeira, sendo que um dos trabalhos pioneiros foi o de seleção de carteiras de investimento feito por Markowitz em 1952, que salientou a necessidade de se preocupar tanto com retorno esperado como com variância, sendo que risco poderia ser definido como a variância do retorno [46].

As organizações executam diversas atividades, visando alcançar objetivos ou cumprir uma missão, contando com força de trabalho, capital e infraestrutura para isso. O risco pode ser entendido como um evento ou condição incerta que, ocorrendo, tem efeito positivo ou negativo sobre os objetivos [40]. Portanto, o risco pode ser considerado o "efeito da incerta nos objetivos" [59].

Esta incerteza pode dizer respeito a circunstâncias específicas. O risco poderia ser definido então como um conjunto particular de circunstâncias que, se ocorrerem, podem afetar adversamente a organização, como a exposição a perdas financeiras, perda de reputação ou a falha em entregar projetos ou políticas de forma econômica, eficiência ou efetiva [4].

O risco pode ser definido através de duas variáveis, uma com relação à possibilidade de um evento ou exposição ocorrer que resultaria em danos (probabilidade) e o nível de danos ou prejuízos resultantes do dano ou exposição (impacto) [45]. Estas duas variáveis podem ser multiplicadas para se obter um valor para o risco.

A Tabela 2.1 contém uma matriz de risco, com descrição para as categorias de probabilidade e impacto.

Tabela 2.1: Matriz de Avaliação de Riscos

	Probabilidade e Valores				
Impacto e Valores	**Muito Baixo (1)**	**Baixo (2)**	**Média (3)**	**Alto (4)**	**Muito Alto (5)**
Muito alto (5)	5	10	15	20	25
Alto (4)	4	8	12	16	20
Média (3)	3	6	9	12	15
Baixo	2	4	6	8	10
Muito Baixo (1)	1	2	3	4	5

Descrições da probabilidade de exposição ou incidente

Muito Baixa ou Inexistente: Improvável de acontecer

Baixa: Remota, mas pode ocorrer

Média: Pode ocorrer algumas vezes

Alta: Pode ocorrer várias vezes

Muito Alta: Frequente, pode ocorrer repetidamente

Descrições do impacto de exposição ou incidente

Muito Baixo: Negligível - Dano insignificante ou inexistente

Baixo : Mínimo - Dano mínimo, degradação mínima da missão

Médio: Mediano - Degradação da missão, exposição de dados ou similares

Alto: Crítico - Falha grande no sistema, exposição de dados confidenciais ou similares

Muito Alto : Catastrófico - Colapso do sistema, completa falha na missão, morte ou similares

Adaptado de: [45]

Embora o termo probabilidade, traduzido do inglês “probability”, apareça, no contexto da pesquisa o termo não diz respeito à proposição matemática, e sim à percepção do usuário em relação à quantidade de vezes que o evento pode ocorrer. A palavra “perspectiva” e mesmo “repetição” poderiam substituir o termo. Conforme pode ser visto na Tabela 2.1, o risco foi calculado, ou classificado, de acordo com duas variáveis que representam a percepção qualitativa do usuário em relação à repetição do evento bem como a extensão de suas consequências, sendo que tais escalas são representadas por valores.

O valor do risco pode indicar ações diferentes a serem tomadas. A Tabela 2.2 indica as ações corretivas a serem tomadas dependendo do valor do risco.

Tabela 2.2: Ações a Serem Tomadas Baseadas no Peso do Risco

Valor do Risco	**Categoria**
Menor que 4	Categoria 1: Ação corretiva é discricionária
4 a 8	Categoria 2: Ação corretiva a ser tomada em momento adequado
9 a 14	Categoria 3: Ação corretiva deve ter alta prioridade
15 ou mais	Categoria 4: Operação não permitida ou ação imediata necessária

Adaptado de: [45]

O estudo sobre risco cresceu desde Markowitz e recebeu diversas contribuições, resultando em uma área de estudo específica de gerenciamento de riscos.

2.4 Gestão de Riscos

As organizações estão sujeitas a riscos. Quanto maiores, complexas, demoradas e caras forem suas atividades e objetivos, maior pode ser a frequência de riscos a que estão expostas, bem como a intensidade dos impactos de sua possível concretização. Assim cabe às organizações tomar medidas para identificá-los e tomar ações corretivas antes que aconteçam, realizando o gerenciamento de riscos.

Pode não ser possível ou desejável mitigar todos os riscos de uma organização [28]. Existe a questão do custo-benefício e ainda a relevância do risco. A aplicação de técnicas e quantificação gera informações para tomada de decisão em relação aos riscos. Desta forma, o gerenciamento de risco pode ser entendido também como a maneira pela qual as organizações ativamente escolhem quais riscos querem correr [14].

Melhores práticas são práticas difundidas e aceitas amplamente como guia ou referência. Podem ser definidas como “uma forma otimizada reconhecida pela indústria para alcançar um objetivo ou finalidade declarada” [39]. A ISO 31000 e seu complemento,

a ISO 31010, são exemplos de melhores práticas de gestão de riscos de tecnologia da informação.

2.4.1 ABNT NBR ISO 31000

A ANBT NBR ISO 31000 é uma norma que oferece princípios e diretrizes genéricas para o gerenciamento de riscos e pode ser usada por qualquer empresa, para qualquer tipo de risco [59]. A sua aplicação principal será servir de guia geral para o estabelecimento de contexto de gerenciamento de riscos, bem como servir de norteadora para o processo de gerenciamento de riscos.

A Figura 2.2 mostra os processos de gestão de riscos segundo a ISO 31000.

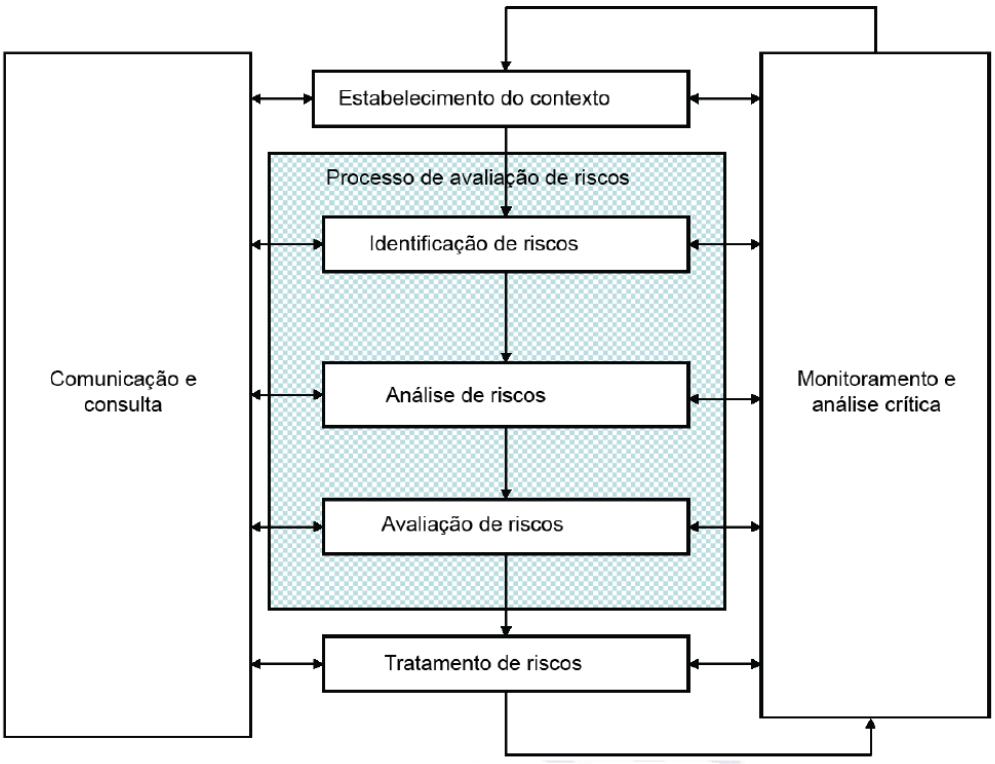


Figura 2.2: Processo de Gestão de Riscos
Adaptado de: [59]

2.4.2 ABNT NBR ISO 31010

A ANBT NBR ISO 31010 fornece apoio à ANBT NBR ISO 31000 no tocante à seleção e aplicação de técnicas sistemáticas na avaliação do risco. A avaliação de risco permite agregar informações que advenham de evidência e análise para escolha e tomada de decisão [60]. Será utilizada no contexto da organização como referência para seleção das

técnicas recomendadas. A Tabela 2.3 apresenta as ferramentas descritas na norma e sua aplicabilidade no processo de avaliação de riscos.

Tabela 2.3: Aplicabilidade das Ferramentas Utilizadas para o Processo de Avaliação de Riscos

Ferramentas e Técnicas	**Identificação de Riscos**	**Impacto**	**Probabilidade**	**Nível de Risco**	**Avaliação de Riscos**
Brainstorming	FA	NA	NA	NA	NA
Entrevistas estruturadas ou semi-estruturadas	FA	NA	NA	NA	NA
Delphi	FA	NA	NA	NA	NA
Lista de verificação	FA	NA	NA	NA	NA
Análise preliminar de perigos (APP)	FA	NA	NA	NA	NA
Estudo de perigos e operabilidade (HAZOP)	FA	FA	A	A	A
Análise de perigos e pontos críticos de controle (APPCC)	FA	FA	NA	NA	FA
Avaliação de risco ambiental	FA	FA	FA	FA	FA
Técnica estruturada “e se” (SWIFT)	FA	FA	FA	FA	FA
Análise de cenários	FA	FA	A	A	A

FA - Fortemente aplicável NA - Não Aplicável A - Aplicável

Tabela 2.3 Aplicabilidade das Ferramentas Utilizadas para o Processo de Avaliação de Riscos (continuação)

Ferramentas e Técnicas	**Identificação de Riscos**	**Impacto**	**Probabilidade**	**Nível de Risco**	**Avaliação de Riscos**
Análise de impactos no negócio	A	FA	A	A	A
Análise de causa-raiz	NA	FA	FA	FA	FA
Análise de modos de falha e controle	FA	FA	FA	FA	FA
Análise de árvore de falhas	A	NA	FA	A	A
Análise de árvore de eventos	A	FA	A	A	NA
Análise causa e consequência	A	FA	FA	A	A
Análise de causa e efeito	FA	FA	NA	NA	NA
Análise de camadas de proteção (LOPA)	A	FA	A	A	NA
Árvore de decisões	NA	FA	FA	A	A
Análise de confiabilidade humana	FA	FA	FA	FA	A
Análise “Bow tie”	NA	A	FA	FA	A
Manutenção centrada em confiabilidade	FA	FA	FA	FA	FA

FA - Fortemente aplicável NA - Não Aplicável A - Aplicável

Tabela 2.3 Aplicabilidade das Ferramentas Utilizadas para o Processo de Avaliação de Riscos (continuação)

Ferramentas e Técnicas	**Identificação de Riscos**	**Impacto**	**Probabilidade**	**Nível de Risco**	**Avaliação de Riscos**
Sneak analysis (SA) e *Sneak circuit analysis (SCA)*	A	NA	NA	NA	NA
Análise de Markov	A	FA	NA	NA	NA
Simulação de Monte Carlo	NA	NA	NA	NA	FA
Estatística Bayesiana e Redes de Bayes	NA	FA	NA	NA	FA
Curvas FN	A	FA	FA	A	FA
Índices de risco	A	FA	FA	A	FA
Matriz de probabilidade e consequência	FA	FA	FA	FA	A
Análise de custo/benefício	A	FA	A	A	A
Análise de decisão por multicritérios (MCDA)	A	FA	A	FA	A

FA - Fortemente aplicável NA - Não Aplicável A - Aplicável

Adaptador de: [60]

Muitas vezes, para implementar melhores práticas, normas internas ou recomendações, podem ser usadas listas de verificação, também conhecidas como *checklists*, na forma de passos a serem executados ou checados para chegar a um fim. Listas de verificação podem ser definidas portanto como uma lista de fatores, propriedades, aspectos, componentes, critérios, tarefas ou dimensões, a presença, referência ou quantidade que devem ser considerados separadamente para realizar determinada tarefa [53]. Fazem parte também das ferramentas definidas na ISO 31010.

Grande parte das organizações possui uma infraestrutura de tecnologia da informação para prover ou suportar serviços, bem como auxiliar no desenvolvimento das mais diversas tarefas. Esta infraestrutura também está sujeita a riscos, sendo que estes riscos também podem ser administrados através do processo de gestão de riscos.

2.5 Infraestrutura de Tecnologia da Informação

A infraestrutura compreende aspectos físicos, processuais e humanos de uma organização. Brockway e Mckay foram precursores na definição de infraestrutura de tecnologia da informação [47]. Segundo eles, a infraestrutura poderia ser considerada o conjunto composto por componentes de tecnologia (computadores, impressoras, sistemas operacionais etc.), recursos humanos (incluindo conhecimentos, habilidades, políticas e experiência necessária) e serviços de tecnologia da informação compartilhados (incluindo serviços estáveis ao longo do tempo, como o gerenciamento de bases de dados compartilhadas) [11].

A Figura 2.3 mostra os elementos da infraestrutura de tecnologia da informação.

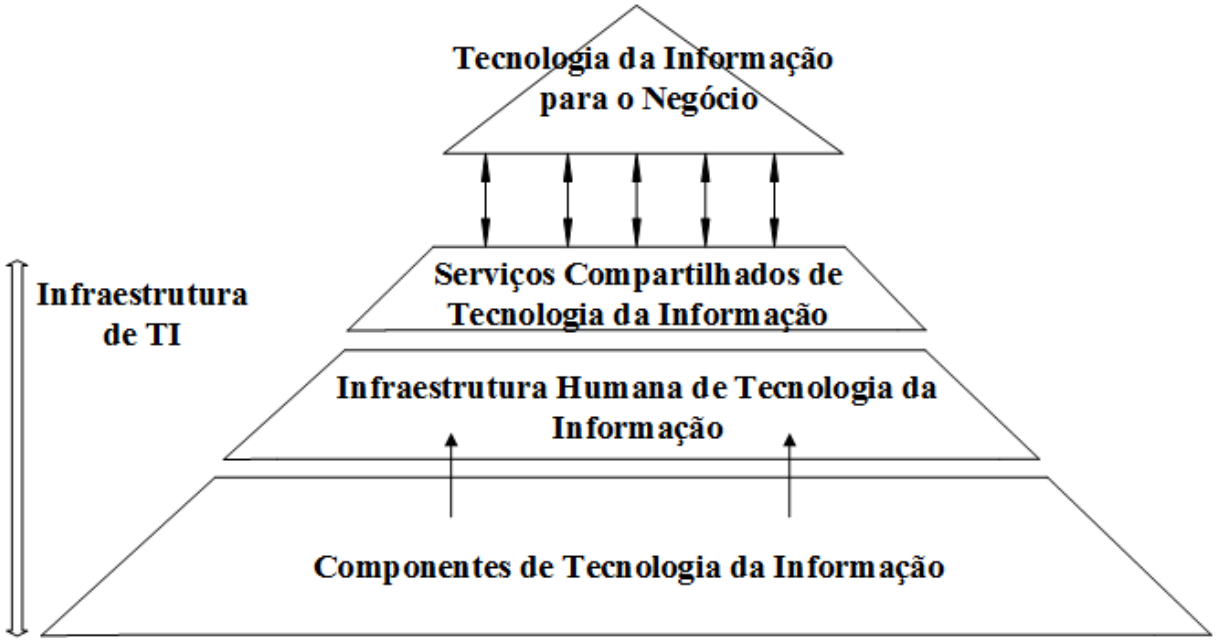


Figura 2.3: Elementos da Infraestrutura de Tecnologia da Informação Adaptado de: [11] [47]

Hardware de computador pode ser definido como o conjunto de elementos tangíveis do computador. São todos os componentes físicos que compõe o sistema computacional, desde a CPU até a memória, e dispositivos de entrada e saída [12].

Programa pode ser considerado o conjunto de instruções que executam tarefas através de instruções de *hardware*. *Software* pode ser considerado o conjunto de programas executáveis em um computador de qualquer porte ou arquitetura [50], sua documentação associada e dados de configuração para fazer com que os programas operem corretamente [56].

Computadores *desktops* são os populares computadores destinados aos usuários em geral, sejam domésticos ou corporativos. Sua ênfase está em entregar boa performance a um usuário por vez com um custo baixo, executando *softwares* de terceiros [31]. *Notebooks* são basicamente computadores em um acondicionamento menor, tendo essencialmente os mesmos componentes de *hardware* de um computador comum, mas em tamanho reduzido [58].

Servidores são computadores pensados para a entrega de serviços específicos para vários usuários ou computadores de forma simultânea, sendo destinados a suportar grande carga de trabalho. São construídos a partir da mesma estrutura básica dos *desktops*, mas permitem maior expansão do poder computacional e da entrada e saída, tendo também ênfase na dependabilidade [31].

Datacenter pode ser considerado a parte central de uma infraestrutura de tecnologia de uma organização. Normalmente se referem a salas ou prédios desenhados para lidar com as necessidades de energia, resfriamento e redes de um número de servidores. [31].

A informação administrada pela organização e mantida através da infraestrutura também é, em muitos casos, um ativo fundamental para o negócio. Gestão de segurança da informação é o processo de reduzir riscos relativos à informação. A informação e sua segurança pode depender de aspectos específicos da infraestrutura.

Os componentes da infraestrutura constituem um emaranhado de ativos para dar apoio à missão institucional. Alguns desses ativos podem ser considerados indispensáveis, críticos, para o desempenho das atividades da organização.

2.6 Ativos Críticos de Tecnologia da Informação

Ativos de tecnologia da informação podem ser definidos como elementos tangíveis ou intangíveis, recursos ou habilidades que tenham algum valor para a organização [5]. Os ativos podem, portanto, ser classificados em categorias, como informação, pessoas, *hardware*, *software* e instalações.

Os ativos podem ser considerados críticos quando sua divulgação, modificação, destruição ou mau uso podem trazer consequências nocivas à missão e objetivos de unidades da instituição ou da instituição como um todo, ou ainda podem fornecer benefícios não intencionados e não desejados a alguém [65].

A Tabela 2.4 apresenta critérios que podem definir ativos críticos para uma universidade ou instituição similar.

Tabela 2.4: Critérios para Ativos Críticos

Descrição
O ativo é requerido para executar as atividades-fim e de suporte da instituição
O ativo diz respeito a dados sensíveis ou que exijam algum outro tipo de restrição
O ativo é requerido para apoiar o ensino
O ativo é requerido para desempenhar outras atividades essenciais para a missão de uma unidade da instituição

Adaptado de: [65]

A administração de ativos críticos bem como o processo de gestão de riscos pode ser feitos com o apoio de *softwares* especializados.

2.7 *Softwares* de Gestão de Riscos

Esta seção contém alguns *softwares* de avaliação e gerenciamento de riscos. A European Union Agency for Network and Information Security (ENISA) define vários *softwares* de gerenciamento e avaliação de riscos e detalhes das mesmas [21]. Parte desta informação está presente nesta seção.

Callio

Callio Secura 17799 é uma ferramenta *web* com suporte a base de dados desenvolvida pela Callio technologies, tendo origem no Canadá. Oferece suporte à ISO 17999 (atualizada para 27002) e ao BS 7799-2 (precursora da ISO 27001), podendo ser considerado parcialmente desatualizado. Sua primeira versão foi em 2001 e última versão conhecida em 2005. Voltada para a implementação e certificação de um Sistema de Gerenciamento de Segurança da Informação, oferece a opção para identificar vulnerabilidades/ameaças, associá-las a ativos e também sugere lista de ameaças [21][52]. Propõe uma lista flexível de controles baseados na ISO 1799, bem como criar e avaliar diferentes cenários.

A arquitetura para seu funcionamento inclui uma base de dados que pode ser MySQL/SQL Server, e *web server* que pode ser IIS/Apache. Disponível em inglês, francês e espanhol, o preço especificado pela companhia era de 4.495 euros (licença para dois usuário), 6.495 euros (licença para 5 usuários) e 9.995 euros (licença para 10 usuários). Voltado para o governo, grandes corporações, grandes, médias e pequenas empresas.

Casis

Casis é uma ferramenta desenvolvida pela Aprico Consultants, tendo origem na Bélgica. Pode ser definida como um "Analisador Avançado de Pistas de Auditoria de Segurança" (Advanced Security Audit Trail Analyzer) [21], seu objetivo é analisar arquivos de *log* de diversos sistemas, correlacionando esses dados e gerando alertas de segurança de acordo com regras definidas pelo usuário. Disponível somente em língua inglesa, é voltado para grandes, médias e pequenas empresas.

Control Compliance Suite

Control Compliance Suite 11 Risk Manager é uma ferramenta desenvolvida pela Symantec Corporation, tendo origem nos Estados Unidos. Permite automatização avaliação de infraestrutura de TI, incluindo a descoberta de redes e equipamentos não autorizados, relatórios de configuração de segurança baseado em perfis, entre outros [57], entregando uma visão diferente de risco voltada para os diferentes *stakeholders*. Como funcionalidade adicional, possui suporte a EDI Connectors de terceiros, permitindo importação e exportação de dados. Disponível em várias línguas, incluindo inglês, francês, português, alemão e espanhol, é voltado para o governo, grandes corporações, grandes, pequenas e médias empresas. Seu preço é de 227.330 euros para a licença base de até 500 usuários com 12 meses de suporte.

CloudeAssurance

CloudeAssurance é uma ferramenta desenvolvida pela eFortresses Inc., com origem nos Estados Unidos. Sua primeira versão é de março de 2012, e a versão mais recente de 2014. Voltado para clientes de serviços em nuvem, provedores de serviços em nuvem, auditores de serviços em nuvem e intermediários de serviços em nuvem - incluindo integradores, plataformas de *big data*, vendedores de seguro e financiadores [20]. É uma solução de *software* como serviço, sendo uma plataforma de avaliação de segurança de serviços em nuvens, *benchmarking*, monitoramento e educação. Disponível em língua inglesa. Compatível com diversos padrões, incluindo ISO/IEC 27001 e ISO/IEC 21827. Voltada para o governo, largas corporações, grandes, pequenas e médias empresas. A ferramenta ajuda

a organização à obtenção de certificação em diversos padrões, incluindo CAAP Validation (Cloud Security Validation) e ISO/IEC 27001.

Cobra

Cobra é uma ferramenta desenvolvida pela C&A Systems Security, com origem no Reino Unido e cobertura local. É uma aplicação autônoma. Sua primeira versão foi lançada nos anos 90. Atualmente o produto não está disponível para compra, estando em fase de re-desenvolvimento [54]. Compatível com a ISO 17799, está desatualizado para as versões mais recentes do padrão da ISO. Permite à organização ter foco na segurança de ativos com risco [2]. Relaciona os riscos identificados com implicações para o negócio organização.

CounterMeasures

CounterMeasures é uma ferramenta desenvolvida pela Alion, com origem nos Estados Unidos. Oferece gerenciamento de riscos baseado em dois padrões americanos, US-NIST 800 e OMB Circular A-130 USA, permitindo ao usuário padronizar critérios de avaliação e, através de uma lista de checagem, o *software* determina critérios de conformidade e segurança. A sua versão *enterprise* custa 14.500 dólares. Disponível como aplicação *desktop* e também como aplicação *web*.

O *software* aceita entradas de pessoas com diferentes papéis na organização, e a partir daí calcula a vulnerabilidade e o risco. O fabricante dá o exemplo em que se procura avaliar a segurança de um prédio, no qual é necessário informar ao *software* quais prédios estão próximos, que tipo de janelas o prédio tem, a distância das portas à rua e que tipos de regulação governamental se aplicam ao prédio [1]. Será então gerada informação para tomada de decisão e ações corretivas. O *software* é voltado para o governo e grandes corporações, e está disponível em língua inglesa.

Cramm

Cramm é uma ferramenta desenvolvida pela Insight Consulting, com origem no Reino Unido. A ferramenta implementa o método Cramm desenvolvido pela Insight Consulting, cobrindo todos os três estágios. Possui três versões, CRAMM expert, CRAMM express and BS 7799

A versão expert sai a 2.950 libras esterlinas por cópia mais 875 libras esterlinas de licença anual. Voltada para o governo, agências, grandes, pequenas e médias empresas.

EAR / PILAR

EAR / PILAR se refere a dois *softwares*, sendo que EAR é uma versão comercial e PILAR é uma versão restrita para administração pública da Espanha (sendo patrocinado pela agência de segurança nacional espanhola), desenvolvidos por A.L.H. J. Mañas. Implementa e expande a Metodologia Magerit. Voltado para o governo, agências, grandes, médias e pequenas empresas. Disponível em inglês, francês, espanhol e italiano, sua última versão comercial é de 2016.

Ebios

Ebios é uma ferramenta desenvolvida pela Divisão Central de Sistemas de Segurança na Informação da França. Foi desenvolvido para dar suporte ao método Ebios. É uma ferramenta *open source* e livre.

GSTool

GSTool é uma ferramenta desenvolvida pelo Gabinete Federal para a Segurança Federal da Alemanha para dar suporte aos Catálogos de Proteção de Linha de Base de Tecnologia da Informação, que serve como referência para a proteção de ambientes de tecnologia da informação. O *software* consiste em uma aplicação autônoma com suporte a bases de dados. O usuário entra com os dados na aplicação e tem acesso às análises estruturadas. O custo de 21-40 licenças é 23.200 euros.

KRiO

KRiO é um sistema desenvolvido pela SIGEA Sistemas de Protección de la información, com origem na Espanha. É uma ferramenta *web* baseada na ISO 31000 que permite a análise de múltiplos cenários de risco, incluindo riscos financeiros, tecnológicos, operacionais, ambientais, regulatórios e de reputação. Disponível em espanhol, inglês e português, a ferramenta tem conformidade com os padrões ISO/IEC27001, ISO/IEC 27002, ISO 9001, ISO 14001, ISO 22301, ISO 19600, ISO 28000 e ISO 50001.

ISAMM

ISAMM tool é uma ferramenta desenvolvida por Telindus N.V., com origem na Bélgica. É uma ferramenta para análise e monitoramento de segurança da informação, seguindo as informações da ISO/IEC 27002, tendo uma abordagem voltada a ativos. Sua versão mais recente é de 2008, estando disponível em língua inglesa.

Mehari 2010 basic tool

Mehari 2010 basic tool é uma ferramenta livre desenvolvida pelo Club de la Sécurité de l'Information Français, com origem na França. Consiste em uma planilha eletrônica preenchível. Contém múltiplas fórmulas, permitindo a visualização passo-a-passo do resultado das atividades de gerenciamento de riscos.

MIGRA Tool

MIGRA Tool é uma ferramenta *web* desenvolvida pela AMTEC/Elsag Datamat S.p.A., com origem na Itália. É uma ferramenta baseada na metodologia MIGRA. É voltado para desenvolver e manter um sistema de proteção, com referências a ativos tangíveis e de informação. Tem cinco grandes módulos, entre eles a base de conhecimento, em conformidade com ISO 27001, a modelagem de cenário, o módulo de análise e conformidade de risco, o módulo para cenários "what if"(e se) e o módulo de relatórios. O preço do *software* varia de acordo com o tamanho da empresa, começando em 30 mil euros. Está disponível em inglês e italiano.

Modulo Risk Manager

Modulo Risk Manager é uma ferramenta desenvolvida pela Modulo Security, com origem no Brasil. Coleta dados sobre ativos físicos, pessoas, processos e instalações físicas. Possui base de conhecimento para ajudar as organizações a atingir conformidade com diversos padrões, entre eles a ISO 27001. Produz diversos relatórios de conformidade.

Octave

Octave Automated Tool é uma ferramenta desenvolvida pelo Advanced Technology Institute, com origem nos Estados Unidos. É uma aplicação independente com acesso à base de dados. A ferramenta implementa as metodologias Octave e Octave-S. Auxilia o usuário a coletar dados, organizar informações e produzir relatórios. Está disponível em inglês.

Proteus

Proteus é uma ferramenta desenvolvia pela Information Governance Limited, com origem nos Reino Unido. É uma aplicação *web* que permite às organizações implementar várias regulações ou padrões (como a ISO 27001). Disponível em inglês, francês, espanhol, japonês e chinês.

Ra2

Ra2 é uma ferramenta desenvolvida pela AEXIS, com origem na Alemanha. É uma aplicação independente voltada para o gerenciamento de riscos baseado na ISO 17799 e ISO 27001. A ferramenta permite seguir todos os passos descritos na ISO 27001 para produzir a documentação necessária para o processo de gerenciamento de riscos. Cada passo leva à geração de um relatório. É uma aplicação independente, instalável em um computador. Voltado para largas corporações, grandes, médias e pequenas empresas. A versão solo custa 599 libras esterlinas por ano, e a versão profissional custa 6 mil libras esterlinas por ano.

Real ISMS

Real ISMS é uma ferramenta desenvolvida pela Realiso, com origem nos Estados Unidos. É uma ferramenta *web* para gerenciar riscos, controles, e objetivos de controles baseada na ISO 27001. Disponível em língua inglesa, custando 49 dólares por mês.

Resolver*Ballot

Resolver*Ballot é uma ferramenta desenvolvida pela Resolver, com origem no Canada. É uma aplicação independente voltada para avaliação de riscos em grupo, em que os participantes podem dar sua opinião anonimamente sobre a probabilidade e impacto dos riscos na organização. Voltado para o governo, agências, grandes corporações, grandes, médias e pequenas empresas. Disponível em língua inglesa, sendo que a licença para cinco usuários válida por três anos custa 15 mil dólares canadenses.

Resolver*Risk

Resolver*Risk, assim como Resolver*Ballot, é uma ferramenta desenvolvida pela Resolver, com origem no Canada e disponível em língua inglesa. Consiste de uma plataforma *web* voltada para ações corretivas, relatórios e funcionando como base de dados para conformidade, gerenciamento de riscos e governança. Configurável para refletir regulações ou melhores práticas. A licença anual para três usuários custa 15 mil dólares canadenses.

Risicare

Risicare é uma ferramenta desenvolvida pela BUC S.A., com origem na França. É uma aplicação independente destinada à análise de risco e gerenciamento de riscos de acordo com a metodologia Mehari. Condições reais são simuladas e são testadas múltiplas situações ou cenários de ameaça do tipo “e se”, sendo integrável com a ISO 27001 na fase de planejamento. Está disponível em inglês e francês.

Riskwatch

RiskWatch for Information Systems & ISO 17799 é uma ferramenta desenvolvida pela RiskWatch, com origem nos Estados Unidos. Está disponível como aplicação independente e aplicação *web*, e é pra gerenciamento de riscos de sistemas de informação. Inclui controles da ISO 17799 e de regulação específica dos Estados Unidos. Disponível em língua inglesa, com valor de 15 mil dólares.

RM Studio

RM Studio é uma ferramenta desenvolvida pela Stiki – Information Security, com origem na Islândia. É uma aplicação *web* com clientes *desktop* voltada para o gerenciamento de riscos. Inclui importação de dados da organização, bibliotecas de risco (segurança da informação, tecnologia da informação operacional, de projeto, ambiental, estratégico), controles de segurança da ISO/IEC 27001, entre outros. A versão mais recente da ferramenta é de 2016, custando 2.990 euros anualmente, na licença para 3 usuários, com um adicional de 500 euros por usuário. A ferramenta está disponível em inglês, alemão e islandês.

SISMS

Smart Information Security Management System (SISMS) é uma ferramenta desenvolvida pela CYMSOFT BILISIM TEKNOLOJILERI, com origem na Turquia. É uma aplicação *web* para gerenciamento de sistema de segurança da informação destinado a estabelecer, implementar, operar, monitorar, revisar, manter e melhorar o gerenciamento de segurança da informação. Disponível em inglês e turco. Possui um módulo para avaliação de riscos relativos a ativos da informação.

TRICK light

TRICK light é uma ferramenta desenvolvida pela itrust consulting s.à r.l. com origem em Luxemburgo. Consiste de uma aplicação desenvolvida no ambiente VBA do Microsoft Office Excel voltada para gerenciamento e análise riscos seguindo o padrão ISO/IEC 27005. Disponível em inglês e francês, sendo que a última versão do *software* é de 2012.

TRICK Service

TRICK Service, assim como o TRICK Service é uma ferramenta desenvolvida pela itrust consulting s.à r.l. com origem em Luxemburgo. Consiste de uma aplicação *web* voltada para gerenciamento e análise riscos seguindo o padrão ISO/IEC 27005. Disponível em inglês e francês, sendo que a última versão do *software* é de 2015.

Acuity STREAM

Acuity STREAM é uma ferramenta desenvolvida pela Acuity Risk Management LLP, com origem no Reino Unido. É uma aplicação *web* voltada para o gerenciamento de conformidade com padrões, permitindo a importação de vários padrões pelo usuário. Fornece todo o *framework* para um sistema gerenciador de segurança da informação apresentado pela ISO 27000. Disponível em inglês, holandês e russo com a possibilidade de inclusão de outras línguas.

Axur ISMS

Axur ISMS é uma ferramenta desenvolvida pela ISMS Axur Information Security, com origem nos Estados Unidos. É uma aplicação web voltada para o gerenciamento de segurança da informação de acordo com a ISO 27001. Disponível em inglês, custando 995 dólares por mês.

WCK

WCK é uma ferramenta desenvolvida pela WCK, com origem em Israel. Uma Solução de gerenciamento de riscos voltada para cibersegurança, tecnologia da informação e especialmente proteção de infraestrutura crítica, automatizando o ciclo de gerenciamento de riscos. A ferramenta está disponível em inglês, alemão, italiano e hebraico.

A Tabela 2.5 mostra uma comparação entre os softwares de gerenciamento de riscos.

Tabela 2.5: *Softwares* de Gerenciamento de Riscos

Ferramenta	**Análise de Riscos**	**Gerenciamento de Risco**	**Outras Fases**
Callio Secura 17799	Identificação de riscos - identifica vulnerabilidades e ameaças, associa ameaças com ativos, sugere lista de ameaças Análise de riscos - análise e cálculo de riscos	Tratamento de Riscos - Lista Flexível de controle baseada na ISO 17999, criar e avaliar diferentes cenários	Sistema de aprovação de documentos e controle de versão

Tabela 2.5: *Softwares* de Gerenciamento de Riscos (continuação)

Ferramenta	**Análise de Risco**	**Gerenciamento de Risco**	**Outros Tarefas**
Casis			Coleta e analisa dados nativos de auditoria de diversos sistemas e programas
Control Compliance Suite 11 Risk Manager	Identificação de riscos usando padrões técnicos (como ISO 27001 e 27002) ou usando requisitos da própria organização Permite Usar fluxos de trabalho (*workflows*) como operações lógicas para analisar, priorizar e saber onde estão as fraquezas e como tratá-las.	Para o tratamento de riscos, permite definir medidas a serem tomadas, pontuação, tendência e a habilidade de ilustrar como os riscos afetam o processo chave Para a comunicação, permite o estabelecimento de *dashboards* com métricas específicas para cada audiência.	Inventário e avaliação de ativos
CloudeAssurance	Identifica riscos por diversos padrões de segurança e conformidade. Recomendações e base de conhecimento Relatórios de *Benchmarking* e tendências		Avaliação automática de terceiros com relação à cadeia de fornecedores e abastecimento

Tabela 2.5: *Softwares* de Gerenciamento de Riscos (continuação)

Ferramenta	**Análise de Risco**	**Gerenciamento de Risco**	**Outros Tarefas**
Cobra	Identifica ameaças, vulnerabilidades e exposições no sistema Mede o risco para cada área do sistema e como afeta o negócio	Oferece soluções detalhadas e recomendações para reduzir os riscos, bem como relatórios técnicos e de negocio	–
CounterMeasures	Identificação de riscos através de um módulo *survey*/coleta de dados Plataforma de análise de riscos Plataforma de avaliação de riscos	Tratamento e aceitação de riscos - Análise de custo benefício e rastreamento de medidas corretivas	Plano de ação para melhoria da segurança física das instalações
Cramm	Identificação, análise e avaliação de riscos (estágio II do CRAMM)	Tratamento de riscos (estágio III do CRAMM)	Análise de acordo com a BS 7799/ISO 27001
EAR / PILAR	Identificação análise e avaliação de riscos	Evolução da maturidade de políticas e procedimentos Valores potenciais e residuais de risco.	
Ebios	Identificação de riscos (passo 3 e 4 do método Ebios), análise e avaliação de riscos (passo 3 do método Ebios)	Tratamento de riscos (passo 4 e 5 do método Ebios) Aceitação de riscos (passo 4 do método Ebios) Comunicação (relatórios produzidos para cada passo do método Ebios)	Estudo de contexto (passo 1 do método Ebios) Expressão de necessidades de segurança (passo 2 do método Ebios)

Tabela 2.5: *Softwares* de Gerenciamento de Riscos (continuação)

Ferramenta	**Análise de Risco**	**Gerenciamento de Risco**	**Outros Tarefas**
GSTool	Avaliação dos requerimentos de proteção)	Tratamento de riscos (Modelagem de proteção de linha de base, checagem básica de segurança, análise de segurança suplementar) Estimativa de custo, esforço, risco residual	
KRiO	Identificação, análise e avaliação de riscos (ISO 31000 completo)	Processo de avaliação de riscos Processo de aceitação de riscos - definição, seleção e justificativa de controles específicos da ISO Processo de tratamento de riscos - sistema de avaliação de cenários de ameaças e vulnerabilidades) Comunicação (relatórios)	
ISAMM			Avaliação e análise de ativos

Tabela 2.5: *Softwares* de Gerenciamento de Riscos (continuação)

Ferramenta	**Análise de Risco**	**Gerenciamento de Risco**	**Outros Tarefas**
Mehari 2010 basic tool	Identificação de riscos baseada em ativos, ameaças e vulnerabilidades Análise de riscos através de cenários Quantificação dos elementos de riscos	Seriedade do risco dada por probabilidade e impacto Proposta de medidas de segurança para reduzir o risco Opção de aceitar ou transferir o risco	lista proposta de ativos, incluindo serviços, informações e regulações
MIGRA Tool	Identificação, análise e avaliação de riscos	Comunicação de riscos	Modelagem de perímetro de segurança
Modulo Risk Manager	Identificação, análise e avaliação de riscos	Análise de riscos usando estruturas *top-down*, organização de riscos por valores numéricos e mitigação por potencial de redução de risco Sistema de monitoramento para rastrear ações corretivas	Geo-referência de riscos usando Google Earth
Octave Automated Tool	Identificação de Riscos (fase 1 e 2 do Octave), análise de riscos (fase 2 do Octave) e avaliação de riscos (fase 2 do Octave)	Tratamento de riscos (fase 3 do Octave) Aceitação de riscos (fase 2 do Octave)	

Tabela 2.5: *Softwares* de Gerenciamento de Riscos (continuação)

Ferramenta	**Análise de Risco**	**Gerenciamento de Risco**	**Outros Tarefas**
Proteus	Técnicas quantitativas e qualitativas de análise de risco Escalas de risco absoluta e relativas podem ser usadas para adaptar o apetite de risco da organização Suporte a grupo de ativos, ameaças podem ser herdadas via relação de ativos, localização e perfil do ativo	5 processos genéricos mapeáveis para a ISO 27001 ou outras metodologias Planos de ação Trila de auditoria de todas as mudanças do sistema	
Ra2	Lista de Exemplos de vulnerabilidades e ameaças Processo de decisão de risco	Controles sugeridos da ISO 17799 Gerador de relatórios	
REAL ISMS	Identificação, análise e avaliação de riscos	Processo de avaliação, tratamento, aceitação e comunicação de riscos	Gerenciamento de políticas e procedimentos Gerenciamento de incidentes
Resolver*Ballot	Identificação, análise e avaliação de riscos	Processo de avaliação de riscos	Inventário e avaliação de ativos Gerenciamento de projetos Planejamento de ações corretivas

Tabela 2.5: *Softwares* de Gerenciamento de Riscos (continuação)

Ferramenta	**Análise de Risco**	**Gerenciamento de Risco**	**Outros Tarefas**
Resolver*Risk	Identificação, análise e avaliação de riscos.	Processo de avaliação, tratamento, aceitação e comunicação de riscos	Inventário e avaliação de ativos Gerenciamento de projetos Planejamento de ações corretivas
Risicare	Identificação, análise e avaliação de riscos (metodologia Mehari)	Processo de análise, tratamento e comunicação de riscos	
RiskWatch for Information Systems & ISO 17799	Lista pré-definida de ameaças agrupadas por categorias Determinação do impacto financeiro do risco Coleta informações sobre vulnerabilidades	Define detalhes de salvaguarda Cenários “e se”	
RM Studio	Identificação de Riscos (bibliotecas de risco), identificação de riscos por ativo Avaliação de riscos (probabilidade e impacto de riscos)	Processo de avaliação, tratamento, aceitação e comunicação de riscos	Auxílio no desenvolvimento de um plano de continuidade do negócio
Smart Information Security Management System	Identificação, análise e avaliação de riscos	Processo de avaliação, tratamento, aceitação e comunicação de riscos	Determinação do estado de segurança da organização
TRICK light	Identificação, análise e avaliação de riscos (moldado a partir da ISO/IEC 27005)	Processo de análise, tratamento, aceitação e comunicação	Análise de maturidade de medidas de segurança implementadas

Tabela 2.5: *Softwares* de Gerenciamento de Riscos (continuação)

Ferramenta	Análise de Risco	Gerenciamento de Risco	Outros Tarefas
TRICK Service	Identificação, análise e avaliação de riscos	Processo de análise, tratamento, aceitação e comunicação	Análise de maturidade de medidas de segurança implementadas
Acuity STREAM	Identificação, análise e avaliação de riscos	Processo de análise, tratamento, aceitação e comunicação de riscos	Análise de vulnerabilidade (como controles fracos ou faltando) Inventário e avaliação de ativos
Axur ISMS	Identificação, análise e avaliação de riscos	Processo de análise, tratamento, aceitação e comunicação de riscos	Gerenciamento de políticas e procedimentos • Gerenciamento de incidentes
WCK	Identificação, análise e avaliação de riscos	Processo de análise, tratamento, aceitação e comunicação de risco	Análise de dependência e impacto no negócio Análise de conformidade Ciclo de desenvolvimento Continuidade do negócio

Adaptado de: [1] [2] [20] [21][52] [54] [57]

Para o IFB alguns dos *softwares* utilizados poderiam ser adotados. Entre eles, o Control Compliance Suite apresenta um foco voltado para a infraestrutura e segurança de TI, automatizando tarefas e gerenciando ativos, sendo um *software* voltado para gestão de riscos de segurança da informação com ênfase em ativos.

2.8 Avaliação do Risco

Das várias ferramentas analisadas, pode-se notar uma tendência de algumas funcionalidades, com algumas exceções devido ao foco ou natureza da ferramenta. Os passos inicias

envolvem, de uma forma ou de outra, a definição do contexto, identificação dos ativos, o levantamento de ameaças - ou a partir de listas prontas ou de entradas do usuário -, e a avaliação de riscos. Estas funcionalidades ressoam com algumas das melhores práticas previstas na ISO 31000. A avaliação dos riscos pode ser considerada a primeira e mais importante fase da gestão de riscos [66], razão pela qual a maior parte dos *softwares* voltados para gestão de risco, e outros com escopos parecidos implementem esta funcionalidade.

Entretanto, nem sempre usar *softwares* de terceiros para o processo de gerenciamento de riscos pode ser o mais vantajoso para a organização. Em muitos casos existe um custo, ou de compra ou de implantação. Há também a questão das regulamentações internas da organização, da adequação do *software* ao escopo e estrutura da organização e, por fim, às necessidades e capacidades de gestão de riscos da organização. Este levantamento inicial pode ser feito sem auxílio de *softwares* especiais, usando técnicas da ISO 31000, de forma presencial ou eletrônica.

O próximo capítulo apresenta a metodologia a ser usada no desenvolvimento da pesquisa, apresentando conceitos e oferecendo detalhes de sua implementação.

Capítulo 3

Metodologia da Pesquisa

Este capítulo apresenta a metodologia da pesquisa, definindo o método e a estruturação da pesquisa.

3.1 Métodos de Pesquisa

A pesquisa envolveu análise, obtenção e tratamento de informações, buscando realizar um diagnóstico. O uso da metodologia científica auxiliou o cumprimento dos objetivos. A metodologia pode ser entendida como o caminho e os passos a serem seguidos na pesquisa [42]

A pesquisa foi de cunho exploratório. Este tipo de pesquisa tem como objetivo proporcionar maior familiaridade com o tema para tornar sua compreensão mais explícita ou construir hipóteses [27], tendo como estratégia um estudo de caso. O estudo de caso pode ser entendido como um estudo sobre uma entidade bem definida como um programa, instituição, sistema educativo, ou unidade social visando conhecê-lo [22].

A abordagem da pesquisa foi de caráter qualitativo. O tema estudado exigiu a opinião do sujeito da pesquisa, que poderia suscitar algumas questões não mensuráveis. Dessa forma, foi utilizada a pesquisa qualitativa, que abrange aspectos da realidade que não estão sujeitos a quantificação, tendo como centro a explicação da dinâmica das relações sociais [26].

Considerado o tipo de pesquisa para definir as bases propostas, foram usados vários instrumentos de coleta de dados. Foi usado o questionário estruturado, com questões essencialmente abertas, as quais o sujeito respondeu como quis, questões fechadas, as quais o sujeito escolheu dentre as alternativas relacionadas, ou mistas, que incluíram questões abertas e fechadas respondidas pelo questionado [26]. Estes questionários, em situações aplicáveis, foram enviados por e-mail ou outra forma de participação eletrônica. Também foram realizadas entrevistas e observação.

O teste-piloto é um instrumento para identificar pontos fracos na instrumentação ou no projeto utilizando indivíduos da população alvo, sendo que o pré-teste, uma de suas formas, pode basear-se nos representantes dos entrevistados ou neles mesmos, sendo que a opinião dos entrevistados pode ser usada para identificar e mudar perguntas e técnicas confusas, embaraçosas ou ofensivas [13]. Nos casos oportunos, foram usados questionários de pré-teste para melhora do instrumento.

3.2 Estruturação da Pesquisa

Uma visão geral da estrutura da pesquisa é apresentada na Figura 3.1, apresentando também ferramentas utilizadas. A estrutura foi elaborada para alcançar o objetivo geral e objetivos específicos da pesquisa.

