LUIZ FERNANDO FERREIRA DE MEDEIROS LIMA

PERCEPÇÃO DE SEGURANÇA EM SISTEMAS DE INFORMAÇÃO E SUA RELAÇÃO COM A QUALIDADE PERCEBIDA DE SERVIÇOS, PERFIL DE LIDERANÇA E PERFIL DOS SEGUIDORES, ENTRE AS DIRETORIAS DO INMETRO

Dissertação apresentada ao Curso de Mestrado Profissional em Sistema de Gestão da Universidade Federal Fluminense, como requisito parcial para a obtenção do Grau de Mestre em Sistemas de Gestão. Área de atuação: Gestão da Qualidade. Linha de Pesquisa: Sistema de Gestão pela Qualidade Total.

Orientador: Prof. Dr. HEITOR LUIZ MURAT DE MEIRELLES QUINTELLA

NITERÓI
2006

LUIZ FERNANDO FERREIRA DE MEDEIROS LIMA

PERCEPÇÃO DE SEGURANÇA EM SISTEMAS DE INFORMAÇÃO E SUA RELAÇÃO COM A QUALIDADE PERCEBIDA DE SERVIÇOS, PERFIL DE LIDERANÇA E PERFIL DOS SEGUIDORES, ENTRE AS DIRETORIAS DO INMETRO

Dissertação apresentada ao Curso de Mestrado Profissional em Sistema de Gestão da Universidade Federal Fluminense, como requisito parcial para a obtenção do Grau de Mestre em Sistemas de Gestão. Área de atuação: Gestão da Qualidade. Linha de Pesquisa: Sistema de Gestão pela Qualidade Total.

Aprovado em 28 de março de 2006.

BANCA EXAMINADORA

_____

Prof. Heitor Luiz Murat de Meirelles Quintella, D. Sc.
Universidade Federal Fluminense - UFF

_____

Prof. Sérgio José Mecena da Silva Filho, D. Sc.
Universidade Federal Fluminense - UFF

_____

Prof. Ricardo Miyashita, D. Sc.
Universidade do Estado do Rio de Janeiro

Dedico este trabalho

Em primeiro lugar, a Deus e todos aqueles seres que amparam a pesquisa de uma dimensão não física, contribuindo para o desenvolvimento do ser humano.

Às minhas filhas, Marina, Luyza e Beatriz, para que tenham um exemplo de luta e perseverança.

À minha mulher Ana Lucia, pelo amor, apoio, paciência e compreensão pelos problemas causados por este trabalho.

Ao meu pai Luiz, ″in memorian″ e minha mãe Dayse, pelo amor, apoio, educação moral e ética, e por sempre incentivarem o estudo continuado.

À minha avó Odette, meu irmão Fernando Luiz, minha tia Eulice, e a toda minha família, pelo incentivo e torcida de sempre.

À minha sogra Izabel e ao meu cunhado Márcio, pela ajuda de sempre.

Aos meus amigos, colegas e parceiros de trabalho, na pessoa, “in memorian”, do amigo Jorge Caetano, pela enorme ajuda e tolerância com as minhas dificuldades durante estes 24 meses.

Ao meu “irmão” mais velho, Fernando Malta, pois sem seu apoio e ajuda, o caminho seria mais difícil.

AGRADECIMENTOS

Ao INMETRO que me proporcionou esta oportunidade de ingressar em um curso de tamanha importância para meu desenvolvimento humano e profissional.

Ao meu orientador, Prof. Heitor Luiz Murat de Meirelles Quintella, D.Sc; pela amizade, ética, paciência, compreensão, e principalmente "motivação" nos momentos de dificuldades a serem superados.

Aos amigos do INMETRO, em especial, ao meu antigo diretor, Ricardo de Oliveira, ao chefe de informática, Nielsen Oliveira de Moraes, ao chefe substituto da informática, Samuel Mello e ao analista Gil F. do Almo, que permitiram que esse sonho se tornasse realidade.

Aos amigos do Projeto Fatores Humanos e Tecnológicos da Competitividade da UFF, que me apoiaram do início ao fim dessa jornada.

Aos meus amigos de turma, pelo incentivo e afeto.

A todos que contribuíram para a realização deste estudo.

RESUMO

Hoje em dia, a informação é talvez, o mais valioso ativo das empresas, principalmente num mundo globalizado e altamente competitivo. Isto aumenta a responsabilidade e a obrigação de uma instituição federal de se manter em conformidade com as normas de segurança da informação, protegendo seus conhecimentos, sua história, suas informações, estejam elas em papel ou informatizadas; principalmente tendo a organização, a importância e a credibilidade do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (INMETRO). O objetivo dessa pesquisa foi produzir dados e subsídios para resolver ou pelo menos, melhorar a situação da instituição, colocando-a em conformidade com as melhores práticas de segurança da informação, aumentando a qualidade dos sistemas de informação, melhorando as práticas de liderança e o perfil dos seguidores, lembrando que este trabalho foi focado e limitado ao fator humano e na sua participação enquanto usuário dos sistemas de informação. Essa dissertação foi um estudo de caso, onde se procurou estudar os problemas de incidentes de segurança da informação dentro do Inmetro, no âmbito de suas diretorias e a relação desses índices com a percepção da qualidade dos serviços dos sistemas de informação, com o perfil de liderança e com o perfil dos seguidores. Para esse estudo foram utilizados como referenciais teóricos, a Norma ABNT NBR ISO/IEC 17799, para a gestão da segurança da informação; os modelos conceituais de Parasuraman, Zeithaml, e Berry, para analisar a qualidade percebida dos serviços de informática (*Servqual*); os conceitos de Kouzes e Posner, para o perfil de liderança; e os de Kelley, para o perfil dos seguidores. A metodologia da pesquisa foi baseada no método hipotético-dedutivo de Popper. Após a testagem das hipóteses chegou-se a conclusão de que os resultados foram insuficientes para comprovar uma relação significativa entre os índices: de segurança da informação, de percepção de qualidade, de percepção de liderança e do perfil de seguidores. Recomenda-se, para novos estudos sobre o tema, um maior cuidado com as amostras, com o referencial teórico e os instrumentos da pesquisa, e até, com a metodologia, pois os resultados apresentados pareceram estar distorcidos da realidade, provavelmente por causa da forma como os usuários responderam aos questionários.

Palavras-chave: Segurança da Informação, *Servqual*, Liderança e Seguidores.

ABSTRACT

Nowadays, information maybe, the most valuable assets of the companies, mainly in a global and highly competitive world. This increases the responsibility and the obligation of a federal institution of maintaining in accordance with the safety standards of information security, protecting their knowledge, her history, their information, be them in paper or computerized; mainly has the organization, the importance and the credibility of the National Institute of Metrology, Normalization and Industrial Quality (INMETRO). The objective of that research was to produce data and subsidies to solve or at least, to improve the situation of the institution, putting her in accordance with the best practices of information security, increasing the quality of the systems of information, improving the leadership practices and the followers' profile, reminding that this work was focused and limited to the human factor and in his participation while user of the systems of information. This dissertation was a case study, where it tried to study the problems of incidents of information security inside of Inmetro, in the extent of their departments and the relationship of those indexes with the perception of service quality on systems of information, with the leadership profile and with the followers' profile. For that study were used as theoretical referentials, NBR's guideline ISO/IEC 17799, for the administration of information security management; the conceptual models of Parasuraman, Zeithaml, and Berry, to analyze the noticed quality of the computer science services (Servqual); the concepts of Kouzes and Posner, for the leadership profile; and the one of Kelley, for the followers' profile. The methodology of the research was based on the hypothetical-deductive method of Popper. After the experiment of the hypotheses the conclusion was arrived that the results were insufficient to prove a significant relationship among the indexes: of information security, of quality perception, of leadership perception and of the followers' profile. It is recommended, for new studies on the theme, a larger care with the samples, with the theoretical referential and the instruments of the research, and until, with the methodology, because the presented results seemed to be distorted of the reality, probably because of the form as the users answered to the questionnaires.

Keywords: Security Information, *Servqual*, Leadership and Followership.

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT	Associação brasileira de normas Técnicas
INMETRO	Inst. Nacional de Metrologia, Normalização e Qualidade Industrial
NBR	Norma Brasileira
SERVQUAL	Qualidade de Serviços
T.I.	Tecnologia da Informação
UFF	Universidade Federal Fluminense

SUMÁRIO

1 INTRODUÇÃO

1.1 SUMA DO CAPITULO

Neste capítulo é apresentado um panorama sobre o problema da segurança da informação e sua aplicação nos sistemas de informação dentro de cada diretoria do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (INMETRO). Sua importância, o histórico de vulnerabilidades, a não utilização das normas de segurança, como a Norma da ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT), NBR ISO/IEC 17799, e também o não cumprimento dos decretos do governo. Sua ligação com a percepção de qualidade, percepção de liderança e percepção de seguidores.

1.2 CONTEXTUALIZAÇÃO

Figura 1: Estrutura lógica da dissertação
Fonte: Elaboração própria

1.2.1 INMETRO

1.2.1.1 HISTÓRICO

Durante o primeiro Império, foram feitas diversas tentativas de uniformização das unidades brasileiras de medição. Mas apenas em 26 de junho de 1862, Dom Pedro II promulgava a Lei Imperial nº 1157 e com ela oficializava, em todo o território nacional, o sistema métrico decimal francês. O Brasil foi uma das primeiras nações a adotar o novo sistema, que seria utilizado em todo o mundo.