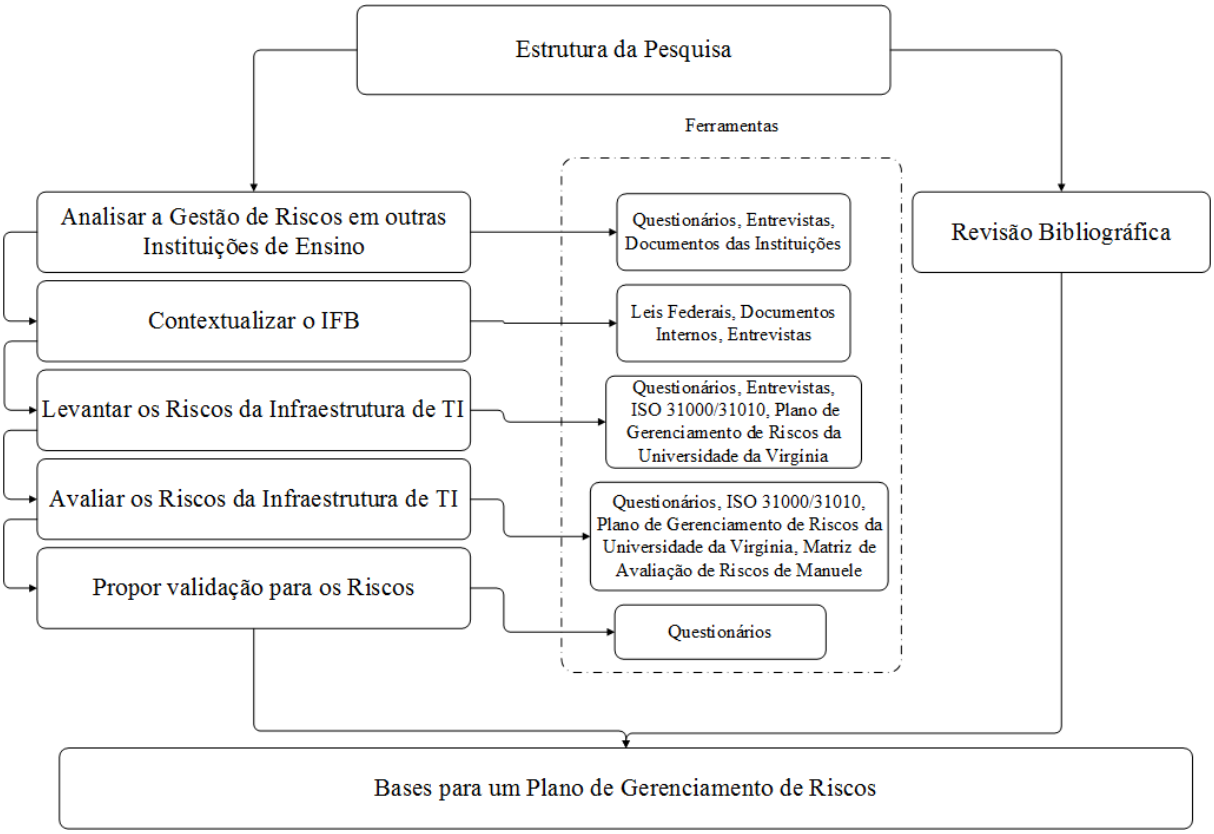


Figura 3.1: Estrutura da Pesquisa

A Tabela 3.1 apresenta as pesquisas realizadas, as instituições alvo, a quantidade de entrevistados ou respondentes e suas funções ou cargos.

Tabela 3.1: Pesquisas Realizadas

Pesquisas	**Instituições**	**Qtd. Entr.**	**Funções ou Cargos**
Gestão de Riscos em Outros Institutos Federais	Institutos Federais	11	Técnicos de Tecnologia da Informação, Analistas de Tecnologia da Informação, Coordenadores
Gestão de Riscos no Centro de Informática (CPD) da Universidade de Brasília (UnB)	CPD da UnB	6	Técnicos de Tecnologia da Informação, Analistas de Tecnologia da Informação, Coordenadores, Diretores, Outros
Visão Geral da Tecnologia da Informação no IFB	Coordenação de Redes do IFB	1	Coordenador
Definição de Ativos Críticos de Tecnologia da Informação da Infraestrutura Comum aos *Campi* do IFB	Coordenação de Redes do IFB	1	Coordenador
Levantamentos de Riscos de Tecnologia da Informação para a Infraestrutura Comum aos *Campi* do IFB	*Campi* do IFB	13	Técnicos de Tecnologia da Informação, Diretores Gerais
Avaliação dos Riscos de Tecnologia da Informação para a Infraestrutura Comum aos *Campi* do IFB	*Campi* do IFB	10	Técnicos de Tecnologia da Informação
Validação dos Riscos de Tecnologia da Informação para a Infraestrutura Comum aos *Campi* do IFB	*Campi* do IFB	77	Diretores Gerais, Diretores, Coordenadores, Cargos Administrativos Diversos

O próximo capítulo apresenta uma breve análise em outras instituições de ensino visando extrair elementos do processo de gestão de risco que poderiam ser aplicadas na avaliação de riscos no IFB.

Capítulo 4

Análise de Outras Instituições

Este capítulo apresenta uma análise da gestão de risco em outras instituições de ensino.

4.1 Universidade da Virgínia

Uma análise dos recursos disponibilizados na internet por universidades nacionais e estrangeiras mostrou que a Universidade da Virgínia (University of Virgia) possui um programa para gerenciamento de riscos relativos à tecnologia da informação. A Universidade da Virgínia tem sede na Virgínia, nos Estados Unidos.

O programa de gerenciamento de riscos da Universidade da Virginia, oficialmente "University of Virginia Information Technology Security Risk Management Program" (Programa de Gerenciamento de Riscos de Segurança de Tecnologia da Informação da Universidade da Virgínia) [65] tem um foco departamental, ou seja, pode ser aplicado para departamentos diferentes, beneficiando o departamento e a Universidade como um todo, conforme declaração no sumário executivo.

Cada departamento pode ter sua infraestrutura de TI e a guarda de equipamentos e informações, podendo portanto ser aplicadas técnicas de gestão de riscos a esses itens.

O plano está dividido em:

- I Suporte Executivo e Declaração de Política.
- II Informação de *Background*.
- III Instruções de Gerenciamento de Riscos e *Templates*:
  - A Visão Geral do Processo.
  - B Análise de Impacto na Missão de TI.
  - C Avaliação de Riscos de TI.

- D Plano de Continuidade da Missão de TI.

- E Avaliação e Reavaliação.

- F Requisitos de Relatório.

- IV Apêndices.

O plano tem várias áreas que tiveram origem ou fazem uso de listas de verificação. Uma das origens das questões de avaliação de riscos é uma lista de verificação interna do Departamento de Segurança da Informação da Universidade. Na seção C do item III é apresentada uma lista de verificação para cenários comuns de ameaça, e a seção D do item III possui uma lista de verificação simples para recuperação de desastres. A presença das listas de verificação no plano da Universidade demonstra atenção voltada para este método que é simples, mas que pode retornar resultados positivos. O Plano também contém modelos prontos de cenários de ameaça e vulnerabilidade.

O plano de gerenciamento de risco da Universidade da Virgínia mostra ser o produto da experiência com situações reais e também de aplicação de melhores práticas. Para os efeitos desta pesquisa, algumas questões do gerenciamento de riscos foram usadas bem como recomendações gerais.

A Tabela 4.1 é um excerto dos cenários de vulnerabilidade, ataque e risco disponíveis na seção C do item III. Faz parte dos modelos de avaliação de riscos baseado em ameaças e contém um cenário de ameaça ou vulnerabilidade em que é feito o uso de dispositivos "black box", dispositivos em que não é possível fazer *upgrades*. É apresentada também uma lista de verificação de estratégias a serem tomadas.

Tabela 4.1: Modelo de Avaliação de Riscos para Dispositivos do Tipo *Black Box* com Lista de Verificação de Estratégias

Ameaça Potencial, Ataque ou Vulnerabilidade	**Ativos Afetados Identificados do Departamento**	**Estratégias Identificadas do Departamento**
B. Dispositivos Caixa-preta (Black Box) - sistemas não atualizáveis, muitas vezes não permitindo mudança de senhas Considerar estes ativos: - Dispositivos especializados com interface *Web* (por exemplo, módulos de controle de instalações) - Dispositivos "inteligentes" na rede que não são computadores; dispositivos habilitados para *web* - Dispositivos de engenharia		☐ Contratos públicos permitindo substituição conforme necessário ☐ Remover dispositivos de redes abertas ☐ Plano de contingência para peças e migração de emergência ☐ Investigar caminho de atualização ☐ _____ ☐ _____

Adaptado de: [65]

O conteúdo do plano foi parcialmente usado para elaborar o questionário de risco destinado a outros IFs, e, identificada a falta de referência de gestão de riscos nas instituições federais do DF e também de alguns IFs, foi usado parcialmente como referência para elaboração da avaliação de riscos no IFB.

4.2 Governança e Gestão de Riscos em Institutos Federais

Foram pesquisados outros Institutos Federais para entender sobre o processo de gestão de riscos e governança nestas instituições similares. O Apêndice A contém o questionário geral e o Apêndice B contém a compilação dos dados obtidos presencialmente.

A intenção principal do questionário foi entender um pouco mais sobre algumas tendências de tecnologia da informação que podem ocorrer na rede dos IFs e identificar a presença de gestão de riscos documentada nestes. Por fim, havendo uma documentação de gestão de riscos bem definida, seria feita uma análise destas documentações para possível aplicação na pesquisa de gestão de riscos voltada para o IFB. O questionário abordou questões de governança, capacitação, e também cenários comuns de vulnerabilidades de TI, incorporando elementos da ISO 31000, do Plano de Gerenciamento de Riscos da Universidade da Virgínia e do Questionário de Governança de TI [64], bem como situações problemáticas também encontradas no IFB. Foram apresentadas questões fechadas e questões abertas para os usuários.

Existem 38 IFs previsto na lei 11892 [8]. Pela dispersão física dos mesmos no território nacional e pelo tempo a ser despendido, não se mostrou viável fazer uma pesquisa ostensiva em todos eles. O contato eletrônico com a área de tecnologia da informação dos mais diversos órgãos através de *e-mails* também não se mostrou frutífero. Desta forma foi feita a opção de aplicação de questionário de forma presencial, aproveitando evento voltado para capacitação *stricto sensu* de funcionários de tecnologia da informação dos IFs na Universidade Federal de Pernambuco (UFPE) em 2015.

Participaram da pesquisa 11 funcionários de IFs diferentes, abrangendo portanto 11 institutos. As perguntas foram respondias por Técnicos de Tecnologia da Informação e Analistas de Tecnologia da Informação, sendo um respondente de cada instituto. Como um dos objetivos foi a tentativa de importação de uma eventual documentação de gerenciamento de riscos, o IFB não foi incluído nesta pesquisa. Embora esta não possa ser considerada uma pesquisa exaustiva, uma vez que abordou somente 11 de um total de 38 institutos federais, a pesquisa fornece dados valiosos no entendimento de determinadas tendências e na identificação de um plano de gerenciamento de riscos que pudesse ser importado para uso na pesquisa.

Participaram Técnicos de Tecnologia da Informação e Analistas de Tecnologia da Informação. Houve uma participação maior de Analistas, conforme Figura 4.1. Mas diferentemente do que ocorre no IFB, em que os Analistas estão concentrados na reitoria, outros IFs mostraram lotação de Analistas nos *campi*.

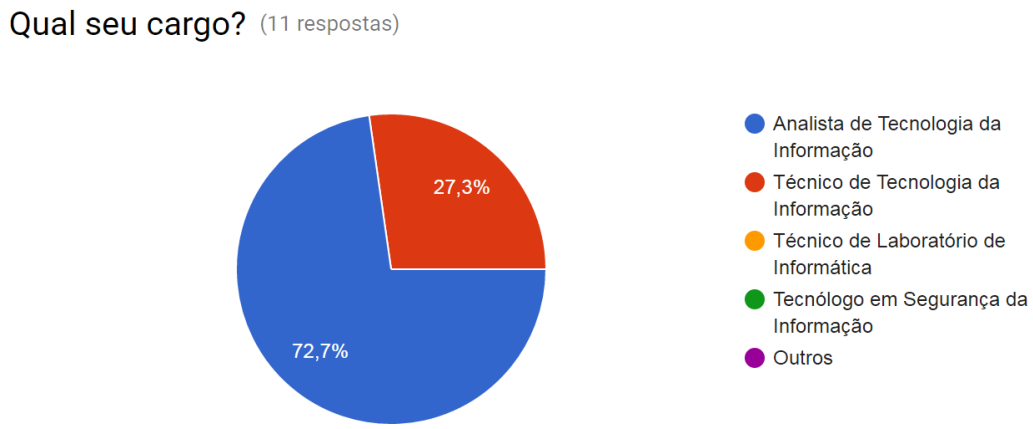


Figura 4.1: Análise dos IFs - Cargo dos Profissionais de TI

A Figura 4.2 mostra a distribuição por local de trabalho dos Técnicos e Analistas. Pouco mais da metade dos entrevistados informaram trabalhar em um *campus*, enquanto o restante informou trabalhar na reitoria. Entre os oito Analistas de Tecnologia da Informação, metade informou trabalhar em *campus*, diferentemente do IFB, em que analistas estão lotados somente na reitoria.

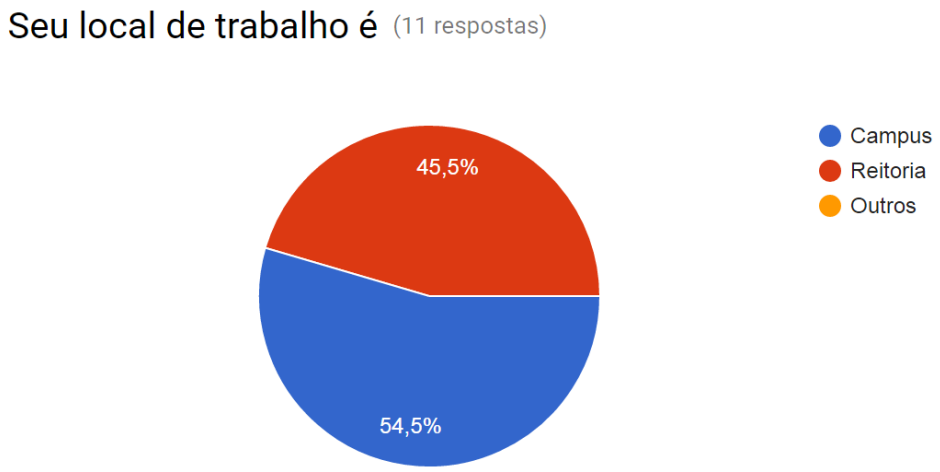


Figura 4.2: Análise dos IFs - Local de Trabalho dos Profissionais de TI

Entre os respondentes, 54,5% dos entrevistados identificaram ocupar algum cargo comissionado ou função gratificada, tendo um perfil técnico mas também de líderes de

equipe. A porcentagem é idêntica à de local de trabalho. Conforme Figura 4.3, a maior parte dos participantes informou que suas atribuições não estavam bem definidas. A atribuição dos cargos pode se mostrar um problema, pois espera-se da tecnologia da informação intervenção em diversas áreas diferentes, mas existe a dependência em relação ao que cada profissional foi contratado para fazer.

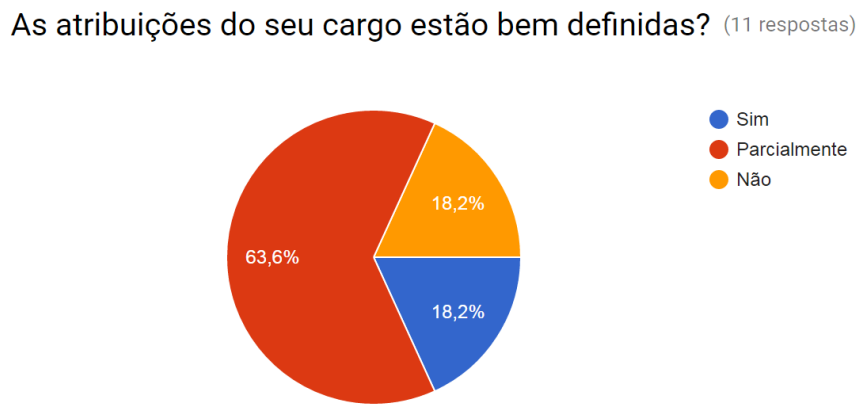


Figura 4.3: Análise dos IFs - Clareza nas Atribuições do Cargo

Quanto à área de atuação, os profissionais foram convidados a marcar uma ou mais opões de atuação, entre desenvolvimento, infraestrutura, suporte e governança. A área que mais participantes identificaram como sua área de atuação foi a de infraestrutura, conforme a Figura 4.4.

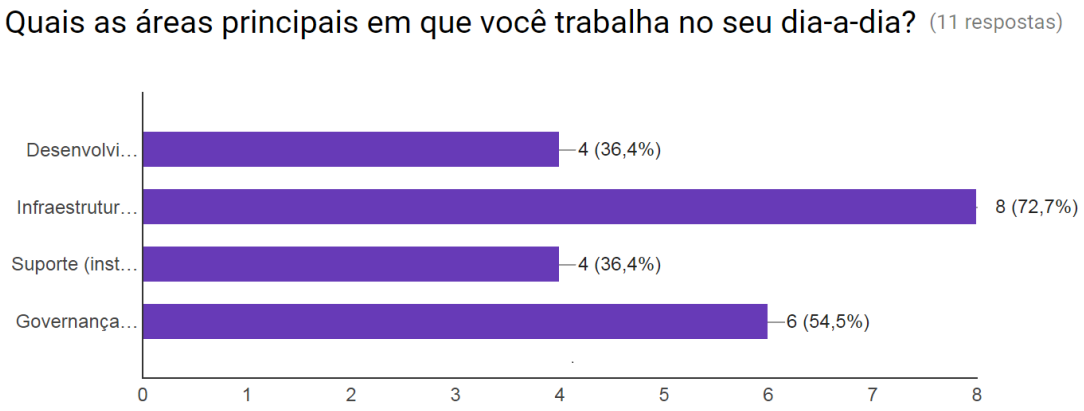


Figura 4.4: Análise dos IFs - Área de Atuação

A capacitação, especialmente na TI é importante, uma vez que se faz uso de tecnologias que estão sempre mudando e evoluindo. Mais de 70% dos entrevistados reconheceram não haver uma política de capacitação voltada para a tecnologia da informação, ou que ela exista apenas parcialmente, conforme Figura 4.5.

Figura 4.5: Análise dos IFs - Capacitação de TI

Com relação à uma política de capacitação voltada para toda organização, a soma das porcentagens dos que reconheceram não haver uma política de capacitação ou que ela exista parcialmente para toda a organização foi similar às da pergunta sobre uma política de capacitação voltada para a TI, conforme apresentado na Figura 4.6. Entretanto um número maior de respondentes entendeu haver parcialmente uma política de capacitação.

Figura 4.6: Análise dos IFs - Capacitação Geral

4.2.1 Governança Corporativa

A maior parte dos entrevistados entendeu não haver uma política de governança formal (documentada e obrigatória) para a organização como um todo, ao passo que parte dos entrevistados entendeu que ao menos o planejamento para tal política havia começado, conforme Figura 4.7.

Figura 4.7: Análise dos IFs - Governança Corporativa Formal

Quanto à governança de tecnologia da informação, pouco menos da metade dos entrevistados entendeu não haver uma política obrigatória, enquanto parte dos entrevistados entendeu haver planejamento iniciado neste sentido, sendo que menos de 1/3 dos entrevistados entendeu haver uma política obrigatória de governança (Figura 4.8).

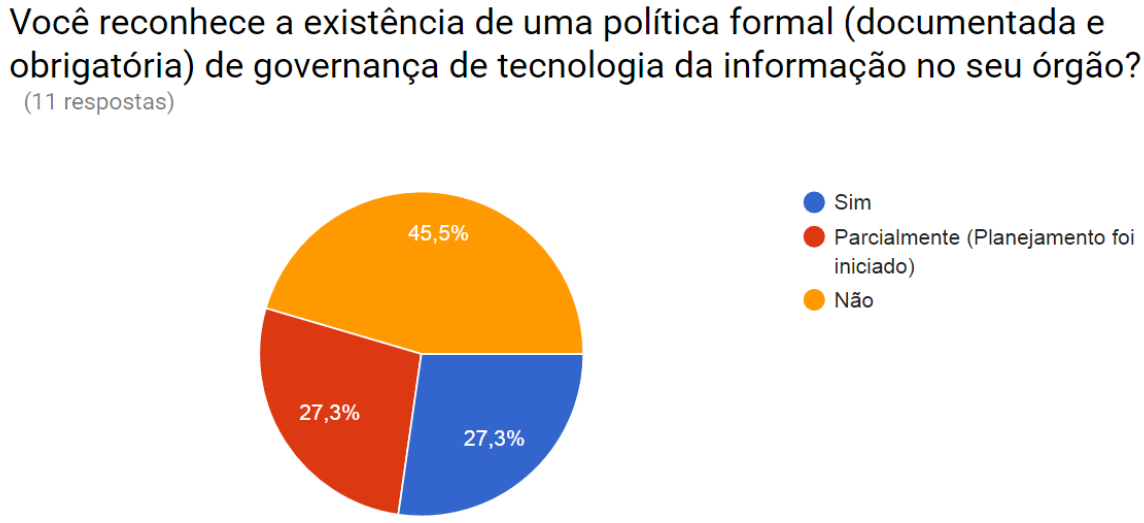


Figura 4.8: Análise dos IFs - Governança de TI Formal

Quanto à participação em um plano diretor de tecnologia da informação, mais da metade dos respondentes participou em sua respectiva instituição (Figura 4.9), reforçando o contato dos entrevistados com governança.

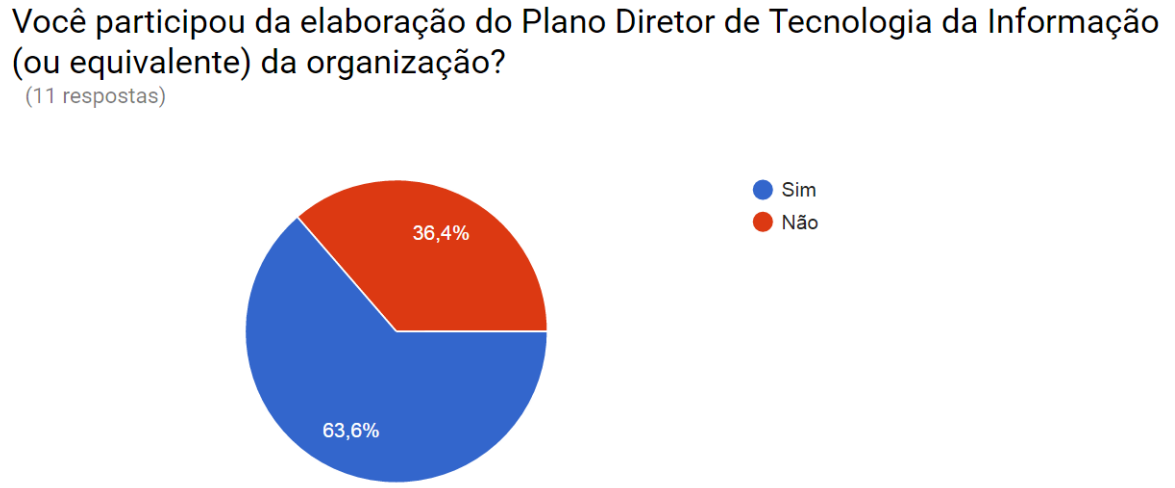


Figura 4.9: Análise dos IFs - Participação em Plano Diretor de TI

Já quanto à informalidade, mais da metade dos respondentes entendeu haver algum tipo de governança não documentada ou não obrigatória (Figura 4.10), indicando uma prevalência da informalidade para a governança de tecnologia da informação nas instituições pesquisadas.

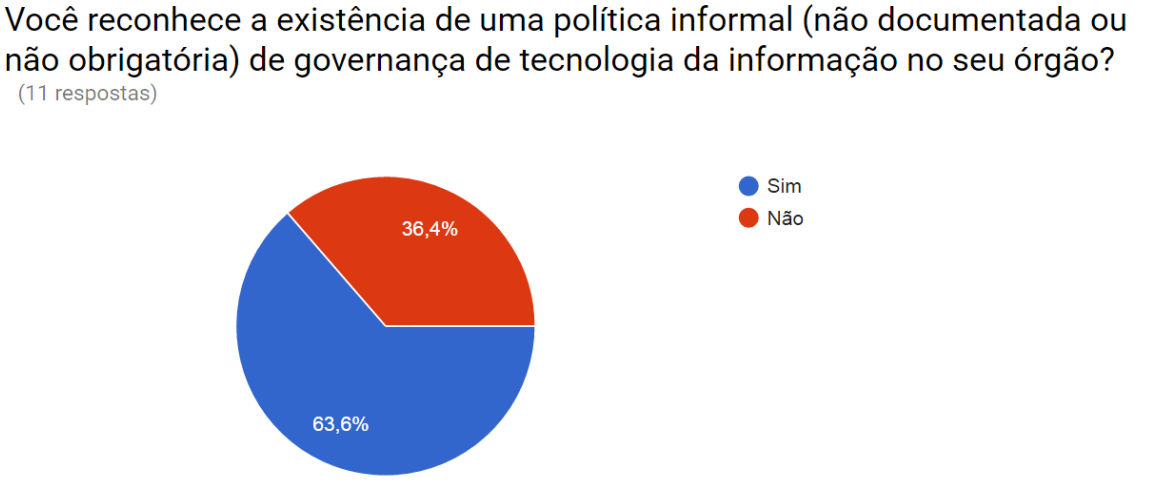


Figura 4.10: Análise dos IFs - Governança de TI Informal

4.2.2 Gestão de Riscos de TI

Quanto à gestão de riscos de TI, nenhum entrevistado entendeu haver uma política formal de gestão de riscos (Figura 4.11). Uma parcela dos entrevistados entendeu haver alguma documentação ou planejamento neste sentido no seu órgão, enquanto a maioria entendeu não haver formalização alguma de uma política de gestão de riscos.

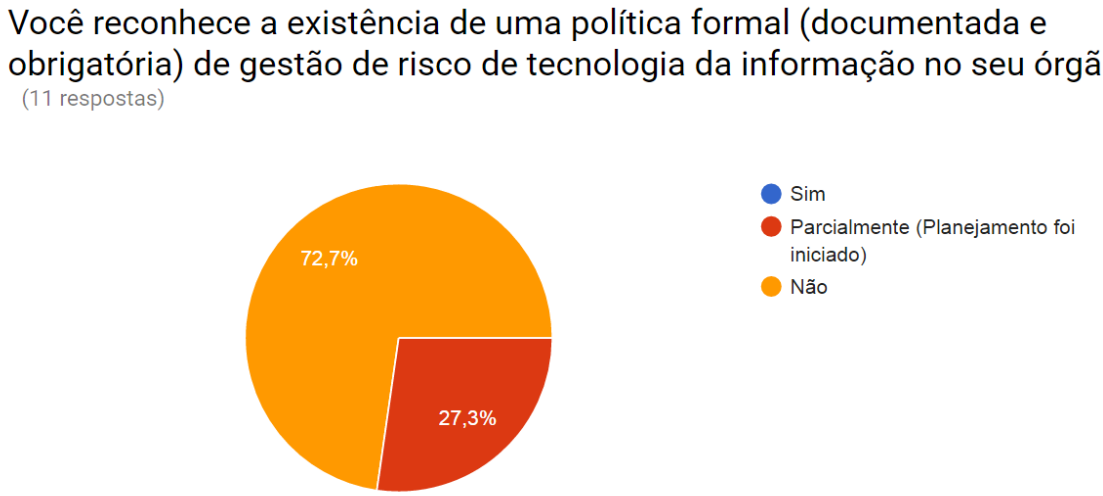


Figura 4.11: Análise dos IFs - Gestão de Riscos Formal

Já quanto às decisões e políticas informais de gestão de riscos, a maioria dos entrevistados entendeu não existir em seu órgão (Figura 4.12). Desta forma, há indicativos de uma ausência de gestão de riscos devidamente estruturada nos órgãos pesquisados.

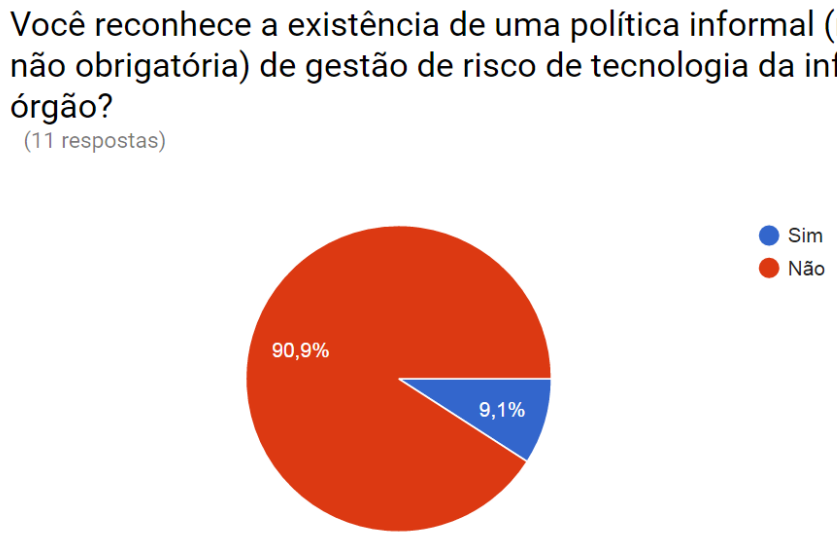


Figura 4.12: Análise dos IFs - Gestão de Riscos Informal

4.2.3 Problemas na Infraestrutura de Tecnologia da Informação nos Institutos Federais

A pesquisa também mostrou alguns problemas na infraestrutura de tecnologia da informação, incluindo falta de pessoal, infraestrutura incompleta e inventários parciais de equipamentos. A ausência de procedimentos para incidentes de segurança também foi indicada pela maioria dos respondentes. Em geral, os servidores que hospedam serviços não estavam em salas com controle ambiental (detectores de temperatura, água e fumaça), embora estivessem ligados a redes estabilizadas/*nobreaks*.

A maioria dos respondentes indicou que a organização como um todo ainda vê a responsabilidade da segurança da informação como responsabilidade "somente da TI".

De forma geral, há indícios da não existência de uma política de gestão de riscos devidamente documentada nos IFs pesquisados. Desta forma não foi possível importar modelos de gestão de riscos para a pesquisa. Limitações impediram uma pesquisa extensiva, e embora os achados não possam ser generalizados para a toda a rede dos IFs, representam tendências importantes em uma parcela deles. Os IFs são estruturas relativamente novas. Embora tenham herdado parte da estrutura das escolas técnicas federais, parte da estrutura é nova ou sofreu expansão, sendo que a governança pode ter sido afetada também em razão disso.

Ainda é possível voltar o olhar a instituições da mesma região geográfica e que tenham estrutura similar para analisar a gestão de riscos e possivelmente importar modelos. Os IFs são instituições de ensino estruturalmente similares às universidades. No DF, a Universidade de Brasília (UnB) é a única universidade pública da região.

4.3 Avaliação da Gestão de Riscos no CPD da UnB

O IFB é, junto da UnB, a única instituição pública federal de ensino do DF [16]. Os Institutos Federais são equiparados às universidades [8], possuindo também uma organização física similar. Desta forma, a instituição foi analisada para identificar se havia algum processo específico de identificação de riscos que pudesse ser utilizado pela pesquisa. O IFB está mais disperso fisicamente do que a UnB, possuindo 10 unidades espalhadas pelo DF. Entretanto, a UnB é, fisicamente, muito maior que o IFB. Possui 505 mil metros quadrados de área construída somente em seu maior *campus*, o Darcy Ribeiro [62], enquanto o IFB chega aos 131 mil metros quadrados, incluindo todos os seus *campi* e reitoria [37].

A Tabela 4.2 mostra a diferença de tamanho das organizações.

Tabela 4.2: Comparativo Geral entre IFB e UnB

	IFB	**UnB**
Alunos	10928	28570
Funcionários	1037	5075
Campi	10	4

Adaptado de: [32] [62]

O Centro de Informática da UnB, também conhecido pela sigla CPD, é um órgão complementar responsável pela tecnologia da informação [61], estando localizado no *campus* Darcy Ribeiro, que é também onde está a maior parte da estrutura da universidade. Pode ser considerado o órgão principal lidando com a infraestrutura de tecnologia da informação. Devido a esses atributos, a pesquisa foi dirigida ao órgão. Seu organograma encontra-se em fase de reestruturação, havendo uma estrutura oficial antiga e uma estrutura informal para melhorar a dinâmica do trabalho, e que espera-se tornar oficial. Nesta fase de transição ainda não havia uma estrutura com uma coordenação de governança devidamente montada, conforme informações prestadas. Desta forma, a Coordenação/Gerência de Redes e Suporte, conforme confirmou a pesquisa, é a coordenação que cuida efetivamente da parte de infraestrutura de tecnologia da informação. Portanto, a entrevista foi dirigida a essa coordenação.

A Figura 4.13 mostra a estrutura oficial do CPD.

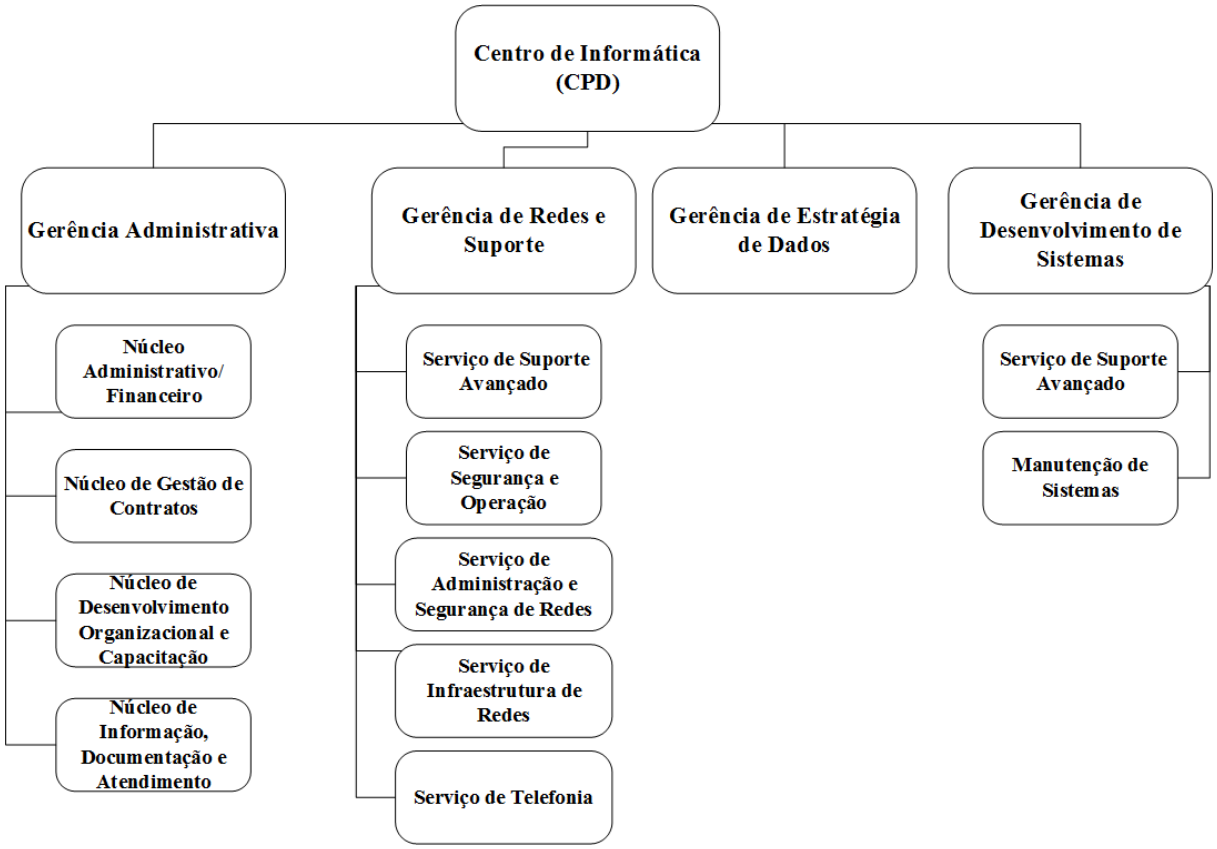


Figura 4.13: Estrutura do Centro de Informática (CPD) da UnB
Adaptado de: [61]

A entrevista foi aplicada à coordenação de redes e suporte e suas sub-coordenações. Seu objetivo foi entender se existia um processo bem definido de gestão de riscos e, em caso positivo, identificá-lo e possivelmente usá-lo como uma das referências para uma identificação de riscos no IFB. Foram realizadas entrevistas semi-estruturadas, permitindo ao entrevistado maior liberdade na elaboração das respostas para perguntas abertas. Os Apêndices C e D contêm o roteiro das entrevistas efetuadas. O Apêndice E contém a compilação das respostas das entrevistas.

Conforme as entrevistas mostraram, a implantação de um processo de gestão de riscos no órgão esbarrou em vários problemas. Entre os desafios enfrentados pela UnB, tem-se: a mudança da época de computadores de grande porte para a microinformática, em que grande parte dos elementos de governança e controle desenvolvidos na época se perderam; a falta de um incentivo governamental inicial à época dessa mudança para o desenvolvimento da governança; a escassez de pessoal; o tamanho da UnB; sua dispersão física; e, a diversidade de perfis educacionais com exigências diferentes, que muitas vezes podem ser conflitantes. Estes desafios contribuíram para a dificuldade da implantação de

uma política não apenas de gestão de riscos, como de governança. Os líderes de setor mostram consciência da necessidade de governança, mas informaram haver dificuldades em sua implantação. A pesquisa também mostrou haver uma relação de interdependência entre os vários *campi* e o CPD. Sendo que muitas vezes intervenções são negociadas e feitas na forma de orientações à distância, ou de forma presencial. Os *campi* também têm liberdade para hospedar seus próprios serviços, se tiverem a estrutura para tal, ou usar aqueles oferecidos pelo CPD.

Foram mostrados sinais de terceirização na parte de suporte e assistência técnica, enquanto a parte de redes ficou predominantemente com a equipe de TI do órgão.

A instituição mostrou ter dado passos em direção à governança e controle, com os *softwares* livres GLPI e CITSmart para gerenciamento de serviços de TI e *helpdesk*. Para parte de infraestrutura de redes, a equipe também conta com o apoio do *software* NetSight da Enterasys. Embora o uso paulatino de *checklists* não foi identificado, existe alguma orientação interna, as homologações de *software*, o apoio realizado por alguns *softwares* e também práticas de controle difundidas na equipe.

Quanto à infraestrutura, a organização possui uma quantidade extensiva de equipamentos, inclusive equipamentos robustos para controle lógico da rede. Encontram problemas de uso indevido da infraestrutura, inclusive ataques contra a infraestrutura e serviços realizados de forma externa e, surpreendentemente, ataques internos. Além de ataque contra os serviços e infraestrutura, há ataques contra outros órgãos realizando a rede interna. A ausência de uma política de governança leva ao tratamento pontual de cada um dos problemas, principalmente quando os ataques partem da rede interna.

Vários equipamentos importantes, voltados para segurança lógica da rede, ficaram desatualizados ou não possuem mais garantia, levando a uma redução relativa dos equipamentos disponíveis. Portanto, a UnB também mostrou sofrer com obsolescência de equipamentos. Alguns funcionários também detinham um conhecimento bem abrangente sobre infraestrutura, mas nem todo conhecimento estava documentado. Parte do conhecimento foi passado à equipe, mas parte foi perdido conforme os funcionários antigos se aposentaram.

Os técnicos e analistas não cuidam prioritariamente do suporte. Com relação aos *softwares* instalados, atuam na administração e homologação, mas deixam o apoio de suporte ao usuário com problemas comuns a uma equipe, sendo que se os problemas não puderem ser resolvidos pelo suporte, são repassados ao setor adequado no CPD.

A pesquisa mostrou indícios da ausência de uma governança de tecnologia da informação consolidada na UnB. Não foi identificado um processo bem definido de gestão de risco na área de tecnologia da informação do órgão. Também não foi identificada uma política de capacitação voltada para a gestão de risco. Apesar disso, foi identificado haver

controle de incidentes através de *softwares* livres para gestão de equipamentos, *helpdesk* e processos de TI, bem como *software* para controle de ativos de infraestrutura de redes. A equipe não recebeu treinamento contínuo especificamente voltado para gestão de riscos, embora existam experiências pessoais de outros empregos trazidas por funcionários e ações isoladas de capacitação voltadas para governança.

Embora haja indícios da falta de um processo formal de gerenciamento de riscos, existem pesquisas acadêmicas para melhoria dos processos existentes. Um estudo de caso foi feito para propor melhorias nos serviços críticos do CPD. Foram identificados e classificados os serviços de TI na visão dos gestores do órgão e identificados os serviços críticos na visão dos clientes de TI. Então foram levantados os riscos dos serviços, identificando vulnerabilidades no processo, bem como foi feito mapeamento e redesenho de processos. Ao final foi proposta uma estrutura baseada em processos de gerenciamento de TI, sendo apresentados um conjunto de documentos elaborados com base em melhores práticas [23].

As instituições nacionais de ensino pesquisadas, 11 IFs e a UnB, apresentaram indícios da falta processos ou políticas bem definidas de gestão de riscos, embora forneceram valiosas informações sobre a estrutura, a governança e a tecnologia da informação destes órgãos, contribuindo para o entendimento de problemas e o estado da tecnologia da informação. Dessa forma, o levantamento de riscos para o IFB seguiu orientações gerais da ISO 31000 que foram complementadas pelo Programa de Gerenciamento de Riscos da Universidade da Virgínia. Enquanto a ISO 31000 pode ser considerada um padrão com princípios e orientações genéricas de gestão de riscos, não restrita a uma indústria ou a um setor, de acordo com seu escopo [59], o Programa de Gerenciamento de Riscos da Universidade da Virgínia especificamente diz respeito à tecnologia da informação [65]. Assim, ambas foram usados na pesquisa.

O próximo capítulo apresenta uma visão geral do IFB bem como os contextos nos quais está inserido, embasando o processo de gestão de riscos da pesquisa.

Capítulo 5

Contextualização do Instituto Federal de Brasília

Este capítulo apresenta a contextualização do órgão, definindo as bases para o estudo de caso. Antes da concepção de uma estrutura de risco é importante avaliar os contextos interno e externo da organização, pois estes podem impactar significantemente na estrutura [59]. Esta seção da pesquisa destina-se a agregar os achados do contexto externo e interno da organização.

5.1 Contexto Externo

O Instituto Federal de Brasília é uma instituição de ensino e tem como natureza jurídica a denominação de autarquia [8], estando sujeita principalmente à política, legislação e regulação federal.

5.1.1 Ambiente Cultural, Social e Político

O Instituto Federal de Brasília é parte de um esforço do governo brasileiro para expandir o ensino técnico, tendo modalidades de ensino bastante diferentes e que normalmente não são encontradas agrupadas na mesma instituição: o ensino médio integrado ao curso técnico, o ensino técnico subsequente, a formação inicial e continuada e o ensino superior.

Do ponto de vista social e cultural, é uma instituição com visão além do ensino puro, tendo também visão social. Um dos objetivos dos institutos federais é:

> "Desenvolver atividades de extensão de acordo com os princípios e finalidades da educação profissional e tecnológica, em articulação com o mundo do trabalho e os segmentos sociais, e com ênfase na produção, desenvolvimento e difusão de conhecimentos científicos e tecnológicos." [8]

5.1.2 Contexto Regulatório Externo

Na área de educação, o Ministério da Educação (MEC) emite memorandos, pareceres, ofícios e normas, sobretudo no que diz respeito à educação, metas educacionais, inclusão social (inclusive tecnológica), entre outros, sendo o superior imediato dos Institutos Federais.

O IFB também faz parte do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP. O SISP é um sistema instituído para gerir recursos de informação da Administração Pública Federal Direta, Autárquica e Fundacional [6], estabelecendo notadamente regras e melhores práticas para a administração pública federal no que diz respeito à tecnologia e informação.

Algumas leis são proeminentemente importantes ao IFB no desempenho de sua missão organizacional e devem ser seguidas e usadas no dia-a-dia como referência para sua missão institucional e administração, bem como para garantir conformidade com regulações federais. É importante ressaltá-las no estabelecimento do contexto externo da organização.

A Lei nº 9.394, de 20 de dezembro de 1996, "Lei de Diretrizes e Bases da Educação" é o guia geral para a educação no Brasil servindo como referência no que diz respeito à educação, aplicável também aos IFs para entender a função do Estado na educação. Além da formação básica, a lei prevê em vários trechos obrigações ou possibilidades na formação do aluno e do professor que incluem a presença da tecnologia, seu ensino e disseminação. Conforme previsto nos artigos: [9]

> Artigo 35. Para o ensino médio, prevê a preparação básica para o trabalho, de onde se pode inferir a obrigação do ensino mínimo de recursos tecnológicos ao aluno.
>
> Artigo 39. Prevê a integração da educação profissional e tecnológica à tecnologia.
>
> Artigo 43. Para o ensino superior prevê a pesquisa e investigação, contribuindo para o desenvolvimento da tecnologia.
>
> Artigo 62. Prevê o uso de recursos e tecnologias de educação à distância para formação docente.

A Lei nº 11.892, de 29 de dezembro de 2008 institui a rede federal de ensino, criando os Institutos Federais, definindo sua estrutura organizacional e administrativa, finalidades e características. Serve como um guia geral de missão e organização para o Instituto Federal de Brasília. No tocante à tecnologia prevê finalidades e objetivos, conforme os artigos: [8]

> Artigo Sexto. Prevê como finalidade e característica a oferta de educação tecnológica (alínea I), o desenvolvimento da educação tecnológica (alínea II), a oferta formativa (alínea IV), capacitação técnica (alínea VI) e programas de extensão e divulgação científica

e tecnológica (alínea VII); elementos que envolvem – direta ou indiretamente – a oferta de recursos de tecnologia da informação.

Artigo Sétimo. Prevê como objetivo dos Institutos Federais a oferta de formação continuada visando capacitação, aperfeiçoamento, especialização e atualização (alínea II), desenvolvimento de atividades de extensão visando também a difusão de conhecimentos técnicos e tecnológicos (alínea II).

Estes itens e diversos outros indicam direta ou indiretamente a necessidade do uso de tecnologia da informação, bem como sua difusão. Espera-se de uma organização que possui uma missão de disseminação de tecnologia que possa administrar seus recursos tecnológicos.

5.1.3 Relação com Partes Interessadas Externas

Fatores externos influenciam os eixos tecnológicos do IFB, isto é, qual área do conhecimento cada *campus* vai ofertar, como administração, química, biologia, computação etc. O fator externo principal é a própria comunidade. Na criação dos *campi* o IFB avalia a pré-disposição da região, a viabilidade financeira e a demanda, efetuando audiência pública composta pela sociedade, incluindo cidadãos e empresários, para definir o eixo. Se aplicável, posteriormente o eixo pode ser expandido ou mudar.

O eixo tecnológico pode influenciar o que diz respeito à quantidade de recursos de tecnologia da informação que serão necessários para atender ao *campus*, bem como pode definir alguma tecnologia adicional que não consta no catálogo dos outros *campi* que será necessária para suprir as demandas de ensino nesse eixo. Por fim, a continuidade dos serviços de tecnologia ou sua falta de continuidade podem impactar na imagem da organização junto à comunidade, possivelmente impactando nas parcerias feitas com a comunidade, inclusive fornecimento de alunos e capital de pesquisa, impactando na organização como um todo.