Com o crescimento industrial do século seguinte, fazia-se necessário criar no país instrumentos mais eficazes de controle que viessem a impulsionar e proteger produtores e consumidores.

Assim, em 1961, foi criado o Instituto Nacional de Pesos e Medidas (INPM), que implantou a Rede Brasileira de Metrologia Legal e Qualidade, os atuais Institutos de Pesos e Medidas (IPEM), e instituiu o Sistema Internacional de Unidades (S.I.) em todo o território nacional.

Logo, verificou-se que isso não era o bastante. Era necessário acompanhar o mundo na sua corrida tecnológica, no aperfeiçoamento, na exatidão e, principalmente, no atendimento às exigências do consumidor. Era necessária a Qualidade.

Em 1973, nascia o Instituto Nacional de Metrologia, Normalização e Qualidade Industrial, o Inmetro, que no âmbito de sua ampla missão institucional, objetiva fortalecer as empresas nacionais, aumentando a sua produtividade por meio da adoção de mecanismos destinados à melhoria da qualidade de produtos e serviços.

1.2.1.2 O QUE É O INMETRO

O Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (INMETRO) - é uma autarquia federal, vinculada ao Ministério do Desenvolvimento, Indústria e Comércio Exterior, que atua como Secretaria Executiva do Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (CONMETRO), colegiado interministerial, que é o

órgão normativo do Sistema Nacional de Metrologia, Normalização e Qualidade Industrial (SINMETRO).

Objetivando integrar uma estrutura sistêmica articulada, o Sinmetro, o Conmetro e o Inmetro foram criados pela Lei 5.966, de 11 de dezembro de 1973, cabendo a este último substituir o então Instituto Nacional de Pesos e Medidas (INPM) e ampliar significativamente o seu raio de atuação a serviço da sociedade brasileira.

No âmbito de sua ampla missão institucional, o Inmetro objetiva fortalecer as empresas nacionais, aumentando sua produtividade por meio da adoção de mecanismos destinados à melhoria da qualidade de produtos e serviços.

Sua missão é promover a qualidade de vida do cidadão e a competitividade da economia através da metrologia e da qualidade.

Dentre as competências e atribuições do Inmetro destacam-se:

- Executar as políticas nacionais de metrologia e da qualidade;
- Verificar a observância das normas técnicas e legais, no que se refere às unidades de medida, métodos de medição, medidas materializadas, instrumentos de medição e produtos pré-medidos;
- Manter e conservar os padrões das unidades de medida, assim como implantar e manter a cadeia de rastreabilidade dos padrões das unidades de medida no País, de forma a torná-las harmônicas internamente e compatíveis no plano internacional, visando, em nível primário, à sua aceitação universal e, em nível secundário, à sua utilização como suporte ao setor produtivo, com vistas à qualidade de bens e serviços;
- Fortalecer a participação do País nas atividades internacionais relacionadas com metrologia e qualidade, além de promover o intercâmbio com entidades e organismos estrangeiros e internacionais;
- Prestar suporte técnico e administrativo ao Conselho Nacional de Metrologia, Normalização e Qualidade Industrial - Conmetro, bem assim aos seus comitês de assessoramento, atuando como sua Secretaria-Executiva;
- Fomentar a utilização da técnica de gestão da qualidade nas empresas brasileiras;
- Planejar e executar as atividades de acreditação (credenciamento) de laboratórios de calibração e de ensaios, de provedores de ensaios de proficiência, de organismos de certificação, de inspeção, de treinamento e de outros, necessários ao desenvolvimento da infra-estrutura de serviços tecnológicos no País; e

Coordenar, no âmbito do Sinmetro, a certificação compulsória e voluntária de produtos, de processos, de serviços e a certificação voluntária de pessoal.

1.2.1.3 ORGANOGRAMA

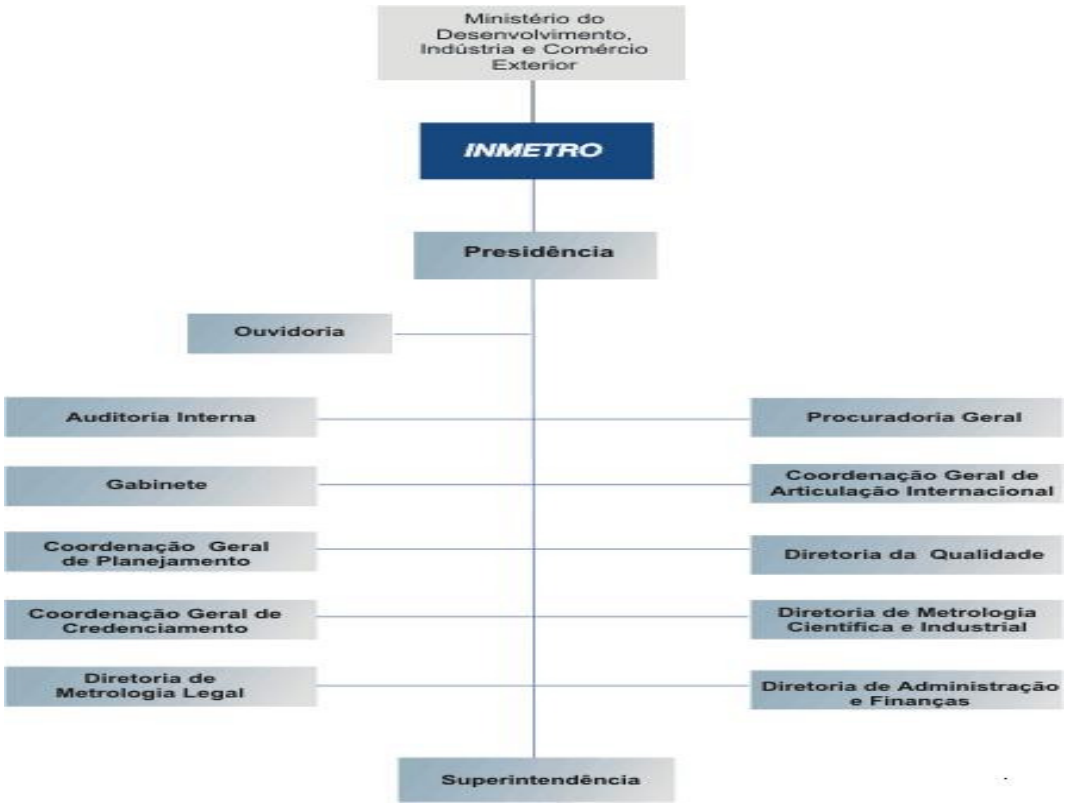


Figura 2 – Organograma do Inmetro
Fonte: O próprio Inmetro

1.2.1.4 AS UNIDADES ORGANIZACIONAIS

O Inmetro é composto das seguintes diretorias:

- **AUDIN** – Auditoria Interna
- **PROGE** – Procuradoria Geral

- **GABIN** – Gabinete
- **CAINT** – Coordenação Geral de Articulação Internacional
- **CPLAN** – Coordenação Geral de Planejamento
- **DQUAL** – Diretoria da Qualidade
- **CGCRE** – Coordenação Geral de Credenciamento
- **DIMCI** – Diretoria de Metrologia Científica e Industrial
- **DIMEL** – Diretoria de Metrologia Legal
- **DIRAF** – Diretoria de Administração e Finanças

1.2.2 NBR ISO/IEC 17799

Norma ABNT para:

- Tecnologia da informação - Código de prática para a gestão da segurança da informação
- Esta Norma é equivalente à ISO/IEC 17799:2000

A ABNT - Associação Brasileira de Normas Técnicas - é o Fórum Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB) e dos Organismos de Normalização Setorial (ABNT/ONS), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).

Esta Norma pode ser considerada como o ponto de partida para o desenvolvimento de recomendações específicas para a organização. Nem todas as recomendações e os controles nesta Norma podem ser aplicados. Além disto, controles adicionais não incluídos nesta Norma podem ser necessários.

1.2.2.1 OBJETIVO

Esta Norma faz recomendações para que a gestão de segurança da informação seja introduzida, implementada ou mantida em organizações. Tem o propósito de prover uma uniformização para o desenvolvimento de normas de segurança organizacional e das práticas efetivas da gestão da segurança da informação.

1.2.2.2 TERMOS E DEFINIÇÕES

Para os efeitos desta Norma, aplicam-se as seguintes definições:

- **segurança da informação**: Preservação da confidencialidade, integridade e disponibilidade da informação.
- **confidencialidade:** Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- **integridade:** Salvaguarda da exatidão e completeza da informação e métodos de processamento;
- **disponibilidade**: Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- **análise de risco:** Análise das ameaças, impactos e vulnerabilidades da informação e das instalações de processamento da informação e da probabilidade de sua ocorrência.
- **gerenciamento de risco:** Processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável.

1.3 ENUNCIADO DO PROBLEMA

Hoje, no início do século XXI, a informação é talvez, o mais valioso ativo das empresas, principalmente num mundo globalizado e altamente competitivo. Percebe-se neste contexto, a existência de duas forças totalmente antagônicas: de um lado encontram-se as empresas e instituições que lutam para manter suas informações intactas e protegidas, e do outro, os maléficos invasores, que, movidos por diversos fatores – lazer, desafios ou um simples protesto – atacam, roubam e fazem adulterações nas informações dessas entidades.