5.2 Contexto Interno

Os Institutos Federais são autarquias e têm estrutura *multicampi* [8]. O IFB conta atualmente com dez *campi*, muitos dos quais estão implantando suas estruturas físico-tecnológicas e didático-pedagógicas. Destes dez, cinco encontra-se em estágio avançado de implantação, estando quase completos. A reitoria compartilha hoje da infraestrutura de um dos *campi* e, para os efeitos de infraestrutura, foi considerada parte dele.

Uma empresa pode ser considerada uma organização em que atividades são projetadas para elaborar, produzir, comercializar e sustentar seu produto, sendo que tais atividades

podem ser representadas usando uma cadeia de valor [25]. Considerando que uma instituição como o IFB é educacional e seus processos e atividades gravitam em torno desta natureza, a Figura 5.1 descreve uma cadeia de valor para a organização objeto do estudo. Ela foi elaborada no desenvolvimento da pesquisa, partindo das atribuições previstas em lei (atividades principais), da estrutura interna prevista em portarias, bem como das atividades gerais realizadas.

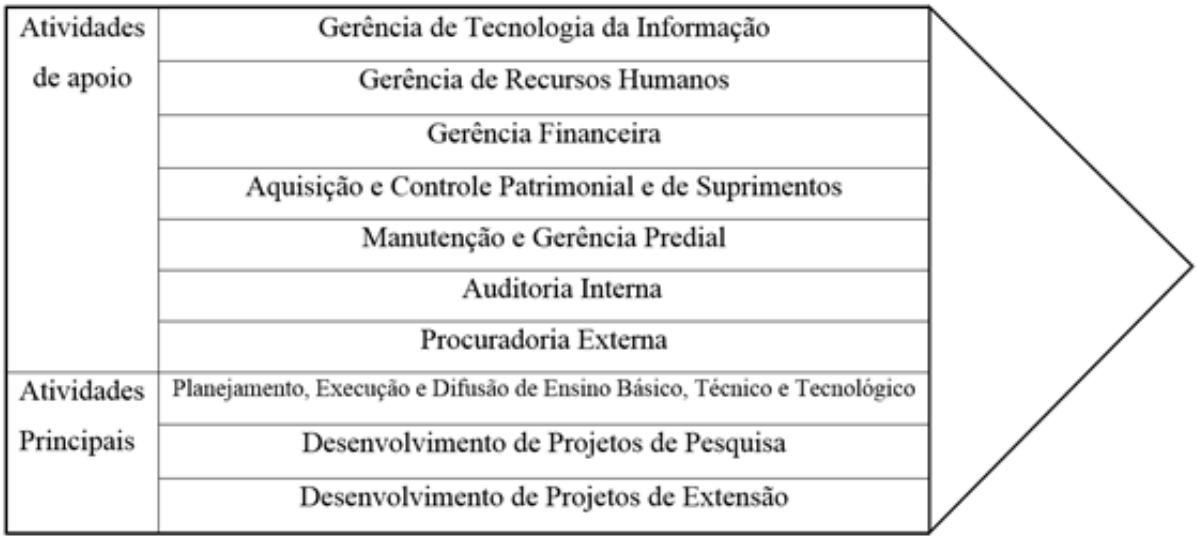


Figura 5.1: Cadeia de Valor do IFB

A cadeia de valor apresenta uma visão macro de atividades organizacionais do ponto de vista de missão institucional, representando também uma pequena parte da organização interna.

5.2.1 Governança, Estrutura Organizacional, Funções e Responsabilidades

Para sua governança, o IFB conta com as leis supracitadas no ambiente externo, normas e planos internos que organizam a instituição e definem políticas a serem seguidas.

O IFB é composto pela reitoria e seus *campi*, representado pela figura do Reitor e do Conselho Superior no âmbito da organização, e do Diretor Geral no âmbito de cada *campus*. Nos Institutos Federais, o órgão superior máximo, de caráter consultivo e deliberativo é o Conselho Superior; composto por estudantes, docentes, servidores técnico-administrativos, egressos, Ministério da Educação e Colégio de Dirigentes [8]. Abaixo do conselho superior estão todos os cargos. Seguindo a hierarquia de cargos, tem-se o Reitor e Pró-reitores e a Direção Geral de cada *campus*.

A resolução interna nº35 do conselho superior do IFB define a estrutura organizacional do órgão, não desrespeitando as características impostas pela Lei n.º 11.892. São definidos os cargos de direção e a subordinação, abrangendo reitoria e *campi*. Vide Figura 5.2.

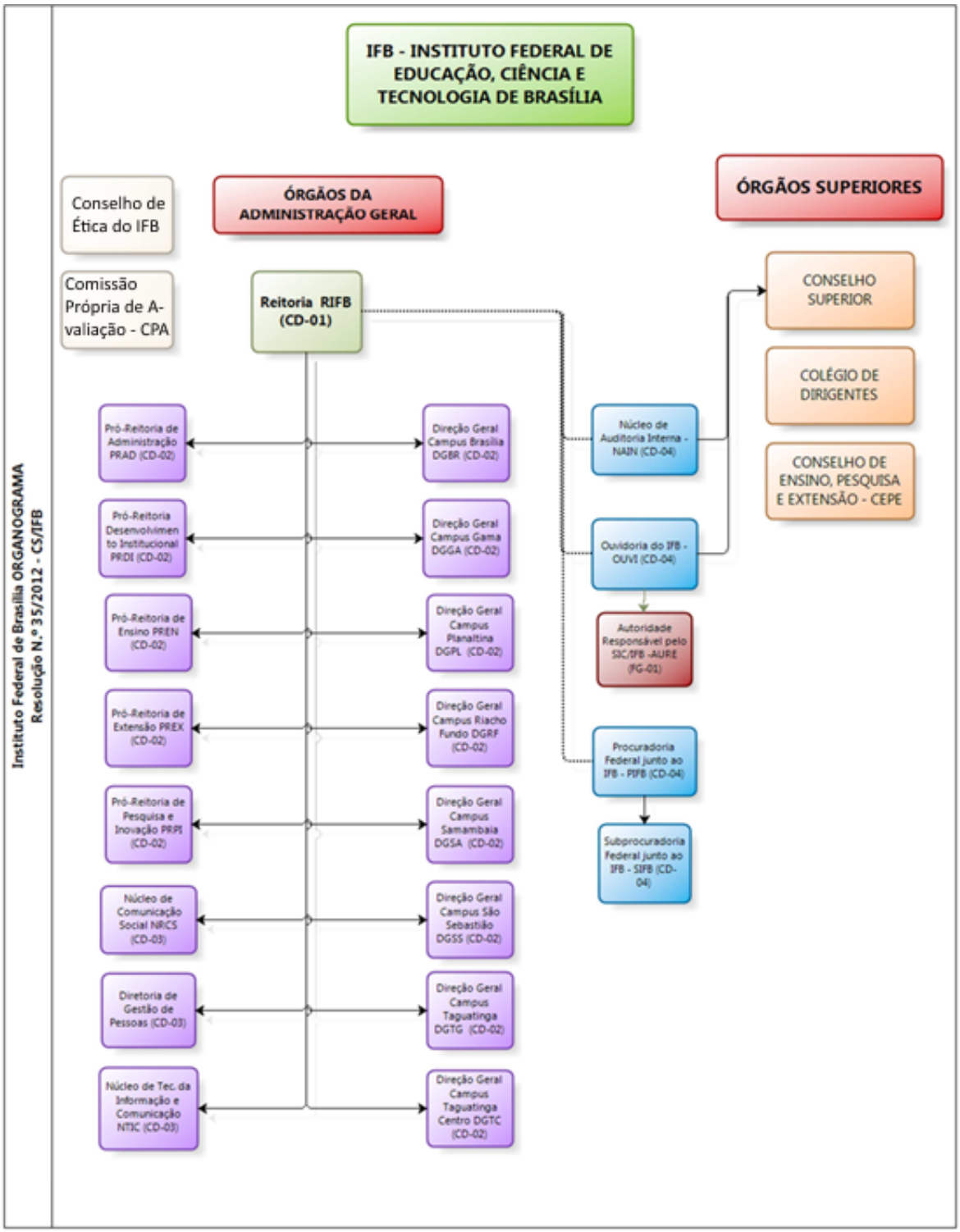


Figura 5.2: Organograma do IFB
Adaptado de: [36]

A estrutura dos *campi* também é definida através da resolução interna nº 35. A Figura 5.3 mostra a estrutura de alguns dos *campi*. A estrutura dos campi pode variar devido ao quantitativo de alunos ou à localização rural.

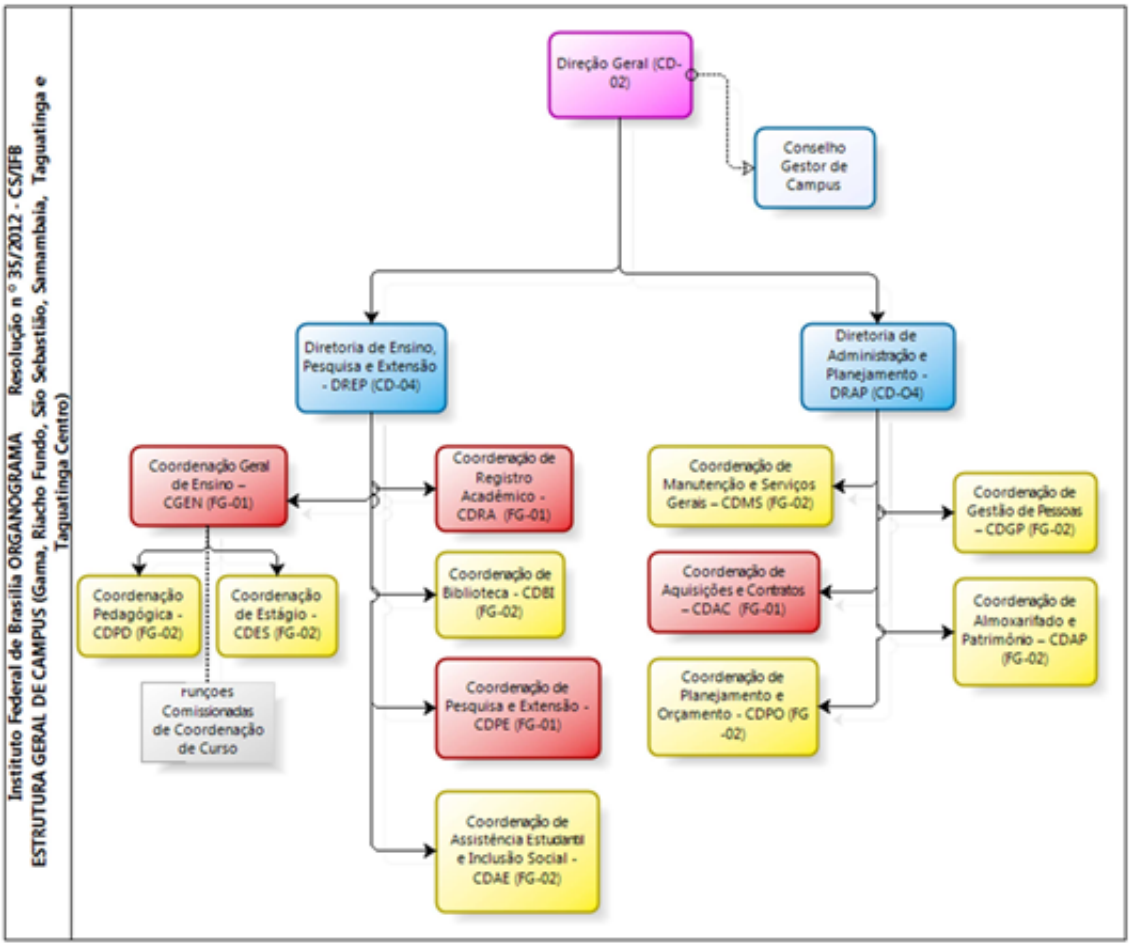


Figura 5.3: Organograma do *Campus*
Fonte: [36]

O IFB conta com um núcleo – não uma direção - atrelado à reitoria para as questões de tecnologia da informação no órgão, o Núcleo de Tecnologia da Informação e Comunicação - NTIC, cabendo a este a função consultiva no que diz respeito aos aspectos tecnológicos.

Ainda de acordo com a resolução interna nº 35, a área de tecnologia da informação não aparece nos *campi*, tendo sido suprimida na última votação de organograma. Desta forma os profissionais de tecnologia da informação dos *campi* encontram-se subordinados diretamente à Diretoria de Administração e Planejamento em cada unidade.

5.2.2 Normas Internas

As normas internas constituem importante arcabouço de referência para a organização no que diz respeito à organização e governança. É relevante citar para o contexto desse trabalho:

Resolução do Conselho Superior Nº12/2012. Define o regimento geral do IFB. No tocante à parte que afeta diretamente a área tecnológica, prevê em seu artigo 203 o compartilhamento de infraestrutura e equipamentos pelos vários órgãos do IFB em situações aplicáveis [35].

Resolução do Conselho Superior Nº35/2012. Define a estrutura Organizacional. Prevê um Núcleo de Tecnologia da Informação atrelado à reitoria, não uma direção, e suprime a área de tecnologia da informação no âmbito de funções gratificadas, cargos comissionados e estrutura, embora a área continue existindo de fato, seus funcionários estão subordinados diretamente à Diretoria de Administração e Planejamento [36].

Plano Diretor Institucional - PDI (2014-2018). Contém os objetivos estratégicos do Instituto Federal de Brasília para o quinquênio 2014-2018. No tocante à parte de infraestrutura e tecnologia prevê dois objetivos estratégicos: [37] 1 – Fomentar e aprimorar o uso de tecnologia da informação 2 – Elaborar e executar o Plano Diretor de Tecnologia da Informação

Por questões de referência, cabe ainda citar o Plano Diretor de Tecnologia da Informação (2011-2012) – Trazia direção e metas da tecnologia da informação para o biênio 2011-2012 [34]. Durante a pesquisa, o IFB ainda não contava com um Plano Diretor de Tecnologia da Informação.

5.3 Visão Geral da Tecnologia da Informação no IFB e Ajuste de Escopo

No IFB, o Núcleo de Tecnologia da Informação e Comunicação (NTIC) é uma das figuras centrais na tecnologia da informação. Devido ao seu papel foi preciso entender melhor sua relação com o *campus* para que o escopo da pesquisa fosse melhor definido. Desta forma, foi aplicada o roteiro de entrevista presente no Apêndice F. O objetivo da pesquisa foi delinear aspectos da tecnologia da informação no IFB, bem como melhor definir parte do escopo para melhor aplicar a pesquisa. O Apêndice G contém a compilação das respostas da entrevista.

Foi escolhida a Coordenação de Redes por ser a coordenação diretamente ligada à infraestrutura de tecnologia da informação e também por sua relação com os *campi*, que possuem uma área de TI bastante ligada à infraestrutura, conforme confirmou a entrevista. A Figura 5.4 mostra a estrutura do NTIC e a subordinação da Coordenação de Redes.

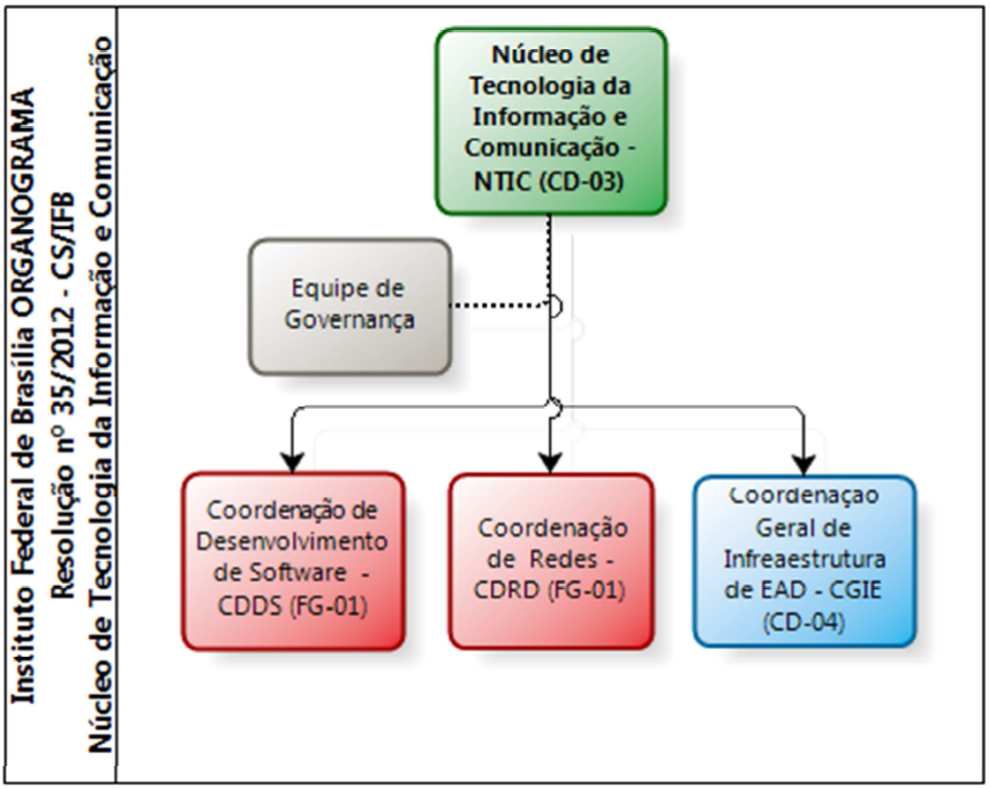


Figura 5.4: Estrutura do NTIC
Fonte: [36]

Conforme a entrevista reafirmou, a missão dos *campi*, na visão da Coordenação de Redes, é uma missão de ensino, pesquisa e extensão, visando formar o aluno, e também uma missão de inclusão social. E a missão da Tecnologia da Informação é de apoio aos diversos setores, apoiando ensino e administração. A entrevista mostrou ainda não haver gestão de risco no âmbito de tecnologia da informação na instituição.

Para concretizar essa missão de apoio, atividades importantes da Tecnologia da Informação são executadas, como suporte ao sistemas utilizados, manutenção, administração da rede, gerência de servidores e serviços, possuindo uma vertente estratégica no *campus*. O núcleo idealmente atua como um ponto de padronização e apoio, bem como administração de determinados sistemas.

Existe uma designação entre os *campi*, estando divididos em implantados e não implantados/em implantação. Do ponto de vista de Tecnologia da Informação, os *campi* implantados são aqueles com uma infraestrutura de rede mínima pronta, interligação

definitiva com a internet, estrutura de *datacenter*, servidores, equipamentos de rede definitivos, incluindo *switches* e *gateways* de voz. Já os *campi* não implantados não possuem os equipamentos adequados ou não possuem a quantidade suficiente, têm servidores improvisados, não possuem internet ou possuem fora do padrão usado, não funcionando com todas as funcionalidades de rede esperadas. Devido à essa natureza, a coordenação recomendou a limitação da pesquisa para obtenção de riscos aos *campi* implantados, pois os mesmos servirão de base para o restante dos *campi*, isto é, a infraestrutura que os mesmos têm é aquela que uma dia se deseja que os *campi* não implantados tenham.

Esta infraestrutura de tecnologia da informação afeta pessoas e ambientes, sendo também afetados por uma gestão de riscos voltada à infraestrutura de tecnologia da informação. A Tabela 5.1 mostra a média dos principais usuários de tecnologia da informação do ponto de vista de ensino e administrativo, bem como parte da infraestrutura predial. Os números, sobretudo de alunos, podem flutuar devido ao ano eletivo, programas de incentivo, demanda do mercado entre outros fatores. Estes usuários e estruturas são afetados pela tecnologia da informação.

Tabela 5.1: Clientes da Tecnologia da Informação no IFB

Afetados	**Quantidade**
Alunos-ano	900-1200
Professores	70
Técnicos Administrativos	35
Salas de Aula/Laboratórios	48

Adaptado de: [32] [33]

5.3.1 *Campi* Implantados do Ponto de Vista de Tecnologia da Informação

Os *campi* implantados do ponto de vista de tecnologia da informação são os *campi* mais antigos: Brasília, Gama, Taguatinga, Planaltina e Samambaia.

5.4 Processo de Gestão de Riscos da Infraestrutura do IFB

O objetivo da gestão de riscos no contexto apresentado é identificar as partes críticas da infraestrutura de tecnologia da informação comum aos *campi* implantados que este-

jam sujeitas a riscos e sejam cruciais para o fornecimento de serviços e avaliar os riscos associados a elas.

5.4.1 Definição das Intenções e Objetivos das Atividades de Gestão de Riscos

O objetivo da gestão de riscos no contexto apresentado é identificar os elementos críticos da infraestrutura de tecnologia da informação comum aos *campi* implantados que estejam sujeitas a riscos e sejam cruciais para o fornecimento de serviços e avaliar os riscos associados a eles. A Tabela 5.2 mostra o resumo das intenções do processo de gerenciamento de riscos.

Tabela 5.2: Intenções do Processo de Gestão de Riscos na Pesquisa

Identificação	**Intenção**
I1	Aplicar entrevista à Coordenação de Redes do Núcleo de Tecnologia da Informação do IFB
I2	Pesquisar gestão de riscos em outras instituições de ensino semelhantes ao IFB
I3	Aplicar questionário para levantamento de riscos com todos os funcionários de TIC dos *campi* implantados e ao menos 51% dos Diretores Gerais destas unidades
I4	Aplicar questionário para avaliação de riscos com todos os funcionários de TIC dos *campi* implantados
I5	Aplicar observação e análise documental no tocante à infraestrutura de TIC
I6	Propor validação para avaliação dos riscos levantados

A Tabela 5.3 mostra o resumo dos objetivos associados às intenções do processo de gestão de riscos.

Tabela 5.3: Objetivos do Processo de Gestão de Riscos na Pesquisa

Identificação	**Objetivo**	**Intenção Relacionada**
OB1	Desenhar Perfil do estado atual da TIC no IFB	I1, I5
OB2	Incorporar possíveis elementos úteis ao processo de levantamento e avaliação de riscos	I2
OB3	Identificar riscos	I3
OB4	Avaliar riscos	I4
OB5	Validar riscos	I6

5.4.2 Definição dos Responsáveis pelo Processo de Gestão de Riscos

O processo de gestão de risco tem responsáveis diferentes, havendo variação de acordo com o nível observado. Embora não seja o foco da pesquisa a elaboração de um plano de gerenciamento de riscos, convêm definir os possíveis responsáveis no caso do estabelecimento de um plano de gerenciamento de riscos completo, que pode usufruir dos dados desta pesquisa.

Entre as partes interessadas de um processo de gestão de riscos estão:

> "a) Os responsáveis pelo desenvolvimento da política de gestão de riscos no âmbito de suas organizações;
> b) Os responsáveis por assegurar que os riscos são eficazmente gerenciados na organização como um todo ou em uma área, atividade ou projeto específicos." [59]

No IFB, poderiam ser considerados:

Os responsáveis pelo desenvolvimento da política de gestão de riscos

No órgão todo (nível estratégico)

- Conselho Superior
- Reitor

Nos *campi* (nível tático)

- Direção Geral
- Diretoria de Administração

Os responsáveis por assegurar que os riscos são eficazmente gerenciados

No órgão todo (nível estratégico):

- Conselho Superior
- Reitor
- Núcleo de Tecnologia da Informação e Comunicação

Nos *campi* (nível tático/operacional):

- Direção Geral (DG)
- Diretoria de Administração (DRAP)
- Funcionários de TIC

5.4.3 Definição das Metodologias do Processo de Avaliação de Riscos

A Tabela 5.4 mostra as técnicas aplicadas na pesquisa. São técnicas da ISO 31010, conforme apresentado na Tabela 2.3, sendo adequadas para identificação e avaliação de riscos.

Tabela 5.4: Técnicas da ISO 31010 Aplicadas na Pesquisa

Ferramentas e Técnicas	**Identificação de Riscos**	**Impacto**	**Probabilidade**	**Nível de Risco**	**Avaliação de Riscos**
Entrevistas estruturadas ou semi-estruturadas	FA	NA	NA	NA	NA
Matriz de probabilidade e consequência	NA	FA	NA	NA	FA

FA - Fortemente aplicável NA - Não Aplicável A - Aplicável

5.4.4 Critérios do Risco, o Cálculo do Risco e o Nível em que o Risco se Torna Aceitável ou Tolerável

Foi usada uma abordagem qualitativa para classificar os riscos. Considerando a subjetividade do risco, mas também a necessidade de sua mensuração, foi utilizado o sistema de escalas apresentado na Tabela 2.1. A matriz elaborada previu uma escala para usos diversos, levando em consideração também sistemas e dados.

As ações a serem tomadas, baseadas no valor do risco, foram as propostas na Tabela 2.2. Desta forma, o risco se tornaria aceitável quando fosse menor que 4.

5.4.5 Evolução no Tempo da Probabilidade e/ou Consequência

A reavaliação dos riscos deve ocorrer novamente ao menos uma vez em um período de até três anos, quando houver significante mudança nos ativos de TI ou quando houver significante mudança no ambiente de riscos, conforme recomendação do Plano de Gerenciamento de Riscos da Universidade da Virgínia [65].

O próximo capítulo apresenta passos tomados para identificar e validar riscos relativos à infraestrutura de tecnologia da informação no IFB.

Capítulo 6

Identificação e Validação de Riscos no IFB

Este capítulo apresenta a identificação e a avaliação de riscos no IFB, oferecendo detalhes sobre sua aplicação e resultados. O Capítulo encontra-se divido em:
Avaliação de Riscos - Apresenta como foi feito o levantamento de ativos críticos, levantado dos riscos e sua classificação
Validação dos Riscos - Apresenta uma proposta de validação para os riscos levantados pela equipe técnica.

6.1 Avaliação de Riscos no IFB

A avaliação de riscos pode ser definida como um processo em que os riscos são levantados e classificados de acordo com critérios definidos. A avaliação de riscos na pesquisa usou a ISO 31000 como guia geral e usou o Modelo da Universidade da Virgínia como referência prática.

Os ativos críticos devem ser levantados, riscos associados aos mesmos devem ser definidos e esses riscos devem ser avaliados usando a percepção da equipe em relação à possibilidade de reincidência e ao eventual impacto de sua concretização. A pesquisa envolveu os cinco *campi* implantados.

A Figura 6.1 apresenta o fluxo de gerenciamento de riscos proposto pela Universidade da Virgínia.

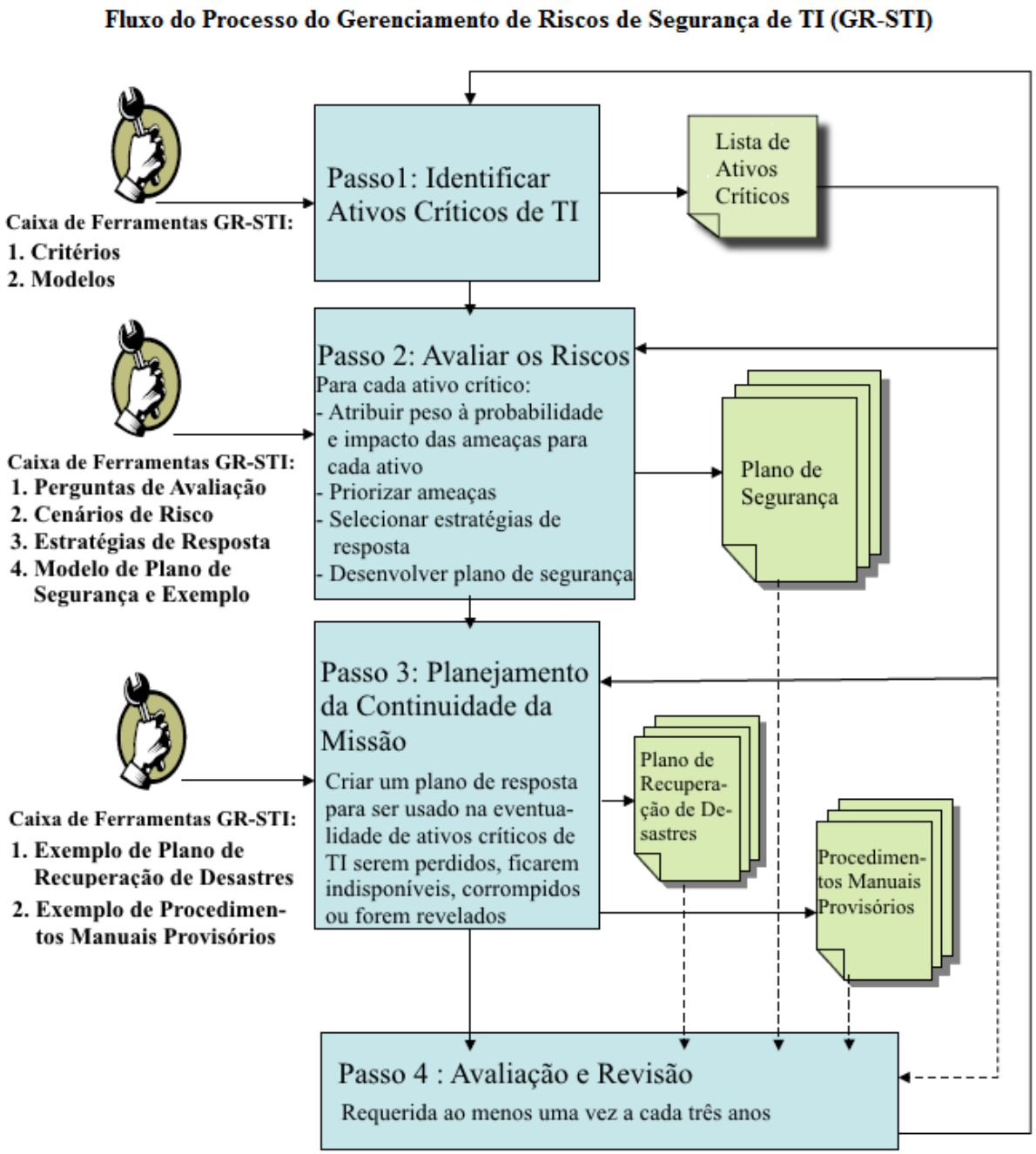


Figura 6.1: Fluxo de Gestão de Riscos definido pela Universidade da Virgínia Adaptado de: [65]

Para avaliação de riscos foi utilizado parcialmente o modelo da Universidade da Virgínia, presente na Figura 6.1, mais especificamente o passo 1 e o passo 2 até a priorização dos riscos. Entretanto não foram usados diretamente os *templates* fornecidos, optando-se

por uma abordagem que levou em consideração a estrutura do IFB apresentada no Capítulo 5, seu conjunto de ativos e seus problemas peculiares associados identificados pela equipe técnica, em detrimento de cenários prontos de risco.

6.1.1 Definição de Ativos Críticos

Os riscos estão associados a ativos. Para avaliação dos riscos devem ser definidos os ativos críticos. Um ativo crítico pode ser considerado aquele que afeta a missão da instituição se for revelado, modificado, destruído ou mal-usado, podem ser categorizados em *hardware*, *software*, informação e pessoas [65].

O roteiro de entrevista presente do Apêndice H foi aplicado à Coordenação de Redes com objetivo de identificar ativos críticos, estruturas e serviços comuns aos *campi* implantados aliado à observação do ambiente de TI. Foram elaboradas tabelas com o resumo das informações. Conforme previsto, por razões de segurança algumas informações não estarão completamente disponíveis.

A Tabela 6.1 contém os principais ativos para manter a rede interna funcionando, bem como sua idade aproximada.

Tabela 6.1: Ativos de *Hardware* - Equipamentos de Rede

Nome	**Quantidade Aproximada**	**Idade Aproximada (anos)**
Distribuidor Interno Óptico	6	1-5
Servidor Dedicado	2	3-5
Switch "Core"	1	4-5
Switch PPOE	1	4-5
Switch de Distribuição	14	1-5
Gateway de Voz "Core"	1	3-5
Gateway de Voz de Distribuição	2	1-5

A Tabela 6.2 contém informações sobre os computadores disponíveis. Ao menos cinco modelos diferentes de estações de trabalho existem nos *campi*, cada um representando um fabricante e/ou configuração. Existem ao menos três modelos de *notebooks*.

Tabela 6.2: Ativos de *Hardware* - *Desktops* e *Notebooks*

Nome	**Quantidade Aproximada**	**Idade Aproximada (anos)**
Desktop Modelo 1	50	6
Desktop Modelo 2	150	4-5
Desktop Modelo 3	100	3
Desktop Modelo 4	60	6
Desktop Modelo 5	40	5-6
Notebook Modelo 1	5	5-6
Notebook Modelo 2	5	5-6
Notebook Modelo 3	5	5-6

A Tabela 6.3 contém as principais instalações presentes nos *campi*. Elas atuam como abrigo de equipamentos de hardware e também estão interligadas aos mesmos.

Tabela 6.3: Ativos - Instalações

Nome	**Quantidade Aproximada**
Solução de Contenção de Calor, *Rack* para Equipamentos e *Nobreak* (Estrutura do Datacenter)	1
Sala Técnica	5
Cabeamento Estruturado (pontos)	500
Rede Elétrica	

A Tabela 6.4 contém os sistemas operacionais utilizados. No que tange a infraestrutura comum, há uma predominância dos sistemas operacionais Windows nas estações de trabalho.

Tabela 6.4: Ativos de *Software* - Sistemas Operacionais

Nome	**Finalidade**
Microsoft Windows XP	Estação de Trabalho
Microsoft Windows Vista	Estação de Trabalho
Microsoft Windows 7	Estação de Trabalho
Microsoft Windows 8/8.1	Estação de Trabalho
Microsoft Windows Server	Servidores Diversos
Linux (Distribuições)	Servidores Diversos

A Tabela 6.5 contém os softwares mais usados no dia-a-dia instalados nas estações de trabalho.

Tabela 6.5: Ativos de *Software* - Aplicativos

Nome	**Observação**
Microsoft Office 2010/2013	
Internet Explorer/ Mozilla Firefox/ Chrome	
Libre Office (Versões Diversas)	
Leitor PDF	
Autocad	
Plugins (Java, Flash)	
Antivírus	Solução adquirida pela organização
Compactador/Descompactador	Não existe um padrão
Softwares do Serpro	Setores específicos

A Tabela 6.6 contém os ativos da informação mais comumente gerados ou mantidos sob a guarda dos *campi*.

Tabela 6.6: Ativos de Informação

Tipo	**Detalhes**
Documentos e bases de dados diversas	Compartilhados em rede, podem conter dados sensíveis. Fundamentais para o desempenho das atividades administrativas e de ensino

A Tabela 6.7 contém os ativos humanos relativos à tecnologia da informação. Os *campi* contam com apenas duas pessoas cada um.

Tabela 6.7: Ativos - Pessoas

Cargo	**Quantidade**
Técnico de Tecnologia da Informação	2 por *campus*

Conforme a pesquisa, ainda foram informados os serviços da Tabela 6.8 como os serviços principais de tecnologia da informação percebidos pelo usuário como prestados pelo *campus* e ligados diretamente ou indiretamente aos ativos críticos. Estes serviços também servem de trampolim para outros serviços oferecidos no âmbito da organização, como *e-mail* institucional, sistemas acadêmicos, sistemas administrativos, entre outros.

Tabela 6.8: Serviços de TI - *Campus*

Nome do Serviço	**Relação com os Ativos de TI**
Serviço de Compartilhamento de Arquivos	Direta
Serviço de Impressão	Direta
Serviço de Internet e Redes	Direta
Serviço de Telefonia Fixa	Direta
Suporte à Infraestrutura de TI	Direta
Rede Elétrica Estabilizada	Direta (Parcial)

6.1.2 Identificação de Riscos

A pesquisa mostrou que cada *campus* possui somente dois funcionários de tecnologia da informação, ocupantes do cargo Técnico de Tecnologia da Informação, sendo efetivamente as pessoas detentoras de conhecimento técnico e realizando as mais diversas atividades de TI no *campus*. Embora existam outros cargos técnico-administrativos relativos à tecnologia da informação no âmbito das Instituições Federais de Ensino vinculadas ao MEC [7],

os *campi* só possuem o cargo citado. Uma decisão interna aloca os Analistas de Tecnologia da Informação na Reitoria, e embora o *campus* possa teoricamente solicitar outros cargos de tecnologia que não o de Analista, existe a limitação do quantitativo geral de técnicos por *campus*, conformidade com planejamentos internos feitos e a limitação aos cargos previstos nos concursos. Isso levou a uma situação em que os Técnicos de Tecnologia da Informação representam a TI do *campus*, não estando ligados a uma coordenação específica de tecnologia, e sim ligados diretamente à Diretoria de Administração do *campus* (normalmente somente os coordenadores estão diretamente ligados à Diretoria e os demais funcionários ligados a cada setor).

Desta forma, o levantamento de riscos foi dirigido a esses funcionários. Conforme ajuste de escopo apresentado no Capítulo 5, a pesquisa está restrita aos *campi* com estrutura definitiva de tecnologia da informação. Existem dois técnicos por *campus*, sendo cinco *campus* implantados, constituindo uma população de 10 pessoas.

No levantamento de riscos, além da opinião da equipe técnica, também é interessante obter a opinião dos administradores [65], desta forma a pesquisa também abordou o segundo grupo. Nos *campi*, a alta gestão é representada pelo Diretor Geral [36], sendo o cargo máximo administrativo e político do *campus*. Há um Diretor Geral por *campus*, totalizando uma população de cinco Diretores Gerais.

Um pré-teste foi aplicado com um funcionário de TI e um Diretor Geral. Não houveram sugestões ou reclamações quanto à forma ou conteúdo, sendo aplicados sem alterações.

O questionário dos Apêndice I foi aplicado aos Técnicos de TI dos *campi* implantados e o questionário do Apêndice J foi aplicado aos Diretores Gerais. Os questionários possuem campos para riscos relativos à *hardware*, *software*, pessoas (equipe técnica) e informação, e também um quinto campo para informações que os entrevistados eventualmente entendessem que não se encaixavam nas outras categorias, mas fossem fonte de riscos.

Aparte da explicação inicial, os questionários são idênticos. Devido à alta carga de trabalho da Direção Geral e à dificuldade de contato em tempo hábil, foi estabelecido uma participação mínima de 51%, isto é, mais da metade dos Diretores Gerais.

Conforme contato inicial com os participantes, ao menos duas Direções Gerais expressaram a preferência por questionários digitais para seu *campus*, uma vez que os turnos de trabalho e a disponibilidade do funcionário no momento pudessem inviabilizar a aplicação presencial. Dessa forma, conforme previsto na pesquisa, os questionários foram aplicados de forma eletrônica, permitindo ao respondente maior liberdade na disponibilização de tempo para responder bem como permitindo acompanhamento à distância pelo pesquisador.

As respostas não precisavam estar vinculadas especificamente a um único ativos crítico, embora os mesmos estivessem disponíveis para consulta.

6.1.3 Resultados da Identificação de Riscos

Participaram todos os Técnicos de Tecnologia da Informação dos cinco *campi* implantados do ponto de vista de tecnologia da informação, totalizando dez técnicos, bem como três dos cinco Diretores Gerais.

Diretores e técnicos levantaram questões bem parecidas ou que se complementaram. As respostas foram compiladas em um segundo questionário para avaliação dos mesmos. Não houveram maiores dificuldades por parte dos usuários para responder o levantamento.

6.1.4 Avaliação de Riscos

Foi elaborado o questionário presente no Apêndice L com as respostas de diretores e técnicos transformadas em perguntas. Como em alguns casos foram levantados riscos parecidos, os mesmos foram combinados em um único risco. Para obter o peso do risco, os problemas compilados foram apresentados na forma de duas perguntas fechadas para cada risco levantado, uma para probabilidade e outra para o impacto do risco ocorrer. Foram apresentadas escalas para probabilidade e impacto [45]. Somente os técnicos foram consultados nesta etapa. Desejava-se a opinião da gestão no levantamento, o que foi obtido, e então formulado o questionário de avaliação. Os Diretores Gerais foram consultados novamente junto do restante dos usuários na proposta de validação.

6.1.5 Pré-teste da Avaliação de Riscos

Após elaborado o questionário inicial, o mesmo foi submetido a dois técnicos que fazem parte da população de respondentes dos Técnicos de Tecnologia da Informação dos *campi* implantados para análise e melhora. A última questão permitia ao candidato enviar sugestões. O respondente também poderia se expressar verbalmente ou enviar *e-mail* para sugestões. O pesquisador também sugeriu alterações ao respondente e registrou se o mesmo concordava. O Apêndice K contém as principais considerações feitas em relação ao questionário, resultando no questionário presente no Apêndice L.

6.1.6 Resultados da Avaliação de Riscos

O Apêndice M contém as respostas do questionário. Dez técnicos participaram desta etapa da pesquisa, perfazendo a população total dos profissionais de tecnologia da informação dos *campi* implantados.

Uma vez obtidas as respostas, cada risco foi calculado multiplicando probabilidade pelo impacto usando valores numéricos para cada categoria [45]. Como se tratavam de 10 respostas, foram calculados 10 valores para cada risco, um para cada técnico, e usada a

média simples de forma que:
Risco=(Risco1+Risco2+...+Risco10)/10 para cada um dos 27 riscos levantados.

Os riscos foram classificados usando a média das avaliações feitas pela equipe técnica e organizados do maior para o menor. Foram atribuídas as categorias de tratamento sugeridas na matriz de risco de Manuele [45]. A Tabela 6.9 contém o resultado final da avaliação de riscos. A primeira coluna representa uma identificação para os riscos, a segunda coluna contém a descrição do risco. A terceira coluna contém o valor do risco - a média das avaliações feitas pela equipa técnica. Por fim, a quarta coluna contém a categoria de ação de acordo com o valor do risco.

Tabela 6.9: Riscos da Infraestrutura de TI do IFB

ID	**Descrição do Risco**	**Valor**	**Ação**
R01	Equipamentos de tecnologia da informação (como Desktops, Notebooks, Switches, Servidores) ficarem sem garantia ou manutenção especializada em seu tempo de vida útil	17	Categoria 4 (Ação imediata necessária)
R02	Ser necessária manutenção para a solução de *Datacenter* do *campus*, incluindo solução de contenção de calor e *nobreak*, e não haver manutenção contratada	16	Categoria 4 (Ação imediata necessária)
R03	A equipe de TI do *campus* não ser suficiente para atender as demandas	14,9	Categoria 3 (Ação corretiva deve ter alta prioridade)
R04	A internet do campus ser usada para cometer crimes virtuais (como DDOS, disseminação de arquivos indevidos, injúria) através dos computadores de acesso público ou *Wi-Fi*	14,4	Categoria 3 (Ação corretiva deve ter alta prioridade)
R05	O técnico não possuir capacitação básica para lidar com alguma ou várias das tecnologias necessárias para o funcionamento saudável da tecnologia da informação do *campus*	13,9	Categoria 3 (Ação corretiva deve ter alta prioridade)
R06	A falta de uma Coordenação de Tecnologia da Informação afetar a qualidade dos serviços prestados pela equipe de TI	13,9	Categoria 3 (Ação corretiva deve ter alta prioridade)

Tabela 6.9 Riscos da Infraestrutura de TI do IFB (continuação)

ID	Descrição do Risco	Valor	Ação
R07	Políticas e decisões de tecnologia da informação que afetam os *campi* sejam tomadas sem que o *campus* seja devidamente consultado	13,8	Categoria 3 (Ação corretiva deve ter alta prioridade)
R08	Ser necessário restaurar arquivos, sistemas, servidores ou serviços através de *backup*, mas o *backup* não existir	13,5	Categoria 3 (Ação corretiva deve ter alta prioridade)
R09	Pessoas não autorizadas (servidores ou não) terem acesso às salas técnicas e *datacenter*	13,4	Categoria 3 (Ação corretiva deve ter alta prioridade)
R10	Equipamentos serem danificados devido ao mau uso ou depredação nas salas de aula e laboratórios	13,3	Categoria 3 (Ação corretiva deve ter alta prioridade)
R11	Falta de proteção na rede elétrica (*nobreak*, rede estabilizada) causar danos aos equipamentos de tecnologia da informação	13,3	Categoria 3 (Ação corretiva deve ter alta prioridade)
R12	Equipamentos de tecnologia da informação (como *Desktops*, *Notebooks*, *Switches*, Servidores) obsoletos continuarem sendo utilizados	13	Categoria 3 (Ação corretiva deve ter alta prioridade)
R13	O *firmware* dos equipamentos de rede (*switches*, *gateways* de voz, etc.), *desktops* (BIOS) e outros equipamentos de TI estarem desatualizados	12,8	Categoria 3 (Ação corretiva deve ter alta prioridade)
R14	*Desktops* e *Notebooks* e/ou seus componentes serem roubados devido à falta de segurança física (cadeados, cabos de aço, câmeras, vigilância)	12,7	Categoria 3 (Ação corretiva deve ter alta prioridade)
R15	Falta de clareza nas atribuições do cargo de Técnico de Tecnologia da informação afetar os serviços de TI que se espera do *campus*	12,2	Categoria 3 (Ação corretiva deve ter alta prioridade)

Tabela 6.9 Riscos da Infraestrutura de TI do IFB (continuação)

ID	Descrição do Risco	Valor	Ação
R16	Sistemas operacionais Windows Server descontinuados continuarem sendo usados nos servidores	12	Categoria 3 (Ação corretiva deve ter alta prioridade)
R17	O técnico se acidentar com *nobreaks* e equipamentos de estabilização de rede elétrica instalados no *datacenter* ou salas técnicas	11,9	Categoria 3 (Ação corretiva deve ter alta prioridade)
R18	Aquisições de tecnologia da informação destinadas aos *campi* sejam feitas sem que o campus seja devidamente consultado	11,9	Categoria 3 (Ação corretiva deve ter alta prioridade)
R19	Sistemas operacionais Windows descontinuados continuarem sendo utilizados em *desktops* e *notebooks*	11,8	Categoria 3 (Ação corretiva deve ter alta prioridade)
R20	A falta de uma política de segurança da informação atualizada afetar a qualidade dos serviços prestados pela equipe de TI	11,6	Categoria 3 (Ação corretiva deve ter alta prioridade)
R21	*Softwares* antivírus não estarem instalados em servidores e computadores em geral	11,3	Categoria 3 (Ação corretiva deve ter alta prioridade)
R22	Brechas de segurança ou incidentes devido à falta de gerenciamento de senhas de administrador	11,1	Categoria 3 (Ação corretiva deve ter alta prioridade)
R23	Sistemas operacionais Windows com suporte a atualizações serem utilizados sem a aplicação das atualizações em *desktops* e *notebooks*	11,1	Categoria 3 (Ação corretiva deve ter alta prioridade)
R24	*Softwares* instalados para uso no dia-a-dia nos *desktops* estarem desatualizados ou obsoletos	10,3	Categoria 3 (Ação corretiva deve ter alta prioridade)

Tabela 6.9 Riscos da Infraestrutura de TI do IFB (continuação)

ID	Descrição do Risco	Valor	Ação
R25	A equipe de TI não manter uma lista de *softwares* testados e aprovados (homologados) que possam ser instalados nos computadores	10	Categoria 3 (Ação corretiva deve ter alta prioridade)
R26	Pessoas não-autorizadas, de forma intencional ou não, terem acesso às pastas compartilhadas em rede devido à má configuração do controle de acesso	10	Categoria 3 (Ação corretiva deve ter alta prioridade)
R27	O uso alternado do Microsoft Office e Libre Office inutilizar documentos ou gerar incompatibilidades nos documentos utilizados	8,1	Categoria 2 (Ação corretiva a ser tomada em momento adequado)

Todos os riscos entraram em categorias que indicam que precisam ser tratados. Os riscos R01 e R02 foram os de maior peso, indicando maior urgência, de acordo com a avaliação. A manutenção dos equipamentos de fato pode ser um fator crítico, uma vez que um conjunto de equipamento de tecnologia é necessário para fornecer os serviços de tecnologia da informação para o usuário. A manutenção do *datacenter* também recebeu prioridade máxima. Os *datacenters* podem ser considerados o coração da tecnologia da informação, centralizando equipamentos importantes e distribuindo serviços. Seu colapso pode efetivamente impossibilitar o uso da tecnologia da informação em uma organização.