Aqui, dentro da nossa instituição, não seria diferente. O Inmetro possui esse "bem", a informação e, portanto, deve resguardá-la dos invasores, sejam eles internos ou externos. De acordo com a norma brasileira, a NBR ISO/IEC 17799, é função da segurança da informação, proteger os dados da instituição de diversos tipos de ameaças, visando garantir a continuidade dos negócios, minimizar os danos e maximizar o retorno ao mesmo. A informação pode se apresentar de formas diversas. Ela pode estar em papel, escrita ou impressa, em filmes, em fitas de áudio, em conversas, e ainda, em meio eletrônico, digitalizada e armazenada em computadores, utilizadas em sistemas de informação.

Como manter a confidencialidade, a integridade e a disponibilidade dessa informação, é a função da segurança da informação. E para a instituição, são essenciais os controles da proteção de dados, da privacidade de informações pessoais, dos registros organizacionais e dos direitos de propriedade intelectual.

É fato, que a segurança da informação engloba vários itens, como segurança física, segurança de perímetro da rede de computadores, segurança da estação de trabalho local, treinamento e comportamento do usuário, afetando, como um todo, os sistemas de informação.

Os sistemas de informação são colocados à prova todos os dias. Vários tipos de ataques tentam encontrar vulnerabilidades para que possam conseguir seu objetivo, seja esse, por lazer, por desafio ou por protesto. Essas invasões maléficas acontecem por intermédio de vírus de computador, e-mails, acesso indevido e outros motivos.

Conforme uma empresa especializada em segurança da informação, a Módulo Security Solutions S/A, publicou na sua nona pesquisa de segurança da informação (pág. 9), as principais ameaças à segurança da informação são:

Tabela 1 – Tipos e porcentagem de incidentes de segurança

Vírus	66 %
Funcionários insatisfeitos	53 %
Divulgação de senhas	51 %
Acessos indevidos	49 %
Vazamento de informações	47 %
Fraudes, erros e acidentes	41 %
Hackers	39 %
Falhas na segurança física	37 %
Uso de notebooks	31 %
Fraudes em e-mail	29 %

Fonte: Módulo
Observação: o total de citações é superior a 100% devido a múltiplas respostas

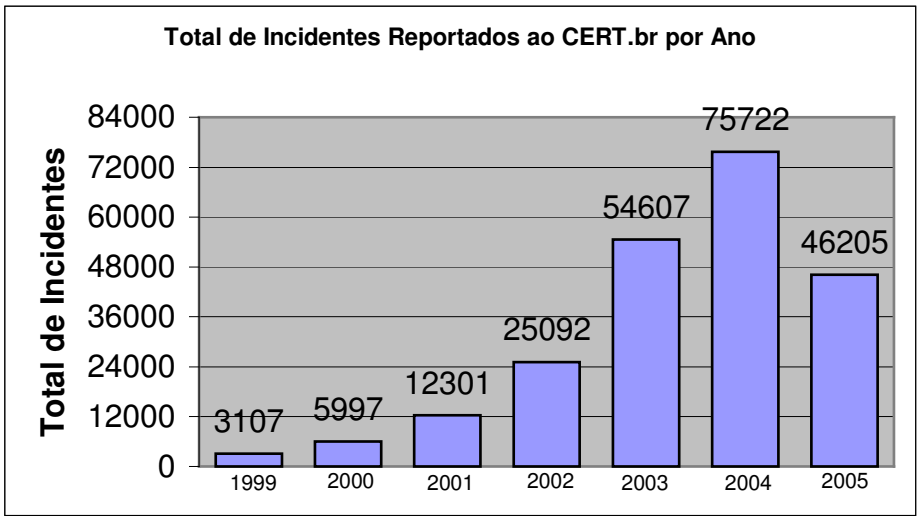
Sabe-se que, hoje em dia, o conhecimento do usuário sobre segurança da informação é essencial para que a instituição esteja protegida contra essas pragas virtuais, que visam de alguma forma, destruir, roubar ou simplesmente ter acesso aos dados da empresa ou de seus funcionários.

O papel do usuário na segurança da informação é estratégico. Ele é o primeiro combatente. A disseminação da cultura de segurança é fundamental para a instituição, e somente um esforço no sentido de convencer o usuário da importância de sua atuação, pode fazer com que essa cultura seja espalhada por toda a organização.

No âmbito do Governo Federal, emergiram estratégias e procedimentos para garantir o sigilo de informações valiosas, através da criação do Centro de Tratamento de Incidentes de Redes (CETIR), que tem por objetivo a atuação como agente de colaboração no monitoramento da segurança para evitar danos maiores no caso de violação da integridade das redes dos órgãos da administração direta e indireta do governo. Nas redes privadas, como é o caso da internet, tem-se o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), onde foi lançada uma cartilha para aumentar o conhecimento dos usuários de redes de computadores e sistemas de informação.

Na figura abaixo, tem-se a estatística dos incidentes de segurança da informação reportados ao CERT.BR, desde sua criação:

Valores acumulados: 1999 a setembro de 2005



* Notificações reportadas até setembro de 2005.

Figura 3 - Estatísticas dos Incidentes Reportados ao CERT.BR
Fonte: CERT.BR

Tem-se então, a visão do aumento do numero de incidentes de segurança da informação, ano após ano. Tornando então, o elo mais fraco da corrente, o usuário, como o principal fator do estudo desta pesquisa, já que ele é a "variável" com a maior dificuldade de controle no âmbito da segurança da informação.

1.4 OBJETIVOS DO ESTUDO

O objetivo deste projeto é estudar a Percepção de Segurança em Sistemas de Informação e sua relação com a Qualidade Percebida (*Servqual*), Perfil de Liderança (*Leadership*) e Perfil dos Seguidores (*Followership*).

Esta pesquisa tem o intuito de começar um estudo de caso (Caso Inmetro), dando início para pesquisas posteriores e mais aprofundadas, sobre o comportamento do elo mais fraco da segurança da informação: o fator humano. Sobre como os índices de incidentes de segurança da informação estão relacionados com os índices da qualidade de serviços dos sistemas de informação, com a percepção de liderança e a percepção dos seguidores.

1.5 JUSTIFICATIVA

Os motivos que tornam esta dissertação justificável são os seguintes:

- **De ordem pessoal**

Como profissional de Ciência e Tecnologia, ligado à área de informação e qualidade, a essência desta dissertação traz informações para meu crescimento profissional e pessoal. Tornando minha visão do conhecimento aumentada, com a metodologia cientifica, me capacitando para difundir e multiplicar este conhecimento para outras pessoas.

- **De ordem profissional**

Este trabalho visa a colaborar com a instituição no sentido de melhorar a proteção de seus dados, suas informações vitais para o negócio. Com esta pesquisa pretendo contribuir de forma a melhorar o conhecimento dos usuários em relação à segurança da informação, aos seus superiores em relação à qualidade do serviço dos sistemas de informação, aperfeiçoando nossas lideranças e seus seguidores.

Este trabalho faz parte também da pesquisa conduzida pela Universidade Federal Fluminense em andamento sobre os Fatores Humanos e Tecnológicos da Competitividade (QUINTELLA, 1997).

- **De ordem acadêmica**

Disponibilizar mais conhecimentos para a área de gestão de segurança da informação, baseados na Norma NBR ISO/IEC 17799, devido a pouca literatura disponível e o reduzido número de trabalhos publicados nessa área em relação a outras mais estudadas e mais antigas.

1.6 HIPÓTESES E/OU QUESTÕES

Esta dissertação apresenta as seguintes hipóteses de trabalho:

- **Hipótese 1**

As diretorias do Inmetro, com "Percepção de Segurança da Informação" mais elevada (menor quantidade de incidentes de segurança), são aquelas que possuem "Percepção de Qualidade" mais alta.

  - **Questão 1**

    Qual é o índice de incidentes de segurança da informação nestas diretorias?

  - **Questão 2**

    Qual é o grau de satisfação dos clientes do Sistema de Informação destas diretorias?

- **Hipótese 2**

As diretorias do Inmetro com maior índice de "Percepção de Segurança da Informação" (menor quantidade de incidentes de segurança), têm seus "Líderes" com mais alto grau de eficácia.

  - **Questão 1**

    Qual é o índice de incidentes de segurança da informação nestas diretorias?

  - **Questão 2**

    Os líderes (diretores/gerentes) destas diretorias do Inmetro têm alto grau de eficácia?

- **Hipótese 3**

As diretorias do Inmetro com maior índice de "Percepção de Segurança da Informação" (menor quantidade de incidentes de segurança), têm um alto grau de "Seguidores Exemplares".

  - **Questão 1**

    Qual é o índice de incidentes de segurança da informação nestas diretorias?

- **Questão 2**

  Qual o grau de “Seguidores Exemplares” destas diretorias?

1.7 REFERENCIAL TEÓRICO OU CONCEITUAL

Para realizar este trabalho foram utilizados os seguintes referenciais teóricos ou conceituais em relação às hipóteses e questões formuladas anteriormente:

- **Hipótese 1**

As diretorias do Inmetro, com “Percepção de Segurança da Informação” mais elevada (menor quantidade de incidentes de segurança), são aquelas que possuem “Percepção de Qualidade” mais alta.

- **Questão 1**

  Qual é o índice de incidentes de segurança da informação nestas diretorias?