Entre os riscos mais brandos, a corrupção de arquivos pelo uso alternado de editores diferentes está presente. O Instituto Federal de Brasília começou a usar originalmente o BrOffice, migrando para o LibreOffice e finalmente usando concomitantemente a versão comercial da suíte de escritórios da Microsoft, o Microsoft Office, o que pode gerar problemas ao combinar a edição do mesmo arquivo com os dois programas diferentes.

Esta constituiu a avaliação dos riscos de tecnologia da informação, conforme a equipe de tecnologia da informação dos *campi* implantados. A equipe tem um foco técnico-administrativo, sendo detentoras de conhecimento e estando ligada ao ativos e serviços, sendo peça fundamental da tecnologia da informação. Sua opinião é válida e deve ser considera importante. Os riscos presentes na Tabela 6.9 representam portanto a visão de toda a população da equipe técnica. Conforme mostrou a Figura 2.2, o processo de gestão de riscos é um ciclo. Entretanto, devidos às limitações de tempo e escopo da pesquisa,

esse ciclo não pode ser fechado. Portanto, é necessário validar os riscos levantados pela equipe técnica.

O gerenciamento de riscos tem uma missão maior, que é um bem para a organização. A priorização ou não pode levar em consideração a opinião ou validação de outros setores da organização, os usuários, beneficiários de fato do serviços e infraestrutura.

A próxima seção apresenta uma proposta de validação para os riscos avaliados.

6.2 Validação da Pesquisa

O serviço principal ofertado pelo IFB é o ensino pesquisa e extensão. A Tecnologia da Informação apoia esta tarefa, através de infraestrutura e serviços. A organização é representada primariamente por funcionários públicos, que atuam nos mais diversos setores para fornecimento desta tarefa principal. Pode-se afirmar que esses funcionários são os principais usuários da tecnologia da informação para cumprimento da missão institucional. O processo de gerenciamento de riscos traz benefícios portanto para estes usuários, afetando a organização como um todo.

6.2.1 População

Formadores de opinião podem ser definidas como pessoas que, através de sua educação ou profissão, têm expertise para os quais as pessoas escutam ou respondem, líderes de opinião têm uma posição social ou proximidade com as pessoas, podendo ser vistos como pessoas que têm influência [51].

Foram escolhidos os Coordenadores e Diretores, e pessoas indicadas por eles, formando um conjunto de decisores e formadores de opinião.

A Tabela 6.10 contém o quantitativo de Coordenações e Direções de cada *campus*.

Tabela 6.10: Quantitativo de Coordenações dos *Campi*

Campus	**Quantidade de Coordenações**
Brasília	16
Gama	15
Planaltina	19
Samambaia	15
Taguatinga	15

Adaptado de: [36]

As diversas coordenações de curso não aparecem discriminadas nominalmente no organograma, uma vez que flutuam em relação ao eixo do *campus*, seu nível de implantação, quantidade de cursos entre outros fatores, sendo referenciada genericamente como Coordenação de Curso. Desta forma não foram contadas para o quantitativo de coordenações, sendo contadas como parte integrante da CGEN para respostas.

Novamente, o questionário foi aplicado por meios digitais. Sabe-se que questionários *online* podem ter um nível de resposta inferior a outras abordagens [24]. Uma série de fatores poderia impossibilitar a participação de determinadas coordenações, inclusive férias, carga de trabalho e motivação. Objetivou-se atingir ao menos 51% do conjunto das coordenações, sendo que todos os *campi* deveriam estar representados por cerca de metade de suas coordenações.

6.2.2 Impacto dos Riscos nos Serviços Prestados pela TI

Os funcionários dos mais diversos setores não são especialistas em tecnologia, lidando com as especialidades das suas áreas de atuação. Desta forma, simplesmente apresentar os riscos de tecnologia para os funcionários pode se mostrar problemático, uma vez que alguns riscos podem não fazer sentido para eles.

A infraestrutura de tecnologia da informação abrange diversos componentes, incluindo os serviços compartilhados de tecnologia da informação destinados a sustentar um processo maior de tecnologia da informação para o negócio [11] [47]. Os serviços de tecnologia da informação são percebidos de forma mais clara para os usuários do que alguns componentes para fornecer o serviço. Assim, os riscos levantados pela equipe de TI foram traduzidos em serviços afetados e equipamentos fundamentais para os usuários como computadores, de forma a dar uma noção clara ao usuário do que estaria sendo afetado. A tradução foi proposta com base na experiência do pesquisador.

A Tabela 6.11 mostra a "pergunta a ser feita" ao usuário e sua relação com os riscos levantados, que podem ter maior ou menor grau de relação. A Tabela também relaciona os serviços, equipamentos, processos e *softwares* afetados do ponto de vista do usuário.

Tabela 6.11: Correlação entre Riscos e Serviços

Pergunta para o Usuário	**Riscos Relacionados Diretamente**	**Riscos Relacionados Indiretamente**	**Serviços, Softwares, Processos e Equipamentos Relacionados**
Não ter internet disponível afeta meu trabalho	R01, R02, R08, R11, R12, R13	R03, R04, R05, R09, R16, R22	Serviço de Internet e Redes
Não poder imprimir arquivos afeta meu trabalho	R01, R02, R08, R11, R12, R13	R03, R04, R05, R09, R12, R16, R19, R22	Serviço de Impressão
Não ter compartilhamento de arquivos em rede (pastas em rede, pastas corporativas) disponível afeta meu trabalho	R01, R02, R03, R05, R08, R12, R13	R05, R09, R16	Serviço de Compartilhamento de Arquivos
Perder arquivos compartilhados em rede (pastas em rede, pastas corporativas) afeta meu trabalho.	R01, R02, R08, R11, R26	R03, R04, R09, R16, R20, R21, R22, R26	Serviço de Compartilhamento de Arquivos
O telefone fixo do campus não estar funcionando afeta meu trabalho	R01, R02, R08, R11, R12, R13	R03, R04, R05, R09, R13, R22	Serviço de Telefonia Fixa
Não ter suporte da área de tecnologia da informação para solucionar problemas afeta meu trabalho.	R03, R05, R06, R15, R17, R25	R20	Suporte à infraestrutura
Picos de energia que podem desligar ou danificar meu computador e outros equipamentos afeta meu trabalho	R02,R11	R09	Energia Elétrica Estabilizada

Tabela 6.11: Correlação entre Riscos e Serviços (continuação)

Pergunta para o Usuário	**Riscos Relacionados Diretamente**	**Riscos Relacionados Indiretamente**	**Serviços, Processos, Softwares, Processos e Equipamentos Relacionados**
Ter arquivos corrompidos porque foram feitos no Microsoft Office mas editados no Libre Office e vice-versa afeta meu trabalho	R27	R20	*Softwares* de Escritório
Computadores com defeito afetam meu trabalho	R01, R12	R13, R14	Computadores
Continuar usando computadores muito antigos afeta meu trabalho	R12		Computadores
Continuar usando sistemas operacionais antigos (como o Windows XP) afeta meu trabalho	R19		Sistemas Operacionais
Ter computadores que utilizo depredados ou danificados afeta meu trabalho	R10, R14		Computadores
Mudanças sem aviso prévio de políticas de tecnologia da informação ou equipamentos afetam meu trabalho	R7, R18		Políticas de Tecnologia da Informação
Computadores com vírus afetam meu trabalho	R21		*Softwares* de Escritório
Falta de uma política documentada de segurança da informação afeta meu trabalho.	R20		Políticas de Tecnologia da Informação
Computadores com o Windows sem atualizações afetam meu trabalho	R23		*Softwares* de Escritório
Computadores com versões antigas de programas como Chrome e Java afetam meu trabalho	R24		*Softwares* de Escritório
Terceiros terem acesso à(s) minha(s) pasta(s) compartilhada(s) em rede afeta meu trabalho.	R26	R01, R02, R03, R04	Serviço de Compartilhamento de Arquivos

Desejava-se a opinião do usuário com relação à necessidade do tratamento dos riscos levantados. Se o usuário concordasse que a falta ou problema no serviço ou equipamento afetasse o desempenho das suas atividades, existiria uma confirmação da necessidade de tratamento dos riscos associados.

6.2.3 Questionário

Escalas são usadas para medir atitudes, valores, opiniões e outras características que não sejam facilmente mensuradas, medindo o grau em que cada indivíduo exibe a característica de interesse [3].

Likert desenvolveu um princípio para medir atitudes ou opiniões [44]. Itens de Likert são compostos por duas partes, uma afirmação e a escala de resposta, a escala com cinco itens é vastamente usada, provavelmente representando uma conciliação entre os objetivos conflitantes de oferecer escolhas suficientes e tornar o questionário viável para os respondentes [41]. A escala de cinco itens pode ser considerada tradicional e as típicas nomenclaturas para as categorias são “Concordo Fortemente”,“Concordo”, “Não Concordo nem Discordo”, “Discordo” e “Discordo Fortemente” [43].

A intenção foi identificar a opinião dos entrevistados com relação ao comprometimento de suas atividades pela falta dos serviços. Prezou-se pela uniformidade na declaração, isto é, como o trabalho é afetado pela falta do serviço e a brevidade do questionário levando em consideração o tempo que o usuário iria despender para responder.

A pesquisa se destinou aos formadores de opinião, que fazem parte da gestão ou indicados por elas ou pelas direções. Desta forma, necessariamente não precisavam estar representados pelos coordenadores, mas por alguém que faz parte da Coordenação. Adicionalmente, deve ser levado em consideração o fator de férias, em que determinados respondentes não poderiam responder. No IFB, em alguns casos a Coordenação pode ser representada por uma única pessoa, sendo a pessoa o Coordenador e também único funcionário do setor. Desta forma se a pessoa estiver ausente, por férias ou motivo de saúde, por exemplo, não haverá resposta para a Coordenação. Foi levado em consideração este fator, e também dados os trabalhos escolares, da impossibilidade de resposta devido às atividades inerentes à organização e, por fim, o fator da participação ser voluntária.

6.2.4 Pré-teste e Versão Final

Um pré-teste foi aplicado, originalmente só continha as questão da Tabela 6.11 antes de incorporar alterações baseadas nas opiniões e sugestões presentes no Apêndice N. O questionário foi dirigido a três pessoas de dois *campi* diferentes.

Algumas questões foram melhoradas. A questão sobre uma política de tecnologia da informação mostrou algumas dúvidas dos usuários em relação a quais efeitos distintos teriam, embora relataram entender haver uma melhoria para a organização. A questão foi mantida por dizer respeito a um processo não desenvolvido adequadamente que afetaria outros equipamentos e serviços, embora pudesse não ficar claro ao usuário seus efeitos práticos.

Conforme usuários relataram que os serviços presentes na perguntas impactariam mais ou menos em suas funções, se tornou interessante incorporar uma segunda etapa no questionário em que eram perguntados aos usuários o quanto a falta de cada serviço afetaria o desempenho das atividades.

A segunda parte do questionário levou em consideração o nível em que a falta dos serviços principais afetava o usuário. Na pior das hipóteses ele não conseguiria desempenhar nenhuma atividade e na melhor das hipóteses conseguiria desempenhar todas as atividades, havendo um ponto médio em que ele conseguiria desempenhar razoavelmente as atividades. Alguns serviços, como o de pastas compartilhadas, poderiam não ser utilizados de forma ampla por todas as coordenações ou por todos os membros da coordenação. Desta forma foi adicionada uma opção que indicava que não era feito uso das pastas compartilhadas em rede.

Na ausência dos serviços, na área de rede estabilizada, não se colocou "sem rede elétrica estabilizada", preferindo-se colocar um dos efeitos negativos possíveis para o usuário de forma que ficasse mais claro para ele como suas atividades seriam afetadas, optando-se por "se houverem picos de energia".

Os usuários também relataram nunca ter participado de uma pesquisa de tecnologia da informação, ou mesmo de outras consultas dentro do órgão. Então, indagou-se ao conjunto de participantes se tiveram participação em outras pesquisas para entender se foram consultados ou não.

O questionário piloto foi reaplicado com a segunda etapa incorporada bem como a questão da participação em pesquisas. Os participantes do pré-teste não solicitaram correções ou mudanças.

O Apêndice O contém a versão final do questionário.

6.2.5 Cálculo Aplicado às Respostas dos Usuários

Cada resposta está associada a um único item da proposição, equivalendo portanto a um usuário, entre os possíveis itens "Discordo Fortemente", "Discordo","Nem discordo nem Concordo", "Concordo" e "Concordo fortemente", no *campus*. O total de respostas para cada item no campus foi dado pela soma total de quantas pessoas responderam àquele item, podendo ser definido como QtdItem.

Em cada *campus* o total de respondentes para cada pergunta pode também ser definido como a soma da quantidade de respondentes para cada item de resposta, de forma que:
TotalRespondentes = (QtdItem1 + QtdItem+ ... +QtdItem5)

Entretanto, a quantidade de respondentes para cada *campus* foi diferente, alguns tiveram mais respondentes, outros menos, quando eles deveriam representar porções iguais. Portanto, as respostas devem considerar os pesos.

Com relação à propriedade distributiva da multiplicação em relação à adição, pode-se afirmar que, dados três números naturais quaisquer a, b, c [49] [30]:
(a + b) X c = a X c + b X c

Desta forma os pesos podem ser atribuídos a quantos entrevistados responderam cada item da pergunta no *campus*, uma vez que a soma da quantidade de respondentes de cada item corresponde à soma da quantidade de pessoas que responderam à pergunta, estando aplicado o peso portanto ao todo.

O item com respectivo peso atribuído pode ser definida como:
ItemPesadoCampus= QtdItem X PesoCampus para cada *campus*

Para cada pergunta, destinada a todo o IFB, o valor de cada item da pergunta pode ser definido como a soma das quantidades pesadas de cada item por *campus*, de forma que:
RespostaItemPergunta = (ItemPesadoCampus1+...+ItemPesadoCampus5)

A porcentagem para cada item da pergunta pode ser definida como:
PorcentagemItemPergunta = (RespostaItemPergunta/TotalRespondentes) X 100

A fórmula deve ser aplicada à todas perguntas.

6.2.6 Resultados Esperados X Resultados Obtidos

Esperava-se que os usuários mostrassem uma atitude de concordância com o fato de que problemas com os recursos, serviços ou processos de tecnologia da informação afetassem seus trabalhos, concordando, portanto, com a posição levantada pela equipe de tecnologia da informação de que todos os problemas precisariam ser tratados.

A soma do resultado de PorcentagemItemPergunta, para os itens “Concordo” e “Concordo Fortemente” deveria portanto ser igual ou maior a 51% para todos as proposições feitas para o usuário, indicando concordância tácita da maioria simples com o fato de que o problema precisa ser tratado.

De acordo com o levantamento feito pelos técnicos, os riscos R01 e R02 deveriam ter prioridade máxima, enquanto o risco R27, de menor valor, poderia ter correção tomada em momento adequado.

O questionário foi enviado a Diretores Gerais e/ou respectivos Diretores de Administração/Ensino. Foi solicitado que respondessem e repassassem às suas Coordenações ou outras pessoas que gostariam de indicar e solicitassem que as mesmas respondessem e se possível indicassem alguém para responder o questionário. Um *e-mail* explicativo foi enviado informando detalhes sobre a pesquisa. Se não houvesse participação de determinadas Coordenações depois de alguns dias de envio do questionário, seria tentado contato individual. Nos casos em que não foi possível entrar em contato com Diretores Gerais e/ou Diretores de Administração/Ensino também foi tentado contato direto com as Coordenações.

O questionário obteve 77 respostas com relação aos cinco *campi* implantados. Como houve quantitativos diferentes de resposta para cada *campus*, foi atribuído um peso às respostas, assumindo que cada *campi* deveria ter respondido 1/5 do total de perguntas. O peso foi calculado dividindo a quantidade de respostas que cada *campi* deveria ter respondido para que houvesse participação uniforme (1/5 do total) pela quantidade real de respostas obtidas por cada *campi*, conforme Tabela 6.12. O Apêndice P contém as opiniões sem peso bem como o restante das respostas.

Tabela 6.12: Opinião dos Funcionários - Peso atribuído às Respostas dos *Campi*

Campus	**Quantidade de Respostas**	**20% do Total**	**Peso**
Brasília	12	15,4	1,28
Gama	26		0,59
Planaltina	14		1,10
Samambaia	18		0,86
Taguatinga	7		2,20
Total	77		

A Tabela 6.13 mostra o quantitativo de Coordenações e Direções que participaram.

Tabela 6.13: Opinião dos Funcionários - Quantitativo de Coordenações e Direções Respondentes

Campus	**Quantidade de Coordenações e Direções**	**Quantidade de Coordenações e Direções que Responderam**
Brasília	16	7
Gama	15	13
Planaltina	19	8
Samambaia	15	8
Taguatinga	15	7
Total	80	43

A Tabela 6.14 apresenta os resumos com relação à todas as proposições feitas aos usuários, devidamente pesadas.

Tabela 6.14: Concordância dos Usuários com as Declarações

Proposição	**Disc. Fort.**	**Disc.**	**Nem Disc. nem Conc.**	**Conc.**	**Conc. Fort.**	**Taxa de Concordância**
Não ter internet disponível afeta meu trabalho	3,97%	2,20%	2,22%	15,93%	75,68%	91,61%
Não poder imprimir arquivos afeta meu trabalho	0,00%	5,40%	2,54%	23,54%	68,52%	92,06%
Não ter comp. de arquivos em rede (pastas em rede, pastas corporativas) disponível afeta meu trabalho	0,00%	6,51%	13,63%	28,80%	51,06%	79,87%

Tabela 6.14 Concordância dos Usuários com as Declarações (continuação)

Proposição	**Disc. Fort.**	**Disc.**	**Nem Disc. nem Conc.**	**Conc.**	**Conc. Fort.**	**Taxa de Concordância**
Perder arquivos compartilhados em rede (pastas em rede, pastas corporativas) afeta meu trabalho	0,00%	6,43%	10,61%	21,41%	61,55%	82,96%
Não ter telefone fixo disponível para realizar ou receber ligações afeta meu trabalho	8,60%	8,82%	16,59%	40,92%	25,07%	65,99%
Não ter suporte da área de tecnologia da informação para resolver problemas afeta meu trabalho	0,77%	7,14%	2,54%	20,51%	69,04%	89,55%
Picos de energia que podem desligar meu computador e outros equipamentos afeta meu trabalho	0,00%	0,00%	4,21%	48,57%	47,23%	95,79%
Ter arquivos corrompidos porque foram feitos no Microsoft Office mas editados no Libre Office e vice-versa afeta meu trabalho	3,86%	0,00%	4,42%	37,33%	54,39%	91,72%
Computadores que não funcionam afetam meu trabalho	0,00%	0,00%	3,63%	20,46%	75,92%	96,37%

Tabela 6.14 Concordância dos Usuários com as Declarações (continuação)

Proposição	**Disc. Fort.**	**Disc.**	**Nem Disc. nem Conc.**	**Conc.**	**Conc. Fort.**	**Taxa de Concordância**
Continuar usando computadores muito antigos afeta meu trabalho	1,67%	0,77%	10,96%	35,92%	50,69%	86,61%
Continuar usando sistemas operacionais antigos (como o Windows XP) afeta meu trabalho	3,55%	3,55%	22,08%	48,57%	22,26%	70,83%
Ter computadores que utilizo depredados afeta meu trabalho	0,77%	1,43%	4,21%	34,67%	58,93%	93,60%
As tomadas de decisões de tecnologia da informação sem prévia consulta ao campus afetam meu trabalho	0,00%	1,43%	19,86%	39,41%	39,30%	78,71%
Falta de uma política documentada de segurança da informação afeta meu trabalho	0,00%	1,88%	21,28%	43,30%	33,53%	76,84%
Computadores com vírus afetam meu trabalho	0,00%	0,00%	4,29%	30,35%	65,36%	95,71%
Computadores com o Windows sem atualizações afetam meu trabalho	5,29%	4,76%	15,80%	40,73%	33,41%	74,15%

Tabela 6.14 Concordância dos Usuários com as Declarações (continuação)

Proposição	**Disc. Fort.**	**Disc.**	**Nem Disc. nem Conc.**	**Conc.**	**Conc. Fort.**	**Taxa de Concordância**
Ter que usar versões antigas de programas como Chrome e Java afeta meu trabalho	8,49%	4,63%	12,25%	43,46%	31,16%	74,62%

A concordância pode ser definida como a soma das porcentagens das respostas "Concordo" e "Concordo Fortemente", indicando uma opinião afirmativa quanto à proposição. Todas as proposições tiveram uma taxa de concordância acima de 51%.

"Computadores que não funcionam afetam meu trabalho" teve uma taxa de concordância de 96,37%, sendo o problema que mais teve concordância por parte dos usuários. Nenhum dos entrevistados discordou da afirmação, com apenas 3% optando por uma instância neutra. Entre os riscos levantados pelos técnicos, o risco de número R01, de maior peso, diz respeito à falta de manutenção para equipamentos de TI, incluindo computadores. O fato de que tantos usuários concordaram mostra que o risco levantados pelos técnicos também têm a concordância de prioridade máxima do ponto de vista dos usuários.

"Picos de energia que podem desligar meu computador e outros equipamentos afeta meu trabalho" teve uma concordância de 95,79%, sendo o segundo item com maior concordância. O risco R02, o segundo de maior peso levantado pelos técnicos, diz respeito à solução de *datacenter*, que incluía *nobreak* para dar suporte à rede elétrica estabilizada. Novamente, nota-se uma sincronia entre as prioridades máximas definidas pela equipe técnica e o ponto de vista dos usuários.

Computadores com vírus tiveram 65% dos usuários concordando fortemente que o fato afetaria seu trabalho, sendo que a taxa concordância foi de 95,71%. O terceiro maior em taxa de concordância. Tendo um computador em casa e trabalhando com computadores em suas atividades, é bastante provável que os usuários já tiveram experiências traumáticas com vírus, entendendo seus efeitos e indicando priorização.

A proposição "Não ter telefone fixo disponível para realizar ou receber ligações afeta meu trabalho" foi a que menos teve taxa de concordância, estando em 65,99%.

As proposições tinham relações diretas ou indiretas com os riscos, dessa forma, os dados indicam a concordância tácita da maioria dos usuários com a necessidade do tra-

tamento dos riscos. Validando, portanto, a necessidade de tratamento de todos os riscos levantados.

A Tabela 6.15 contém o nível em que o problema no serviço ou equipamento afeta o desempenho das atividades do usuário, de acordo com a opinião coletada na pesquisa. Os dados estão pesados, da mesma forma que os dados relativos às proposições da Tabela 6.14.

Tabela 6.15: Opinião dos Funcionários - Resumo do Nível em que o Problema Afeta as Atividades

Ausência do Serviço	**Nenhuma atividade**	**Poucas atividades**	**Razoavelmente**	**Muitas atividades**	**Todas tividades**	**Não usa**
Sem Internet	14,35%	55,60%	17,23%	8,28%	4,52%	
Sem Pastas Compatilhadas em Rede	6,94%	29,43%	22,51%	20,98%	10,37%	9,76%
Sem telefonia fixa	1,67%	19,19%	27,01%	32,94%	19,19%	
Sem impressão	7,52%	55,02%	26,84%	10,61%	0,00%	
Sem suporte de tecnologia da informação	15,35%	36,32%	36,52%	9,58%	2,22%	
Se houverem picos de energia	21,37%	31,68%	37,42%	9,52%	0,00%	
Sem computador para usar	53,36%	35,76%	8,65%	2,22%	0,00%	

Os dados da Tabela 6.15 complementam os dados da Tabela 6.14, oferecendo detalhes da forma como os usuários sentem-se prejudicados no desempenho de suas atividades. O item cuja falta ou indisponibilidade mais apresentou impacto foi o computador, em que 53,36% dos usuários informaram que não conseguiriam desempenhar nenhuma atividade, e outros 35,76% conseguiriam desempenhar poucas atividades, totalizando quase 90% de usuários que teriam suas atividades comprometidas de forma severa. O problema com ativo está relacionado ao risco da falta de manutenção ou garantia de equipamentos

A ausência de internet e impressão também tem destaque, nos dois casos, cerca de 55% dos respondentes informaram conseguir poucas atividades com a ausência do serviço. Com a ausência da internet, 14,35% dos usuários também informaram que não conseguiriam

desempenhar nenhuma atividade. A ausência do serviço está ligada aos riscos da falta de manutenção do *datacenter* e a falta de manutenção ou garantia para ativos.

A telefonia fixa apresentou números inferiores se comparada a outros serviços, nas opções em que o usuário seria mais severamente afetado. Apenas 1,67% dos usuários informaram que não conseguiriam desempenhar nenhuma atividade, e outros 19,19% informaram conseguir despenhar poucas atividades. Foi o serviço em que mais usuários conseguiriam desempenhar todas as atividades, totalizando também 19,19%. É provável que, com internet, a maior parte das atividades poderia ser executada. Suprimindo assim necessidade do telefone ou permitindo postergá-las. A ausência do serviço também está ligada aos riscos da falta de manutenção do *datacenter* e a falta de manutenção ou garantia para ativos.

A Figura 6.2 apresenta a participação dos usuários entrevistados em outras pesquisas sobre a tecnologia da informação no órgão. Como a pergunta remete a um dado mais individualizado, e não a uma média por *campus*, os dados não foram pesados.

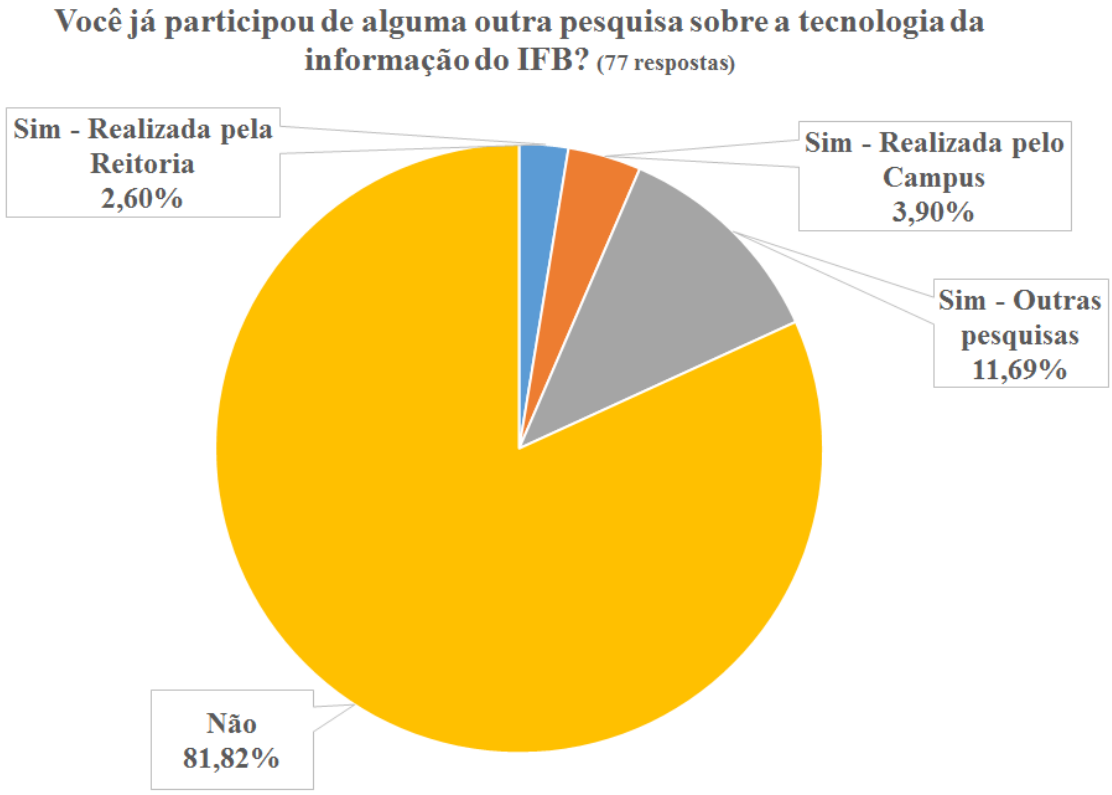


Figura 6.2: Participação dos Funcionários em Pesquisas Sobre a TI

Nota-se que uma maioria de usuários jamais participou de pesquisas relativas à tecnologia da informação no órgão, seja realizadas pelo órgão ou por terceiros. A participação do usuário é importante, até mesmo para aumentar sua conscientização sobre o uso do recursos e também suas responsabilidades.

A maioria dos usuários concordou com as proposições apresentadas de que a falta de determinado serviço de TI afetaria seu trabalho, tendo um índice de concordância de no mínimo 65% e máximo de 96%. Com relação ao nível em que a ausência do serviço ou equipamento afeta as atividades, os itens mostraram afetar de forma variada o usuário. A falta do computador merece destaque, sendo que um total de quase 90% dos usuários informaram ter suas atividades severamente afetadas. Já o serviço de telefonia, no outro extremo, mostrou afetar menos as atividades dos usuários.

Os dados indicaram uma concordância tácita do usuário com a necessidade de tratamento dos riscos e também elicitaram o quanto a concretização do riscos, resultando na ausência ou indisponibilidade de serviços e equipamentos, pode afetar o usuário.

Conforme ficou evidente nas respostas, uma maioria esmagadora de participantes nunca participou de qualquer pesquisa de tecnologia da informação sobre o órgão, sejam pesquisas realizadas pelo próprio órgão, sejam pesquisados de origem diferente. Esta resposta reforça o risco levantado pela equipe de TI com relação ao processo decisório de tecnologia da informação, em que muitas vezes não há consulta aos *campi*. Embora possa não ser possível incluir o usuário em todos as decisões de tecnologia da informação, uma vez que existirão decisões de cunho estritamente técnico que precisarão ser tomadas, limites orçamentários e outros restrições de diversas naturezas, é interessante buscar a participação do usuário quando possível.

A pesquisa validou os riscos levantados pelos técnicos, mais de 65% das respostas para cada questão indicaram concordância com o fato de que a falta do serviço afetaria as atividades, indicando uma concordância tática de que o problema deveria ser tratado.

O próximo capítulo apresenta as conclusões da pesquisa.

Capítulo 7

Considerações Finais

Este capítulo apresenta conclusões sobre a pesquisa e outras considerações.

A pesquisa teve como objetivo definir as bases para um plano de gerenciamento de riscos para a infraestrutura de tecnologia da informação comum aos *campi* do IFB, através da identificação de riscos e informações que eventualmente pudessem ser aproveitadas pela gestão - um diagnóstico.

Primeiro foi estudado o órgão objeto da pesquisa, identificada sua estrutura e peculiaridades. Não havendo um processo de gerenciamento de riscos bem definido no próprio órgão, foram pesquisadas outras instituições de ensino para possível importação ou aproveitando parcial. Foram escolhidos os Institutos Federais, por constituírem uma rede única, com estrutura geral e objetivos iguais definidos em lei, tornando-as instituições irmãs. A pesquisa abrangeu uma porção significativa dos IFs. Foi também pesquisada a UnB, por sua paridade com o IFB no DF como instituição pública federal *multicampi* e oferta do ensino superior, bem como estrutura geral similar.

O gerenciamento de riscos mostrou indícios de ainda caminhar nas instituições pesquisadas. Nos Institutos Federais pesquisados há indícios da ausência de um plano de gerenciamento de riscos devidamente formalizado. A rede dos IFs pode ser considerada nova e ainda existem desafios de gestão. No caso do CPD da UnB, há indícios de que existia um controle maior que se perdeu na transição dos computadores de grande porte para a microinformática, sofrendo a organização também com problemas de uma estrutura grande, diversidade de perfis e falta de pessoal para implementação de uma gestão de riscos. O problema da falta de pessoal também foi citado pelos entrevistados nos IFs pesquisados. O IFB, assim como a UnB, mostrou não ter coordenações específicas de governança devidamente montadas nas estruturas ou grupos responsáveis pela tecnologia da informação no órgão, embora haja movimentação neste sentido. A Universidade da Virgínia mostrou possuir um plano sólido que serviu como base para tomada de decisão ou referência durante a pesquisa, e a ISO 31000 foi usada como guia geral para

desenvolvimento da pesquisa.

Foram pesquisados os *campi* implantados do IFB, aqueles que tinham uma infraestrutura de tecnologia da informação mais avançada e ofereciam serviços e equipamentos no padrão que se esperava da organização, e também cuja infraestrutura serviria de referência para os outros *campi*. Foram levantados dados da infraestrutura e ativos junto ao Núcleo de Tecnologia do IFB. A equipe de tecnologia da informação e parte da gestão dos *campi* implantados foi então convidada a levantar riscos relativos à infraestrutura.

Os riscos foram compilados e apresentados em nova lista para a equipe técnica, que atribuiu valores à frequência com que poderiam ocorrer e a possível consequência de sua concretização, efetuando o processo de avaliação dos riscos. A lista final contendo os riscos avaliados foi elaborada, totalizando 27 riscos. Destes riscos, dois teriam prioridade máxima de acordo com a literatura usada como referência, outros 24 prioridade alta e um risco poderia ter ações corretivas tomadas em momento adequado. Ainda de acordo com a literatura utilizada, todos eles deveriam ser tratados. Os dois principais riscos levantados envolveram a falta de garantia ou manutenção especializada para equipamentos de TI bem como a falta de manutenção para a solução do *datacenter*. Riscos de infraestrutura encontrados no IFB também puderam ser encontrados em outros IFs e na UnB, como a obsolescência de ativos ou a falta de pessoal.

Os riscos avaliados representaram a opinião da equipe técnica, únicos mantedores da infraestrutura nos *campi* e portanto sua opinião foi considerada. Entretanto, o processo de gestão de risco é um ciclo, e como a pesquisa teve limitações de escopo e, naturalmente, tempo, não foi possível concretizar o ciclo, havendo apenas uma área de confluência entre o ciclo e a pesquisa. Não foi feito um processo de gerenciamento de riscos completo em que a organização oficialmente levantou, validou os riscos e acompanhou seu desenvolvimento, com as devidas peças de comunicação. Foi então proposta uma validação para a pesquisa.

Os funcionários da instituição, principais usuários da tecnologia da informação no intuito de executar a atividade fim, foram perguntados com relação aos riscos. Foram escolhidos formadores de opinião e pessoas indicadas por eles para validar os riscos. Os riscos foram traduzidos na forma como afetariam os serviços e equipamentos principais do ponto de vista do usuário, sendo apresentados na forma de proposições. Esperava-se que a maioria dos usuários concordassem com as proposições. De forma complementar, também foi perguntada a opinião do usuário com relação ao comprometimento de suas atividades com a ausência de determinado serviço ou equipamento, cuja interrupção ou indisponibilidade também estava relacionada com os riscos levantados.

Todas as proposições tiveram uma taxa de concordância acima de 51%. As proposições tinham relações diretas ou indiretas com os riscos, dessa forma, os dados indicaram a concordância tácita da maioria dos usuários com a necessidade de tratamento dos riscos.

Validando, portanto, a necessidade de tratamento de todos os riscos levantados. Os usuários também informaram em que nível suas atividades eram afetadas com a ausência de determinados serviços ou equipamentos, com destaque para o computador, em que quase 90% dos usuários informaram que suas atividades estariam altamente comprometidas. E a ausência de telefonia, que se mostrou o serviço que menos afetou o desempenho das atividades dos usuários.

A pesquisa sucedeu em sua proposição, definindo um contexto, levantando os riscos segundo a equipe técnica e, por fim, validando-os com os usuários. Culminando em um documento que pode atuar como diagnóstico da infraestrutura comum aos *campi* e servir à gestão como referência para estabelecimento de um Plano de Gerenciamento de Riscos. Forneceu também dados valiosos com relação à visão do usuário e os serviços essenciais para ele.

O criação de um Plano de Gerenciamento de Riscos deverá contar com uma equipe mista, envolvendo gestão e equipe técnica. A pesquisa sugeriu os responsáveis pelo processo dentro da organização. As causas dos riscos devem ser estudadas para definição de possíveis soluções. Alguns dos riscos podem requerer ajuda externa para elaboração de estudo específico, proposta de solução ou consulta, uma vez que podem envolver mudanças, conhecimentos ou orientações que extrapolem o conhecimento ou a área de atuação da equipe da instituição.

Os problemas levantados foram parcialmente transpostos nas demandas de um dos *campi* para o Plano Diretor de Tecnologia da Informação (PDTIC) para o biênio 2017-2018 que, até a data de finalização da pesquisa, ainda estava em discussão. Também foram apresentados em sua integridade aos responsáveis pela atualização inicial do Plano, efetivamente podendo ser estudados e trazer benefícios à organização.

Conforme mostrou a pesquisa com a equipe técnica e com os próprios usuários, a organização ainda precisa dar passos mais largos na inclusão efetiva de seus funcionários nas discussões de tecnologia da informação, bem como intensificar a atuação na parte de gerenciamento de riscos.

A pesquisa mostrou haver uma diferença entre os *campi*, sendo divididos entre implantados e não implantados/em implantação e que se esperava que os últimos eventualmente integrassem o mesmo grupo dos primeiros. No decorrer da pesquisa, os *campi* não implantados passaram quase todos para suas sedes definitivas. Entretanto, devido à uma série de limitações de recursos, não tiveram todos os recursos de rede e infraestrutura desejados implantados, incluindo a solução de *datacenter*, criando uma série de novos desafios de governança.

Alguns riscos se concretizaram ou foram solucionados. A falta de um contrato de manutenção para os *datacenters*, que atualmente não encontram-se resguardados por contrato

de manutenção, foi um risco efetivado.

Trabalhos futuros incluem adaptar a identificação e validação de riscos para incluir no processo de gestão de riscos os então considerados *campi* não implantados, agregar os riscos exclusivos da infraestrutura de cada *campi*, abrangendo toda a infraestrutura do órgão. Incluir as demais fases do processo de gerenciamento de riscos sugeridas pela ISO 31000, incluindo comunicação interna e um plano de tratamento e monitoramento dos riscos, construindo um Plano de Gerenciamento de Riscos para a Infraestrutura do IFB.

Referências

[1] ALLION SCIENCE AND TECHNOLOGY CORPORATION. Decision support/risk analysis - countermeasures. 2016. 19, 31

[2] S. ANTOLIK. Risk analysis in information security and tools used for risk analysis. *Advanced Research in Scientific Areas*, 7:1967–1971, 2012. 19, 31

[3] Donald ARY, Lucy Chesar JACOBS, Chris SORENSEN, e Ashgar RAZAVIEH. *Introduction to Reseach in Education*. Cengage Learning, 2009. 81

[4] EUROPEAN COURT OF AUDITORS. Risk assessment in performance audits, 2013. 8

[5] E. K. BEZERRA. *Gestão de Riscos de TI - NBR 27005*. Escola Superior de Redes, 2013. 16

[6] BRASIL. Governo eletrônico. http://www.governoeletronico.gov.br/. 2015. 53

[7] BRASIL. Lei nº 11.891, de 12 de janeiro de 2005. dispõe sobre a estruturação do plano de carreira dos cargos técnico-administrativos em educação, no âmbito das instituições federais de ensino vinculadas ao ministério da educação, e dá outras providências. 70

[8] BRASIL. Lei nº 11.892, de 29 de dezembro de 2008. institui a rede federal de educação profissional, científica e tecnológica, cria os institutos federais de educação, ciência e tecnologia, e dá outras providências. 1, 2, 40, 47, 52, 53, 54, 55

[9] BRASIL. Lei nº 9.394, de 20 de dezembro de 1996. estabelece as diretrizes e bases da educação nacional. 2, 53

[10] Portal Brasil. Surgimento das escolas técnicas. 2011. 1

[11] D. W. BROCKWAY e D. T. MCKAY. Building it infrastructure for the 1990s. *Stage by Stage*, 9(3):1–11, 1989. 15, 78

[12] A. CLEMENTS. *Principles of Computer Hardware*. Oxford University Press, New York, 2006. 16

[13] Donald R. COOPER e Pamela S. SCHINDLER. *Métodos de Pesquisa em Administração*. AMGH Editora, 12 edition, 2016. 34

[14] M. CROUHY, D. GALAI, e R. MARK. *The Essentials of Risk Management*. McGraw-Hill, 2006. 10

[15] MINISTÉRIO DA EDUCAÇÃO. Centenário da rede federal de educação profissional e tecnológica. http://portal.mec.gov.br/component/content/article?id=13175. 2015. 1

[16] MINISTÉRIO DA EDUCAÇÃO. Instituições de educação superior e cursos cadastrados (pesquisa de instituições públicas federais no distrito federal). http://emec.mec.gov.br/. 2015. 47

[17] MINISTÉRIO DA EDUCAÇÃO. Linha do tempo - rede federal de educação profissional e tecnológica. 2015. 1

[18] MINISTÉRIO DA EDUCAÇÃO. Portal do instituto federal de ciência e tecnologia - histórico. http://institutofederal.mec.gov.br/historico. 2015. 1

[19] MINISTÉRIO DA EDUCAÇÃO. Reitor é reemposado e mantém inclusão social como prioridade. 2015. 2

[20] EFORTRESSES. Control compliance suite 11. 2015. 18, 31

[21] ENISA. Inventory of risk management / risk assessment tools, 2006. 17, 18, 31

[22] J. J. S. FONSECA. *Metodologia da Pesquisa Científica.* Universidade Estadual do Ceará, 2002. 33

[23] F. J. A. FREITAS. Proposta de implementação do gerenciamento de serviços de tecnologia da informação no centro de informática da universidade de brasília, 2015. 51

[24] Ronald D. FRICKER e Matthias Schonlau RAND. Advantages and disadvantages of internet research surveys - evidence from the literature. *Field Methods*, 7:347–367, 2002. 78

[25] D. T. GERHARDT, T. E.and SILVEIRA. *Vantagem competitiva: criando e sustentando um desempenho superior.* Campus,Rio de Janeiro, 1989. 55

[26] D. T. GERHARDT, T. E.and SILVEIRA. *Métdos de Pesquisa.* Editora da UFRGS, Porto Alegre, 2009. 33

[27] A. C. GIL. *Como Elaborar Projetos de Pesquisa.* Editora Atlas, São Paulo, 2002. 33

[28] M. GORROD. *Risk Management Systems.* Palgrave Macmillan,New York, 2004. 10

[29] J. GRAHAN, B. AMOS, e T. PLUMPTRE. Principles of corporate governance, 2003. 7

[30] Ronald J. HARSHBARGER e James J. REYNOLDS. *Matemática Aplicada - Administração, Economia e Ciências Sociais e Biológicas.* AMGH Editora, 2013. Tradução Ariovaldo Griese e Oscar Kenjiro N. Asakura. 83

[31] J. L. HENNESSY e D. A. PATTERSON. *Computer Organization and Design - The Hardware Software Interface. 4th ed.* Elsevier, Waltham, 2012. 16

[32] IFB. Ifb em números. http://ifbemnumeros.ifb.edu.br/. 2016. 48, 60

[33] IFB. Ifb notícias. http://www.ifb.edu.br/. 2016. 60

[34] IFB. Plano diretor de tecnologia da informação 2011-2012, 2011. 58

[35] IFB. Resolução nº 12/2012 cs/ifb: Aprova o regimento geral do instituto federal de brasília, 2012. 58

[36] IFB. Resolução nº 35/2012 cs/ifb: Aprova, ad referendum do conselho superior, nova estrutura organizacional para o instituto federal de brasília, 2012. 56, 57, 58, 59, 71, 77

[37] IFB. Plano de desenvolvimento institucional 2014-2018, 2014. 47, 58

[38] INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE. *Board Briefing on IT Governance*. United States, 2003. 7

[39] PROJECT MANAGEMENT INSTITUTE. Organizational project management maturity model (opm3), 2003. 10

[40] PROJECT MANAGEMENT INSTITUTE. *A Guide to the Project Management Body of Knowledge – PMBOK Guide*. PMI, Newtown Square, 2009. 8

[41] R. JOHNS. Likert items and scales. *SURVEY QUESTION BANK: Methods Fact Sheet 1*, March 2010. 81

[42] Fabiana da Silva KAUARK, Fernanda Castro MANHÃES, e Carlos Henrique MEDEIROS. *Metodologia da Pesquisa - um guia prático*. Via Litterarum Editora, Itabuna, Brasil, 2010. 33

[43] Paul J. LAVRAKAS, editor. *Encyclopedia of Survey Reseach Methods*. Sage Publications, 2008. 81

[44] R. LIKERT. A technique for the measurement of attitudes. *Archives of Psychology*, 22(140), 1932. 81

[45] FRED A. MANUELE. Acceptable risk - time for sh&e professionals to adopt the concept. *Professional Safety*, 55(05)), 2010. 8, 9, 10, 72, 73

[46] H. MARKOWITZ. Portfolio selection. *Journal of Finance*, 7(1(March)):77–91, 1952. 8

[47] M. NYRHINEN. It infrastructure - structure, properties and process. *Helsinki School of Economics Working Papers*, W-403, 2006. 15, 78

[48] OECD. Principles of corporate governance, 1999. 7

[49] Célia Maria Carolino PIRES. *Números Naturais e Operações*. Editora Melhoramentos, 2013. 83

[50] Roger S. PRESSMAN. *Engenharia de Software - Uma abordagem profissional*. AMGH Editora, São Paulo, 2011. 16

[51] Neil RICHARDSON e Lucy LAVILLE. *Develop Your PR Skills*. Kogan Page, 2010. 77

[52] R. SALIBA e R. SAINT-GERMAIN. Callio secura 17799 - a tool for implementing the iso 17799 / bs 7799 standard. 17, 31

[53] M. SCRIVEN. The logic and methodology of checklists, 2000. 14

[54] CA SYSTEMS SECURITY. Cobra. 2016. 19, 31

[55] Caetana Juracy Rezende Silva. *INSTITUTOS FEDERAIS LEI 11.892, de 29/12/2008 - COMENTÁRIOS E REFLEXÕES*. Editora IFRN, Brasília, Brasil, 2009. 1

[56] Ian SOMMERVILE. *Engenharia de Software*. Addison Wesley, São Paulo, 2003. 16

[57] SYMATEC CORPORATION. Control compliance suite 11. 2015. 18, 31

[58] Andrew S. TANENBAUM. *Organização Estruturada de Computadores*. Pearson - Addison Wesley, 2006. 16

[59] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Abnt nbr iso 31000: Gestão de riscos - princípios e diretrizes, 2009. 4, 8, 11, 51, 52, 62

[60] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Abnt nbr iso 31010: Gestão de riscos - técnicas para o processo de avaliação de riscos, 2011. 11, 14

[61] UnB. Cpd - centro de informática. http://www.cpd.unb.br/. 2016. 48, 49

[62] UnB. Sobre a instituição. http://www.unb.br/. 2015. 47, 48

[63] TRIBUNAL DE CONTAS DA UNIÃO. *Governança Pública - Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública e Ações Indutoras de Melhoria*. Brasil, 2014. 7

[64] TRIBUNAL DE CONTAS DA UNIÃO. Questionário de governança de ti 2014, 2014. 40

[65] UNIVERSITY OF VIRGINIA. University of virginia information technology security risk management (its-rm) program, 2013. 17, 37, 39, 51, 64, 66, 67, 71

[66] E. ZAMBON, S. ETALLE, R. J. WIERINGA, et al. Model-based qualitative risk assessment for availability of it infrastructures. *Software & Systems Modeling*, 10:553–580, 2011. 32

Apêndice A

Questionário sobre Gestão de Riscos e Tecnologia da Informação nos Institutos Federais

Pesquisa Governança e Gestão de Risco – Rede Federal de Ensino

PARTE 1: VISÃO GERAL DA TECNOLOGIA DA INFORMAÇÃO E GESTÃO

Qual seu sexo? *
( ) Feminino
( ) Masculino

Qual seu órgão? *
( ) Instituto Federal do Acre
( ) Instituto Federal de Alagoas
( ) Instituto Federal do Amapá
( ) Instituto Federal do Amazonas
( ) Instituto Federal da Bahia
( ) Instituto Federal Baiano
( ) Instituto Federal de Brasília
( ) Instituto Federal do Ceará
( ) Instituto Federal do Espírito Santo
( ) Instituto Federal de Goiás
( ) Instituto Federal Goiano
( ) Instituto Federal do Maranhão
( ) Instituto Federal de Minas Gerais
( ) Instituto Federal do Norte de Minas Gerais
( ) Instituto Federal do Sudeste de Minas Gerais
( ) Instituto Federal do Sul de Minas Gerais
( ) Instituto Federal do Triângulo Mineiro
( ) Instituto Federal de Mato Grosso
( ) Instituto Federal de Mato Grosso do Sul
( ) Instituto Federal do Pará
( ) Instituto Federal da Paraíba
( ) Instituto Federal de Pernambuco
( ) Instituto Federal do Sertão Pernambucano,
( ) Instituto Federal do Piauí
( ) Instituto Federal do Paraná
( ) Instituto Federal do Rio de Janeiro
( ) Instituto Federal Fluminense
( ) Instituto Federal do Rio Grande do Norte
( ) Instituto Federal do Rio Grande do Sul
( ) Instituto Federal Farroupilha
( ) Instituto Federal Sul-rio-grandense
( ) Instituto Federal de Rondônia
( ) Instituto Federal de Roraima
( ) Instituto Federal de Santa Catarina
( ) Instituto Federal Catarinense
( ) Instituto Federal de São Paulo
( ) Instituto Federal de Sergipe
( ) Instituto Federal do Tocantins
( ) Outro (especificar):_____

Qual seu cargo? *
( ) Analista de Tecnologia da Informação
( ) Técnico de Tecnologia da Informação
( ) Técnico de Laboratório de Informática
( ) Tecnólogo em Segurança da Informação
( ) Outro (especificar): _____

Possui função gratificada ou cargo comissionado? *
( ) Sim (especificar): _____
( ) Não

Seu local de trabalho é *:
( ) Campus
( ) Reitoria
( ) Outro (especificar): _____

Quais as áreas principais em que você trabalha no seu dia-a-dia? *
(MARCAR UMA OU MAIS)
[ ] Desenvolvimento de Sistemas (desenvolvimento e manutenção de sistemas web e/ou aplicativos para outras plataformas)
[ ] Infraestrutura (redes, switches, internet, controle de acesso, etc.)