  - Norma ABNT **NBR ISO/IEC 17799**
  - Pesquisa de Segurança da **Módulo**
  - Pesquisa de Segurança do **CERT.BR**
  - Conhecimento e Formação do Autor em Análise de Sistemas e Segurança da Informação

- **Questão 2**

  Qual é o grau de satisfação dos clientes do Sistema de Informação destas diretorias?

  - PARASURAMAN, A.; ZEITHAML, Valarie A.; BERRY, Leonard L. **A conceptual Model of Service Quality and Its Implicans for Future Research.**

- **Hipótese 2**

As diretorias do Inmetro com maior índice de "Percepção de Segurança da Informação" (menor quantidade de incidentes de segurança), têm seus "Líderes" com mais alto grau de eficácia.

  - **Questão 1**

    Qual é o índice de incidentes de segurança da informação nestas diretorias?

    - Norma ABNT **NBR ISO/IEC 17799**
    - Pesquisa de Segurança da **Módulo**
    - Pesquisa de Segurança do **CERT.BR**
    - Conhecimento e Formação do Autor em Análise de Sistemas e Segurança da Informação

  - **Questão 2**

    Os líderes (diretores/gerentes) destas diretorias do Inmetro têm alto grau de eficácia?

    - KOUZES, James M.; POSNER, Barry Z. **O Desafio da Liderança.** 3ª ed. Rio de Janeiro: Campus, 2003.

- **Hipótese 3**

As diretorias do Inmetro com maior índice de "Percepção de Segurança da Informação" (menor quantidade de incidentes de segurança), têm um alto grau de "Seguidores Exemplares".

  - **Questão 1**

    Qual é o índice de incidentes de segurança da informação nestas diretorias?

    - Norma ABNT **NBR ISO/IEC 17799**
    - Pesquisa de Segurança da **Módulo**
    - Pesquisa de Segurança do **CERT.BR**
    - Conhecimento e Formação do Autor em Análise de Sistemas e Segurança da Informação

- **Questão 2**

  Qual o grau de "Seguidores Exemplares" destas diretorias?

  - KELLEY, Robert E. **O poder dos seguidores:** como criar os verdadeiros líderes. 1. ed. São Paulo: Siciliano, 1993.

Relacionamento das Hipóteses, Questões-chave, Referencial Teórico e Instrumentos de Medida			
Hipóteses	**Questões-chaves**	**Referencial Teórico**	**Instrumentos de Medida**
Hipótese 1: As diretorias do Inmetro, com "Percepção de Segurança da Informação" mais elevada (menor quantidade de incidentes de segurança), são aquelas que possuem "Percepção de Qualidade" mais alta.	a) Qual é o índice de incidentes de segurança da informação nestas diretorias?	❑ Norma ABNT NBR ISO/IEC 17799 ❑ Pesquisa de Segurança da Módulo ❑ Pesquisa de Segurança do CERT.BR ❑ Conhecimento e Formação do Autor em Análise de Sistemas e Segurança da Informação	Questionário sobre segurança da informação, tipos e quantidades de incidentes de segurança da informação.
	b) Qual é o grau de satisfação dos clientes do Sistema de Informação destas diretorias?	PARASURAMAN, A.; ZEITHAML, Valarie A.; BERRY, Leonard L. **A conceptual Model of Service Quality and Its Implicans for Future Research**	Questionário para medir a qualidade de serviços, Servqual.
Hipótese 2: As diretorias do Inmetro com maior índice de "Percepção de Segurança da Informação" (menor quantidade de incidentes de segurança), têm seus "Líderes" com mais alto grau de eficácia.	a) Qual é o índice de incidentes de segurança da informação nestas diretorias?	❑ Norma ABNT NBR ISO/IEC 17799 ❑ Pesquisa de Segurança da Módulo ❑ Pesquisa de Segurança do CERT.BR ❑ Conhecimento e Formação do Autor em Análise de Sistemas e Segurança da Informação	Questionário sobre segurança da informação, tipos e quantidades de incidentes de segurança da informação.
	b) Os líderes (diretores/gerentes) destas diretorias do Inmetro têm alto grau de eficácia?	KOUZES, James M.; POSNER, Barry Z**. O Desafio da Liderança**	Questionário *LPI* do perfil de liderança.
Hipótese 3: As diretorias do Inmetro, com "Percepção de Segurança da Informação" mais elevada (menor quantidade de incidentes de segurança), têm um alto grau de "Seguidores Exemplares".	a) Qual é o índice de incidentes de segurança da informação nestas diretorias?	❑ Norma ABNT NBR ISO/IEC 17799 ❑ Pesquisa de Segurança da Módulo ❑ Pesquisa de Segurança do CERT.BR ❑ Conhecimento e Formação do Autor em Análise de Sistemas e Segurança da Informação	Questionário sobre segurança da informação, tipos e quantidades de incidentes de segurança da informação.
	b) Qual o grau de "Seguidores Exemplares" destas diretorias?	KELLEY, Robert E. **O poder dos seguidores:** como criar os verdadeiros líderes.	Questionário do perfil de seguidores.

Quadro 1: Relacionamento das Hipóteses, Questões-chave, Referencial Teórico e Instrumentos de Medida.
Fonte: Elaboração própria**.**

1.8 DELIMITAÇÃO DO ESTUDO

Para Lakatos e Marconi (1999, p. 29), “a caracterização do problema define e identifica o assunto estudado, ou seja, um problema muito abrangente torna a pesquisa mais complexa. Quando bem delimitado, simplifica e facilita a maneira de conduzir a investigação“.

Esta pesquisa foi realizada no INMETRO**,** autarquia federal, situada no Estado do Rio de Janeiro. O INMETRO conta com uma força de trabalho de cerca de 1400 (mil e quatrocentas) pessoas, onde aproximadamente, são 800 (oitocentos) funcionários públicos e 600 (seiscentos) contratados através de empresas terceirizadas.

Este trabalho não tem a pretensão de fazer uma pesquisa em profundidade em toda a extensão da Segurança da Informação, limitando-se ao estudo das ocorrências de incidentes de Segurança da Informação em relação aos usuários do Inmetro, correspondentes a suas diretorias. Não serão estudados os problemas de segurança da informação em relação às dependências físicas ou do perímetro da rede. Somente os usuários finais dos Sistemas de Informação e o fornecimento destes pelo Setor de Informática. Confrontando estes dados com os índices de Percepção de Qualidade dos Sistemas de Informação, com o grau de Percepção de Liderança e com o índice de Seguidores Exemplares, dentro do universo dos funcionários do Inmetro com acesso aos sistemas de informação e em relação as suas respectivas diretorias. Este estudo não se aprofunda em percepção de qualidade, no perfil de liderança e também, no perfil dos seguidores, pois não é o escopo da pesquisa, utilizando esses conceitos para realizar a comparação dos índices entre as diretorias do Inmetro e comprovar ou não, a relação entre eles.

Esta dissertação serve como uma pesquisa inicial sobre o tema, preparando terreno para próximas e mais extensas pesquisas sobre o assunto.

1.9 SUMÁRIO CONCLUSIVO DO CAPÍTULO

Este capítulo permitiu entender os objetivos e delimitação da pesquisa onde a partir dos testes das hipóteses levantadas procuram-se as respostas para o problema identificado.

2 REVISÃO DA LITERATURA

2.1 SUMA DO CAPÍTULO

Neste capítulo são apresentados alguns trabalhos feitos sobre segurança da informação que tratam o assunto de uma forma geral e específica. São utilizadas as seguintes fontes de investigação: – a Norma NBR ISO/IEC 17799, teses, dissertações e artigos de especialistas no assunto que trazem uma contribuição fundamental para este trabalho sobre segurança da informação.

2.2 HISTÓRICO DO PROBLEMA

Caracteriza-se como Segurança da Informação:

> A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida. A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio. (ABNT NBR ISO/IEC 17799, 2001, pág. 1)

A segurança perfeita é algo inatingível, utópico. Portando, deve-se prevenir ou reduzir a probabilidade de danos. Esses danos podem ser provenientes de:

- mau uso (acidental ou proposital);
- dano por vandalismo;
- invasão intencional;
- fraude;
- sabotagem;
- desastres por fogo, água, terremotos, furacões, etc.

Cox (2002) salienta outros três aspectos básicos da segurança de dados que se subdividem em vários tópicos:

- **Prevenção**: tentar evitar que aconteça.

    - ***proteção de hardware:*** normalmente chamado de segurança física, é de vital importância. Negando acessos físicos não autorizados a infra-estrutura da rede, previne-se de possíveis roubos de dados, desligamento de equipamentos e demais danos possíveis quando se está fisicamente no local;

    - ***proteção de arquivos e dados***: providenciado por autenticação, controle de acesso, antivírus e conscientização do usuário. No processo de autenticação, é verificado se quem está pedindo acesso é realmente quem diz ser. No processo de controle de acesso, só são disponibilizadas as transações realmente pertinentes a essa pessoa (ex.: só leitura de arquivos, leitura e escrita, quais pastas ou arquivos a pessoa pode utilizar, etc.);

    - ***proteção do perímetro da rede***: ferramentas do tipo *Firewall*, *IDS*, *IPS*, e *Proxy* cuidam desse aspecto, mantendo a rede protegida contra invasões de usuários não autorizados.

- **Detecção**: detectar o problema o mais cedo possível.