[ ] Suporte (instalação de equipamentos, auxílio ao usuário, montagem de computador)
[ ] Governança e Gestão de Risco

As atribuições do seu cargo estão bem definidas? *
( ) Sim
( ) Parcialmente
( ) Não

Você reconhece que exista uma política de capacitação voltada para a tecnologia da informação no seu órgão? *
( ) Sim
( ) Parcialmente
( ) Não

Você reconhece que exista uma política de capacitação geral no seu órgão? *
( ) Sim
( ) Parcialmente
( ) Não

Você participou da elaboração do Plano Diretor de Tecnologia da Informação (ou equivalente) da organização? *
( ) Sim
( ) Não

Você participou da elaboração do Plano de Desenvolvimento Institucional (ou equivalente) da organização? *
( ) Sim
( ) Não

Você reconhece a existência de uma política formal (documentada e obrigatória) de governança corporativa no seu órgão? *
( ) Sim
( ) Parcialmente (planejamento foi iniciado)
( ) Não

Você reconhece a existência de uma política informal (não documentada ou não obrigatória) de governança corporativa no seu órgão? *
( ) Sim
( ) Não

Você reconhece a existência de uma política formal (documentada e obrigatória) de governança de tecnologia da informação no seu órgão? *
( ) Sim
( ) Parcialmente (plano foi iniciado)
( ) Não

Você reconhece a existência de uma política informal (não documentada ou não obrigatória) de governança de tecnologia da informação no seu órgão? *
( ) Sim
( ) Não

Você reconhece a existência de uma política formal (documentada e obrigatória) de gestão de risco de tecnologia da informação no seu órgão? *
( ) Sim
( ) Parcialmente (plano foi iniciado)
( ) Não

Você reconhece a existência de uma política informal (não documentada ou não obrigatória) de gestão de risco de tecnologia da informação no seu órgão? *
( ) Sim
( ) Não

Existem quantas pessoas para atender as demandas de TIC na sua unidade (campus, etc.)? * _____

A equipe de TIC atual é suficiente para atender às demandas na sua unidade? *
( ) Sim, plenamente
( ) Parcialmente
( ) Não

A auditoria interna possui pessoal capacitado para avaliar a gestão de TIC? *
( ) Sim, plenamente
( ) Parcialmente
( ) Não

A estrutura física de TIC necessária para a sua unidade já está 100% disponível? *
( ) Sim
( ) Parcialmente
( ) Não

Existe um inventário acurado de todo o equipamento e software?
( ) Sim
( ) Parcialmente
( ) Não

A organização dispõe de um comitê de TI formalmente instituído, composto por representantes de áreas relevantes da organização? *
( ) Sim, plenamente
( ) Parcialmente
( ) Não

A organização define formalmente diretrizes para avaliação do desempenho dos serviços de TI ? *
( ) Sim, plenamente
( ) Parcialmente (iniciou plano)
( ) Não

O seu campus/unidade possui datacenter ou mini-datacenter? Como é feito o controle de acesso físico?

Existe auditoria interna de TI (não a auditoria geral do órgão, e sim auditoria do setor para o próprio setor)? *

Os serviços e contratos possuem Acordo de Nível de Serviço (SLA)? *

Se seu órgão for parte do SISP (como no caso dos Institutos Federais) o que é usado de fato no dia – a – dia? *

As perguntas a seguir estão divididas em seções. Leia cada sessão. Se você não souber ou não trabalhar na área não é necessário responder determinadas seções.

INFRAESTRUTURA

O que a sua organização usa para guardar dados do alunos e corporativos? Sistemas web? Planilhas no Excel? Eles estão em servidores ou computadores locais?

Os sistemas críticos estão em servidores em salas trancadas com acesso físico restrito?

Os servidores estão em salas com controle ambiental, como detectores de temperatura, água e fumaça?

Existem dispositivos de uso individual com dados sensíveis em áreas acessíveis ao público?

Os servidores estão longe de áreas com grande circulação de pessoas, como salas de aula?

Os computadores destinados ao público possuem dispositivos antifurto?

Os servidores e hardwares importantes estão ligados a Unidades de Fornecimento de Energia Ininterrupta (UPS) com controle de picos de energia?

Existe uma política de segurança relativa aos meios físicos de TI (acesso físico de pessoas a lugares, uso de dispositivos antifurto e coisas semelhantes)?

O seu datacenter e salas técnicas também possuem instalação elétrica predial como disjuntores e quadros de luz do bloco/prédio que não são da TI, funcionando também como uma "sala da energia elétrica"? Você considera isso problemático?

Os <u>funcionários</u> possuem login individual para acesso aos sistemas e computadores?

Os <u>alunos</u> possuem login individual para acesso ao sistemas e computadores?

Proteção contra picos de energia é usadas nos desktops? (ex.: rede estabilizada, proteção individual)

Existe um procedimento definido e documentado para definir nível de privilégio de acesso a pastas e documentos em servidores?

Existe um procedimento para incidentes de segurança (roubo, uso não autorizado, equipamentos comprometidos)? Os incidentes são documentados?

Os funcionários exonerados ou que mudaram de setor tem suas contas terminadas ou privilégios removidos em curto prazo?

A organização enfatiza que as credenciais de login são a chave para a identidade digital do usuário?

SEGURANÇA DA INFORMAÇÃO

Existe um plano de segurança da informação no seu órgão?
( ) Sim, plenamente
( ) Parcialmente
( ) Não

A segurança da informação é entendida como responsabilidade do órgão todo ou "somente da TI"?

Existe um processo bem definido para assegurar que problemas identificados são atendidos?

O que podem ser considerados ativos críticos da informação o seu órgão (dados de alunos, banco de dados de sistemas, etc.)?

Qual o tempo de resposta quando uma intrusão é detectada?

Quão bem a organização avalia e mitiga ameaças?

CONTINUIDADE DO NEGÓCIO

O seu órgão tem um plano de continuidade do negócio (para a organização)?
( ) Sim, plenamente
( ) Parcialmente (iniciou plano, algumas áreas)
( ) Não possui
( ) Não sei

Existe algum mecanismo para dificultar ataques feitos à organização?

O plano de continuidade do negócio é testado?
( ) Sim, plenamente
( ) Parcialmente
( ) Não, não é testado
( ) Não se aplica

Que vulnerabilidades existem na área de segurança da informação? Elas estão bem documentadas?

Existe um plano de recuperação de desastres de TI no seu órgão?

( ) Sim, plenamente
( ) Parcialmente (iniciou plano, algumas áreas)
( ) Não, não possui
( ) Não sei

O plano de recuperação de desastres de TI é testado?

( ) Sim, plenamente
( ) Parcialmente
( ) Não, não é testado
( ) Não se aplica

O plano de continuidade do negócio está alinhado com o plano de recuperação de desastres

( ) Sim
( ) Não
( ) Não se aplica

O plano de continuidade do negócio é bem comunicado?

( ) Sim
( ) Parcialmente
( ) Não
( ) Não se aplica

DISPOSITIVOS MÓVEIS

Como sua organização implementa o BYOD (Traga seu próprio dispositivo)?

Existe uma política para dispositivos móveis (pessoais ou corporativos)?

Quais vulnerabilidades nos dispositivos móveis podem ser exploradas e como a organização lida com elas?

Como sua organização lida com dispositivos móveis perdidos ou roubados?

CLOUD COMPUTING

Sua organização usa computação em nuvem (cloud computing) para alguma coisa?

Se sua organização usa computação em nuvem foram definidos dispositivos de segurança no contrato? Como responsabilidade nas perdas de dados?

VISÃO GERAL DA TECNOLOGIA DA INFORMAÇÃO E GESTÃO

A organização tem um inventário do uso de serviços em nuvem na TI e na organização?

Existe alguma vulnerabilidade no serviço usado nas nuvens?

Existe um levantamento de rico compreensivo que cubra todas as áreas?

RISCOS DE TIC

Como o processo de levantamento de riscos é efeito?

Quão bem sua organização lida com identificação de riscos?

O que é feito quando um risco é identificado?

Como o processo de gerenciamento de riscos pode ser melhorado?

Como os riscos são identificados e gerenciados ?

Há a oportunidade de combinar auditoria interna de TI com a auditoria do órgão?

A responsabilidade pelo risco estão claramente definida? Existe alguma responsabilidade documentada e seguida pelo comitê?

A organização usa software GRC ?
(Governança, Risco e Conformidade) Qual?

Como os riscos de projetos são levantados e gerenciados?

PROJETOS

A organização possui os processos e controles adequados para entrega de projetos em tempo dentro do orçamento e uso adequado de recursos?

Existe um processo de governança adequado para alinhar projetos e programas com os objetivos organizacionais?

Existe algum processo para medir benefícios alcançados depois de um projeto completado comparativamente com os benefícios que se esperava ao iniciar o projeto?

O risco pode ser considerado um evento incerto que terá efeitos negativos nos objetivos desejados. Os riscos estão associados a vulnerabilidades de software, hardware, humanas, estratégias e logísticas. Se desejar, você pode fazer abaixo descrição de quais riscos de tecnologia (ou corporativos que afetam a TI) que você acha que seu órgão enfrenta e suas causas. É um espaço livre para considerações. Você também pode falar de coisas que você acha que deveriam haver no seu órgão e que não existem.

A metodologia de gerenciamento de projetos está sendo seguida corretamente?

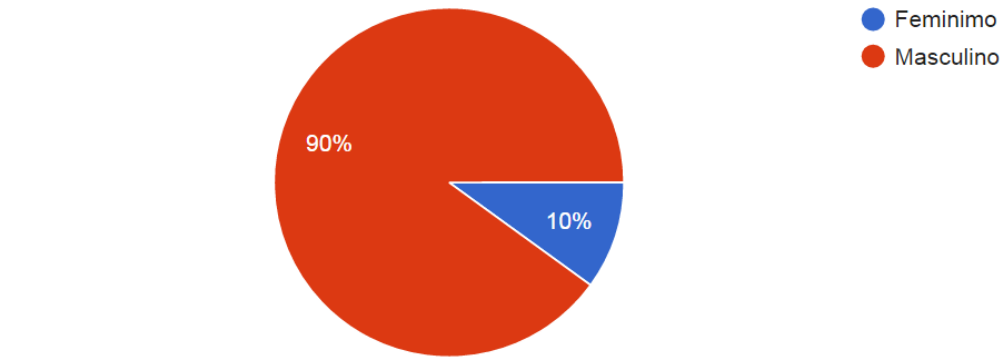
O que é feito quando um projeto está tendo um desempenho ruim?

Apêndice B

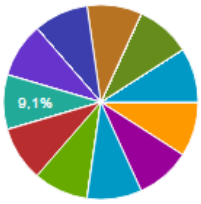
Questionário sobre Gestão de Riscos e Tecnologia da Informação nos Institutos Federais - Respostas

Pesquisa Governança e Gestão de Risco - Rede Federal de Ensino (respostas)

Qual seu sexo? (10 respostas)

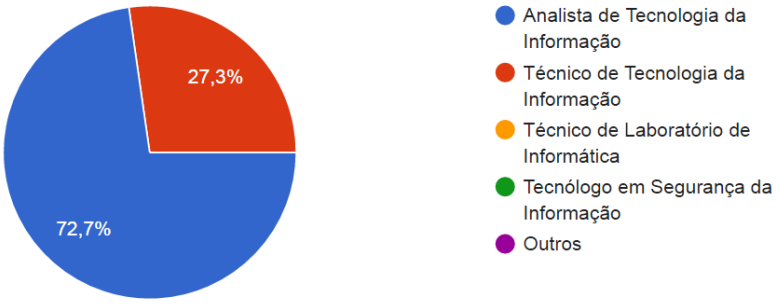


Qual seu órgão?

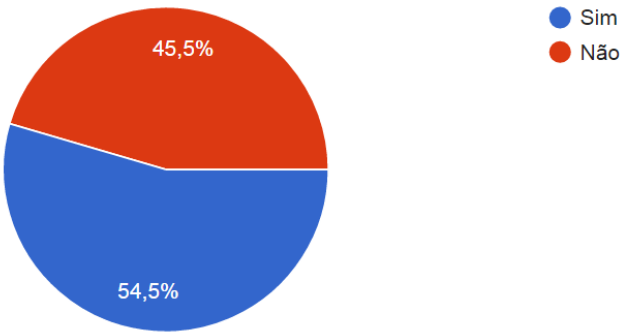


Instituto Federal do Acre	0	0%
Instituto Federal de Alagoas	0	0%
Instituto Federal do Amapá	1	9.1%
Instituto Federal do Amazonas	0	0%
Instituto Federal da Bahia	1	9.1%
Instituto Federal Baiano	1	9.1%
Instituto Federal de Brasília	0	0%
Instituto Federal do Ceará	1	9.1%
Instituto Federal do Espírito Santo	1	9.1%
Instituto Federal de Goiás	0	0%
Instituto Federal Goiano	0	0%
Instituto Federal do Maranhão	1	9.1%
Instituto Federal de Minas Gerais	0	0%
Instituto Federal do Norte de Minas Gerais	1	9.1%
Instituto Federal do Sudeste de Minas Gerais	0	0%
Instituto Federal do Sul de Minas Gerais	0	0%
Instituto Federal do Triângulo Mineiro	0	0%
Instituto Federal de Mato Grosso	0	0%
Instituto Federal de Mato Grosso do Sul	0	0%
Instituto Federal do Pará	1	9.1%
Instituto Federal da Paraíba	1	9.1%
Instituto Federal de Pernambuco	0	0%
Instituto Federal do Sertão Pernambucano	0	0%
Instituto Federal do Piauí	0	0%
Instituto Federal do Paraná	0	0%
Instituto Federal do Rio de Janeiro	0	0%
Instituto Federal Fluminense	0	0%
Instituto Federal do Rio Grande do Norte	1	9.1%
Instituto Federal do Rio Grande do Sul	0	0%
Instituto Federal Farroupilha	0	0%
Instituto Federal Sul-rio-grandense	0	0%
Instituto Federal de Rondônia	0	0%
Instituto Federal de Roraima	0	0%
Instituto Federal de Santa Catarina	0	0%
Instituto Federal Catarinense	0	0%
Instituto Federal de São Paulo	0	0%
Instituto Federal de Sergipe	1	9.1%
Instituto Federal do Tocantins,	0	0%
Outros	0	0%

Qual seu cargo? (11 respostas)



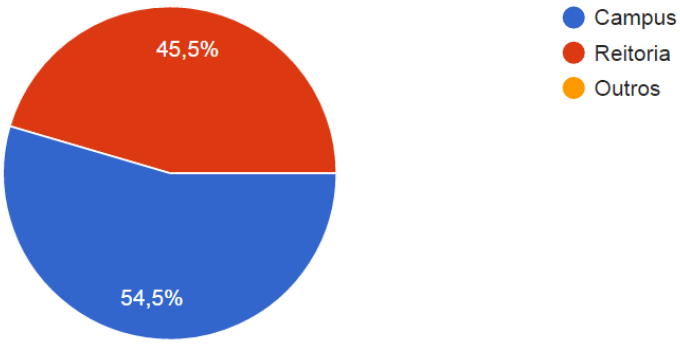
Possui função gratificada ou cargo comissionado? (11 respostas)



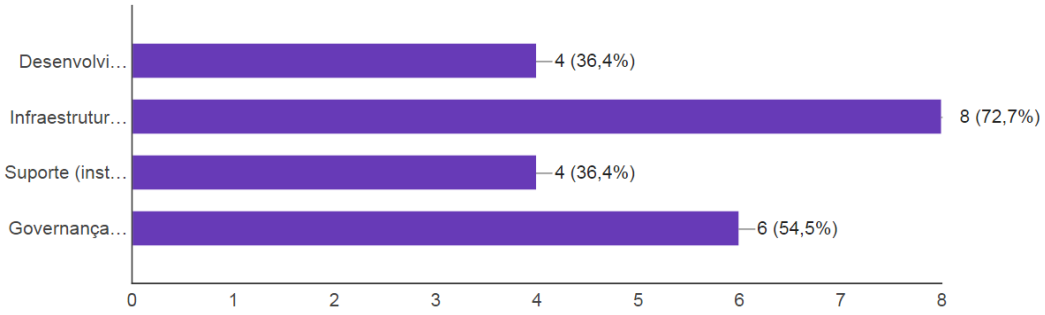
Qual função gratificada? (5 respostas)

Coordenador de TI
Coordenador de TI
CD-04
FG-2
FG2

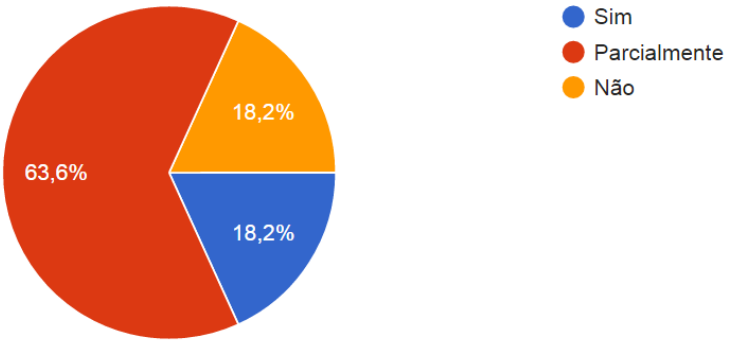
Seu local de trabalho é (11 respostas)



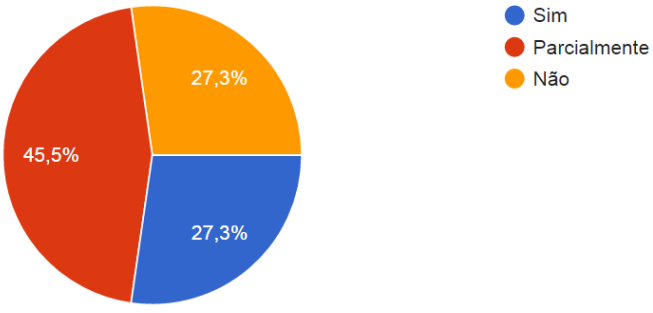
Quais as áreas principais em que você trabalha no seu dia-a-dia? (11 respostas)



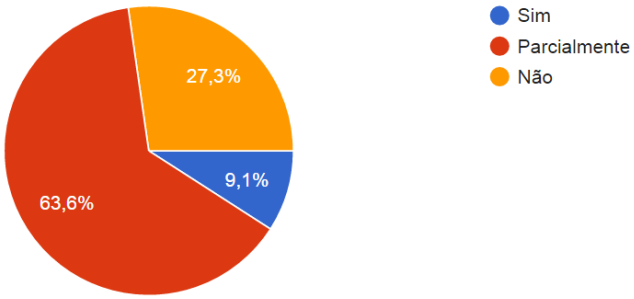
As atribuições do seu cargo estão bem definidas? (11 respostas)



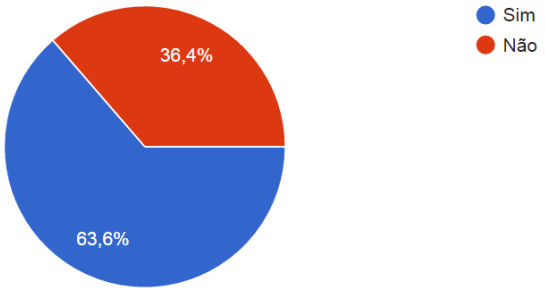
Você reconhece que exista uma política de capacitação voltada para a tecnologia da informação no seu órgão?
(11 respostas)



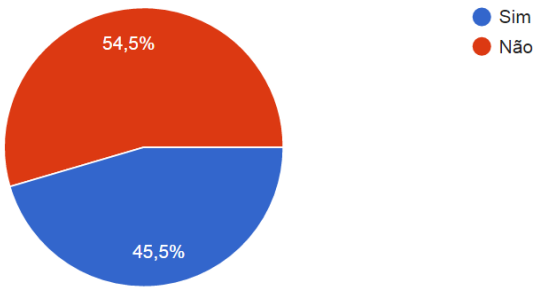
Você reconhece que exista uma política de capacitação geral no seu órgão?
(11 respostas)



Você participou da elaboração do Plano Diretor de Tecnologia da Informação (ou equivalente) da organização?
(11 respostas)

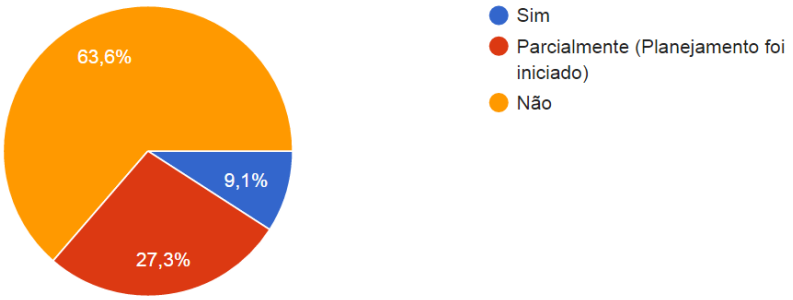


Você participou da elaboração do Plano de Desenvolvimento Institucional (ou equivalente) da organização?
(11 respostas)



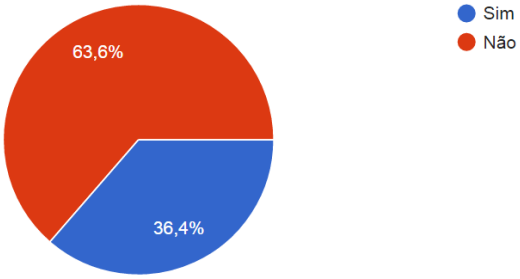
Você reconhece a existência de uma política formal (documentada e obrigatória) de governança corporativa no seu órgão?

(11 respostas)



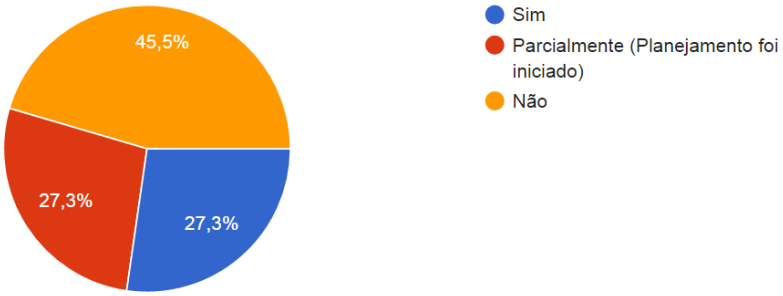
Você reconhece a existência de uma política informal (não documentada ou não obrigatória) de governança corporativa no seu órgão?

(11 respostas)

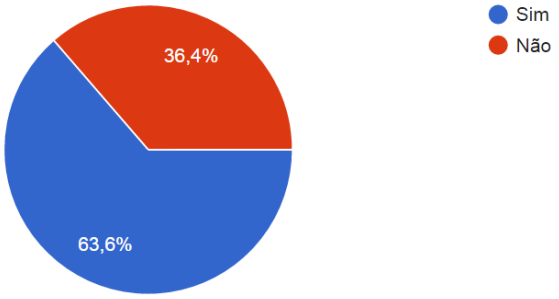


Você reconhece a existência de uma política formal (documentada e obrigatória) de governança de tecnologia da informação no seu órgão?

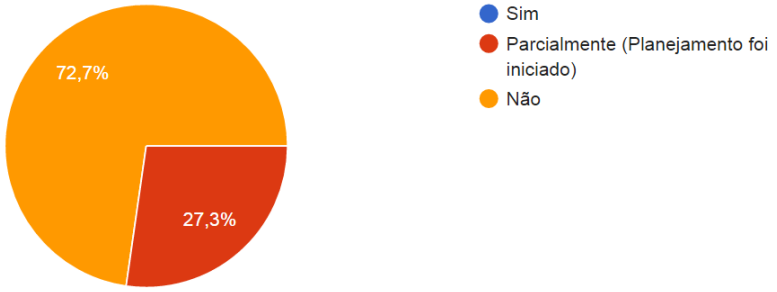
(11 respostas)



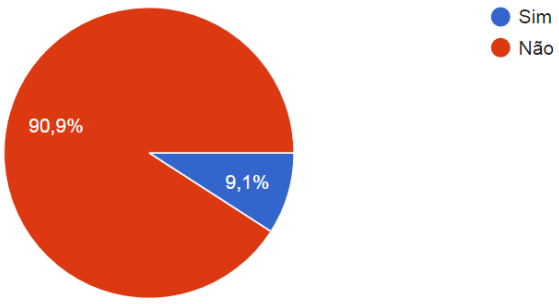
Você reconhece a existência de uma política informal (não documentada ou não obrigatória) de governança de tecnologia da informação no seu órgão?
(11 respostas)



Você reconhece a existência de uma política formal (documentada e obrigatória) de gestão de risco de tecnologia da informação no seu órgão?
(11 respostas)



Você reconhece a existência de uma política informal (não documentada ou não obrigatória) de gestão de risco de tecnologia da informação no seu órgão?
(11 respostas)



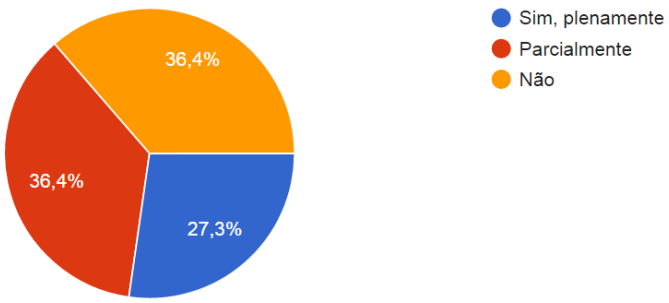
Existem quantas pessoas para atender às demandas de TIC na sua unidade (campus, etc.)?

(11 respostas)

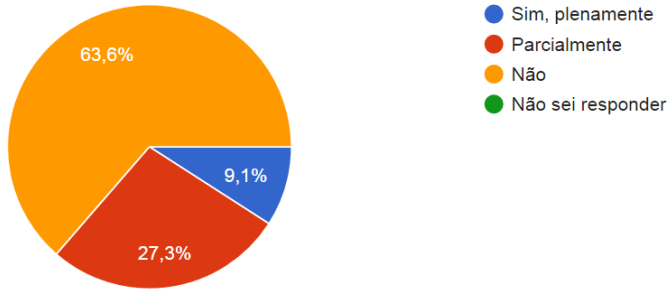
22
22
6
6
89 todos os campi, 9 meu campus
03
3
4
25
10
8

A equipe de TIC atual é suficiente para atender às demandas na sua unidade?

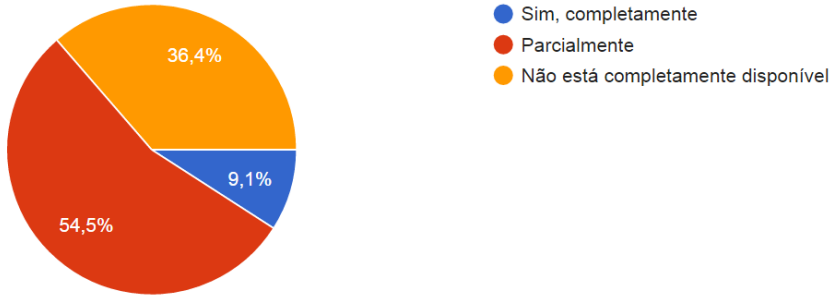
(11 respostas)



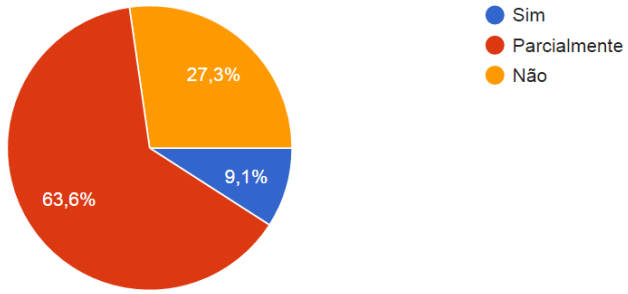
A auditoria interna possui pessoal capacitado para avaliar a gestão de TIC?
(11 respostas)



A estrutura física de TIC necessária para a sua unidade já está completamente disponível?
(11 respostas)

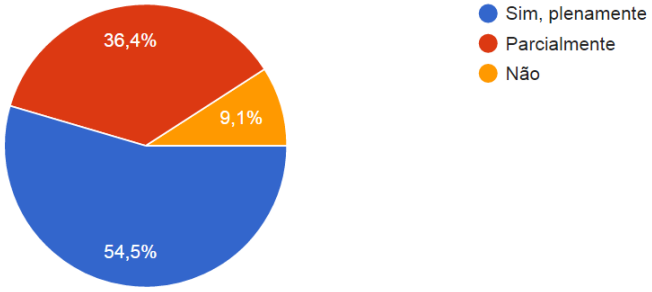


Existe um inventário acurado de todo o equipamento e software? (11 respostas)



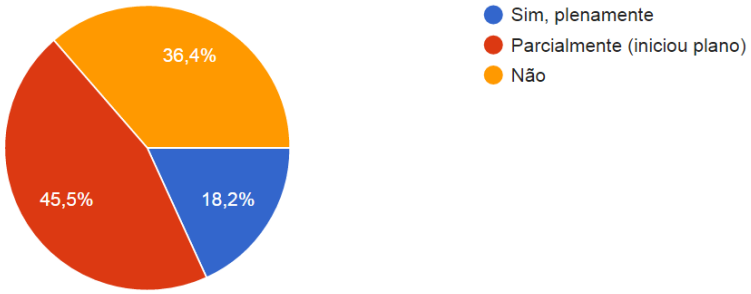
A organização dispõe de um comitê de TI formalmente instituído, composto por representantes de áreas relevantes da organização?

(11 respostas)



A organização define formalmente diretrizes para avaliação do desempenho dos serviços de TI ?

(11 respostas)



O seu campus/unidade possui datacenter ou mini-datacenter? Como é feito o controle de acesso físico?

(11 respostas)

Sem controle de acesso formal. Acesso interno livre a todos do setor.
Não possui. Existe uma sala reservada onde estão montados os servidores, mas não tem controle rigoroso de acesso.
Não possui.
Possui um mini-datacenter. O acesso é feito via código de impressões digitais
Sim. Apenas com cadeados com chaves unicamente com o pessoal da TI
Mini-datacenter. Com fechaduras e cadeados.
Sim, o controle de acesso é biométrico, por leitura de impressão digital.
Sim, sem controle
Sim. Cadeados e as chaves ficam com os profissionais envolvidos na manutenção deste
Sim. manualmente
Sim. Não possui controle de acesso.

Existe auditoria interna de TI (não a auditoria geral do órgão, e sim auditoria do setor para o próprio setor)?

(11 respostas)

Não
Não
Não
Não
Não
Não
Não.
Não.
Não existe.
Nâo
Não. Auditoria é institucional.

Os serviços e contratos possuem Acordo de Nível de Serviço (SLA)?

(11 respostas)

Não
Não
Não
Não
Não
Não
Alguns.
Alguns.
Sim.
Não sei.
Sim

Seu órgão faz parte do SISP (caso dos Institutos Federais e universidades), você sabe informar o que é usado de fato no dia – a – dia em relação à diretrizes do órgão?

(11 respostas)

-
-
-
-
-
-
Muita coisa, visto que os documentos são baseados nos modelos do SISP.
Nada.
Modelos e metodologia de gerenciamento de projetos
Não entendi
Desconheço

O que a sua organização usa para guardar dados do alunos e dados institucionais? Sistemas web? Planilhas no Excel? Eles estão em servidores ou computadores locais?

(11 respostas)

Sistemas web em servidores.
Sistemas web em servidores.
Sistemas web em servidores.
Storage
Servidores. Os arquivos estão em servidores específicos.
Sistema Web. Local.
Planilhas e sistemas em implantação
Sistemas web no datacenter
Existem dados de alunos em servidores de datacenter, não sei se existem em outros lugares
Uma mistura de tudo citado na pergunta.
Banco de dados armazenados em datacenter.

Os sistemas críticos estão em servidores em salas trancadas com acesso físico restrito?

(10 respostas)

Sim
Sim
Sim
Sim
Não. Controle apenas restrito à equipe do setor.
Na reitoria.
Sim.
Sim, existe um datacenter com combate a incêndio e controle de acesso biométrico
Não
Não, há projeto em andamento.

Os servidores estão em salas com controle ambiental, como detectores de temperatura, água e fumaça?

(10 respostas)

Não
Não
Não
Não.
Não.
Não, ainda.
Não
Sim
Não sei
Não, há projeto em andamento.

Os servidores estão longe de áreas com grande circulação de pessoas, como salas de aula?

(10 respostas)

Sim
Sim
Sim
Sim
Sim
Sim
Não.
Sim.
Sim.
Não, há projeto em andamento para retirada

Os servidores e hardwares importantes estão ligados a Unidades de Fornecimento de Energia Ininterrupta (UPS) com controle de picos de energia?

(10 respostas)

Sim
Sim
Sim
Sim.
Sim.
Não
Não
Rede estabilizada.
Não existe
Não, há projeto em andamento

O seu datacenter e salas técnicas também possuem instalação elétrica predial como disjuntores e quadros de luz do bloco/prédio que não são da TI, funcionando também como uma “sala da energia elétrica”? Você considera isso problemático?

(9 respostas)

Sim.
Acho importante mas não possuímos.
Sim.
Sim, sem problemas
O nosso datacenter tem uma estrutura de energia elétrica separada
Sim
Sim. Já tivemos problemas com essa questão.
Bastante problemático
Sim, é problemático com certeza

Proteção contra picos de energia é usadas nos desktops? (ex.: rede estabilizada, proteção individual)

(11 respostas)

Não.
Não.
Não
Não
Sim.
Sim.
Sim
Sim, nobreaks
Sim, proteção individual com nobreaks para cada estação de trabalho
Não existe
Sim, nobreak

Existe um procedimento para incidentes de segurança (roubo, uso não autorizado, equipamentos comprometidos)? Os incidentes são documentados?

(11 respostas)

Não.
Não.
Não.
Não
Não
Não
Não.
Somente processos administrativos
Não existe
Não sei
Não. Fica a critério do diretor.

Existem dispositivos de uso individual com dados sensíveis em áreas acessíveis ao público?

(11 respostas)

Não
Não
Não
Não
Não.
Não.
Sim
Sim
Sim.
Não.
Sim muitos

Os computadores destinados ao público possuem dispositivos antifurto?

(11 respostas)

Não
Não
Não
Não.
Não.
Sim
Sim
Sim.
Sim.
Não sei
Alguns

Existe uma política de segurança relativa aos meios físicos de TI (acesso físico de pessoas alugares, uso de dispositivos antifurto e coisas semelhantes)?

(11 respostas)

Não.
Não.
Não.
Não
Não
Sim.
Sim
Não existe
Nâo
Não sei
Desconheço

Os funcionários possuem login individual para acesso aos sistemas e computadores?

(11 respostas)

Sim
Sim
Sim
Sim
Sim
Sim
Sim.
Sim.
Não
Sim.
Sim e forte

Os alunos possuem login individual para acesso ao sistemas e computadores?

(11 respostas)

Não
Não
Não
Não
Não
Sim
Sim
Sim
Sim.
Sim.
Sim.

Existe um procedimento definido e documentado para definir nível de privilégio de acesso a pastas e documentos em servidores?

(11 respostas)

Não
Não
Não
Sim.
Sim.
Não.
Definido, porém não documentado
Sim
Não sei
Documentado não existe
Não é documentado

Os funcionários exonerados ou que mudaram de setor tem suas contas terminadas ou privilégios removidos em curto prazo?

(11 respostas)

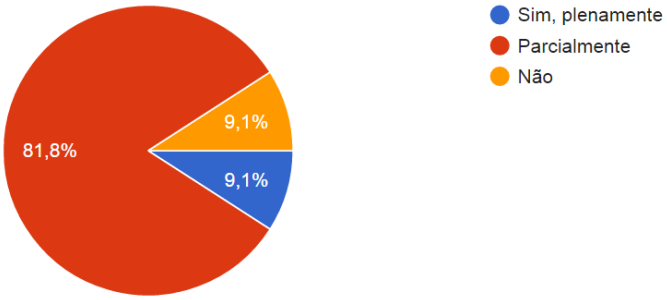
Não.
Não.
Sim.
Não
Sim
Em médio prazo
Sim, as contas de usuário são removidas automaticamente
Parcialmente
Não sei
Não é realizado
Sim, automatizado

A organização enfatiza que as credenciais de login são a chave para a identidade digital do usuário?

(10 respostas)

Sim
Sim
Sim
Sim
Não
Não
Não
Sim.
Não.
Sim, dentro do catálogo de TI

Existe um plano de segurança da informação no seu órgão? (11 respostas)



A segurança da informação é entendida como responsabilidade do órgão todo ou "somente da TI"?

(11 respostas)

Somente da TI
Somente da TI
Parcial entre todos.
A coordenação de TI tenta conscientizar os usuários.
Somente da TI.
Somente de TI.
Somente TI
Todo
Ainda é entendida como responsabilidade da TI
TI
De toda a instituição mas com ações apenas em alguns setores unidades.

O que podem ser considerados ativos críticos da informação no seu órgão (dados de alunos,banco de dados de sistemas, etc.)?

(9 respostas)

Arquivos, banco de dados, sistemas, equipamentos de rede
Dados de alunos e setor financeiro.
Dados administrativos Dados da comunidade externa Dados sobre ativos
Bancos de Dados
Dados de alunos e servidores
Bancos de dados do ERP (acadêmico e administrativo), emails, portal institucional, conteúdo de aulas, sites dos professores
Todos os arquivos armazenados nos servidores de aplicação
Não sei.
Há um comitê classificando essas informações

Quão bem a organização avalia e mitiga ameaças? (7 respostas)

Pouco faz.
Mal.
Monitoramento da rede
Relativamente bem
Não sei
Desconheço
As ameaças são tratadas à medida que são identificadas, não há prevenção

Existe algum mecanismo para dificultar ataques feitos à organização?

(10 respostas)

Firewall
Firewall
Firewall.
Sim, baseado nas características dos ativos.
Sim, firewall e regras de segurança
Antivírus, anti-spam, web Application firewall, Next Generation Firewall, anti-spyware
Sim
Não sei
Desconheço
Não

Que vulnerabilidades existem na área de segurança da informação? Elas estão bem documentadas?

(10 respostas)

Não estão bem documentadas. Diversas: - Salas de TI sem controle de acesso físico - Políticas de login sem expiração - Não tem definição da função dos administradores de rede
Não estão bem documentadas - Falta de níveis de autenticação
Não estão bem documentadas.
Não há documentação
Parcialmente
Não existem vulnerabilidades documentadas.
Nâo
Não sei
Não
Não, não são avaliadas

Existe um processo bem definido para assegurar que problemas identificados são atendidos?

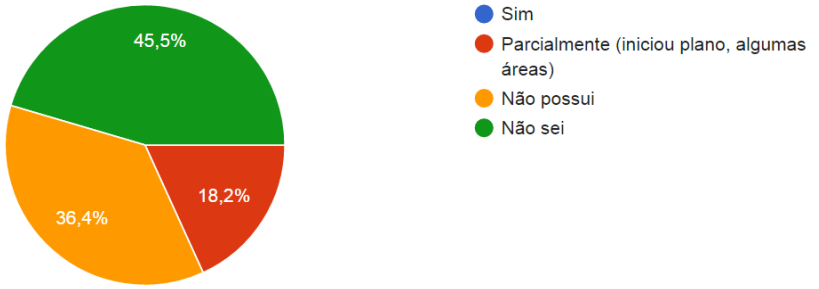
(10 respostas)

Não
Não
Não
Não
Não.
Parcialmente
Existe uma central de serviços de TI para tal fim
Sim
Não sei
Claramente definidos

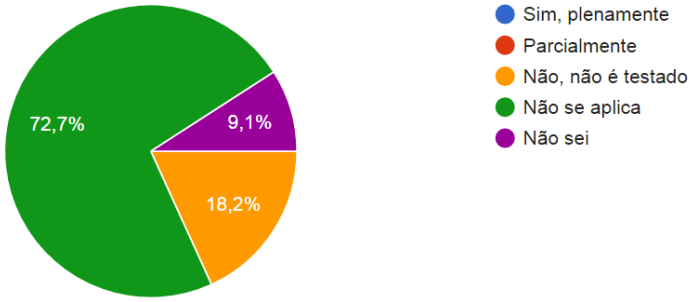
Qual o tempo de resposta quando uma intrusão é detectada? (10 respostas)

Não existe esta informação.
Não é possível mensurar
O tempo de percepção.
Imediata
Quase imediata
Não mensurado
Não há definição
Não sei
Todo dinâmico
Não há tempo definido

O seu órgão tem um plano de continuidade do negócio (para a organização)?
(11 respostas)

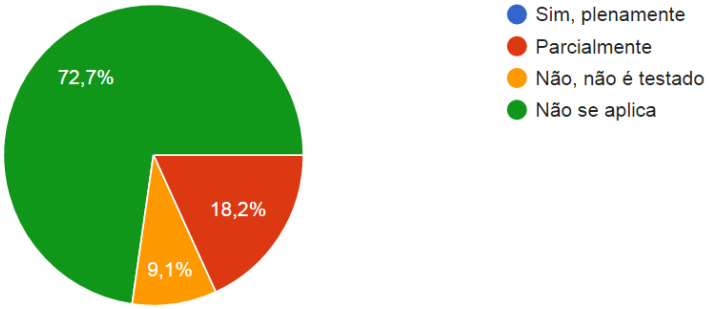


O plano de continuidade do negócio é testado? (11 respostas)

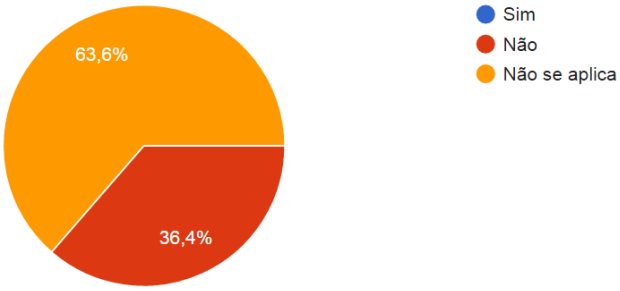


Existe um plano de recuperação de desastres de TI no seu órgão? (11 respostas)

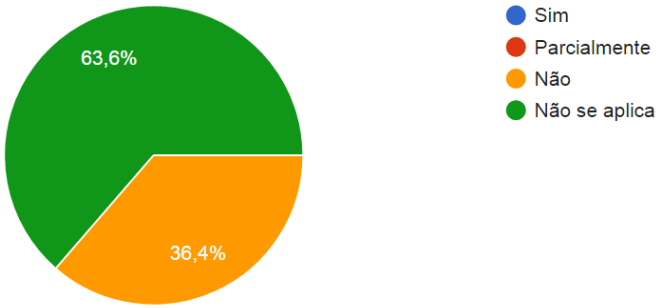
O plano de recuperação de desastres de TI é testado? (11 respostas)



O plano de continuidade do negócio está alinhado com o plano de recuperação de desastres
(11 respostas)



O plano de continuidade do negócio é bem comunicado? (11 respostas)



Como sua organização implementa o BYOD (Traga seu próprio dispositivo)?

(10 respostas)

Não
Não
Não
Não há qualquer controle. É disponibilizado um link de internet aberto para alunos e visitantes, e um link com controle por senha para servidores.
Não há prática definida a nível institucional.
Somente wi-fi disponível
Sim
Não se aplica
Rede wi-fi aberta com acesso através de login/senha igual ao acesso dos computadores
De acordo com a vontade do diretor

Existe uma política para dispositivos móveis (pessoais ou corporativos)?

(10 respostas)

Não
Não
Não
Não
Não.
Não.
não
Wi-fi disponível
Sim
Desconheço

Quais vulnerabilidades dos dispositivos móveis podem ser exploradas e como a organização lida com elas?

(9 respostas)

Não identificado
Não há qualquer controle.
As mesmas dos PCs normais.
Não se aplica
Rede exclusiva para o wi-fi
Vazamento de dados, vírus. Não existe tratamento para vazamento de dados. Para vírus, existe um antivírus da rede
Não sei
A organização não avalia as vulnerabilidades
Não são avaliadas

Como sua organização lida com dispositivos móveis perdidos ou roubados?

(9 respostas)

Não possui informação
É comunicado à direção do campus.
Denuncia à P.F. ou anúncios na secretaria.
Não se aplica
Achados e perdidos
Processo de sindicância
Não sei
Desconheço
Há controle de localização dos que possuem conta corporativa instalada e os dados podem ser apagados remotamente

Sua organização usa computação em nuvem (cloud computing) para alguma coisa?

(10 respostas)

Não
Não
Não
Não.
Sim.
Somente virtualização de servidores e um drop interno
Sim. E-mail para os alunos.
Não sei
Sim, portal institucional
O e-mail é nas nuvens (Google)

Se sua organização usa computação em nuvem, foram definidos dispositivos de segurança no contrato? Como responsabilidade nas perdas de dados?

(8 respostas)

Não se aplica
Não se aplica
Sim.
Contrato padrão do Microsoft 365. Não sei explicar os detalhes.
Não
Não sei
Desconheço
Não há contrato

A organização tem um inventário do uso de serviços em nuvem na TI e na organização?

(10 respostas)

Não
Não
Não
Não
Não se aplica
Não se aplica
Não.
Não.
Não sei
Desconheço

Existe alguma vulnerabilidade no serviço usado nas nuvens? (7 respostas)

Sim
Sim
Ainda não detectadas.
Não se aplica
Não conheço.
Não sei
Desconheço

Quão bem sua organização lida com identificação de riscos? (6 respostas)

60%
Não identifica
De forma precária
Não há análise de riscos.
Muito fracamente
Não há

O que é feito quando um risco é identificado? (7 respostas)

Iniciativas diversas, partindo da experiência de cada gerente.
Resolvido de imediato
É tentado minimizar seus efeitos
Tentativa de mitigação ad-hoc
Não sei
Não é avaliado
São tratados à medida que são identificados

Como os riscos são identificados e gerenciados? (6 respostas)

Sem método padrão.
Ao acaso.
Não há análise de riscos
Não sei
Desconheço
Não há metodologia. Normalmente quando é descoberto a instituição já sofreu alguma perda.

A responsabilidade pelo risco estão claramente definida? Existe alguma responsabilidade documentada e seguida por um comitê de TI? (6 respostas)

Não
Não
Não.
Não existe
Não. Não.
Desconheço

Existe um levantamento de rico compreensivo que cubra todas as áreas?
(6 respostas)

Não
Não
Não
Não
Não.
Não sei.

Como o processo de levantamento de riscos é efeito? (7 respostas)

Sem método definido.
Não se aplica
Não há esse processo
Não existe processo
Não sei.
Desconheço
Não existe

Como o processo de gerenciamento de riscos pode ser melhorado?
(8 respostas)

Criado.
Padronização, documentação.
Começando
Discussão entre os envolvidos
Primeiramente, precisa ser definido
Não sei.
Criação de um plano de riscos que contemple a instituição como um todo
Criação de uma política

Há a oportunidade de combinar auditoria interna de TI com a auditoria do órgão?

(8 respostas)

Não. Não existe auditoria interna de TI.
Não, não há auditoria interna de TI.
Não se aplica
Deve-se criar a auditoria de TI
Essa oportunidade ainda não foi mapeada
Não tenho conhecimento.
Certamente, servidores de TI em conjunto com a auditoria
Nunca foi proposta

A organização usa software GRC (Governança, Risco e Conformidade)? Qual?

(9 respostas)

Não
Não
Não
Não.
Não.
Não.
Não usa
Não sei.
Desconhecer

A organização possui os processos e controles adequados para entrega de projetos em tempo dentro do orçamento e uso adequado de recursos?

(9 respostas)

Não
Não
Não
Não
Não
Sim, mas é muito pouco utilizado. Basicamente, no momento, apenas na reitoria.
Ainda não.
Desconheço
Não, há projeto para criação

Existe algum processo para medir benefícios alcançados depois de um projeto completado comparativamente com os benefícios que se esperava ao iniciar o projeto?

(8 respostas)

Não
Não
Não
Não
Não.
Não.
Não utiliza
Não, há projeto em andamento

A metodologia de gerenciamento de projetos está sendo seguida corretamente?

(7 respostas)

- Ainda não.
- Não se aplica
- Não existe
- Não.
- Não existe metodologia
- Não
- Ainda não está em execução

O que é feito quando um projeto está tendo um desempenho ruim? (7 respostas)

- Ainda não há rotina definida.
- Muda-se os componentes
- Nada
- Não há uma medição de desempenho de projetos
- Não existe acompanhamento
- Desconheço as medidas tomads
- Ainda não está em execução

Como os riscos de projetos são levantados e gerenciados? (7 respostas)

- Ainda não há rotina definida.
- Não se aplica
- Não há levantamento
- Não há metodologia de gerenciamento de riscos
- Não são acompanhados
- Desconheço
- Ainda não está em execução

Existe um processo de governança adequado para alinhar projetos e programas com os objetivos organizacionais?
(7 respostas)

Não
Não
Não
Ainda não.
Não se aplica
Sim, o plano de ação anual, que deve estar alinhado ao PDI
Desconheço

O risco pode ser considerado um evento incerto que terá efeitos negativos nos objetivos desejados. Os riscos estão associados a vulnerabilidades de software, hardware,humanas, estratégias e logísticas. Se desejar,você pode fazer abaixo descrição de quais riscos de tecnologia (ou corporativos que afetam a TI) que você acha que seu órgão enfrenta e suas causas. É um espaço livre para considerações. Você também pode falar de coisas que você acha que deveriam haver no seu órgão e que não existem.
(2 respostas)

Um item que deve ser levantado é o papel da TI que hoje é operacional, mas deveria ser estratégico
O risco é algo certo. Se deve haver mais encontros dos servidores para troca de ideias e discussões. Criação de um conselho

Apêndice C

Roteiro de Entrevista com o Coordenador de Redes e Suporte do CPD da UnB (Tecnologia da Informação e Gestão de Riscos na UnB)

Entrevista CPD - UNB

Esta entrevista faz parte de uma pesquisa desenvolvida no Mestrado Profissional em Computação Aplicada da Universidade de Brasília, voltada para gestão de riscos no Instituto Federal de Brasília. O objetivo deste questionário é entender aspectos da gestão de riscos de tecnologia da informação na Universidade de Brasília.

Para o Coordenador de Redes

1. O que sua coordenação faz? Qual o seu papel na coordenação?

2. O que você entende por infraestrutura de tecnologia da informação?

3. Como é a integração entre o CPD e a área de tecnologia da informação de cada campus?

4. Existe uma política de gestão de riscos de tecnologia da informação na UNB, formal ou informal? Se sim, quais setores ela cobre? Vocês usam alguma ferramenta específica para gestão de riscos?

Definições

Risco pode ser entendido como um evento incerto que, ocorrendo, pode ter impacto negativo nos objetivos da organização. É a combinação da possibilidade de eventos danosos para a organização ocorrerem e seu respectivo impacto para a organização.

Apêndice D

Roteiro de Entrevista com os Setores Subordinados à Coordenação de Redes e Suporte do CPD da UnB (Tecnologia da Informação e Gestão de Riscos na UnB)

Entrevista CPD - UNB

Esta entrevista faz parte de uma pesquisa desenvolvida no Mestrado Profissional em Computação Aplicada da Universidade de Brasília, voltada para gestão de riscos no Instituto Federal de Brasília. O objetivo deste questionário è entender aspectos da gestão de riscos de tecnologia da informação na Universidade de Brasília.

Para os líderes de setor

1. O que o seu setor faz? Qual o seu papel no setor?

2. Você ou a equipe recebeu algum treinamento específico para lidar com riscos de tecnologia da informação?

3. Você acha importante o uso de checklitsts (lista de verificação) para garantir conformidade com as melhores práticas?

4 . O setor usa alguma checklist (lista de verificação) para garantir conformidade com as melhores práticas? Se sim, usa listas públicas? Usa listas próprias?

5. O setor efetua algum outro tipo de controle de riscos?

6. Existe um histórico com riscos que foram concretizados ou não? Existe um histórico de incidentes?

Definições

Risco pode ser entendido como um evento incerto que, ocorrendo, pode ter impacto negativo nos objetivos da organização. É a combinação da possibilidade de eventos danosos para a organização ocorrerem e seu respectivo impacto para a organização.

Apêndice E

Compilação das Respostas das Entrevistas com a Coordenação de Redes e Suporte do CPD da UnB (Tecnologia da Informação e Gestão de Riscos na UnB)

Entrevista CPD – UNB - Respostas

Pesquisador: P

Entrevistado: E

Coordenação de Redes e Suporte (Coordenador)

E: Eu coordeno a área de suporte avançado, segurança e operação, redes, e na área de segurança e operação está incluída a área de helpdesk. E o NOC, que faz a verificação de todos os serviços que estão na universidade, coordenados pelo CPD, se estão funcionando ou não.

P: Então basicamente você coordena a infraestrutura.

E: Isso. Tenho coordenadores em cada área.

P: O que você como gestor dessas áreas entende por infraestrutura de tecnologia da informação?

E: Vai desde a preparação de um ambiente para receber uma rede, em que você deve ver toda a parte de fibra, cabeamento, pontos de rede, até você chegar no ambiente em que ficam os serviços hospedados dentro da universidade, responsabilidade do CPD, devendo ter toda uma estrutura, desde uma sala propícia para isso até o hardware que vai receber esses serviços.

P: Como é a relação entre CPD e campus? Cada campus tem sua área de tecnologia da informação?

E: Pelo campus ser distante do CPD, há técnicos e analistas que ficam nesses locais. Mas a rede toda é feita pelo pessoal do CPD. Ou seja, quem toma conta da rede da Universidade de Brasília é a coordenação da área de redes. Então existe uma equipe em cada campus, mas quem passa para eles a distribuição, a configuração dos switches, etc., somos nós. Há alguma independência, porque algumas vezes eles precisam fazer alguma coisa, até um técnico nosso ter condições de ir para lá, não podemos deixar o serviço lá parar, então eles entram em contato e, por telefone, a nossa equipe orienta eles a como tomar algumas atitudes, se houver a necessidade. Agora, se eles precisarem, por exemplo, colocar mais switches para habilitar mais pontos de rede, é a equipe do CPD quem faz a configuração e passa para eles. Todos os switches da rede da Universidade de Brasília, ou redume, como chamados aqui, ela é monitorada, instalada e configurada pela equipe daqui. Termos cerca de mil switches aqui.

P: No IFB temos bem menos.

E: A UnB é uma verdadeira cidade.

P: Como é a governança de tecnologia da informação aqui? Em muitos Institutos Federais a governança de tecnologia da informação ainda está caminhando.

E: Aqui também. A UnB saiu da época de computadores de grande porte, em que havia uma estrutura de governança maior montada - por incrível que pareça. Quando ela saiu para a microinformática, isso se perdeu. Então o CPD foi fazendo aquilo que podia ser feito, dentro das melhores práticas, o próprio governo federal também não mostrou um grande interesse de levar a governança adiante. Hoje em dia é diferente e existe uma cobrança maior. Então o CPD foi se adaptando e buscando melhorias. Existem alguns conflitos quanto a isso. A direção superior, como eu poderia dizer? Deveria fazer as políticas, e nestas políticas criar toda uma ambientação. Nós usamos mais a governança no sentido do que vem de fora pra dentro.

P: E quanto à gestão de riscos, existe alguma coisa na UnB, oficial ou extraoficial?

E: Não temos. A área de segurança e helpdesk te darão mais informações. Fazemos também de acordo com as melhores práticas.

P: Existe algum entrave para não termos gestão de riscos aqui?

E: Tudo dentro da universidade depende das políticas, inclusive o CPD, depende das políticas de tecnologia da informação da Universidade de Brasília. E essas políticas não existem dentro da Universidade de Brasília. Quando o ambiente passou para microinformática, o CPD foi seguindo aquelas políticas/práticas que já tinha relacionadas ao ambiente antigo, e foi se adaptando às melhores práticas, ao que o ambiente de internet cobrava. Criamos algumas políticas, mas há muitos conflitos. As vezes o usuário pergunta: "fizeram isso baseados no quê?", "onde é que está escrito isso?". Temos essas situações. A UnB é uma cidade. Temos um ambiente muito diversificado. Nós controlamos, mas por exemplo, às vezes vamos proibir alguma coisa por causa de A, mas B precisa. Então ainda não foi feito um estudo, que acho que deva incluir a direção superior, para determinar o que pode e o que não pode ser feito de políticas de segurança dentro da universidade. Nós temos ambientes, temos firewalls, pois temos que ter um controle. Para se ter uma ideia, até 2007-8 nós tínhamos firewalls internos, mas não tínhamos firewalls externos, que fazia toda a avaliação do que saía e do que chegava aqui.

Então não existe uma política aqui. E nós sofremos muitos ataques. Internos e externos! Por incrível que pareça. Então o ataque, quando vem de fora temos o firewall. Agora internamente, qual a política da universidade de uso da rede? Não existe oficialmente. Nós recebemos informações de vários órgãos, reclamando de situações de saídas nossas (da rede da UnB) atacando, e então temos que tomar algumas posições e soluções. Mas internamente, o que cada um pode fazer aqui dentro, realmente? Todo mundo acha que a internet tem que ser livre, eu posso usar, eu posso baixar isso, baixar aquilo. Será que pode mesmo? Isso ainda não tem uma política oficial da Universidade de Brasília. É difícil, pois é um ambiente de pesquisa, então fica muito difícil criar essas políticas.

P: E descendo mais um nível, e as listas de verificação para manter compliance, etc., vocês usam alguma coisa?

E: Usamos, nós temos equipamentos que fazem esse trabalho. Agora mesmo adquirimos equipamentos novos, quem vai te informar melhor é o responsável pela segurança. Criamos regras. Antigamente tínhamos mais equipamentos de segurança em alguns lugares, ficaram desatualizados, fora de garantia, etc.

P: Por exemplo, para configurá-los, vocês usam alguma lista de verificação? Até do próprio fabricante?

E: A coordenação de segurança vai te dar detalhes. Hoje estamos aproveitando os equipamentos antigos, porque a rede da UnB funciona através de um anel, então temos switches principais dentro do CPD, dentro da FT, dentro da FINATEC e dentro do ICC. E agora vamos criar alguns firewalls para atacar diretamente esses ambientes antes da rede ser distribuída. As soluções são determinação do grupo, em reunião conversamos chegamos a essas soluções. Então vamos tentar bloquear condições de ataque externo e interno. Aumentar a segurança, atender a demanda.

P: Muito obrigado pela participação.

SETORES

Suporte Avançado

E: Meu setor é o de Suporte Avançado, mexe com pastas de sistema Linux, sistemas operacionais, atualizações, data center.

P: Você coordena o pessoal que dá suporte na UNB toda?

E: Não, é o helpdesk.

P: Você e sua equipe receberam treinamento na parte de gestão de riscos?

E: Não.

P: Você acha importante o uso de checklists para consolidar melhores práticas?

E: Sim.

P: Seu setor usa alguma checklist, alguma recomendação de uso público, da ISO1799/27002 ou alguma coisa daqui de dentro também?

E: Não. Só experiência pessoal de iniciativa privada e experiência de trabalho.

P: Você aplicou alguma coisa aqui?

E: Apenas algumas regras de documentação da ISO e técnica, mais nada.

P: Você tem algum controle de incidentes?

E: Não.

P: Qual é a relação entre o CPD e os Campi?

E: Atualmente são interdependentes. O CPD oferece o suporte de serviços institucionais como o e-mail, hospedagem de site etc. Só que cada campus tem sua interdependência, ele pode ter o seu próprio CPD ou usar os serviços que o CPD oferece. Tem CPDs em outros campi que a estrutura é só deles, o próprio site, é tudo deles. Já outros não tem essa estrutura e usam os recursos do CPD.

P: Então eles são independentes, mas podem usufruir da estrutura do CPD.

E: Isso mesmo.

P: Muito obrigado pela participação.

Infraestrutura

E: Meu setor trabalha com a parte física da Rede, então a gente é responsável pelas salas de rack e condicionamento dessas salas, a questão do ar condicionado, nobreak, o setor cuida também dos ares-condicionados prediais e nobreaks prediais, mas não fazemos a manutenção propriamente dita e sim monitoramos, identificamos problemas e abrimos chamados para o setor responsável poder realizar a manutenção.

P: Vocês têm uma inter-relação com os campi? Vocês vão lá?

E: Sim. Por exemplo, temos que fazer uma intervenção no Campus Gama, dependendo da intervenção nós temos que ir lá ver o que precisa ser feito e tentar arranjar uma solução para o problema, então tem deslocamento para os campi.

P: Vocês obrigatoriamente fazem intervenções nos campi (visitas) ou só se eles solicitarem?

E: Depende da situação. Cada caso é um caso.

P: O campus é completamente independente de vocês?

E: Não. Algumas situações não precisamos ir até lá, por exemplo no Campus Ceilândia tem uma central do CPD lá e temos servidores do CPD lá, eles entram em contato com a gente e negociamos à distância o que precisa ser feito e as vezes a gente só vai lá para fazer intervenção direta, não precisamos ir lá para ver o que está acontecendo primeiro, então existe essa possibilidade de não precisar se deslocar, mas não é regra.

P: Qual foi a intervenção que você fez (a última)? Para termos um exemplo.

E: No campus Gama, por exemplo, tinha um problema em que o restaurante universitário utilizava a conexão externa em vez de utilizar a conexão da UNB, para fazer eles usarem nossa conexão era necessário fazer a passagem da fibra, então visitei o campus, verifiquei o que seria necessário para fazer essa passagem de fibra, pedimos apoio para a PRC [Prefeitura do Campus] e a PRC fez o cabeamento que estava faltando, o pouco trajeto que precisava, lançou a fibra para a gente, então acionamos uma empresa terceirizada para fazer a fusão dos dois lados para então o pessoal da outra equipe colocar o switch.

P: Você ou alguém da sua equipe já recebeu algum treinamento sobre gestão de riscos?

E: Não. Gestão de riscos não.

P: Sobre as checklists, você acha interessante usá-las para manter a conformidade?

E: O meu setor é bem peculiar. No meu setor, todos os servidores aposentaram. Haviam três senhores com um conhecimento absurdo do que é UnB, aí primeiro aposentou um, depois outro e o último que aposentou consegui ficar com ele uns 2 meses, foi um transição um pouco complicada. Aproveitamos a documentação que eles tinham, mas muito se perdeu nessa transição, então estamos começando a fazer um padrão para se fazer essa verificação.

P: Vocês não tem a checklist formalmente, mas sim o esboço do que vai usar?

E: Sim, estamos começando a fazer

P: Além do GLPI, vocês tem algum outro controle que possa se caracterizar como controle de risco?

E: O pessoal antigo do setor não utilizava o GLPI, depois da transição nós já fomos direto para o CITSmart que está em implementação ainda, pulamos o GLPI e fomos para a fase adiante. Antes era manual o controle das coisas, antes tínhamos uma pasta com as ordens de serviço do que era para ser feito, hoje já é colocado no sistema que foi aberta uma ordem de serviço referente ao nobreak, por exemplo, ou alguma coisa que alguém do setor precisava. Se pesquisar vai direto no sistema não vai na pasta, mantemos essa pasta de garantia, mas já temos o sistema.

P: Muito obrigado pela participação.

Núcleo de Administração de Redes

P.: Sou do IFB. Podemos imaginar como uma universidade com foco no ensino técnico. Estou fazendo uma pesquisa para definir as bases para um plano de gerenciamento de riscos e estou fazendo um benchmarking com outras instituições, no caso a que mais se parece conosco aqui no DF é a UnB.

E: São parecidas as estruturas?

P: Lá basicamente temos a estrutura de reitoria e campus, os campi tem sua independência administrativa, certa independência financeira, ofertamos cursos, só que com a grande diferença que ofertamos ensino médio integrado ao ensino técnico, uma das nossas obrigações.

E: Certo.

P: Então, poderia falar um pouco sobre o seu setor?

E: Nosso núcleo é o núcleo de redes de dados, e até pouco tempo trabalhávamos com a área de telefonia, hoje temos a função de gerenciar, administrar a rede de dados da universidade. Basicamente gerenciamos todos os ativos de rede, desde switches a roteadores de saída da universidade. Exceto a parte de firewall que fica com o núcleo de segurança. O nosso trabalho é o de configuração, gerenciamento desses ativos na rede, para que a comunicação possa ocorrer de forma mais ágil possível.

P: Para realizar essas atividades, vocês tiveram algum treinamento formal em gerenciamento de riscos? Foi ofertada alguma coisa para a equipe?

E: Não. Foram ofertados cursos voltados para a área de gestão de TI, não gestão de riscos, na Escola Superior de Redes.

P: Governança?

E: Isso. Quem fez foi uma funcionária do setor, ela fez, mas hoje está integrando outra unidade da Universidade. No meu caso cursei mestrado.

P: Você deve conhecer a existência de checklists, para manter compliance, prevenir os riscos. Você acha importante usar checklists, fazem uso de alguma checklist, pública ou privada, checklists de atualização de firmware, checklists de configuração de servidor, etc.?

E: No setor de redes, temos uma atividade cotidiana, por exemplo, no caso do firmware, se estão atualizados ou em conformidade com os firmwares considerados stable no mercado. Mas não seguimos um checklist na prática. Não temos um documento.

P: Por exemplo, quando um novo funcionário chega, há uma documentação?

E: Não temos o documento, mas a atividade está consolidada, e vamos multiplicando a nossa prática de como executar esse conferência.

P: Então o que vocês têm é uma conferência informal que está difundida na equipe?

E: Exato. E o próprio sistema, que gerencia todos os ativos de rede. Que são em torno de 850 mais outros 500 equipamentos da área de wireless.

P: É um sistema desenvolvido por vocês?

E: É feito por um fabricante, a Enterasys, o sistema é o Netsight. É um sistema que nos auxilia a fazer a conferência e também atualização dos equipamentos.

P: Então além da difusão das práticas na equipe, há o Netsight?

E: Isso. O Netsight auxilia na gerência de ativos.

P: Há algum outro tipo de controle de riscos?

E: Não.

P: Algumas vezes associamos riscos a incidentes. Não sei o quanto isso se aplicaria à sua coordenação, mas você tem um controle de incidentes? Uma falha técnica que impactou de alguma forma no fornecimento dos serviços?

E: Há um registro de incidentes por e-mail. Mas não posso garantir que todos os incidentes sejam registrados no sistema. Há o GLPI, por meio dele são feitas várias solicitações. Mas muitas das nossas demandas não são nem solicitadas pelo usuário lá na ponta, são solicitadas por nós mesmos do setor. Passamos muitos anos com uma equipe defasada, hoje temos 10 pessoas para tomar conta de uma quantidade muito grande de equipamentos. Antes, quando tínhamos duas ou três pessoas, era muito mais difícil gerenciar. Se hoje é difícil, no passado era muito mais. Então, muita coisa deixou de ser feita no passado, e hoje estamos tentando corrigir. Estas demandas são registradas em reunião do setor. Então cada pessoas fica com as demandas por tempo determinado, prazos determinados em reunião.

P: Qual a relação do seu setor, com a relação do setor de tecnologia da informação de cada campus.

E: Em nível técnico?

P: Em nível técnico. Vocês vão lá, vocês resolvem problemas do campus, por exemplo.

E: A nossa gerência tem reflexo sim lá do outro lado. Por mais que os centros, os campus, ou as faculdades, elas sejam independentes (administrativamente), elas dependem de nós. Portanto, toda atividade que dependa da configuração de switches, por exemplo, todas essas atividades relativas à mudança de estrutura de topologia lógica e física das redes, são feitas pela equipe de redes. Então por mais que existam analistas do outro lado, por mais que existam técnicos do outro lado, eles não tem a especialidade em fazer as mudanças para o setor, a solução como um todo. Eles podem ter uma independência relacionada aos serviços internos. Mas à rede em si, não.

P: Muito obrigado pela participação.

Segurança e Operação

E: Meu setor é responsável por toda a segurança da informação da universidade, gerenciamento de firewalls, antivírus, ferramentas de atualização, ferramentas de análise de vulnerabilidades, active diretory, servidor de arquivos.

P: Vocês tem um AD integrado com os campi?

E: É um AD para todos os campi. Uma única árvore, um único domínio, e é agregado para toda a universidade. Cuidamos da parte de homologação de softwares de grande risco. Não se instala nada na universidade sem passar pela área de segurança. Também fazemos parte da consultoria de segurança para todas as áreas da UnB.

P: Essa política de instalação de software também se aplica aos desktops do usuário?

E: Temos uma nomenclatura de localidades. Temos uma lista de softwares homologados, qualquer pessoa que solicite a instalação de software através do sistema de chamados - GLPI e CITSmart - que esteja nessa lista, o helpdesk é autorizado a instalar. Para um software que não esteja nessa lista, é aberta uma solicitação que vem para a área de segurança, a gente vai verificar se o software pode ser homologado ou não, e autorizamos ou não a instalação.

P: E quanto à gestão de risco, você recebeu algum treinamento? Fizeram algum curso?

E: Na UnB não. Vim com formação de fora. Sou formado em Gestão de Risco na parte de pós-graduação em gestão de riscos, pós graduação em gestão de pessoas. Agora estou cursando mestrado.

P: Você considera o uso de checklists, as listas de verificação, importantes?

E: A área de segurança tem um troubleshoot para o que vamos fazer.

P: Essa lista de verificação é pública ou privada?

E: Tem pública e privada. Principalmente o helpdesk usa. O helpdesk não faz nenhuma ação sem seguir uma lista.

P: Além dessas listas de verificação, vocês gerenciam riscos de alguma forma? Vocês tem o GLPI para chamados.

E: Sim. Temos a ferramenta CITSmart que ainda está sendo implantada, o GLPI já está implantado em toda parte administrativa e ainda está sendo implantada a parte docente.

P: Existe um histórico de incidentes?

E: Sim, através da ferramenta de atendimento ao usuário.

P: Além dela?

E: Só ela. Alimentamos só essa base de conhecimento.

P: Vocês poderiam fornecer essas listas de verificação?

E: Não, elas são específicas nossas, montamos especificamente para nossos softwares.

P: Então você não pode fornecê-la?

E: Não podemos, é prioritária nossa.

P: E são listas de configuração.

E: De tudo. Por exemplo, um usuário liga aqui falando que um computador dele está sem antivírus, a pessoa pega o checklists de verificação do antivírus, vai lá, se não tiver, pega outro checklists de instalação do antivírus e instala o antivírus.

P: Não pode ser fornecida.

E: Não pode ser fornecida também porque fica dentro do nosso software, não é uma lista impressa.

P: Muito obrigado pela participação.

Helpdesk

E: Meu setor é o Helpdesk. Solicitações chegam lá. Fazemos uma triagem dos chamados. Tem uma empresa que faz essa triagem. Essa triagem faz o encaminhamento. Se for possível resolver no primeiro nível, então tudo OK. Senão, será repassado para o segundo nível, que envia o técnico ao local para resolver o problema de software.

P: Vocês não fazem manutenção, instalação de computadores?

E: Não. Quem instala computadores é o CME [Centro de Manutenção de Equipamentos]. Eles tem uma equipe para abrir o computador. Nós inclusive somos proibidos de abrir os computadores. Uma empresa faz o serviço.

P: O Helpdesk é todo terceirizado? Tanto a parte de instalação como a parte de manutenção é toda terceirizada?

E: Exato. Mas só quem faz a manutenção são eles. Podem trocar, podem substituir. Nós não podemos fazer isso.

P: Vocês receberam algum treinamento de risco? Seja de instalação de software, seja de manutenção.

E: Nós só instalamos softwares livres, depois de verificado pelo setor de segurança. Não podemos instalar softwares que não sejam homologados.

P: Mas, por exemplo, juntaram a equipe e deram algum treinamento referente a riscos?

E: Não, é sempre o pessoal da segurança.

P: Você acha importante usar listas de verificação?

E: Nós já temos. Acho importante, até pela segurança dos computadores. É possível que instalemos algum software que não esteja homologado, e ele pode ser um software que venha com algum componente malicioso.

P: O que as checklists que você tem hoje cobrem? Do que se tratam?

E: Por exemplo, checamos antivírus. Se vamos instalar um software, ele deve ser original ou software livre.

P: As listas de verificação podem ser fornecidas?

E: Não... Cada departamento é peculiar. Um usa um software, outro usa outra. O básico é o Windows/Office.

P: No caso da minha pesquisa estamos analisando outro órgão parecido, identificando se algo de gestão de risco pode ser reusado.

E: Temos que ver mas acho que não vai ser útil para você... Cada departamento usa um software.

P: Mas é mais o caso da verificação que é feita.

E: A própria ferramenta do AD também faz verificações.

P: Mas uma lista, um papel com as orientações, você tem?

E: Não. Mas é como te falei, temos alguns softwares, como o sistema de controle da secretaria de assuntos acadêmicos, é por exemplo um dos softwares que você instala na máquina, tem o SIPAC, SIPOS, do mestrado/doutorado, cada setor tem um software. Os softwares que nós instalamos, que eu citei, não são via web, você monta na estação. É um sistema antigo que estão tentando melhorar. Inclusive só funciona dentro da universidade.

P: Como no IFB, temos vários softwares que só funcionam na intranet.

E: Inclusive o GLPI é só intranet. Se quiser fazer um pedido de fora da universidade, não vai conseguir fazer.

P: Então é isso. A ideia da entrevista é ter uma visão geral. No caso do suporte também, que é terceirizado.

E: O segundo nível. Se não conseguem resolver, o técnico vai ao local para resolver o problema.

P: Vocês usam acesso remoto aqui?

E: Também.

P: Tem uma política de acesso remoto?

E: Tem. Se estiverem no AD, a operadora pede permissão e acessa, se ela não consegue resolver, o técnico vai ao local.

P: Entendi.

E: Ganhamos bastante tempo com isso. Toda a reitoria está no AD.

P: Similar ao IFB, também usamos AD. Reitoria e campi. Mas aqui o tamanho é maior.

E: Colocamos primeiro a reitoria no AD estrategicamente. Conseguindo implantar lá, vai ser mais fácil implantar no restante da universidade. Requer bastante pessoal para fazer essa implantação. Mas estamos começando a implantar o AD, já tendo sido implantando em vários departamentos.

P: E os chamados são todos pelo GLPI?

E: Isso. Está sendo implantado o CITSmart, que faz a mesma coisa, mas para emitir o relatório é muito mais fácil.

P: Obrigado. Tive uma visão geral do setor. No IFB, não tem muito essa distinção de suporte, o técnico de TI muitas vezes faz a parte de suporte.

E: Aqui é o seguinte, por exemplo, chegou problema de redes, mandamos para a área de redes. O que podemos fazer aqui é instalar, formatar, etc. O que for identificado que é de outras áreas, será encaminhado. Por exemplo, um problema no sistema de administração acadêmica, mandamos para o setor competente. Desde que seja uma solicitação do pessoal administrativo que cuida dessa parte, o SA. Se for problemas encontrados por outros setores no sistema de administração acadêmica, mandamos entrar primeiro em contato com o pessoal do SA. Se houver algum problema, o técnico de lá vai entrar em contato com o técnico daqui.

P: E os campi, você tem representante do helpdesk lá?

E: Só em Planaltina.

P: E quando tem que fazer algum intervenção, vocês tem que ir lá?

E: A empresa ocasionalmente visita. Já a equipe de técnicos da UnB lá foi treinada aqui no CPD e faz a parte de redes.

P: Nos outros campi não tem equipe do helpdesk?

E: Só em Planaltina, tem uma pessoa do helpdesk, que era o único que estava com poucos técnicos. E lá também tem a equipe de TI da UnB para resolver os problemas. Se eles não conseguem resolver, passam para a gente e vamos resolver.

P: Então em Ceilândia, por exemplo, a própria equipe de TI instala o software, se precisar?

E: Isso.

P: Muito obrigado pela participação.

Apêndice F

Roteiro de Entrevista com a Coordenação de Redes do IFB (Visão Geral da Tecnologia da Informação no IFB)

Entrevista Visão Geral da Tecnologia da Informação – Coordenação de Redes do IFB

Senhor(a) respondente, esta entrevista faz parte de uma pesquisa desenvolvida no Mestrado Profissional em Computação Aplicada da Universidade de Brasília, na linha de pesquisa de gestão de riscos. O objetivo desta entrevista é entender melhor aspectos gerais da tecnologia da informação no IFB.

Missão dos Campi e o Papel da Tecnologia da Informação

1. Qual é a missão dos campi? Quais as atividades principais que são executadas para atingir essa missão?

2. Existe uma missão da tecnologia da informação? Quais as atividades principais de tecnologia da informação que são executadas para atingir essa missão?

3. Como é a integração NTIC-Campus? Como é a integração da Coordenação de Redes com o campus?

4. O que podemos afirmar sobre a existência de uma política de gestão de riscos de tecnologia da informação no IFB?

5. O que são os campi "não implantados" e os campi "implantados"?

6. Para promover ações de gerenciamento de riscos voltadas para a infraestrutura de tecnologia da informação comum aos campi (equipamentos, serviços, pessoas) no momento atual, seria interessante ter quais campi como referência?

Definições

Risco pode ser entendido como um evento incerto que, ocorrendo, pode ter impacto negativo nos objetivos da organização. É a combinação da possibilidade de eventos danosos para a organização ocorrerem e seu respectivo impacto para a organização.

Infraestrutura de Tecnologia da Informação pode ser considerada o conjunto composto por componentes de tecnologia (computadores, impressoras, etc.), recursos humanos (incluindo conhecimentos, habilidades, políticas e experiência necessária) e serviços de tecnologia da informação compartilhados, como o gerenciamento de bases de dados

Apêndice G

Compilação das Respostas da Entrevista com a Coordenação de Redes do IFB (Visão Geral da Tecnologia da Informação no IFB)

Entrevista Visão Geral da Tecnologia da Informação – Coordenação de Redes do IFB - Respostas

P: Pesquisador

E: Entrevistado

P: Qual é a missão dos campi? Quais as atividades principais que são executadas para atingir essa missão?

E: Todas as missões dos campi estão integradas à missão do IFB em si, que é fornecer ensino pesquisa e extensão, e uma qualidade de ensino técnico voltada para o estudante, o IFB é voltado para a área educacional, para a área de ensino, educação, e esta é a missão de todos os campi. Difusão de conhecimento, contribuir com uma formação mais sólida para os estudantes.

P: Quais as atividades principais que são executadas para atingir essa missão?

E: Ofertar uma variedade de cursos, seja na parte de cursos da área de FIC (Formação Inicial e Continuada), como também de cursos técnicos que, dependendo do campus, possam ser concomitantes (como PROEJA), ou então técnicos subsequentes – é aquele em que o estudante já fez o ensino médio e está querendo se profissionalizar em algum tipo de curso técnico. Além disso, o portfólio, o leque e a variedade de cursos oferecidos ajudam o estudante a escolher a profissão que ele quer, e aí se direcionar no curso em específico que ele procura. Além disso o que fomenta muito os alunos procurarem, principalmente os alunos de baixa renda, são os programas sociais que o IFB fomenta através das políticas institucionais de assistência ao estudante. Isso também é muito válido. Os programas lançados pelo governo que tem como carro-chefe o IFB, a exemplo do PRONATEC, é um leque, uma variedade de cursos técnicos.

P: Quais as atividades de apoio principais? Podemos considerar a TI como atividade concomitante, principal para cumprir essa missão maior?

E: Sim, a TI suporta todos esses setores que diretamente atendem ao aluno. Por exemplo, o registro acadêmico, uma CDAE – que também tem os programas de assistência estudantil, por exemplo, os laboratórios de informática que são utilizados pelos professores nos cursos, são suportados pela TI. Se um laboratório não funciona, o professor não tem como dar andamento a um curso técnico destes, ou um curso que o IFB oferece, então a TI se relaciona dando um suporte necessário para que esses outros setores funcionem, tanto a parte dos professores, coordenados pela DREP, entre outros setores que são vitais nos campi.

P: Então podemos dizer que existe uma missão de tecnologia da informação?

E: Sim.

P: E qual seria essa missão?

E: No caso dos campi, suportar toda parte, os setores que têm atendimento direto ao aluno – Biblioteca, Registro Acadêmico, CDAE, laboratórios de informática e pesquisa, a também o sistema administrativo, pois sem o administrativo o aluno também não consegue ter algum tipo de informação/assistência.

P: E para suportar essa atividade, o que você considera dentro da TI a atividade principal? Podemos quebrar a TI em várias partes?

E: Primeiro, suportar os sistemas que os setores utilizam. Fazer a manutenção dos laboratórios de informática (é muito importante porque garante a operabilidade dos laboratórios sempre que puderem ser utilizados). Podemos colocar também como ponto principal a administração da rede, porque em todos os campi hoje temos uma infraestrutura de redes a nível de servidores e que

precisam ser gerenciados, muitos serviços que precisam ser gerenciados, e a TI é quem faz essa gerência. Não só a gerência, mas quando dá algum problema de suporte, a intervenção de algum tipo de terceirizado ou empresa terceirizada no negócio, tem que abrir chamado, tem que fazer acompanhamento, tem que participar das capacitações e tem que participar das implantações em que eventualmente sistemas novos são implantados. Então a TI se relaciona em uma vertente muito grande de funções dentro do campus. E ela pode ser enquadrada nisso aí, em um nível de suporte bem direto, bem estratégico.

P: Como é a integração NTIC-Campus? Como é a integração da Coordenação de Redes com o campus?

E: Temos uma equipe que faz parte de uma centralização maior no IFB que é o núcleo de tecnologia, o NTIC. Então precisamos de um núcleo de tecnologia para poder padronizar as nossas ações e também servir de suporte nos mais diversos níveis, segundo nível, terceiro nível, dependendo da necessidade. Como os campi tem uma infraestrutura de redes bem semelhante, bem parecida entre eles, precisamos de um núcleo que nos faça, por exemplo, servir de base nos procedimentos que a gente tenha que adotar dentro dos campi, no nosso dia-a-dia, no nosso trabalho rotineiro. Então, por exemplo, a gente precisa de uma forma de abrir chamados técnicos, então o núcleo suporta o GLPI. Nós precisamos, por exemplo, de algum suporte na rede, alguma coisa que os campi não tenham conhecimento, vamos supor que eu não consiga implantar um firewall dentro da minha unidade, eu precisarei de um núcleo que tenha analistas, que tenha pessoas para me auxiliar na implantação daquela determinada tecnologia. Então a função do núcleo geralmente é essa.

Embora ele seja centralizador com relação à tecnologia, ele serve de suporte, serve de análise – caso um técnico de TI precise por exemplo de algum apoio, de algum tipo de entendimento, de capacitação, o núcleo está ali para poder orientar, para poder ajudar no momento que precise. Então o técnico pode ver no NTIC, no núcleo, um apoio direto às suas necessidades no campus que ele não consegue atender. É claro que os atendimentos de primeiro nível, os técnicos conseguem fazer naturalmente, mas os de segundo e terceiro nível que podem vir a depender de alguma alteração em um sistema que ele não tem permissão para poder fazer, o núcleo é acionado nesse tipo de situação, então o núcleo serve para esse apoio.

P: Existe uma política de gestão de riscos no IFB?

E: Não.

P: No IFB, seja no site ou conversando com gestores, há duas designações, uma divisão na nomenclatura dos campus, os campus implantados e os campus não implantados, o que podemos considerar do ponto de vista de tecnologia da informação como campus implantado e campus não implantado?

E: O núcleo entende como campus implantando todo aquele campus que tem uma infraestrutura mínima de rede e telecomunicações implantada para que o campus funcione. Para que um campus funcione a nível implantando, ele deve estar interligado hoje à rede giga candanga, que é aquela que fornece o link de 1GB, que é um link com capacidade que atenda a todos os sistemas que estejam implantados no campus. No caso de um campus não-implantado, ele não tem essa infraestrutura mínima. Em alguns casos há campus que não tem nem link definitivo, tem campus que não tem link algum de internet, tem campus que contrata link provisório, via rádio ou via concessionária pagando com recursos próprios do campus provisoriamente até o link definitivo chegar. E além disso existe todo um aparato de datacenter que o campus recebe, e que no caso o campus não implantado não possui. A exemplo, os campus que já são implantados, já tem servidores definitivos, link de internet definitivo, ativos de redes definitivos, como switches de redes, switches de borda, gateway de voz para utilização de voz sobre IP, e os campi que não

estão implantados ainda não tem esse tipo de ativos de rede. Normalmente há switches fora do padrão adotado em toda a rede, ou quando tem switches não tem a quantidade necessária. Não há servidores específicos de rede, aqueles em que virtualizamos servidores nele. Então nesses campi provisórios estão máquinas normais desktop que desempenham a função de servidor. O campus para ser considerado definitivo tem de ter toda uma infraestrutura de rede já montada, instalada e configurada para funcionamento. O campus que ainda está em implantação funciona de forma provisória, podemos dizer que sem todas as funcionalidades de rede ativas naquele campus. Ele só passa a ser definitivo ou implantado quando essa infraestrutura de rede toda (que foi descrita) é montada.

P: Na proposta dessa pesquisa, queremos chegar a uma base, em caminho de gerenciamento de risco para a infraestrutura comum. Para esta proposta, você acha importante usar todos os campi ou limitar esse escopo, pois há a questão dos campi implantado e os campi não implantados.

E: Acho interessante trabalhar em cima dos que já foram implantados, porque são eles que vão servir de base, para quando os que não foram implantados passarem a ser implantados, termos uma linha de escopo definida, então esses que são implantados podemos direcionar a pesquisa para cima deles porque os que não são implantados um dia vão se transformar nisso.

P: Então o que eles têm é provisório e eventualmente eles terão algo similar com o que os definitivos têm?

E: Exatamente isso, terão a mesma estrutura.

P: Muito obrigado pela participação.

Apêndice H

Roteiro de Entrevista com a Coordenação de Redes do IFB (Ativos, Serviços e Estruturas de TI Críticas para o Funcionamento do Campus)

Entrevista Ativos e Serviços Críticos Comum aos Campi que Impactam na Missão - Coordenação de Redes do IFB

Senhor(a) respondente, esta entrevista faz parte de uma pesquisa desenvolvida no Mestrado Profissional em Computação Aplicada da Universidade de Brasília, na linha de pesquisa de gestão de riscos. Seu objetivo é levantar ativos críticos que impactam na missão dos campi implantados do Instituto Federal de Brasília.

1. Qual a infraestrutura de hardware de tecnologia da informação que aparece em todos os campi e pode ser considerada crítica para que possam ser executadas as atividades principais dos campi?

> Quais as instalações associadas à tecnologia da informação que aparece em todos eles e podem ser consideradas críticas para que possam ser executadas as atividades principais dos campi?

2. Quais softwares ou serviços que existem em todos os campi e que podem considerados críticos para que possam ser executadas as atividades principais dos campi?

3. Quais ativos de dados são essenciais para executar as atividades principais dos campi e estão sob a guarda da TI dos campi?

4. Quais pessoas são essenciais para o funcionamento da tecnologia da informação da informação dos campi?

5. Quais podem ser considerados os serviços principais de tecnologia da informação conforme visto pelos usuários e prestados ou suportados diretamente pelo campus?

Apêndice I

Questionário - Riscos da Infraestrutura de Tecnologia da Informação do IFB na Visão dos Profissionais de TI dos Campi

Riscos da Infraestrutura de Tecnologia da Informação do IFB na Visão dos Profissionais de TI dos Campi

Este questionário faz parte de uma pesquisa sobre riscos relativos à infraestrutura de tecnologia da informação comum aos campi do Instituto Federal de Brasília (IFB) como parte do Mestrado Profissional em Computação Aplicada da Universidade de Brasília.

O Objetivo é entender a visão dos profissionais de tecnologia da informação de alguns campi do IFB quanto às principais ameaças, vulnerabilidades e ataques a que estão sujeitos os ativos dos campi, ou seja, a visão de risco dos profissionais de TI.

Risco pode ser entendido como um evento incerto que, ocorrendo, pode ter impacto negativo nos objetivos da organização É a combinação da possibilidade de eventos danosos para a organização ocorrerem e seu respectivo impacto para a organização.

Ameaça é a capacidade ou intenção de causar algum dano (falha de hardware, software).

Ataque é um conjunto bem definido de ações feita por um agente ativo (ameaça) que, tendo sucesso, poderia danificar um ativo, impactando na missão do campus.

Vulnerabilidade é uma fraqueza, é uma característica que pode ser explorada ou danificada por um ato não intencional causado por ação humana, como exemplo temos a inundação da sala em virtude da forte chuva, ou gerenciamento de senhas inadequado

Em uma situação hipotética, um possível cenário de risco é haver problemas de infiltração no datacenter ou salas técnicas, sendo que tais infiltrações podem deixá-los inundados, danificando equipamentos e impossibilitando o uso de internet e vários outros recursos de tecnologia da informação de forma prolongada.

Em outra cenário hipotético, funcionários que não deveriam ter acesso a determinados arquivos compartilhados podem ter acesso aos mesmos devido à falta de padronização na requisição de acesso, sendo que estes podem acabar fazendo alterações ou deletando permanentemente arquivos que não deveriam.

Podemos ainda ter uma situação hipotética em que há a necessidade de instalar equipamentos para disponibilizar internet para mais setores, mas a equipe de TI não tem o conhecimento necessário para configurar o equipamento, resultando no atraso ou na não disponibilização dos serviço de internet para os locais desejados.

Neste questionário perguntamos a sua visão de riscos com relação a determinadas áreas da tecnologia da informação. Ou seja, quais os principais problemas que você acha que podem ocorrer na área de infraestrutura de tecnologia da informação do seu campus. Quais seriam as coisas que mais o preocupam como técnico da área de tecnologia da informação, que poderiam se concretizar e precisam ser prevenidas. Se tiver uma sugestão de solução para o problema que você levantar, você também poderá indicá-la nas respostas.

As respostas dessas questões serão analisadas e poderão aparecer como problemas comuns que também afetam outros campi em um questionário a ser aplicado posteriormente.