    - ***alertas***: sistemas de detecção de intrusos podem avisar os administradores e responsáveis pela segurança da rede a qualquer sinal de invasão ou mudança suspeita no comportamento da rede que pareça um padrão de ataque ou mude o comportamento normal da rede. Os avisos podem ser via e-mail, via mensagem no terminal do administrador, etc.;

    - ***auditoria***: periodicamente deve-se analisar os componentes críticos do sistema a procura de mudanças suspeitas. Esse processo pode ser realizado por ferramentas que procuram, por exemplo, modificações no tamanho nos arquivos de senhas, usuários com inatividade longa, etc.

- **Recuperação**: como voltar ao funcionamento normal após um incidente.

    - ***cópia de segurança dos dados (Backup)***: manter completa, atualizada e testada, a cópia de segurança dos dados deve ser em meio diferente e separado dos servidores;

    - ***aplicação para realizar o Backup***: ferramentas que proporcionem recuperação rápida dos dados do *backup*;

    - ***backup do Hardware***: a compra ou utilização de *backup* de *hardware* (ex.: servidor reserva, *nobreak* reserva, linhas de dados reserva, etc.) podem ser justificados levando-se em conta o custo de uma parada do sistema e determinando-se a importância da informática para a organização.

Outro autor, Rabener (2002) define a segurança como algo essencial. Salienta que a segurança não é apenas um *firewall*, não é somente um *IDS*, não é um *software* antivírus. É uma peça integrante do ambiente de computação, onde um elemento único não pode proteger efetivamente uma rede. O fator humano é crítico. O gerenciamento precisa ficar alerta dos riscos e apoiar os esforços para proteger os recursos da corporação. Os funcionários de tecnologia precisam compreender seus papéis e responsabilidades. Os usuários devem ser treinados nas regras de segurança para proteger a si mesmos e aos bens da companhia. Kisser (2000) confirma essa visão, salientando que "segurança sólida é um processo e não um produto".

2.3 SANS INSTITUTE

O *SysAdmin, Audit, Network, Security* (SANS) é o mais confiável e sem dúvida a maior fonte de segurança de informação e certificação no mundo. Também desenvolve, mantém, e disponibiliza, a maior coleção de documentos de pesquisa sobre vários aspectos de segurança de informação. O SANS Institute iniciou em 1989 como uma cooperativa de pesquisa e organização para treinamento e educação. Seus programas alcançam mais de

165.000 profissionais de segurança, auditores, administradores de sistema, administradores de rede, gerentes em segurança de informação, e diretores de informática que compartilham os ensinamentos que aprenderam e que agora, juntamente, acham soluções para os desafios que eles enfrentam.

O SANS congrega muitos especialistas em segurança da informação que estão em agências de governo, corporações, e universidades ao redor do mundo, e que, investem centenas de horas cada ano em pesquisa, ensinando e ajudando a comunidade de segurança de informação no mundo inteiro.

2.4 CERT

Estabelecido em 1988, o *Computer Emergency Readiness Team* (CERT) é um centro de perícias de segurança na Internet, situado no Instituto de Engenharia de Software (*Software Engineering Institute - SEI*), um centro de pesquisa e desenvolvimento, fundado e operado pela Universidade Carnegie Mellon (*Carnegie Mellon University*).

Conforme o CERT, redes ficaram indispensáveis para administrar o negócio dentro do governo, em organizações comerciais e acadêmicas. Sistemas transmitidos em rede permitem acessar a informação rapidamente, melhorar comunicações enquanto reduz o custo delas. Enquanto as redes de computadores revolucionam o modo que você negocia, os riscos que elas introduzem podem ser fatal a um negócio. Ataques em redes podem conduzir a perda de dinheiro, tempo, produtos, reputação, informação sensível, e até mesmo vidas.

Sistemas, redes, e informação sensível podem ser comprometidos por ações maliciosas ou inadvertidas, apesar dos melhores esforços de um administrador. Até mesmo quando administrador sabe o que fazer, eles freqüentemente não têm tempo para fazer isto. As preocupações operacionais do dia-a-dia e a manutenção do funcionamento dos sistemas têm prioridade sobre a segurança desses sistemas.

O conhecimento que a maioria dos administradores de rede e de sistemas têm sobre proteção e segurança desses sistemas vêm tipicamente da experiência e do boca-a-boca, não vêm da consulta a uma série de procedimentos publicados, que geralmente servem de padrões de fato para a comunidade dos administradores. Por esta e outras razoes, um administrador precisa de fácil acesso, fácil compreensão, e facilidade de implementação das práticas de

segurança. As práticas de segurança do CERT para sistemas e rede, satisfazem estas necessidades.

Elas são organizadas em cinco tópicos:

- Aumentar a segurança
- Preparar
- Descobrir
- Responder
- Melhorar

As práticas para enrijecer e aumentar a segurança formam uma base forte, estabelecendo configurações seguras dos ativos computacionais. Preparar, descobrir, responder e melhorar, estas ações assumem que as práticas de enrijecer e aumentar a segurança foram implementadas e provêm orientação adicional para o que fazer quando algo suspeito, inesperado, ou incomum acontece.

2.5 CERT.BR

Aqui no Brasil, temos o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR) – que é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, mantido pelo Comitê Gestor da Internet (CGI) no Brasil. Ele é o grupo responsável por receber, analisar e responder a incidentes de segurança em computadores, envolvendo redes brasileiras conectadas à Internet.

Além do processo de resposta a incidentes em si, o CERT.BR também atua através do trabalho de conscientização sobre os problemas de segurança.

Ele é um ponto único para notificações de incidentes de segurança no Brasil, de modo a prover a coordenação e o apoio necessário no processo de resposta a incidentes, colocando as partes envolvidas em contato quando necessário. Estabelece um trabalho colaborativo com outras entidades, como as polícias, provedores de acesso e serviços Internet e backbones. Dá suporte ao processo de recuperação e análise de sistemas comprometidos, além de oferecer treinamento na área de resposta a incidentes de segurança.

Como o CERT.BR auxilia o tratamento de qualquer incidente envolvendo redes conectadas à Internet no Brasil, o grupo recebe notificações de quaisquer atividades que sejam julgadas um incidente de segurança pelas partes envolvidas. Estes incidentes podem ser varreduras (*scans*), tentativas de invasão, ataques de negação de serviço, ataques de engenharia social, entre outros.

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

São exemplos de incidentes de segurança:

- tentativas de ganhar acesso não autorizado a sistemas ou dados;
- ataques de negação de serviço;
- uso ou acesso não autorizado a um sistema;
- modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema;
- desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

Abaixo, temos os índices dos incidentes reportados de Julho a Setembro de2005.

Tabela 2 - Incidentes Reportados ao CERT.BR -- Julho a Setembro de 2005

Tabela: Totais Mensais e Trimestral Classificados por Tipo de Ataque.

Mês	Total	worm	(%)	af	(%)	dos	(%)	invasão	(%)	aw	(%)	scan	(%)	fraude	(%)
Jul	5146	1329	25	3	0	2	0	15	0	22	0	1045	20	2730	53
Ago	5718	1144	20	7	0	5	0	45	0	41	0	1522	26	2954	51
Set	5361	1075	20	2	0	2	0	87	1	64	1	1527	28	2604	48
Total	16225	3548	21	12	0	9	0	147	0	127	0	4094	25	8288	51

Legenda:

- af: Ataque ao usuário final;
- dos: Denial of Service;
- aw: Ataque a servidor Web.

Fonte: CERT.BR

2.6 TESES E DISSERTAÇÕES SOBRE SEGURANÇA DA INFORMAÇÃO

2.6.1 A Aplicação de um Modelo de Gestão de Segurança da Informação e a sua Influência na Percepção de Competitividade no Setor de Telecomunicações e Informática – Dissertação de Rosangela Caubit, UFF, Rio de Janeiro, 2003.

2.6.1.1 RESUMO DA DISSERTAÇÃO

Esta dissertação se dispõe a estudar a aplicação do modelo de gestão de segurança da informação previsto no *framework* da BS 7799-2 (equivalente a NBR ISO/IEC 17799), como elemento de geração de percepção de diferencial competitivo e obtenção de maior garantia de continuidade do negócio e melhores resultados às empresas no segmento de Telecomunicações e Informática.

O modelo estudado trata de forma integrada a segurança física e lógica, o treinamento e a conscientização das pessoas, busca um maior entendimento dos processos críticos de negócio garantindo sua continuidade e a otimização das ferramentas de tecnologia da informação que visam proteger os ativos da informação sendo eles: *hardware, software* e pessoas. Os requisitos e controles previstos pela norma BS 7799-2, quando implementados, adequadamente, garantem um nível satisfatório de amplitude para implementação e melhoria do sistema de gestão de segurança em qualquer empresa.

2.6.1.2 REFERENCIAL TEÓRICO EMPREGADO NA DISSERTAÇÃO

O Referencial Teórico utilizado nesta dissertação foi o modelo de gestão da segurança da informação a partir do código de práticas internacionalmente aprovadas (BS 7799, 2002), os critérios de desenvolvimento de sistemas seguros e, por fim, as definições de competitividade e posicionamento estratégico segundo um dos mais renomados autores sobre o assunto, Michael Porter.

2.6.1.3 METODOLOGIA APLICADA NA DISSERTAÇÃO

Esta dissertação utilizou o método de abordagem da pesquisa que é o método hipotético-dedutivo baseado nas idéias de Popper proposta no livro: A Lógica da Pesquisa Científica (1975).

2.6.1.4 RELAÇÃO DA DISSERTAÇÃO COM ESTE TRABALHO

Esta dissertação citada tem alguma relação com este trabalho, pois considera como referencial teórico a Norma ISO/IEC 17799, que é um padrão para implementação de um sistema de gestão da Segurança da Informação.

2.7 CONFERÊNCIAS E SIMPÓSIOS

2.7.1 CONGRESSO NACIONAL DE AUDITORIA DE SISTEMAS E SEGURANÇA DA INFORMAÇÃO (CNASI)

A preservação dos dados confidenciais de cada empresa, bem como a disponibilidade e integridade de aplicações e serviços e credibilidade junto a sua base de clientes são os maiores fatores críticos de sucesso dos negócios, visto que as corporações buscam cada vez mais um relacionamento continuamente seguro com os seus parceiros e fornecedores.

O CNASI tem como objetivo atualizar e capacitar todos os profissionais envolvidos com a área de segurança da informação e auditoria de sistemas nas corporações. O evento possui cursos de qualificação básicos e avançados, palestras técnicas, painéis, apresentação de soluções e produtos, além da participação de renomados especialistas nacionais e internacionais.

O CNASI-2005 contou com cerca de 60% de seu público, composto por executivos envolvidos nas decisões estratégicas de suas empresas. Apresentou as principais tendências que tanto aproximaram fornecedores de soluções a executivos e dirigentes das corporações, a fim de que pudessem, de maneira concreta e eficaz, conhecer as melhores ferramentas e serviços que podem melhorar o desempenho e dinamizar os negócios de suas empresas, enquanto qualificam e desenvolvem profissionais através de palestras técnicas.

Para quem participou do evento encontrou conceituados especialistas que debateram os principais tópicos da Segurança da Informação e sua vulnerabilidade, além de uma abordagem sobre as iniciativas que podem determinar o fracasso ou o sucesso de uma "missão". Os cursos tiveram caráter formativo e duração de 2 a 6 horas. Eles permitiram aos participantes uma imersão de conteúdo e aprendizado, pontos fundamentais para a formação de gestores de segurança e auditoria.

2.7.1.1 RELAÇÃO DO CNASI COM ESTE TRABALHO

O CNASI contribuiu fundamentalmente para enriquecer este trabalho no sentido de conhecer a opinião de profissionais de vulto internacional, ligados à segurança da informação que apresentaram as dificuldades inerentes a todas as organizações, não só no Brasil, como também nas organizações internacionais. Executivos de segurança, gerentes e outros executivos da alta direção das empresas nacionais e estrangeiras, discutiram durante o evento, sobre as atuais soluções de segurança da informação e apresentaram depoimentos sobre como venceram as ameaças mais comuns à segurança da informação em suas organizações.

Foi extremamente produtiva a presença neste evento, de vultosa importância, dentro da comunidade de Segurança da Informação.

2.8 SUMÁRIO CONCLUSIVO DO CAPÍTULO

Neste capítulo promoveu-se o levantamento de temas relacionados com a Segurança da Informação. Os itens citados acima permitem uma visão mais completa do tema a partir de diferentes tendências e metodologias.

3 REFERENCIAL TEÓRICO OU CONCEITUAL

3.1 SUMA DO CAPÍTULO

Neste capítulo são apresentados fundamentos sobre Percepção de Segurança da Informação - a Norma NBR ISO/IEC 17799, os fundamentos sobre Percepção de Qualidade – *Servqual* de Parasuraman et al., os fundamentos sobre Percepção de Liderança – Kouzes e Posner, e por fim, os fundamentos sobre Percepção de Seguidores – Kelley.

3.2 SEGURANÇA DA INFORMAÇÃO – NBR ISO/IEC 17799

A NBR ISO/IEC 17799 é a publicação da Associação Brasileira de Normas Técnicas (ABNT) do código de práticas para implementação de segurança da informação adotado pela *International Organization of Standarization* (ISO) cuja sigla significa "Organização Internacional para Normalização", uma organização internacional, não governamental, que elabora normas no âmbito internacional. A ISO foi fundada em 1947, com sede em Genebra, na Suíça, e hoje fazem parte dela entidades de normalização de mais de 100 países.

No Brasil a ABNT é membro fundador da ISO e também é o Fórum Nacional de Normalização. A missão da ISO é promover o desenvolvimento da normalização e atividades relacionadas no mundo, com a visão de facilitar trocas internacionais de bens e serviços e o desenvolvimento da cooperação nos domínios intelectuais, científicos, tecnológicos e econômicos.

A NBR ISO/IEC 17799:2001 é equivalente à ISO/IEC 17799:2000, mantendo seu foco na gestão do risco, a partir da análise do risco e os dispositivos de controle e avaliação permanente das ameaças e vulnerabilidades que incidem sobre os ativos da informação de uma empresa.

Neste trabalho, não se utiliza a totalidade da Norma, somente os itens que se relacionam com os usuários finais dos sistemas de informações são vistos nesta pesquisa, já que conforme Rabener (2002) e Kisser (2000), os usuários são os elos mais fracos da segurança da informação, a razão deste estudo.

3.2.1 O QUE É SEGURANÇA DA INFORMAÇÃO

Acredita-se que o principal ativo de uma instituição é a informação. É importante para os negócios, tem valor para a organização e, portanto, deve ser necessariamente protegida. A Segurança da Informação protege a informação de diversos tipos de ameaças, garantindo assim, a continuidade do negócio, minimizando os danos, e também, o tempo do retorno do negócio da organização.

A informação pode existir em muitas formas. Pode estar em papel, em filmes, falada em conversas ou armazenada eletronicamente em sistemas de informação. Mas independentemente da forma, ela deve ser caracterizada pela preservação de:

- **Confidencialidade**

  A informação somente é acessível por pessoas autorizadas.

- **Integridade**

  A informação exata e completa.

- **Disponibilidade**

  A informação ter acesso por pessoas autorizadas, sempre que necessário.

Segurança da informação é obtida implementando de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de *software*. Estes controles precisam ser estabelecidos para garantir que os objetivos de segurança específicos da organização sejam atendidos.

3.2.2 A NECESSIDADE DA SEGURANÇA DA INFORMAÇÃO

A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Confidencialidade, integridade e disponibilidade da informação podem ser essenciais para preservar o atendimento aos requisitos legais e a imagem da organização no mercado.

Cada vez mais as organizações são colocadas à prova por diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo e inundação. Problemas causados por vírus, *hackers* e ataques de *denial of service* estão se tornando cada vez mais comuns e muito mais sofisticados.

As instituições estão mais dependentes dos sistemas e serviços de informação, o que significa que as organizações estão mais vulneráveis às ameaças de segurança. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída dificulta a implementação de um controle de acesso centralizado realmente eficiente.

A gestão da segurança da informação necessita, pelo menos, da participação de todos os funcionários da organização.

3.2.3 ESTABELECENDO REQUISITOS DE SEGURANÇA

O primeiro é obtido na avaliação de riscos dos ativos de informação.

O segundo é a legislação vigente, os estatutos, a regulamentação e cláusulas contratuais.

O terceiro é o conjunto de princípios, objetivos e requisitos para o processamento da informação da organização em suas operações.

3.2.4 AVALIANDO OS RISCOS

Análise de risco é uma consideração sistemática de:

- O impacto nos negócios é o resultado de uma falha de segurança
- A probabilidade de tal falha realmente ocorrer

3.2.5 SELEÇÃO DE CONTROLES

Os controles devem ser selecionados baseados nos custos de implementação em relação aos riscos que serão reduzidos e as perdas potenciais se as falhas na segurança ocorrerem. Devem ser levados em consideração, prejuízos na reputação da organização.

Os controles essenciais, do ponto de vista legal, para uma organização, incluem:

- proteção de dados e privacidade de informações pessoais
- salvaguarda de registros organizacionais
- direitos de propriedade intelectual

Também se têm os controles considerados como melhores práticas:

- documento da política de segurança da informação
- definição das responsabilidades na segurança da informação
- educação e treinamento em segurança da informação
- relatório dos incidentes de segurança
- gestão da continuidade do negócio

3.2.6 FATORES CRÍTICOS DE SUCESSO

Alguns fatores são críticos para que a implementação da segurança da informação tenha sucesso na organização:

- política de segurança, objetivos e atividades, que reflitam os objetivos do negócio;
- um enfoque para a implementação da segurança que seja consistente com a cultura organizacional;
- comprometimento e apoio visível da administração;
- um bom entendimento dos requisitos de segurança, análise de risco e gerenciamento de risco;

- divulgação eficiente da segurança para todos os gerentes e funcionários;
- distribuição das diretrizes sobre as normas e política de segurança da informação para todos os funcionários e fornecedores;
- proporcionar educação e treinamento adequados;
- um abrangente e balanceado sistema de medição, que é usado para avaliar o desempenho da gestão de segurança da informação e obtenção de sugestões para a melhoria.

3.2.7 ATRIBUINDO RESPONSABILIDADES

É essencial que as áreas pelas quais cada gestor é responsável estejam claramente estabelecidas; em particular recomenda-se que os itens seguintes sejam cumpridos.

- Convém que os vários ativos e processos de segurança associados com cada sistema sejam identificados e claramente definidos;
- Convém que o gestor responsável por cada ativo ou processo de segurança esteja de acordo e os detalhes dessa responsabilidade sejam documentados;
- Convém que os níveis de autorização sejam claramente definidos e documentados.