*Obrigatório

Você é técnico de qual campus? *

- ◯ Brasília
- ◯ Gama
- ◯ Planaltina
- ◯ Samambaia
- ◯ Taguatinga

Quais os principais problemas que poderiam se concretizar com relação aos ativos de hardware do seu campus, como computadores, notebooks e outros equipamentos de TI? *

Sua resposta

Quais os principais problemas que poderiam se concretizar com relação aos ativos de software do seu campus, como sistemas operacionais e aplicativos em geral? *

Sua resposta

Quais os principais problemas que poderiam se concretizar com relação à equipe de tecnologia da informação do seu campus? *

Sua resposta

Quais os principais problemas que poderiam se concretizar com relação aos dados armazenados pelo campus, como planilhas, documentos de texto, pastas individuais ou compartilhadas? *

Sua resposta

Existem outros riscos ou problemas que possam vir a afetar a área de tecnologia da informação do seu campus que você acha importante citar? *

Sua resposta

Você teve alguma dificuldade respondendo este questionário?

Sua resposta

Apêndice J

Questionário - Riscos da Infraestrutura de Tecnologia da Informação dos Campi do IFB na Visão da Direção Geral

Riscos da Infraestrutura de Tecnologia da Informação dos Campi do IFB na Visão da Direção Geral

Este questionário faz parte de uma pesquisa sobre riscos relativos à infraestrutura de tecnologia da informação comum aos campi do Instituto Federal de Brasília (IFB) como parte do Mestrado Profissional em Computação Aplicada da Universidade de Brasília.

O Objetivo é entender a visão da alta gestão (Direção Geral) de alguns campi do IFB quanto aos riscos de tecnologia da informação.

Risco pode ser entendido como um evento incerto que, ocorrendo, pode ter impacto negativo nos objetivos da organização.

Em uma situação hipotética, um possível cenário de risco é haver problemas de infiltração no datacenter ou salas técnicas, sendo que tais infiltrações podem deixá-los inundados, danificando equipamentos e impossibilitando o uso de internet e vários outros recursos de tecnologia da informação de forma prolongada.

Em outra cenário hipotético, funcionários que não deveriam ter acesso a determinados arquivos compartilhados podem ter acesso aos mesmos devido à falta de padronização na requisição de acesso, sendo que estes podem acabar fazendo alterações ou deletando permanentemente arquivos que não deveriam.

Podemos ainda ter uma situação hipotética em que há a necessidade de instalar equipamentos para disponibilizar internet para mais setores, mas a equipe de TI não tem o conhecimento necessário para configurar o equipamento, resultando no atraso ou na não disponibilização dos serviço de internet para os locais desejados.

Neste questionário perguntamos a sua visão de riscos com relação a determinadas áreas da tecnologia da informação. Ou seja, quais os principais problemas que você acha que podem ocorrer na área de infraestrutura de tecnologia da informação do seu campus. Quais seriam as coisas que mais o preocupam como diretor geral, que poderiam se concretizar e precisam ser prevenidas. Se tiver uma sugestão de solução para o problema que você levantar, você também poderá indicá-la nas respostas.

As respostas dessas questões serão analisadas junto com as respostas dos técnicos de TI e poderão aparecer como problemas comuns que também afetam outros campi em um questionário a ser aplicado posteriormente.

*Obrigatório

Você é diretor de qual campus? *

- ◯ Brasília
- ◯ Gama
- ◯ Planaltina
- ◯ Samambaia
- ◯ Taguatinga

Quais os principais problemas que poderiam se concretizar com relação aos ativos de hardware do seu campus, como computadores, notebooks e outros equipamentos de TI? *

Sua resposta

Quais os principais problemas que poderiam se concretizar com relação aos ativos de software do seu campus, como sistemas operacionais e aplicativos em geral? *

Sua resposta

Quais os principais problemas que poderiam se concretizar com relação à equipe de tecnologia da informação do seu campus? *

Sua resposta

Quais os principais problemas que poderiam se concretizar com relação aos dados armazenados pelo campus, como planilhas, documentos de texto, pastas individuais ou compartilhadas? *

Sua resposta

Existem outros riscos ou problemas que possam vir a afetar a área de tecnologia da informação do seu campus que você acha importante citar? *

Sua resposta

Você teve alguma dificuldade respondendo este questionário?

Sua resposta

Apêndice K

Probabilidade e Impacto dos Riscos - Considerações Referentes ao Questionário Piloto

Considerações - Questionário Piloto - Probabilidade e Impacto dos Riscos

Explicação das Categorias
É melhor que a descrição das categorias de probabilidade e impacto fique no começo do questionário.

ex.:
Muito Baixa ou inexistente (improvável de acontecer)
Baixa (remota mas pode ocorrer)
Catastrófico (colapso do sistema, completa falha na missão, morte ou similares)

E nas questões fique apenas o nome
Muito Baixa ou inexistente
Baixa
Catrastrófico

Desta forma o texto fica visualmente mais limpo e não apresenta a ideia de um texto complexo ou cansativo.

Título
É interessante colocar um título para separar cada questão, ajudará, visualmente, a manter as questões mais organizadas e visualmente menos cansativo.

Ajuste de Perguntas - Acesso Não Autorizado

Descrição do Problema
Foi discutido que não é necessário pormenorizar determinados problemas, pois uma vulnerabilidade pode acarretar uma gama de problemas, dessa forma é melhor "exemplo 1" do que ter "exemplo 2" e "exemplo 3" no questionário ao mesmo tempo. Assim a leitura fica menos cansativa, o técnico conhece seu ambiente e entende até certo ponto a extensão de determinadas vulnerabilidades ou problemas.

Exemplo 1: Qual a probabilidade de pessoas não autorizadas (servidores ou não) terem acesso às salas técnicas e datacenter.
Exemplo 2: Qual a probabilidade de equipamentos serem roubados devido ao acesso de pessoas não autorizadas (servidores ou não) às salas técnicas e datacenter?
Exemplo 3: Qual a probabilidade de danos causados por acesso não autorizado às salas técnicas e datacenters?

Ajuste de Perguntas - Equipamentos Obsoletos

Original:
Qual a probabilidade de Desktops e notebooks obsoletos continuarem sendo utilizados?
Qual a probabilidade de Switches obsoletos continuarem sendo utilizados?
Qual a probabilidade de Servidores obsoletos continuarem sendo utilizados?

Alterado:
Qual a probabilidade de equipamentos de tecnologia da informação (como Desktops, Notebooks, Switches, Servidores) obsoletos continuarem sendo utilizados?

Razão: Melhor análise do usuário. Mais objetividade. O parque envelhece atualmente de forma quase uniforme, então quando um estiver velho, é provável que outros estejam velhos também.

Ajuste de Perguntas - Coordenação de TI

Original: Qual o impacto de haver comprometimento na qualidade dos serviços prestados pela equipe de TI do campus devido à falta de uma Coordenação de Tecnologia da Informação no Campus ?

Alterado: Qual o impacto na qualidade dos serviços prestados pela equipe de TI com a falta de uma Coordenação de Tecnologia da Informação?

Razão: Maior fluidez e objetividade da pergunta.

Ajuste de Perguntas - Coordenação de TI
Original: Qual a probabilidade de não haver um contrato vigente de manutenção para a solução da APC no Datacenter do campus?

Alterado: Qual a probabilidade de ser necessária manutenção para a solução de Datacenter do campus, incluindo solução de contenção de calor e nobreak, e não haver manutenção contratada?

Razão: Objetividade, clareza. Removido nome de marca/empresa e usado nomes das soluções que integram o todo.

Ajuste de Perguntas - Políticas de Segurança da Informação

Original: Qual a probabilidade da falta de uma política de segurança da informação atualizada afetar o andamento do trabalho de tecnologia da informação:

Alterado: Qual a probabilidade da falta de uma política de segurança da informação atualizada afetar a qualidade dos serviços prestados pela equipe de TI ?

Razão: Maior fluidez e objetividade da pergunta.

Apêndice L

Probabilidade e Impacto dos Riscos - Questionário

Riscos de Infraestrutura de TI nos Campi do IFB - Probabilidade e Impacto

Esta parte da pesquisa se destina a analisar os riscos que foram levantados anteriormente. Aqui solicitamos que atribua uma probabilidade e impacto a cada um dos problemas que podem se concretizar no seu campus, com relação a hardware, software, pessoal e outras áreas da Tecnologia da Informação.

Probabilidade - A frequência com a qual você acha que o problema possa ocorrer:
Muito Baixa ou Inexistente (improvável de acontecer)
Baixa (remota mas pode ocorrer)
Média (pode ocorrer algumas vezes)
Alta (pode ocorrer várias vezes)
Muito Alta (frequente, pode ocorrer repetidamente)

Impacto - As consequências que você entenda que o problema possa causar
Negligível (dano insignificante ou inexistente)
Mínimo (dano mínimo, degradação mínima da missão)
Mediano (degradação da missão, exposição de dados ou similares)
Crítico (falha grande no sistema, exposição de dados confidenciais ou similares)
Catastrófico (colapso do sistema, completa falha na missão, morte ou similares)

*Obrigatório

Você é técnico de qual campus? *

- ◯ Brasília
- ◯ Gama
- ◯ Planaltina
- ◯ Samambaia
- ◯ Taguatinga

Garantia e Manutenção Especializada

Qual a probabilidade dos equipamentos de tecnologia da informação (como Desktops, Notebooks, Switches, Servidores) ficarem sem garantia ou manutenção especializada em seu tempo de vida útil? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual a impacto da falta de garantia, reposição ou manutenção especializada para os equipamentos de tecnologia da informação em seu tempo de vida útil? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Ativos Obsoletos

Qual a probabilidade de equipamentos de tecnologia da informação (como Desktops, Notebooks, Switches, Servidores) obsoletos continuarem sendo utilizados? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual a impacto de equipamentos de tecnologia da informação obsoletos continuarem sendo utilizados? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Manutenção - Datacenter

Qual a probabilidade de ser necessária manutenção para a solução de Datacenter do campus, incluindo solução de contenção de calor e nobreak, e não haver manutenção contratada? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto de ser necessária manutenção para a solução de Datacenter do campus, incluindo solução de contenção de calor e nobreak, e não haver manutenção contratada? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Furto de Equipamentos

Qual a probabilidade de Desktops e Notebooks e/ou seus componentes serem roubados devido à falta de segurança física (cadeados, cabos de aço, câmeras, vigilância)? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual a impacto do roubo de Desktops e Notebooks e/ou seus componentes? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Backup

Qual a probabilidade de ser necessário restaurar arquivos, sistemas, servidores ou serviços através de backup? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual a impacto de não haver backup para restauração de arquivos, sistemas, servidores ou serviços? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Mau Uso e Depredação

Qual a probabilidade de equipamentos serem danificados devido ao mau uso ou depredação nas salas de aula e laboratórios? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual a impacto da depredação de equipamentos de TI nos salas de aula e laboratórios? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Rede Estabilizada

Qual a probabilidade da falta de proteção na rede elétrica (nobreak, rede estabilizada) causar danos aos equipamentos de tecnologia da informação? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual a impacto de danos causados aos equipamentos de tecnologia da informação devido à falta de proteção na rede elétrica (nobreak, rede estabilizada)? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Rede Estabilizada - Contato com equipamento elétrico

Qual a probabilidade do técnico se acidentar com nobreaks e equipamentos de estabilização de rede elétrica instalados no datacenter ou salas técnicas ? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual a impacto de acidentes com nobreaks e equipamentos de estabilização de rede elétrica instalados no datacenter ou salas técnicas ? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Atualização de Firmware

Qual a probabilidade do firmware dos equipamentos de rede (switches, gateways de voz, etc.), desktops (bios) e outros equipamentos de TI estarem desatualizados ? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual a impacto dos firmwares estarem desatualizados (com relação a ataques, exploração de vulnerabilidades, etc.) ? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Acesso ao Datacenter e Salas Técnicas

Qual a probabilidade de pessoas não autorizadas (servidores ou não) terem acesso às salas técnicas e datacenter ? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual a impacto do acesso de pessoas não autorizadas (servidores ou não) às salas técnicas e datacenter? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Senhas

Qual a probabilidade de ocorrer brechas de segurança ou incidentes devido à falta de gerenciamento de senhas de administrador? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto da exploração de brechas de segurança ou concretização de incidentes devido à falta de gerenciamento de senhas de administrador? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Sistemas Operacionais - Updates

Qual a probabilidade de sistemas operacionais Windows com suporte a atualizações serem utilizados sem a aplicação das atualizações em desktops e notebooks? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto da utilização de sistemas operacionais Windows com suporte a atualizações sem a aplicação das mesmas em desktops e notebooks? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Sistemas Operacionais Descontinuados - Desktops

Qual a probabilidade de sistemas operacionais Windows descontinuados continuarem sendo utilizados em desktops e notebooks? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto de sistemas operacionais Windows descontinuados continuarem sendo utilizados em desktops e notebooks? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Sistemas Operacionais Descontinuados - Servidores

Qual a probabilidade de sistemas operacionais Windows Server descontinuados continuarem sendo usados nos servidores ? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual a impacto de sistemas operacionais Windows Server descontinuados continuarem sendo usados nos servidores ? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Softwares de Uso Geral - Atualização

Qual a probabilidade de softwares instalados para uso no dia-a-dia nos Desktops estarem desatualizados ou obsoletos? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto de softwares instalados para uso no dia-a-dia nos Desktops estarem desatualizados ou obsoletos? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Antivírus

Qual a probabilidade de softwares antivírus não estarem instalados em servidores e computadores em geral? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto de softwares antivírus não estarem instalados em servidores e computadores em geral? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Microsoft Office e Libre Office

Qual a probabilidade do uso alternado do Microsoft Office e Libre Office inutilizar documentos ou gerar incompatibilidades nos documentos utilizados? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto do uso alternado do Microsoft Office e Libre Office inutilizar documentos ou gerar incompatibilidades nos documentos utilizados? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Softwares- Homologação

Qual a probabilidade da equipe de TI não manter uma lista de softwares testados e aprovados (homologados) que possam ser instalados nos computadores? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto da equipe de TI não manter uma lista de softwares testados e aprovados (homologados) que possam ser instalados nos computadores? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Pastas Compartilhadas - Controle de Acesso

Qual a probabilidade de pessoas não-autorizadas, de forma intencional ou não, terem acesso às pastas compartilhadas em rede devido à má configuração do controle de acesso? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto de pessoas não-autorizadas, de forma intencional ou não, terem acesso às pastas compartilhadas em rede devido à má configuração do controle de acesso? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Uso da Internet do Campus

Qual a probabilidade da internet do campus ser usada para cometer crimes virtuais (como DDOs, disseminação de arquivos indevidos, injúria) através dos computadores de acesso público ou Wi-Fi ? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto da internet do campus ser usada para cometer crimes virtuais (como DDOs, disseminação de arquivos indevidos, injúria) através dos computadores de acesso público ou Wi-Fi ? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico

Técnico de TI - Capacitação

Qual a probabilidade do técnico não possuir capacitação básica para lidar com alguma ou várias das tecnologias necessárias para o funcionamento saudável da tecnologia da informação do campus? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual a impacto do técnico não possuir capacitação básica para lidar com alguma ou várias das tecnologias necessárias para o funcionamento saudável da tecnologia da informação do campus? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Equipe de TI - Atribuições

Qual a probabilidade da falta de clareza nas atribuições do cargo de técnico de tecnologia da informação afetar os serviços de TI que se espera do campus? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto da falta de clareza nas atribuições do cargo de técnico de tecnologia da informação afetar os serviços de TI que se espera do campus? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Equipe de TI - Quantitativo de Pessoal

Qual a probabilidade da equipe de TI do campus não ser suficiente para atender as demandas? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto da equipe de TI do campus não ser suficiente para atender as demandas? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Equipe de TI

Qual a probabilidade da falta de uma Coordenação de Tecnologia da Informação afetar a qualidade dos serviços prestados pela equipe de TI? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto na qualidade dos serviços prestados pela equipe de TI com a falta de uma Coordenação de Tecnologia da Informação? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Políticas de Segurança da Informação

Qual a probabilidade da falta de uma política de segurança da informação atualizada afetar a qualidade dos serviços prestados pela equipe de TI ? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual a impacto da falta de uma política de segurança da informação atualizada afetar a qualidade dos serviços prestados pela equipe de TI? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Relação Reitoria - Campus: Decisões e Políticas

Qual a probabilidade que políticas e decisões de tecnologia da informação que afetam os campi sejam tomadas sem que o campus seja devidamente consultado? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual a impacto de políticas e decisões de tecnologia da informação tomadas sem que os campi seja devidamente consultado? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Relação Reitoria - Campus: Aquisições

Qual a probabilidade de aquisições de tecnologia da informação destinadas aos campi sejam feitas sem que o campus seja devidamente consultado? *

- ◯ Muito Baixa ou Inexistente
- ◯ Baixa
- ◯ Média
- ◯ Alta
- ◯ Muito Alta

Qual o impacto de aquisições de tecnologia da informação destinadas aos campi feitas sem que o campus seja devidamente consultado? *

- ◯ Negligível
- ◯ Mínimo
- ◯ Mediano
- ◯ Crítico
- ◯ Catastrófico

Gostaria de fazer algum comentário com relação ao questionário?

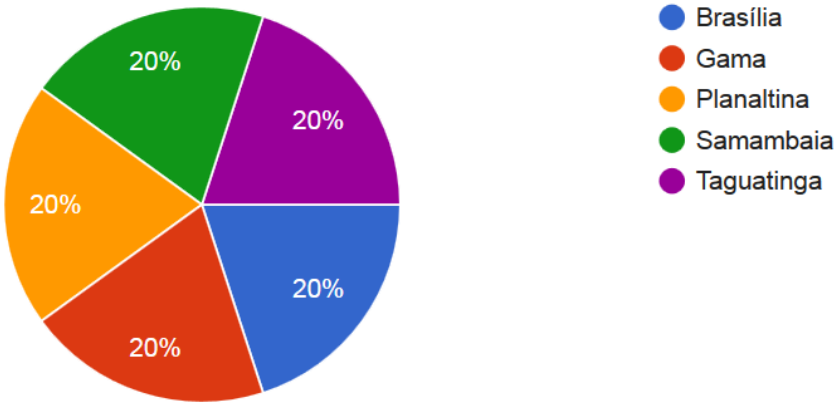
Sua resposta

Apêndice M

Probabilidade e Impacto dos Riscos - Respostas

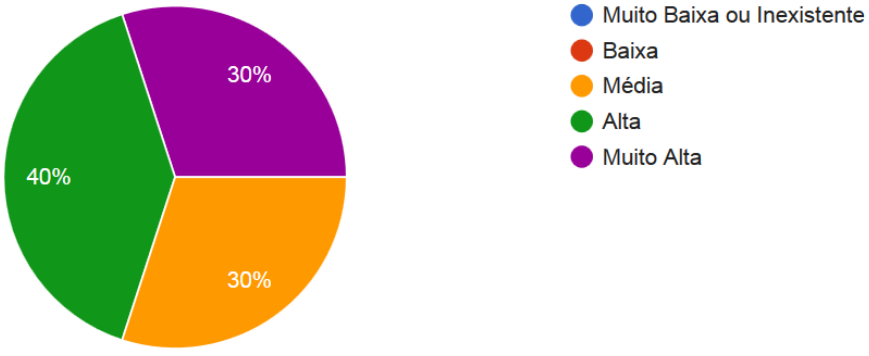
10 respostas

Você é técnico de qual campus? (10 respostas)



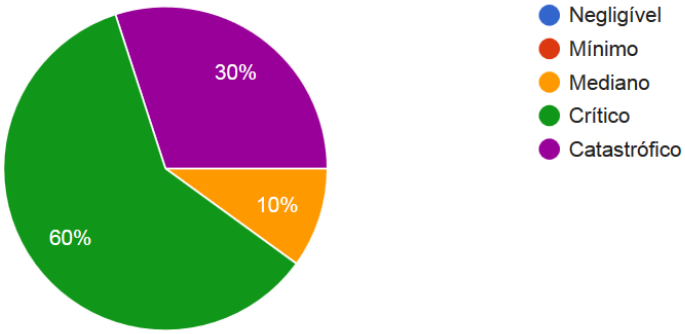
Garantia e Manutenção Especializada

Qual a probabilidade dos equipamentos de tecnologia da informação (como Desktops, Notebooks, Switches, Servidores) ficarem sem garantia ou manutenção especializada em seu tempo de vida útil?
(10 respostas)



Qual a impacto da falta de garantia, reposição ou manutenção especializada para os equipamentos de tecnologia da informação em seu tempo de vida útil?

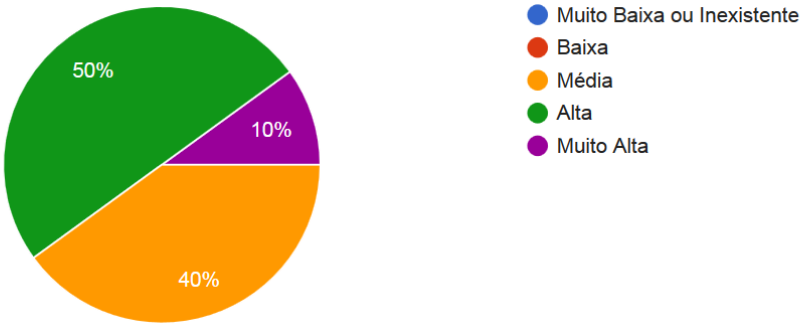
(10 respostas)



Ativos Obsoletos

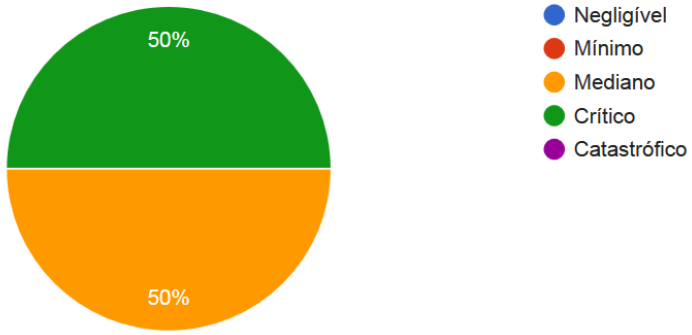
Qual a probabilidade de equipamentos de tecnologia da informação (como Desktops, Notebooks, Switches, Servidores) obsoletos continuarem sendo utilizados?

(10 respostas)



Qual a impacto de equipamentos de tecnologia da informação obsoletos continuarem sendo utilizados?

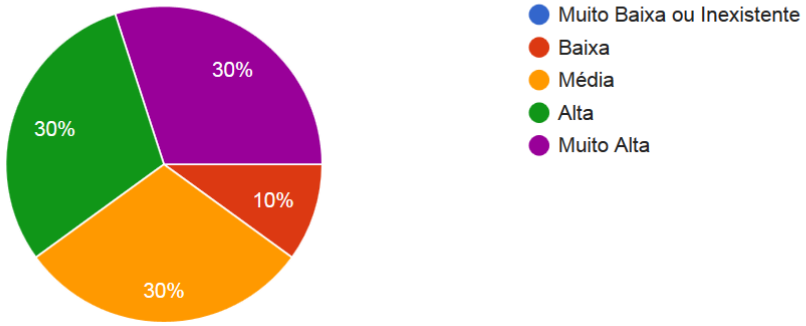
(10 respostas)



Manutenção - Datacenter

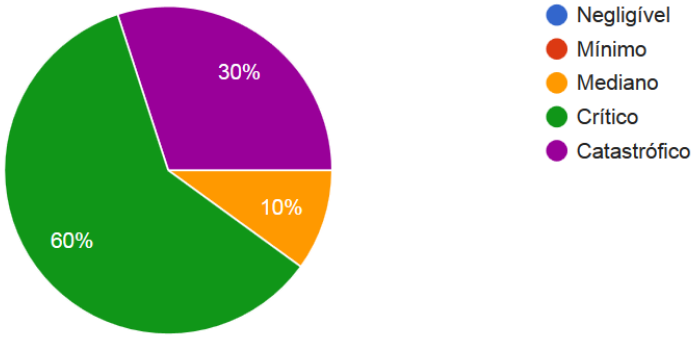
Qual a probabilidade de ser necessária manutenção para a solução de Datacenter do campus, incluindo solução de contenção de calor e nobreak, e não haver manutenção contratada?

(10 respostas)



Qual o impacto de ser necessária manutenção para a solução de Datacenter do campus, incluindo solução de contenção de calor e nobreak, e não haver manutenção contratada?

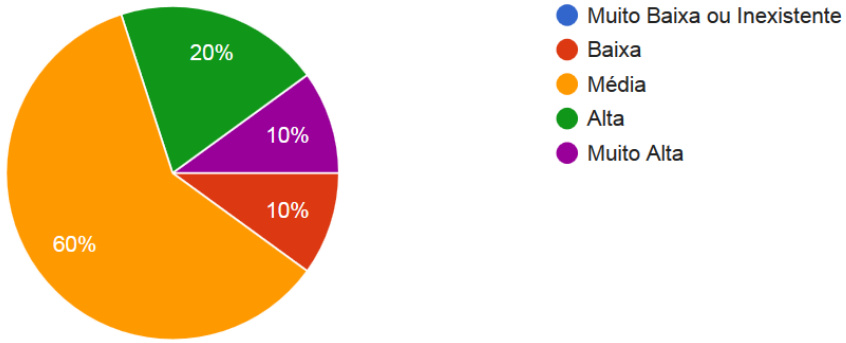
(10 respostas)



Furto de Equipamentos

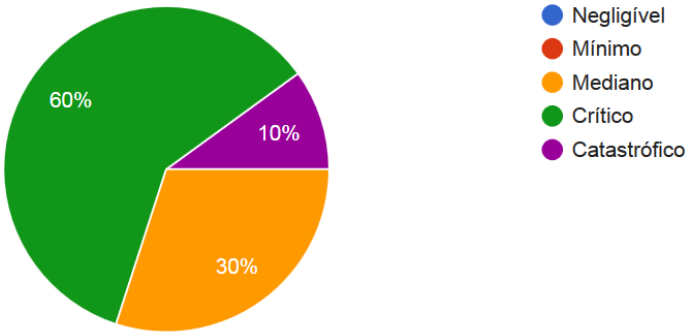
Qual a probabilidade de Desktops e Notebooks e/ou seus componentes serem roubados devido à falta de segurança física (cadeados, cabos de aço, câmeras, vigilância)?

(10 respostas)



Qual a impacto do roubo de Desktops e Notebooks e/ou seus componentes?

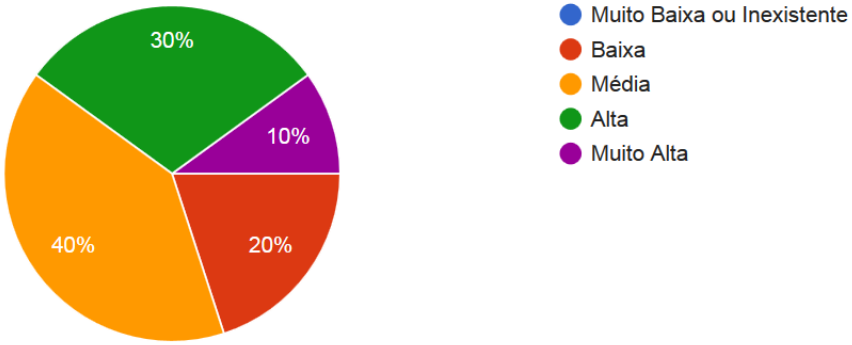
(10 respostas)



Backup

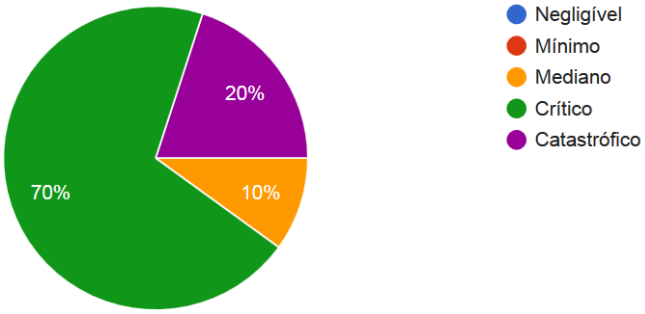
Qual a probabilidade de ser necessário restaurar arquivos, sistemas, servidores ou serviços através de backup?

(10 respostas)



Qual a impacto de não haver backup para restauração de arquivos, sistemas, servidores ou serviços?

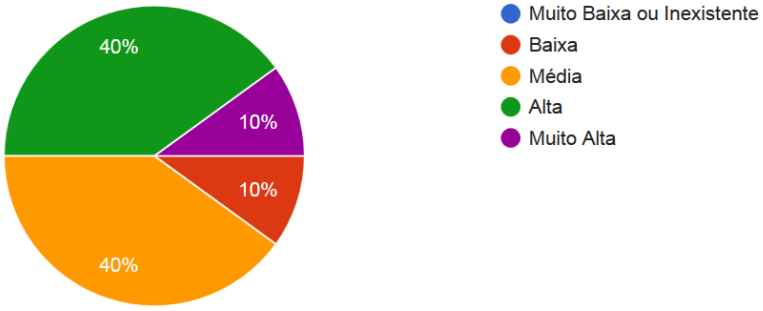
(10 respostas)



Mau Uso e Depredação

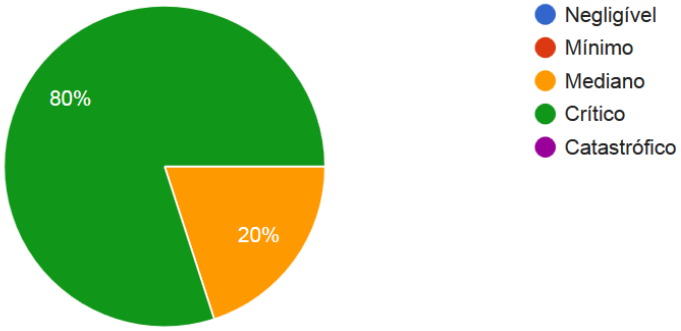
Qual a probabilidade de equipamentos serem danificados devido ao mau uso ou depredação nas salas de aula e laboratórios?

(10 respostas)



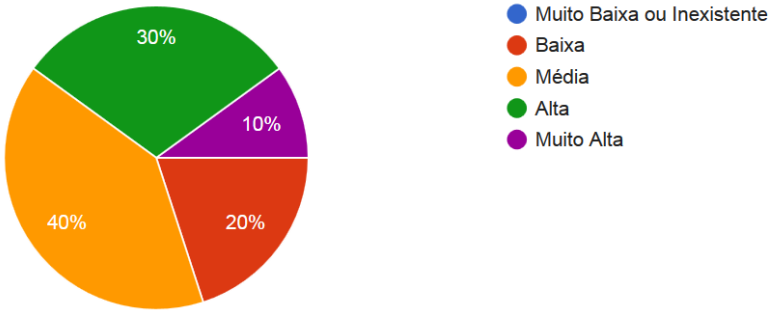
Qual a impacto da depredação de equipamentos de TI nos salas de aula e laboratórios?

(10 respostas)

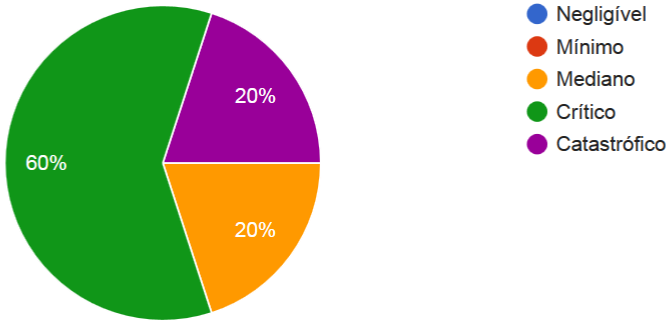


Rede Estabilizada

Qual a probabilidade da falta de proteção na rede elétrica (nobreak, rede estabilizada) causar danos aos equipamentos de tecnologia da informação?
(10 respostas)

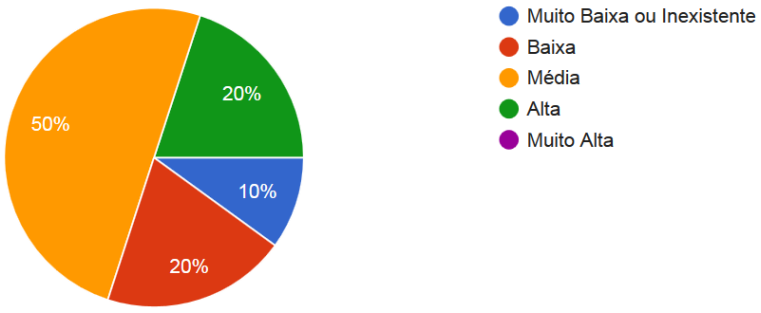


Qual a impacto de danos causados aos equipamentos de tecnologia da informação devido à falta de proteção na rede elétrica (nobreak, rede estabilizada)?
(10 respostas)



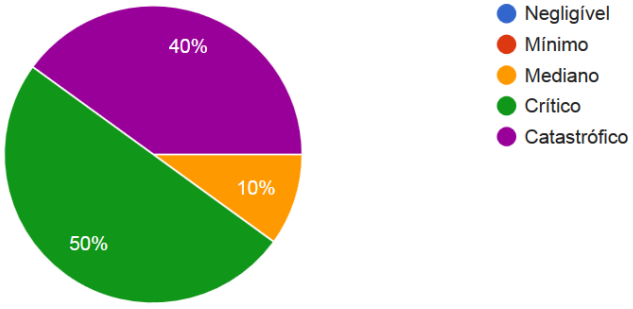
Rede Estabilizada - Contato com equipamento elétrico

Qual a probabilidade do técnico se acidentar com nobreaks e equipamentos de estabilização de rede elétrica instalados no datacenter ou salas técnicas ?
(10 respostas)



Qual a impacto de acidentes com nobreaks e equipamentos de estabilização de rede elétrica instalados no datacenter ou salas técnicas ?

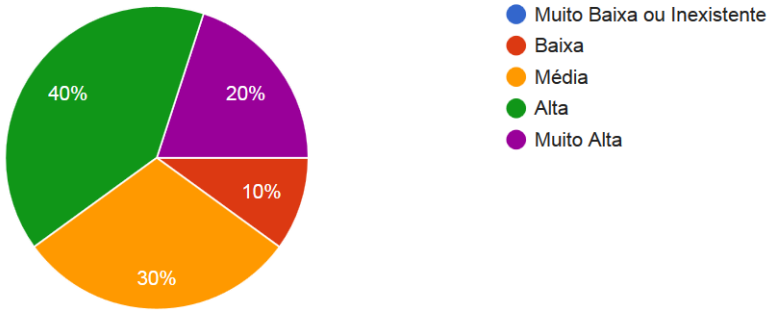
(10 respostas)



Atualização de Firmware

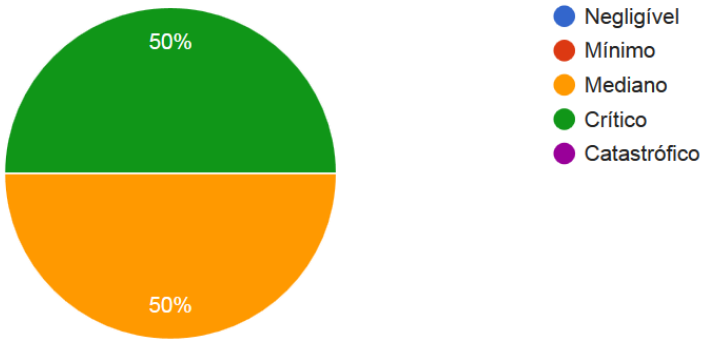
Qual a probabilidade do firmware dos equipamentos de rede (switches, gateways de voz, etc.), desktops (bios) e outros equipamentos de TI estarem desatualizados ?

(10 respostas)



Qual a impacto dos firmwares estarem desatualizados (com relação a ataques, exploração de vulnerabilidades, etc.) ?

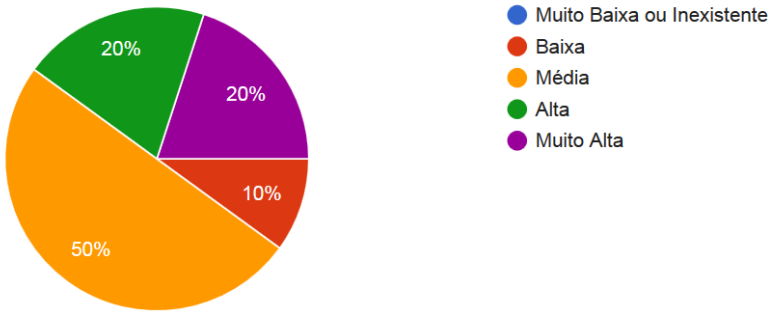
(10 respostas)



Acesso ao Datacenter e Salas Técnicas

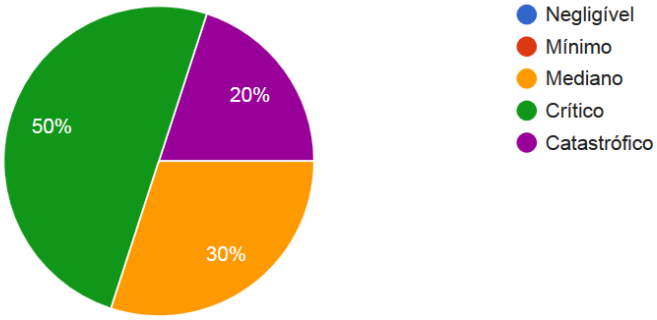
Qual a probabilidade de pessoas não autorizadas (servidores ou não) terem acesso às salas técnicas e datacenter ?

(10 respostas)



Qual a impacto do acesso de pessoas não autorizadas (servidores ou não) às salas técnicas e datacenter?

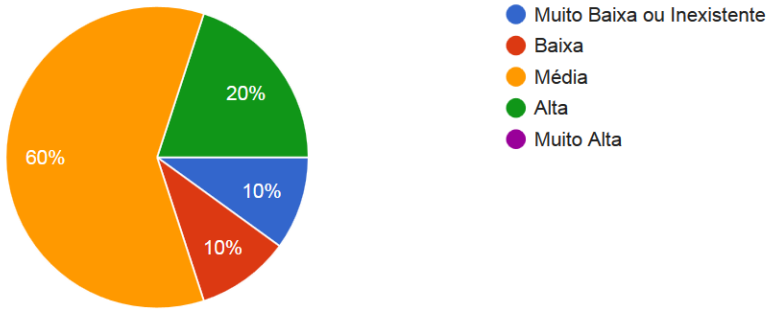
(10 respostas)



Senhas

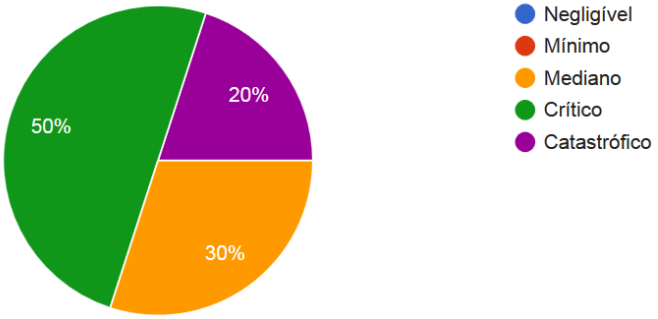
Qual a probabilidade de ocorrer brechas de segurança ou incidentes devido à falta de gerenciamento de senhas de administrador?

(10 respostas)



Qual o impacto da exploração de brechas de segurança ou concretização de incidentes devido à falta de gerenciamento de senhas de administrador?

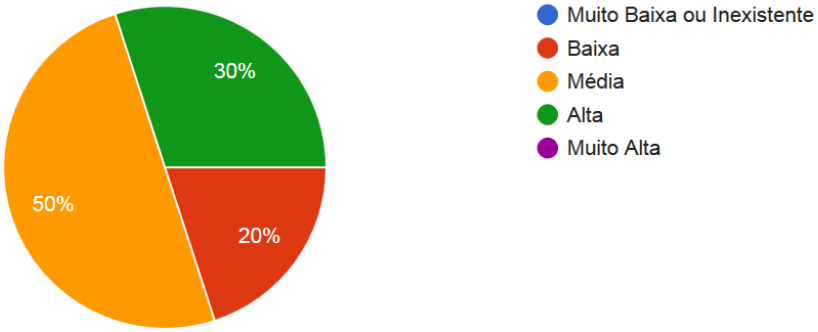
(10 respostas)



Sistemas Operacionais - Updates

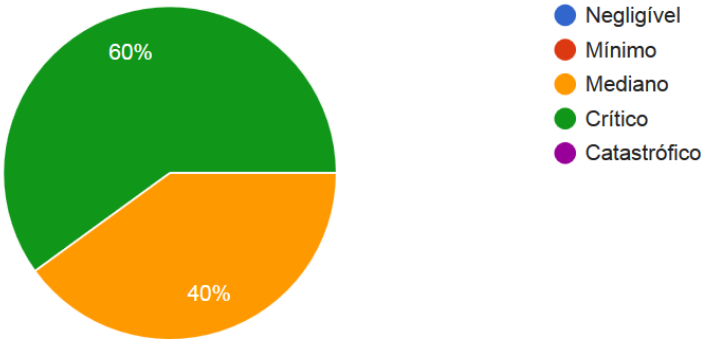
Qual a probabilidade de sistemas operacionais Windows com suporte a atualizações serem utilizados sem a aplicação das atualizações em desktops e notebooks?

(10 respostas)



Qual o impacto da utilização de sistemas operacionais Windows com suporte a atualizações sem a aplicação das mesmas em desktops e notebooks?

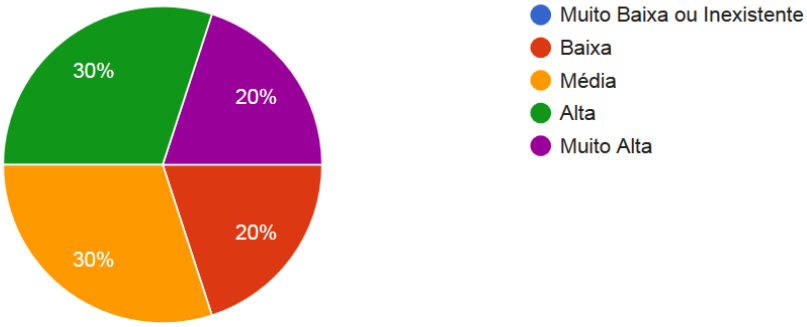
(10 respostas)



Sistemas Operacionais Descontinuados - Desktops

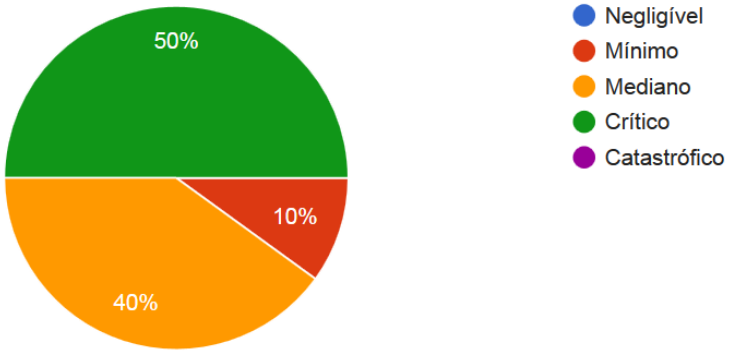
Qual a probabilidade de sistemas operacionais Windows descontinuados continuarem sendo utilizados em desktops e notebooks?

(10 respostas)



Qual o impacto de sistemas operacionais Windows descontinuados continuarem sendo utilizados em desktops e notebooks?

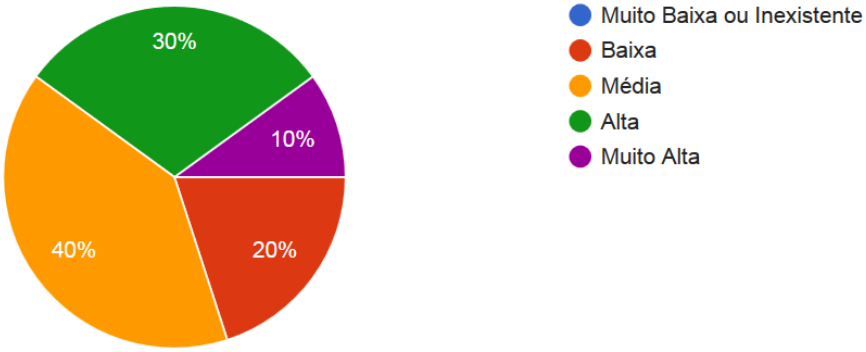
(10 respostas)



Sistemas Operacionais Descontinuados - Servidores

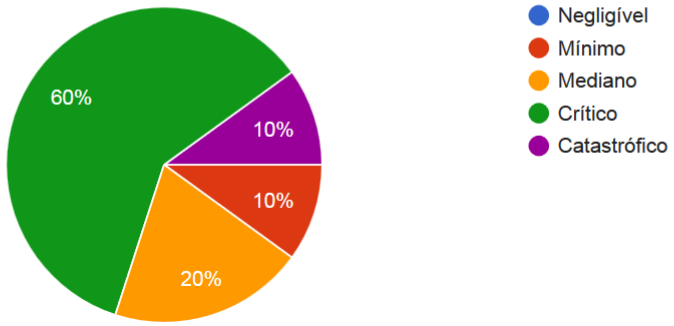
Qual a probabilidade de sistemas operacionais Windows Server descontinuados continuarem sendo usados nos servidores ?

(10 respostas)



Qual a impacto de sistemas operacionais Windows Server descontinuados continuarem sendo usados nos servidores ?

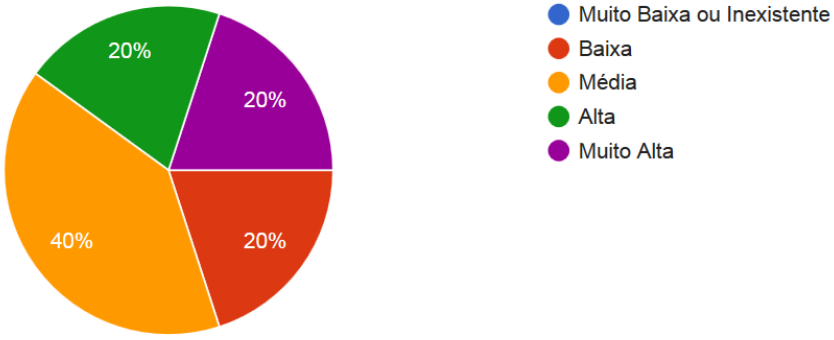
(10 respostas)



Softwares de Uso Geral - Atualização

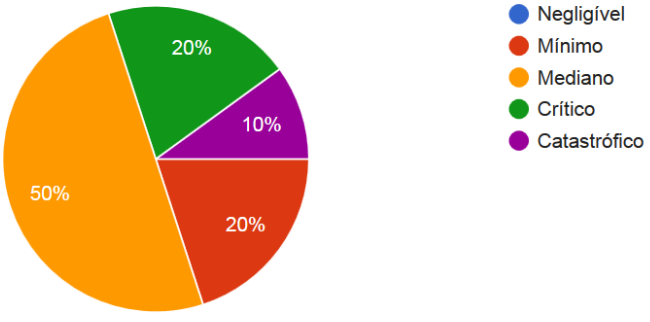
Qual a probabilidade de softwares instalados para uso no dia-a-dia nos Desktops estarem desatualizados ou obsoletos?