3.2.8 CONFIDENCIALIDADE

Acordos de confidencialidade ou de não divulgação são usados para alertar que a informação é confidencial ou secreta. Os funcionários devem assinar tais acordos como parte dos termos e condições iniciais de contratação.

Para colaboradores e terceiros convém que seja exigida a assinatura do acordo de confidencialidade, antes de ter acesso às instalações de processamento da informação da organização.

3.2.9 TREINAMENTO DOS USUÁRIOS

Tem por objetivo garantir que os usuários estão cientes das ameaças e das preocupações de segurança da informação.

Todos os funcionários da organização devem receber treinamento adequado sobre as políticas e procedimentos organizacionais. Assim como treinamento sobre o correto uso das instalações de processamento da informação como, por exemplo, procedimentos de acesso ou utilização dos *softwares,* antes de ter acesso aos serviços ou informações.

3.2.10 RESPONDENDO AOS INCIDENTES E AO MAU FUNCIONAMENTO

Para minimizar os danos originados pelos incidentes de segurança e mau funcionamento, convém que todos os incidentes sejam notificados o mais rapidamente possível.

Todos os funcionários devem estar conscientes dos procedimentos para notificação dos incidentes (violação de segurança, ameaças, falhas ou mau funcionamento) que possam impactar na segurança dos ativos institucionais.

Convém que os usuários sejam informados que eles não podem, sob nenhuma circunstância, tentar averiguar uma falha suspeita, pois a investigação de uma falha pode ser interpretada como um potencial uso impróprio do sistema.

3.2.11 PROTEÇÃO CONTRA *SOFTWARES* MALICIOSOS

Tem por objetivo a proteção da integridade do *software* e da informação. Para que isso aconteça é necessário à adoção de precauções para prevenir e detectar a introdução de *software* malicioso.

3.2.12 CONTROLES CONTRA PROGRAMAS MALICIOSOS

Os ambientes de processamento de informação e os *softwares* são vulneráveis à introdução de arquivos maliciosos, tais como vírus, cavalos de Tróia e outros.

É essencial que sejam tomadas precauções para a detecção e prevenção de vírus em computadores pessoais. Convém que a proteção contra esses programas seja baseada na conscientização da segurança. Os seguintes controles devem ser considerados:

- uma política formal exigindo conformidade com as licenças de uso dos *softwares* e proibindo o uso de programas não autorizados
- uma política formal para proteção contra os riscos associados com a importação de arquivos obtidos de ou através de redes externas, ou por qualquer outro meio, indicando quais as medidas preventivas que devem ser adotadas
- instalação e atualização regular de programas de detecção e remoção de vírus para o exame de computadores e meios magnéticos, tanto de forma preventiva como de forma rotineira
- revisões regulares de *softwares* e dos dados dos sistemas que suportam processos críticos do negócio. Convém que a presença de qualquer arquivo ou atualização não autorizada seja formalmente investigada
- verificação, antes do uso, da existência de vírus em qualquer arquivo em meio magnético de origem desconhecida ou não autorizada, e em qualquer arquivo recebido a partir de redes não confiáveis
- verificação, antes do uso, da existência de *software* malicioso em qualquer arquivo recebido através de correio eletrônico ou importado (*download*). Essa avaliação pode ser feita em diversos locais, como, por exemplo, nos servidores de correio eletrônico, nos computadores pessoais ou quando da sua entrada na rede da organização
- procedimentos de gerenciamento e respectivas responsabilidades para tratar da prevenção de vírus no sistema, treinamento nesses procedimentos, relato e recuperação de ataques de vírus
- planos de contingência adequados para a recuperação em caso de ataques por vírus, incluindo os procedimentos necessários para salva e recuperação dos dados e programas

- procedimentos para a verificação de toda informação relacionada a programas maliciosos e garantia de que os alertas sejam precisos e informativos. Convém que os funcionários estejam capacitados a lidar com boatos e cientes dos problemas decorrentes desses.

3.2.13 SEGURANÇA DO CORREIO ELETRÔNICO E SEUS RISCOS

Com o advento do correio eletrônico substituindo meios tradicionais, tais como telex e cartas, e sendo utilizado para as comunicações comerciais, existe a preocupação constante com a segurança. Tem de ser levado em conta à necessidade de controles para a diminuição dos riscos gerados pelo seu uso.

Esses riscos incluem:

- vulnerabilidade das mensagens ao acesso não autorizado, à modificação ou à negação do serviço;
- vulnerabilidade a erro como, por exemplo, endereçamento e direcionamento incorretos, e em geral a falta de confiabilidade e disponibilidade do serviço;
- impacto da mudança do meio de comunicação nos processos do negócio como, por exemplo, o efeito do aumento da velocidade dos encaminhamentos ou o efeito do envio de mensagens formais no âmbito de pessoa para pessoa ao invés de companhia para companhia;
- considerações legais relacionadas com a necessidade potencial de prova de origem, envio, recebimento e aceitação;
- implicações da divulgação externa de listas de funcionários;
- controle sobre o acesso dos usuários remotos às contas de correio eletrônico.

3.2.14 POLÍTICA DE USO DO CORREIO ELETRÔNICO

As organizações devem definir uma política clara para a utilização do correio eletrônico, incluindo:

- ataques ao correio eletrônico, como por exemplo, por vírus e interceptação;
- proteção de anexos de correio eletrônico;

- orientações de quando não se deve utilizar o correio eletrônico;
- responsabilidades dos funcionários de forma a não comprometer a organização, como por exemplo o envio de mensagens difamatórias, uso do correio eletrônico para atormentar pessoas ou fazer compras não autorizadas;
- uso de técnicas de criptografia para proteger a confidencialidade e integridade das mensagens eletrônicas;
- retenção de mensagens que, se guardadas, podem ser descobertas e utilizadas em casos de litígio;
- controles adicionais para a investigação de mensagens que não puderem ser autenticadas.

3.2.15 SISTEMAS DISPONÍVEIS PUBLICAMENTE

As organizações que publicam dados em sites, ou seja, tornam seus dados públicos de alguma forma, devem tomar cuidado para proteger a integridade da informação divulgada eletronicamente, de forma a prevenir modificações não autorizadas, pois isto pode prejudicar a reputação pública da organização.

Convém que exista um processo de autorização formal antes da publicação de uma informação.

3.2.16 CONTROLE DE ACESSO

Tem por objetivo o controle do acesso à informação. É recomendado que este controle tenha uma política que leve em conta o seguinte:

- requisitos de segurança de aplicações específicas do negócio;
- identificação de toda informação referente às aplicações do negócio;

- políticas para autorização e distribuição de informação, por exemplo, a necessidade de conhecer os princípios e níveis de segurança, bem como a classificação da informação;
- compatibilidade entre o controle de acesso e as políticas de classificação da informação dos diferentes sistemas e redes;
- legislação vigente e qualquer obrigação contratual considerando a proteção do acesso a dados ou serviços;
- perfil de acesso de usuário padrão para categorias de trabalho comuns;
- gerenciamento dos direitos de acesso em todos os tipos de conexões disponíveis em um ambiente distribuído e conectado em rede.

Tem-se também a especificação de regras para controle de acesso. Convém que alguns cuidados sejam tomados e considerados:

- diferenciação entre as regras que sempre devem ser cumpridas das regras opcionais ou condicionais;
- estabelecimento de regras baseadas na premissa “Tudo deve ser proibido a menos que expressamente permitido“;
- modificações nos rótulos de informação que são atribuídos automaticamente pelos recursos de processamento de dados e dos atribuídos a critério de um usuário;
- modificações nas permissões de usuários que são atribuídas automaticamente por um sistema de informação daquelas atribuídas por um administrador;
- diferenciação entre regras que requerem aprovação do administrador ou outro funcionário antes da liberação e aquelas que não necessitam tal aprovação.

Nas organizações têm de existir procedimentos formais para controlar a concessão de direitos de acesso aos sistemas de informação e serviços.

3.2.17 REGISTRO DE USUÁRIO

É fundamental para a organização que exista um procedimento formal de registro e cancelamento de usuários, a fim de controlar os acessos a todos os sistemas de informação e serviços multiusuários.

Este procedimento formal deve incluir:

- utilização de identificador de usuário (ID) único de forma que cada usuário possa ser identificado e feito responsável por suas ações. Convém que o uso de identificador (ID) de grupo somente seja permitido onde for necessário para a execução do trabalho;
- verificação que o usuário tem autorização do proprietário do sistema para a utilização do sistema de informação ou serviço. Aprovação do direito de acesso pelo gestor do usuário pode também ser necessária;
- verificação de que o nível de acesso concedido está adequado aos propósitos do negócio e está consistente com a política de segurança da organização;
- entrega de um documento escrito aos usuários sobre seus direitos de acesso;
- solicitação da assinatura dos usuários indicando que eles entenderam as condições de seus direitos de acesso;
- garantia de que o provedor de serviço não fornecerá direitos de acesso até que os procedimentos de autorização sejam concluídos;
- manutenção de um registro formal de todas as pessoas cadastradas para usar o serviço;
- remoção imediata dos direitos de acesso de usuários que tenham mudado de função ou saído da organização;
- verificação periódica para remoção de usuários (ID) e contas redundantes;
- garantia de que identificadores de usuários (ID) redundantes não sejam atribuídos para outros usuários.