(10 respostas)



Qual o impacto de softwares instalados para uso no dia-a-dia nos Desktops estarem desatualizados ou obsoletos?

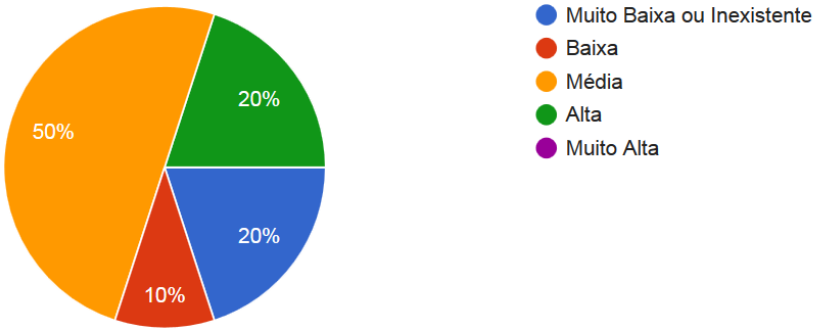
(10 respostas)



Antivírus

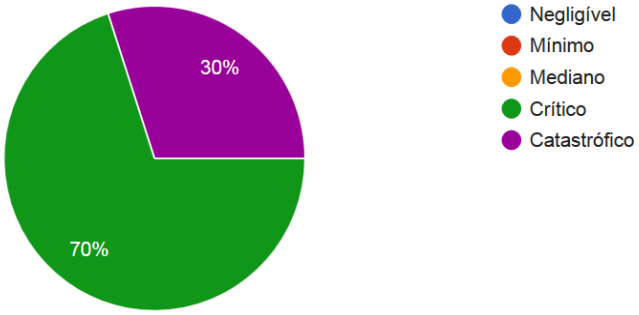
Qual a probabilidade de softwares antivírus não estarem instalados em servidores e computadores em geral?

(10 respostas)



Qual o impacto de softwares antivírus não estarem instalados em servidores e computadores em geral?

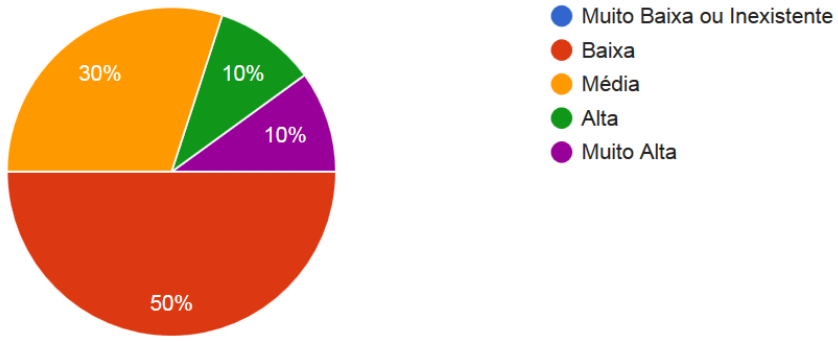
(10 respostas)



Microsoft Office e Libre Office

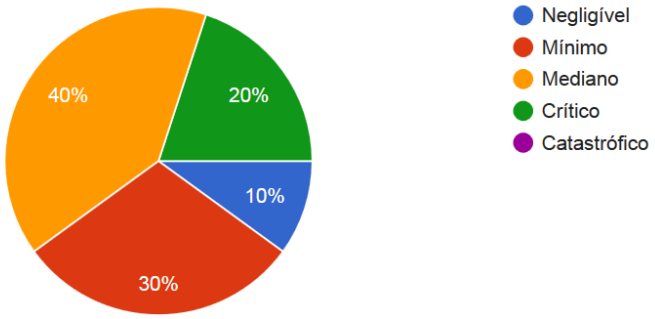
Qual a probabilidade do uso alternado do Microsoft Office e Libre Office inutilizar documentos ou gerar incompatibilidades nos documentos utilizados?

(10 respostas)



Qual o impacto do uso alternado do Microsoft Office e Libre Office inutilizar documentos ou gerar incompatibilidades nos documentos utilizados?

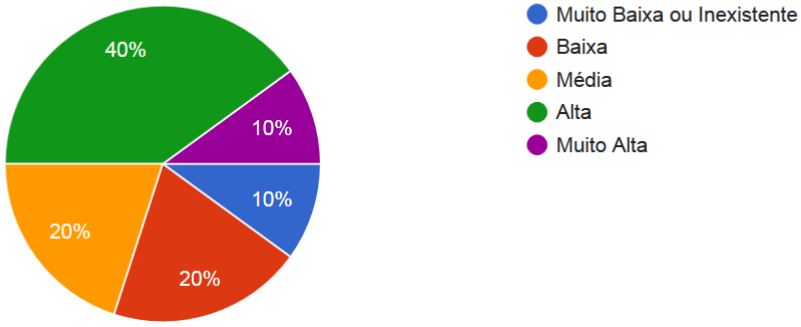
(10 respostas)



Softwares- Homologação

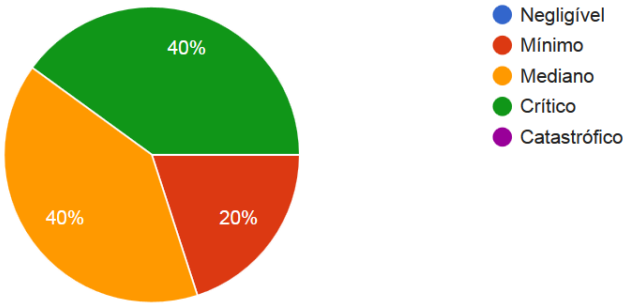
Qual a probabilidade da equipe de TI não manter uma lista de softwares testados e aprovados (homologados) que possam ser instalados nos computadores?

(10 respostas)



Qual o impacto da equipe de TI não manter uma lista de softwares testados e aprovados (homologados) que possam ser instalados nos computadores?

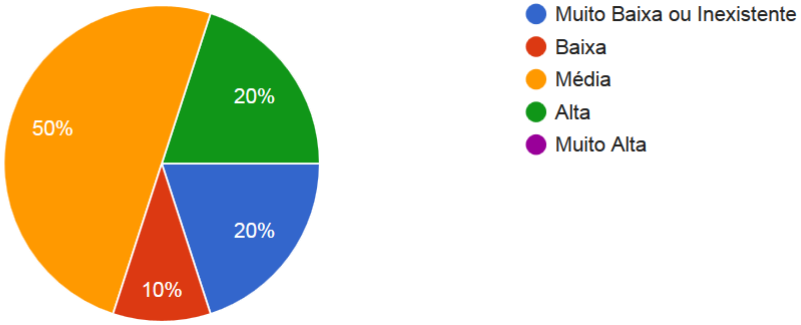
(10 respostas)



Pastas Compartilhadas - Controle de Acesso

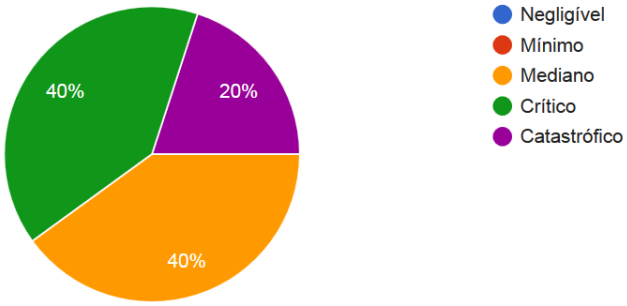
Qual a probabilidade de pessoas não-autorizadas, de forma intencional ou não, terem acesso às pastas compartilhadas em rede devido à má configuração do controle de acesso?

(10 respostas)



Qual o impacto de pessoas não-autorizadas, de forma intencional ou não, terem acesso às pastas compartilhadas em rede devido à má configuração do controle de acesso?

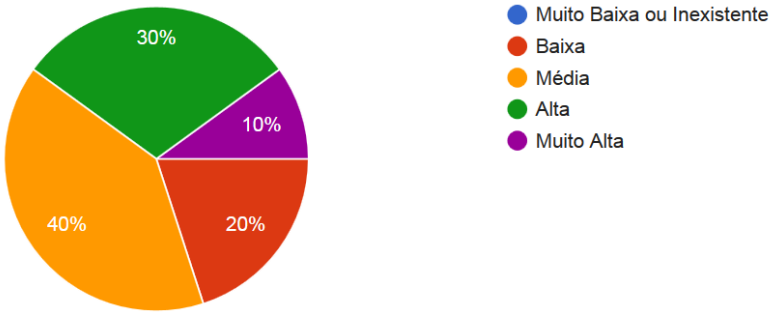
(10 respostas)



Uso da Internet do Campus

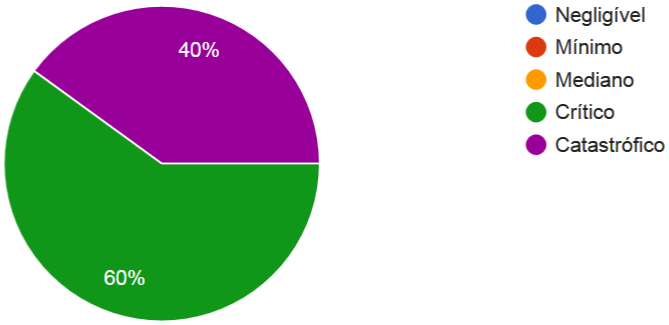
Qual a probabilidade da internet do campus ser usada para cometer crimes virtuais (como DDOs, disseminação de arquivos indevidos, injúria) através dos computadores de acesso público ou Wi-Fi ?

(10 respostas)



Qual o impacto da internet do campus ser usada para cometer crimes virtuais (como DDOs, disseminação de arquivos indevidos, injúria) através dos computadores de acesso público ou Wi-Fi ?

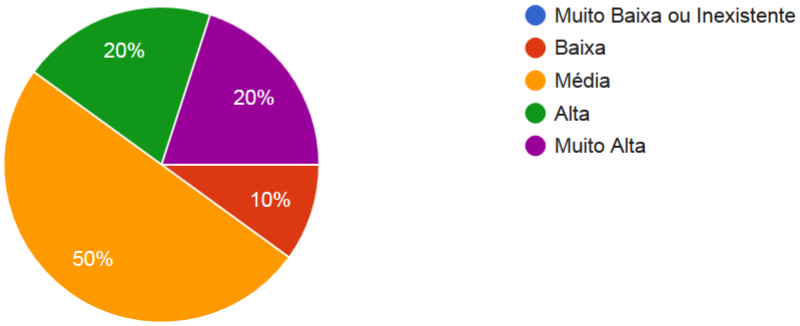
(10 respostas)



Técnico de TI - Capacitação

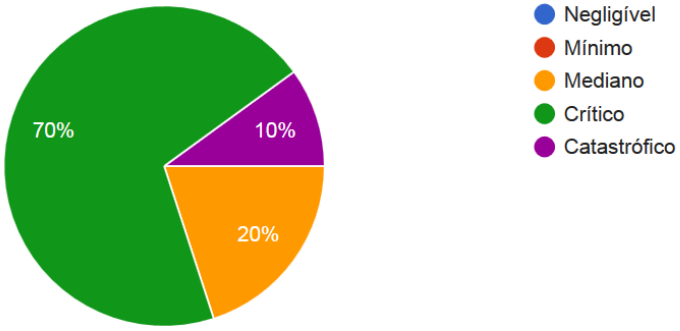
Qual a probabilidade do técnico não possuir capacitação básica para lidar com alguma ou várias das tecnologias necessárias para o funcionamento saudável da tecnologia da informação do campus?

(10 respostas)



Qual a impacto do técnico não possuir capacitação básica para lidar com alguma ou várias das tecnologias necessárias para o funcionamento saudável da tecnologia da informação do campus?

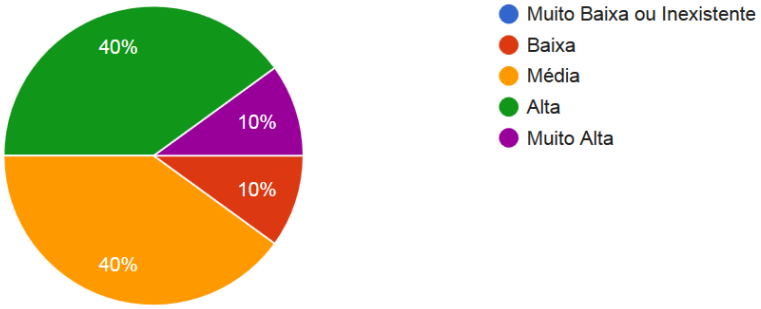
(10 respostas)



Equipe de TI - Atribuições

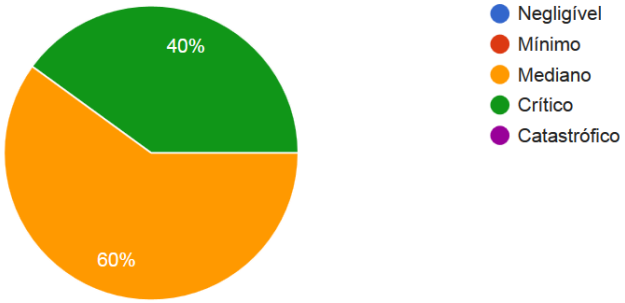
Qual a probabilidade da falta de clareza nas atribuições do cargo de técnico de tecnologia da informação afetar os serviços de TI que se espera do campus?

(10 respostas)



Qual o impacto da falta de clareza nas atribuições do cargo de técnico de tecnologia da informação afetar os serviços de TI que se espera do campus?

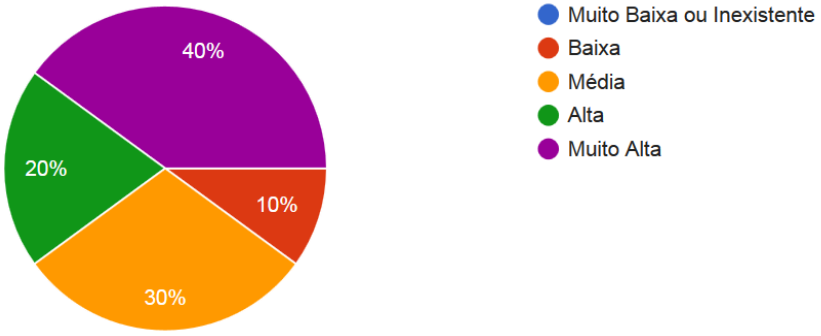
(10 respostas)



Equipe de TI - Quantitativo de Pessoal

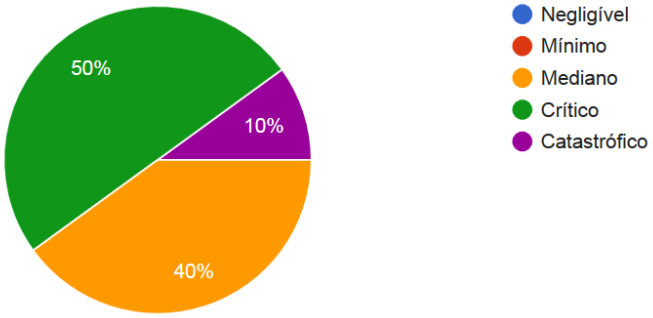
Qual a probabilidade da equipe de TI do campus não ser suficiente para atender as demandas?

(10 respostas)



Qual o impacto da equipe de TI do campus não ser suficiente para atender as demandas?

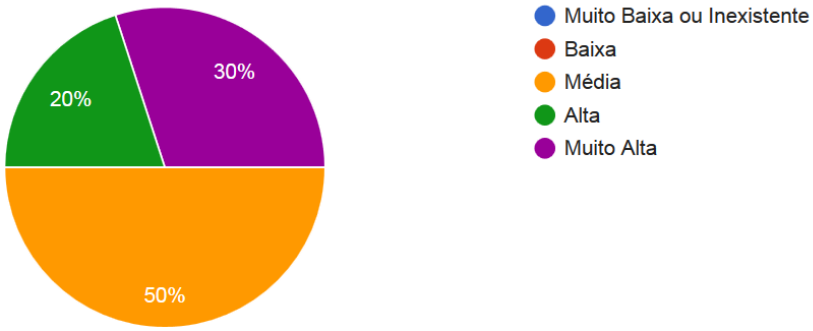
(10 respostas)



Equipe de TI

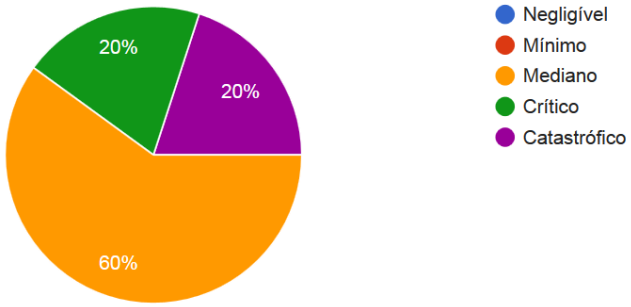
Qual a probabilidade da falta de uma Coordenação de Tecnologia da Informação afetar a qualidade dos serviços prestados pela equipe de TI?

(10 respostas)



Qual o impacto na qualidade dos serviços prestados pela equipe de TI com a falta de uma Coordenação de Tecnologia da Informação?

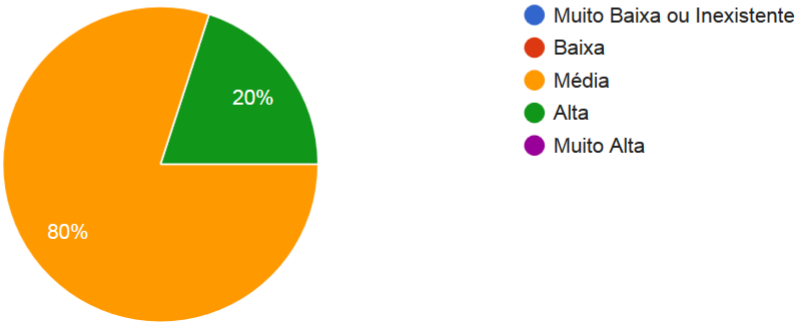
(10 respostas)



Políticas de Segurança da Informação

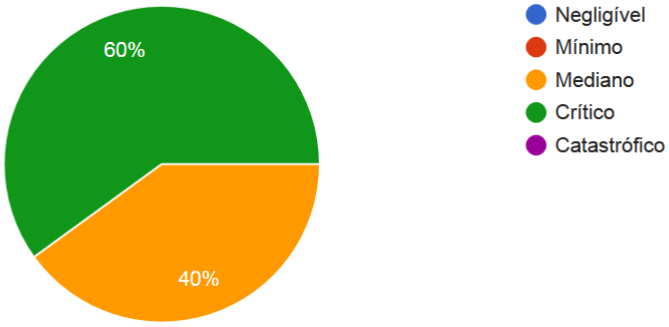
Qual a probabilidade da falta de uma política de segurança da informação atualizada afetar a qualidade dos serviços prestados pela equipe de TI ?

(10 respostas)



Qual a impacto da falta de uma política de segurança da informação atualizada afetar a qualidade dos serviços prestados pela equipe de TI?

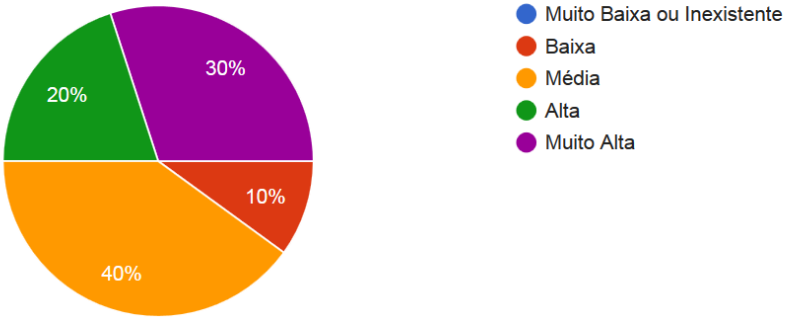
(10 respostas)



Relação Reitoria - Campus: Decisões e Políticas

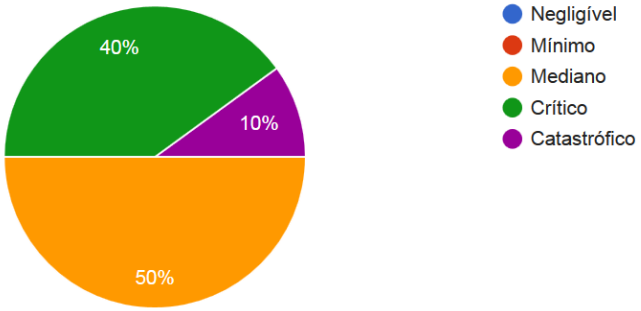
Qual a probabilidade que políticas e decisões de tecnologia da informação que afetam os campi sejam tomadas sem que o campus seja devidamente consultado?

(10 respostas)



Qual a impacto de políticas e decisões de tecnologia da informação tomadas sem que os campi seja devidamente consultado?

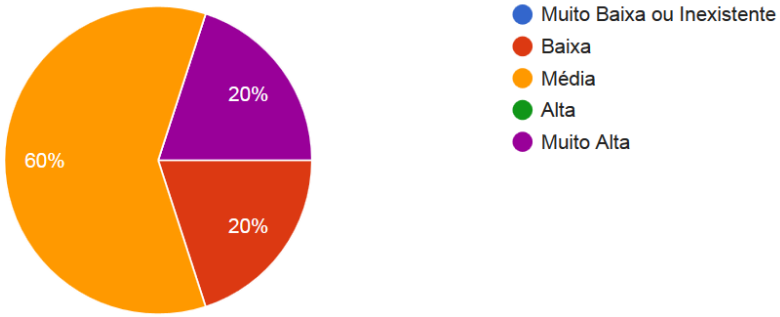
(10 respostas)



Relação Reitoria - Campus: Aquisições

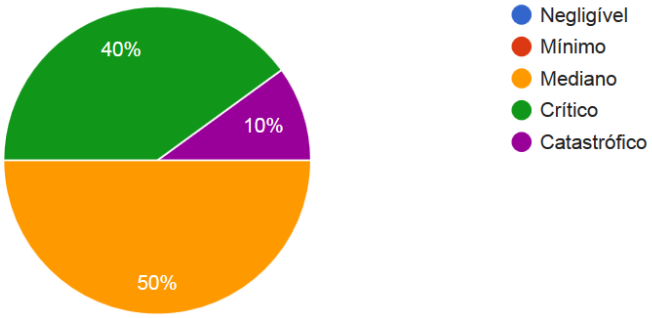
Qual a probabilidade de aquisições de tecnologia da informação destinadas aos campi sejam feitas sem que o campus seja devidamente consultado?

(10 respostas)



Qual o impacto de aquisições de tecnologia da informação destinadas aos campi feitas sem que o campus seja devidamente consultado?

(10 respostas)



Apêndice N

Opinião dos Funcionários - Considerações Referentes ao Questionário Piloto

Considerações - Questionário Piloto - Opinião sobre Serviços de Tecnologia da Informação

Original: Computadores com defeito afetam meu trabalho.
Alterado: Computadores que não funcionam afetam meu trabalho.
Razão: Objetividade.

Original: O telefone fixo do campus não estar funcionando afeta meu trabalho
Alterado: Não ter telefone fixo disponível para realizar ou receber ligações afeta meu trabalho.
Razão: Objetividade

Original: Falta de uma política documentada de segurança da informação afeta meu trabalho.
Observação: Não ficou claro para os usuários o quanto uma política de segurança da informação interferiria em seu trabalho. Relataram saber ser importante por se tratar de uma política para o órgão que melhoraria a tecnologia, assim como existem políticas para outras áreas, entretanto informaram não saber exatamente o que isso afetaria.

Usuários relataram nunca terem sido perguntados sobre nada de tecnologia da informação, incluindo entrevistas ou consultas sobre mudanças.

Usuários relataram a importância de serviços específicos e que sem eles não poderiam ser desempenhadas determinadas atividades ou nenhuma atividade.

Apêndice O

Opinião dos Funcionários - Questionário

Opinião sobre Serviços de Tecnologia da Informação

Esta é uma pesquisa sobre políticas e recursos de tecnologia da informação disponíveis/aplicadas no campus.

*Obrigatório

Qual seu campus? *

- ◯ Brasília
- ◯ Gama
- ◯ Planaltina
- ◯ Samambaia
- ◯ Taguatinga

Seu cargo faz parte dos *

- ◯ Técnicos Administrativos em Educação (Auxiliar Administrativo, TAE, Psicólogo, Assistente Social, etc.)
- ◯ Professores (áreas diversas)
- ◯ Outro: _____

Você faz parte da coordenação ou direção como *

- ◯ Diretor ou Coordenador
- ◯ Membro da Direção ou Coordenação

PRÓXIMA

Direção ou Coordenação

Marque sua função. As coordenações e direções exclusivas de alguns campus estão no final.

Seu cargo de direção ou função gratificada é *

- ( ) Diretor(a) Geral (DG)
- ( ) Diretor(a) de Administração e Planejamento (DRAP)
- ( ) Diretor(a) de Ensino, Pesquisa e Extensão (DREP)
- ( ) Coordenador(a) de Manutenção e Serviços Gerais (CDMS)
- ( ) Coordenador(a) de Gestão de Pessoas (CDGP)
- ( ) Coordenador(a) de Aquisições e Contratos (CDAC)
- ( ) Coordenador(a) de Almoxarifado e Patrimônio (CDAP)
- ( ) Coordenador(a) de Planejamento e Orçamento (CDPO)
- ( ) Coordenador(a) Geral de Ensino (CGEN)
- ( ) Coordenador(a) de Registro Acadêmico (CDRA)
- ( ) Coordenador(a) de Biblioteca (CDBI)
- ( ) Coordenador(a) de Pesquisa e Extensão (CDPE)
- ( ) Coordenador(a) de Assistência Estudantil (CDAE)
- ( ) Coordenador(a) Pedagógico (CDPD)
- ( ) Coordenador(a) de Estágio (CDES)
- ( ) Coordenador(a) de Curso
- ( ) Chefia de Gabinete (Campus Brasília)
- ( ) Diretor(a) de Produção - DRPR (Campus Planaltina)
- ( ) Coordenador(a) de Produção Animal - CDPA (Campus Planaltina)
- ( ) Coordenador(a) de Produção Vegetal - CDPV (Campus Planaltina)
- ( ) Coordenador(a) de Residência Estudantil - CDRE (Campus Planaltina)

VOLTAR PRÓXIMA

Membro de Direção ou Coordenação

Coloque a direção ou coordenação na qual você desempenha suas atividades. As coordenações e direções exclusivas de alguns campi estão no final. Se você for docente e não estiver ligado diretamente a atividades em coordenações, marque professor.

Você faz parte de qual Direção ou Coordenação? *

- ○ Direção Geral (DGGA)
- ○ Direção de Administração e Planejamento (DRAP)
- ○ Direção de Ensino, Pesquisa e Extensão (DREP)
- ○ Coordenação de Manutenção e Serviços Gerais (CDMS)
- ○ Coordenação de Gestão de Pessoas (CDGP)
- ○ Coordenação de Aquisições e Contratos (CDAC)
- ○ Coordenaçãode Almoxarifado e Patrimônio (CDAP)
- ○ Coordenação de Planejamento e Orçamento (CDPO)
- ○ Coordenação Geral de Ensino (CGEN)
- ○ Coordenação de Registro Acadêmico (CDRA)
- ○ Coordenação de Biblioteca (CDBI)
- ○ Coordenação de Pesquisa e Extensão (CDPE)
- ○ Coordenação de Assistência Estudantil (CDAE)
- ○ Coordenação Pedagógica (CDPD)
- ○ Coordenação de Estágio (CDES)
- ○ Coordenação de Curso
- ○ Chefia de Gabinete (Campus Brasília)
- ○ Diretoria de Produção - DRPR (Campus Planaltina)
- ○ Coordenação de Produção Animal - CDPA (Campus Planaltina)
- ○ Coordenação de Produção Vegetal - CDPV (Campus Planaltina)
- ○ Coordenação de Residência Estudantil - CDRE (Campus Planaltina)
- ○ Professor

VOLTAR PRÓXIMA

Opinião sobre os Serviços de Tecnologia da Informação

Com relação a cada afirmação sobre os diversos recursos de tecnologia da informação usados para realizar seu trabalho, selecione a opção que mais lhe parecer adequada.

Não ter internet disponível afeta meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Não poder imprimir arquivos afeta meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Não ter compartilhamento de arquivos em rede (pastas em rede, pastas corporativas) disponível afeta meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Perder arquivos compartilhados em rede (pastas em rede, pastas corporativas) afeta meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Não ter suporte da área de tecnologia da informação para resolver problemas afeta meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Picos de energia que podem desligar meu computador e outros equipamentos afeta meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Ter arquivos corrompidos porque foram feitos no Microsoft Office mas editados no Libre Office e vice-versa afeta meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Computadores que não funcionam afetam meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Continuar usando computadores muito antigos afeta meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Continuar usando sistemas operacionais antigos (como o Windows XP) afeta meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Ter computadores que utilizo depredados afeta meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

As tomadas de decisões de tecnologia da informação sem prévia consulta ao campus afetam meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Falta de uma política documentada de segurança da informação afeta meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Computadores com vírus afetam meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Computadores com o Windows sem atualizações afetam meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Ter que usar versões antigas de programas como Chrome e Java afeta meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Terceiros terem acesso à(s) minhas pastas compartilhadas em rede afeta meu trabalho. *

- ◯ Discordo fortemente
- ◯ Discordo
- ◯ Nem discordo nem concordo
- ◯ Concordo
- ◯ Concordo fortemente

Ausência de serviços

Marque a opção que mais reflete como a falta de um recurso de tecnologia da informação afeta seu trabalho.

Sem internet *

- ◯ Não consigo desempenhar nenhuma atividade
- ◯ Consigo desempenhar poucas atividades
- ◯ Consigo desempenhar razoavelmente minhas atividades
- ◯ Consigo desempenhar muitas atividades
- ◯ Consigo desempenhar todas as atividades

Sem pastas compartilhadas em rede *

- ◯ Não consigo desempenhar nenhuma atividade
- ◯ Consigo desempenhar poucas atividades
- ◯ Consigo desempenhar razoavelmente minhas atividades
- ◯ Consigo desempenhar muitas atividades
- ◯ Consigo desempenhar todas as atividades
- ◯ Não uso pastas compartilhadas em rede

Sem telefonia fixa *

- ◯ Não consigo desempenhar nenhuma atividade
- ◯ Consigo desempenhar poucas atividades
- ◯ Consigo desempenhar razoavelmente minhas atividades
- ◯ Consigo desempenhar muitas atividades
- ◯ Consigo desempenhar todas as atividades

Sem impressão *

- ◯ Não consigo desempenhar nenhuma atividade
- ◯ Consigo desempenhar poucas atividades
- ◯ Consigo desempenhar razoavelmente minhas atividades
- ◯ Consigo desempenhar muitas atividades
- ◯ Consigo desempenhar todas as atividades

Sem suporte de tecnologia da informação *

- ◯ Não consigo desempenhar nenhuma atividade
- ◯ Consigo desempenhar poucas atividades
- ◯ Consigo desempenhar razoavelmente minhas atividades
- ◯ Consigo desempenhar muitas atividades
- ◯ Consigo desempenhar todas as atividades

Se houverem picos de energia *

- ◯ Não consigo desempenhar nenhuma atividade
- ◯ Consigo desempenhar poucas atividades
- ◯ Consigo desempenhar razoavelmente minhas atividades
- ◯ Consigo desempenhar muitas atividades
- ◯ Consigo desempenhar todas as atividades

Sem computador para usar *

- ◯ Não consigo desempenhar nenhuma atividade
- ◯ Consigo desempenhar poucas atividades
- ◯ Consigo desempenhar razoavelmente minhas atividades
- ◯ Consigo desempenhar muitas atividades
- ◯ Consigo desempenhar todas as atividades

Pesquisas e Comentários

Você já participou de alguma outra pesquisa sobre a tecnologia da informação do IFB? *

- ◯ Sim - Realizada pela Reitoria
- ◯ Sim - Realizada pelo Campus
- ◯ Sim - Outras pesquisas
- ◯ Não

Gostaria de deixar algum comentário?

Sua resposta

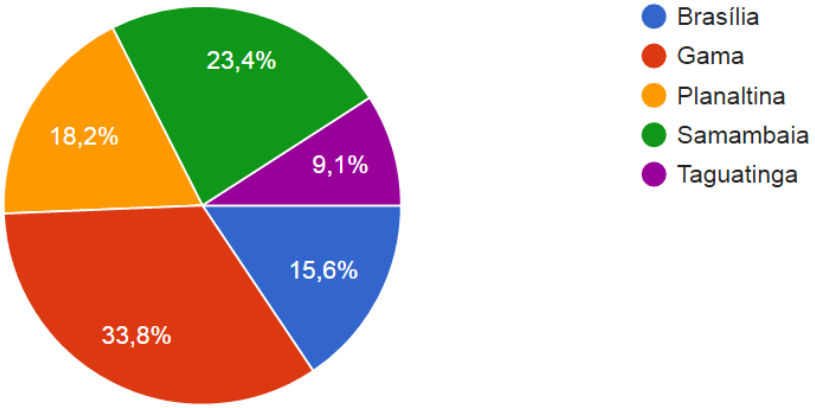
VOLTAR ENVIAR

Apêndice P

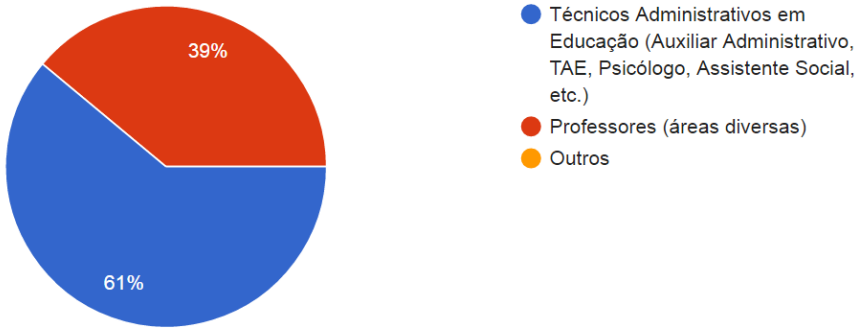
Opinião dos Funcionários - Questionário - Respostas Sem Peso

77 Respostas

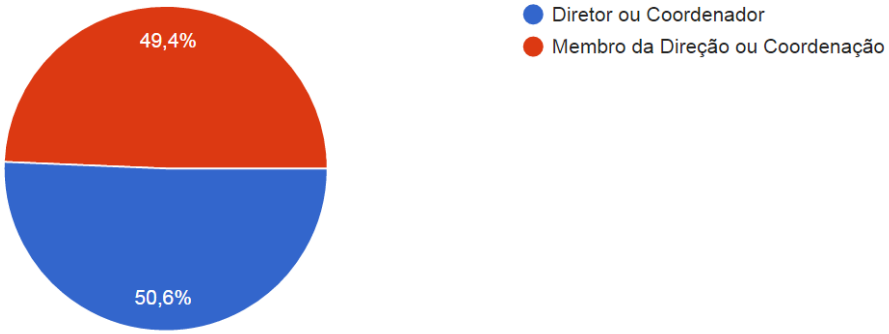
Qual seu campus? (77 respostas)



Seu cargo faz parte dos (77 respostas)



Você faz parte da coordenação ou direção como (77 respostas)



Não ter internet disponível afeta meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília				4	8	12
Gama		1		4	21	26
Planaltina		1		2	11	14
Samambaia	1		2	3	12	18
Taguatinga	1				6	7
TOTAL	2	2	2	13	58	77
PORCENTAGEM	2,60%	2,60%	2,60%	16,88%	75,32%	100,00%

Não poder imprimir arquivos afeta meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília				4	8	12
Gama				11	15	26
Planaltina		1	1	2	10	14
Samambaia		1	1	5	11	18
Taguatinga		1			6	7
TOTAL	0	3	2	22	50	77
PORCENTAGEM	0,00%	3,90%	2,60%	28,57%	64,94%	100,00%

Não ter compartilhamento de arquivos em rede (pastas em rede, pastas corporativas) disponível afeta meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília			4	2	6	12
Gama			1	10	15	26
Planaltina		1	2	3	8	14
Samambaia		2	3	7	6	18
Taguatinga		1		2	4	7
TOTAL	0	4	10	24	39	77
PORCENTAGEM	0,00%	5,19%	12,99%	31,17%	50,65%	100,00%

DF - Discordo Fortemente **D -** Discordo
ND - Nem Discordo nem Concordo
C - Concordo **CF**- Concordo Fortemente

Perder arquivos compartilhados em rede (pastas em rede, pastas corporativas) afeta meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília		1	2	3	6	12
Gama			1	4	21	26
Planaltina		1	1	3	9	14
Samambaia		3	2	3	10	18
Taguatinga			1	2	4	7
TOTAL	0	5	7	15	50	77
PORCENTAGEM	0,00%	6,49%	9,09%	19,48%	64,94%	100,00%

Não ter telefone fixo disponível para realizar ou receber ligações afeta meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília	1		2	5	4	12
Gama	2	3	3	11	7	26
Planaltina	1	1	1	5	6	14
Samambaia	1	2	6	5	4	18
Taguatinga	1	1	1	4		7
TOTAL	6	7	13	30	21	77
PORCENTAGEM	7,79%	9,09%	16,88%	38,96%	27,27%	100,00%

Não ter suporte da área de tecnologia da informação para resolver problemas afeta meu trabalho.						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília				2	10	12
Gama	1			5	20	26
Planaltina		1	1	3	9	14
Samambaia			1	3	14	18
Taguatinga		2		2	3	7
TOTAL	1	3	2	15	56	77
PORCENTAGEM	1,30%	3,90%	2,60%	19,48%	72,73%	100,00%

DF - Discordo Fortemente **D -** Discordo
ND - Nem Discordo nem Concordo
C - Concordo **CF**- Concordo Fortemente

Picos de energia que podem desligar meu computador e outros equipamentos afeta meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília			1	5	6	12
Gama				10	16	26
Planaltina			1	5	8	14
Samambaia			1	10	7	18
Taguatinga				5	2	7
TOTAL	0	0	3	35	39	77
PORCENTAGEM	0,00%	0,00%	3,90%	45,45%	50,65%	100,00%

Ter arquivos corrompidos porque foram feitos no Microsoft Office mas editados no Libre Office e vice-versa afeta meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília	1			4	7	12
Gama	1		1	12	12	26
Planaltina	1		1	4	8	14
Samambaia			2	9	7	18
Taguatinga				2	5	7
TOTAL	3	0	4	31	39	77
PORCENTAGEM	3,90%	0,00%	5,19%	40,26%	50,65%	100,00%

Computadores que não funcionam afetam meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília				3	9	12
Gama			1	4	21	26
Planaltina			2	2	10	14
Samambaia				6	12	18
Taguatinga				1	6	7
TOTAL	0	0	3	16	58	77
PORCENTAGEM	0,00%	0,00%	3,90%	20,78%	75,32%	100,00%

DF - Discordo Fortemente **D -** Discordo
ND - Nem Discordo nem Concordo
C - Concordo **CF**- Concordo Fortemente

Continuar usando computadores muito antigos afeta meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília	1		1	7	3	12
Gama		1	3	8	14	26
Planaltina			1	6	7	14
Samambaia			5	6	7	18
Taguatinga				1	6	7
TOTAL	1	1	10	28	37	77
PORCENTAGEM	1,30%	1,30%	12,99%	36,36%	48,05%	100,00%

Continuar usando sistemas operacionais antigos (como o Windows XP) afeta meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília	1	1	2	7	1	12
Gama	1	1	6	10	8	26
Planaltina			4	7	3	14
Samambaia	1	1	5	7	4	18
Taguatinga			1	4	2	7
TOTAL	3	3	18	35	18	77
PORCENTAGEM	3,90%	3,90%	23,38%	45,45%	23,38%	100,00%

Ter computadores que utilizo depredados afeta meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília			1	3	8	12
Gama	1			7	18	26
Planaltina		1	1	2	10	14
Samambaia			1	9	8	18
Taguatinga				4	3	7
TOTAL	1	1	3	25	47	77
PORCENTAGEM	1,30%	1,30%	3,90%	32,47%	61,04%	100,00%

DF - Discordo Fortemente **D -** Discordo
ND - Nem Discordo nem Concordo
C - Concordo **CF**- Concordo Fortemente

As tomadas de decisões de tecnologia da informação sem prévia consulta ao campus afetam meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília			3	5	4	12
Gama			9	8	9	26
Planaltina		1	2	4	7	14
Samambaia			2	7	9	18
Taguatinga			1	4	2	7
TOTAL	0	1	17	28	31	77
PORCENTAGEM	0,00%	1,30%	22,08%	36,36%	40,26%	100,00%

Falta de uma política documentada de segurança da informação afeta meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília			2	7	3	12
Gama		1	6	11	8	26
Planaltina			3	6	5	14
Samambaia		1	3	8	6	18
Taguatinga			2	2	3	7
TOTAL	0	2	16	34	25	77
PORCENTAGEM	0,00%	2,60%	20,78%	44,16%	32,47%	100,00%

Computadores com vírus afetam meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília				4	8	12
Gama				5	21	26
Planaltina			1	2	11	14
Samambaia				5	13	18
Taguatinga			1	4	2	7
TOTAL	0	0	2	20	55	77
PORCENTAGEM	0,00%	0,00%	2,60%	25,97%	71,43%	100,00%

DF - Discordo Fortemente **D -** Discordo
ND - Nem Discordo nem Concordo
C - Concordo **CF**- Concordo Fortemente

Computadores com o Windows sem atualizações afetam meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília	1		2	6	3	12
Gama	1		3	9	13	26
Planaltina		1	4	6	3	14
Samambaia		3	4	6	5	18
Taguatinga	1			3	3	7
TOTAL	3	4	13	30	27	77
PORCENTAGEM	3,90%	5,19%	16,88%	38,96%	35,06%	100,00%

Ter que usar versões antigas de programas como Chrome e Java afeta meu trabalho						
	Sem Peso					
	DF	**D**	**ND**	**C**	**CF**	**TOTAL**
Brasília	1	1	1	5	4	12
Gama		2	2	11	11	26
Planaltina		1	4	6	3	14
Samambaia	1		3	6	8	18
Taguatinga	2			4	1	7
TOTAL	4	4	10	32	27	77
PORCENTAGEM	5,19%	5,19%	12,99%	41,56%	35,06%	100,00%

DF - Discordo Fortemente **D -** Discordo
ND - Nem Discordo nem Concordo
C - Concordo **CF**- Concordo Fortemente

Sem internet						
	Sem Peso					
	Não consigo desempe-nhar nenhu-ma ativida-de	**Consigo desempe-nhar poucas ativida-des**	**Consigo desempe-nhar razoavel-mente minhas ativida-des**	**Consigo desempe-nhar muitas ativida-des**	**Consigo desempe-nhar todas as atividades**	**TOTAL**
Brasília	3	6	1	1	1	12
Gama	7	11	6	2		26
Planaltina	2	9	1	2		14
Samambaia	1	9	6	2		18
Taguatinga		5	1		1	7
TOTAL	13	40	15	7	2	77
PORCENTAGEM	16,88%	51,95%	19,48%	9,09%	2,60%	100,00%

Sem pastas compartilhadas em rede							
	Sem Peso						
	Não consigo desempe-nhar nenhu-ma ativida-de	**Consigo desempe-nhar poucas ativida-des**	**Consigo desempe-nhar razoavel-mente minhas ativida-des**	**Consigo desempe-nhar muitas ativida-des**	**Consigo desempe-nhar todas as atividades**	**Não uso pastas compartilhadas em rede**	**Total**
Brasília	1	1	3	3	1	3	12
Gama	5	7	11	2	1		26
Planaltina	1	7	2	3		1	14
Samambaia		6	3	4	2	3	18
Taguatinga		2	1	2	2		7
TOTAL	7	23	20	14	6	7	77
PORCENTAGEM	9,09%	29,87%	25,97%	18,18%	7,79%	9,09%	100,00%

Sem telefonia fixa						
	Sem Peso					
	Não consigo desempenhar nenhuma atividade	**Consigo desempenhar poucas atividades**	**Consigo desempenhar razoavelmente minhas atividades**	**Consigo desempenhar muitas atividades**	**Consigo desempenhar todas as atividades**	**TOTAL**
Brasília	1	2	2	6	1	12
Gama		7	12	3	4	26
Planaltina		5	5	3	1	14
Samambaia		3	4	7	4	18
Taguatinga			1	3	3	7
TOTAL	1	17	24	22	13	77
PORCENTAGEM	1,30%	22,08%	31,17%	28,57%	16,88%	100,00%

Sem impressão						
	Sem Peso					
	Não consigo desempe-nhar nenhu-ma ativida-de	**Consigo desempe-nhar poucas ativida-des**	**Consigo desempe-nhar razoavel-mente minhas ativida-des**	**Consigo desempe-nhar muitas ativida-des**	**Consigo desempe-nhar todas as atividades**	**TOTAL**
Brasília	2	5	5			12
Gama	4	12	9	1		26
Planaltina		10	3	1		14
Samambaia	1	8	4	5		18
Taguatinga		5	1	1		7
TOTAL	7	40	22	8	0	77
PORCENTAGEM	9,09%	51,95%	28,57%	10,39%	0,00%	100,00%

Sem suporte de tecnologia da informação						
	Sem Peso					
	Não consigo desempe-nhar nenhu-ma ativida-de	**Consigo desempe-nhar poucas ativida-des**	**Consigo desempe-nhar razoavel-mente minhas ativida-des**	**Consigo desempe-nhar muitas ativida-des**	**Consigo desempe-nhar todas as atividades**	**TOTAL**
Brasília	3	5	4			12
Gama	5	11	6	4		26
Planaltina	3	7	3	1		14
Samambaia	2	6	6	2	2	18
Taguatinga		1	5	1		7
TOTAL	13	30	24	8	2	77
PORCENTAGEM	16,88%	38,96%	31,17%	10,39%	2,60%	100,00%

Se houverem picos de energia						
	Sem Peso					
	Não consigo desempe-nhar nenhu-ma ativida-de	**Consigo desempe-nhar poucas ativida-des**	**Consigo desempe-nhar razoavel-mente minhas ativida-des**	**Consigo desempe-nhar muitas ativida-des**	**Consigo desempe-nhar todas as atividades**	**TOTAL**
Brasília	2	2	6	2		12
Gama	9	9	8			26
Planaltina	3	8	3			14
Samambaia	1	9	5	3		18
Taguatinga	2		4	1		7
TOTAL	17	28	26	6	0	77
PORCENTAGEM	22,08%	36,36%	33,77%	7,79%	0,00%	100,00%

Sem computador para usar						
	Sem Peso					
	Não consigo desempenhar nenhuma atividade	Consigo desempenhar poucas atividades	Consigo desempenhar razoavelmente minhas atividades	Consigo desempenhar muitas atividades	Consigo desempenhar todas as atividades	TOTAL
Brasília	7	2	3			12
Gama	15	11				26
Planaltina	8	5	1			14
Samambaia	4	10	2	2		18
Taguatinga	5	2				7
TOTAL	39	30	6	2	0	77
PORCENTAGEM	50,65%	38,96%	7,79%	2,60%	0,00%	100,00%