3.2.18 RESPONSABILIDADES DO USUÁRIO

3.2.18.1 USO DE SENHAS

Os usuários têm de seguir as boas práticas de segurança na seleção e utilização das senhas. Elas fornecem um meio de validação da identidade do usuário, sendo conseqüentemente, estabelecido os direitos de acesso aos recursos ou serviços do processamento da informação.

Os usuários devem:

- manter a confidencialidade das senhas;
- evitar o registro das senhas em papel, a menos que o papel possa ser guardado de forma segura;
- alterar a senha sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;
- selecionar senhas de qualidade, com um tamanho mínimo de seis caracteres, que sejam:

    - fáceis de lembrar;
    - não baseadas em coisas que outras pessoas possam facilmente adivinhar ou obter a partir de informações pessoais, por exemplo, nomes, números telefônicos, datas de nascimento, etc;
    - isentas de caracteres idênticos consecutivos ou de grupos de caracteres somente numéricos ou alfabéticos.

- alterar a senha em intervalos regulares ou baseado no número de acessos (senhas para contas privilegiadas devem ser alteradas com maior freqüência do que senhas normais) e evitar a reutilização de senhas;
- alterar senhas temporárias no primeiro acesso ao sistema;
- não incluir senhas em processos automáticos de acesso ao sistema, por exemplo, armazenadas em macros ou teclas de função;

- não compartilhar senhas individuais.

No caso de organizações da Administração Pública Federal, isto é considerado "crime", conforme a lei nº 9983, de 14 de julho de 2000.

> "Art. 325. ....."
> "§ 1º Nas mesmas penas deste artigo incorre quem:" (AC)
> "I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública;" (AC)
> "II – se utiliza, indevidamente, do acesso restrito." (AC)
> "§ 2º Se da ação ou omissão resulta dano à Administração Pública ou a outrem:" (AC)
> "Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa." (AC)

3.2.19 CONTROLE DE CONEXÕES DE REDE

São requeridos controles que limitem a capacidade de conexão dos usuários dentro da política de controle de acesso para redes compartilhadas.

Aplicações onde convém ter essas restrições:

- correio eletrônico
- transferência de arquivos
- acesso interativo
- acesso à rede associado à hora do dia ou a data

3.2.20 ENTRADA NO SISTEMA (*LOGON*)

As organizações têm de prover um processo seguro de entrada no sistema (*logon).* Convém que tenha um procedimento bem projetado para minimizar os riscos de acessos não autorizados.

Todos os usuários devem ter um identificador único (ID) para uso pessoal e exclusivo, de modo a permitir que as atividades possam ser rastreadas subseqüentemente a um indivíduo responsável.

Existem várias formas de autenticação. Senhas são as mais comuns de se prover identificação e autenticação, pois são baseadas num segredo que somente o usuário conhece.

Outras formas como *tokens* ou *smartcards* também podem ser utilizadas para identificação e autenticação. A biometria contribui para as autenticações que usam características ou atributos únicos de cada indivíduo e podem ser usadas para autenticar a identidade de uma pessoa. Uma combinação de tecnologias e mecanismos seguramente relacionados resultará em uma autenticação forte.

É conveniente que um sistema de gerenciamento de senhas:

- obrigue o uso de senhas individuais para manter responsabilidades;
- onde apropriado, permita que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;
- obrigue a escolha de senhas de qualidade, como já visto anteriormente;
- onde os usuários mantêm suas próprias senhas, seja obrigada a troca periódica;
- onde os usuários selecionam senhas, obrigue a troca da senha temporária no primeiro acesso;
- mantenha registro das senhas anteriores utilizadas, por exemplo, para os 12 meses passados, e bloqueie a reutilização de senhas;
- não mostre as senhas na tela quando forem digitadas;
- armazene os arquivos de senha separadamente dos dados de sistemas e de aplicação;
- armazene as senhas na forma cifrada, usando um algoritmo de criptografia unidirecional.
- altere senhas-padrão fornecidas pelo fabricante, após a instalação do *software*.

3.2.21 LIMITANDO O TEMPO DE CONEXÃO

Restrições nos horários de conexões proporcionam a organização, uma segurança adicional para suas aplicações. Limitando o período de acesso permitido se reduz à janela de oportunidades para acessos não autorizados.

Uma boa prática para este tipo de restrição inclui:

- utilização de blocos de tempo predeterminados;
- restrição dos horários de conexão às horas normais do expediente;

3.2.22 CONTROLE DE ACESSO ÀS APLICAÇÕES

Objetiva a prevenção de acessos não autorizados à informação contida nos sistemas de informação da empresa.

Convém que a aplicação de controles suporte os requisitos de restrição de acesso:

- fornecendo menus para controlar o acesso às funções dos sistemas de aplicação;
- restringindo o conhecimento do usuário sobre informações ou funções de aplicação do sistema às quais ele não tem autoridade de acesso, com a publicação apropriada de documentação para o usuário;
- controlando os direitos de acesso dos usuários, para ler, escrever, apagar ou executar;
- assegurando que as saídas dos sistemas de aplicação que tratam informações sensíveis contenham apenas a informação que é relevante ao uso de tal saída e é enviada apenas para os terminais e locais autorizados, incluindo revisão periódica de tais saídas para garantir que as informações redundantes são removidas.

3.2.23 COMPUTAÇÃO MÓVEL E TRABALHO REMOTO

Tem como objetivo a garantia de segurança da informação quando se utilizam a computação móvel e o trabalho remoto. Quando se utiliza computação móvel, é conveniente que os riscos de trabalhar em ambiente desprotegido sejam levados em consideração e que sejam aplicadas proteções adequadas. O uso de *notebooks, palmtops* e celulares pedem cuidados especiais para a garantia das informações contidas. É conveniente que a utilização desses objetos incluam políticas de proteção física, controles de acesso, técnicas de criptografia, cópias de segurança e proteção contra vírus e *softwares* maliciosos.

Convém que seja ministrado treinamento para o pessoal que utiliza computação móvel, para que o nível de conscientização seja aumentado a respeito dos riscos adicionais dessa forma de trabalho.

3.3 PERCEPÇÃO DA QUALIDADE EM SISTEMAS DA INFORMAÇÃO

Com o advento da microinformática, a área de Informática teve sua responsabilidade bastante ampliada. Além do seu tradicional papel de construtora de sistemas computacionais, a Informática agora se responsabiliza por uma enorme variedade de serviços voltados às necessidades organizacionais. Na verdade, a informática passou a ser um prestador de serviços para todas as demais áreas da organização. E como fornecedor de serviços, passou a ser cobrada pela qualidade destes.

3.3.1 QUALIDADE DE SERVIÇOS

A. Parasuraman, Valerie A. Zeithaml e Leonard L. Berry iniciaram um estudo em 1983 sobre a qualidade do serviço, com o propósito de responder as seguintes questões:

- O que é qualidade do serviço?
- Quais são as causas dos problemas na qualidade dos serviços?
- Que podem fazer as organizações para resolver estes problemas e melhorar seus serviços?

Desenvolveram então, um modelo visando a captar critérios para avaliação da qualidade em serviços. Os critérios de avaliação, ou dimensões, como nomeadas pelos autores, foram aplicados, considerando-se ou hiatos ou lacunas (*gaps)*, que são as diferenças entre as expectativas dos usuários e o que é realmente oferecido.

De acordo com Parasuraman, Zeithaml e Berry (1988), os usuários avaliam a qualidade do serviço comparando o que desejam ou esperam receber com o que, efetivamente, é recebido.

Parasuraman (1985) propõe um modelo para avaliação da qualidade dos serviços, baseado na seguinte definição:

> Qualidade nos serviços, como percebida por um usuário, depende do tamanho e direção do 'gap' entre o serviço esperado e o serviço percebido (ou recebido), o qual

> por sua vez depende da natureza dos 'gaps' do lado do fornecedor dos serviços associado ao projeto, marketing e entrega dos serviços.

Sob o ponto de vista dos usuários, a qualidade dos serviços é a diferença entre a sua Expectativa (E) do que é esperado e a sua Percepção (P) daquilo que é recebido da área de Informática. Se a expectativa iguala a percepção, o usuário está tecnicamente satisfeito. Quando a percepção excede a expectativa, o usuário está mais do que satisfeito - está encantado ou deliciado. Quando a expectativa excede a percepção, o usuário está insatisfeito e existe um problema de qualidade nos serviços.

O estudo dos autores revelou que existe um conjunto de lacunas (*gaps*) entre a qualidade de serviços que deveria ser fornecida aos usuários, e as tarefas efetivamente associadas ao fornecimento destes serviços. Este estudo apresentou cinco hiatos ou lacunas (*gaps*) com as seguintes características:

- *Gap* 1 = discrepância entre expectativas dos usuários e percepções dos gerentes sobre essas expectativas.

- *Gap* 2 = discrepância entre percepção dos gerentes das expectativas dos usuários e especificação de qualidade nos serviços.

- *Gap* 3 = discrepância entre especificação de qualidade nos serviços e serviços realmente oferecidos.

- *Gap* 4 = discrepância entre serviços oferecidos e aquilo que é comunicado ao usuário.

- *Gap* 5 = discrepância entre o que o usuário espera receber e a percepção que ele tem dos serviços oferecidos.

Os primeiros quatro *gaps* contribuem para o quinto, que é exatamente onde reside o problema: expectativa do usuário "X" percepção dos serviços oferecidos. Assim, a quinta lacuna foi estabelecida como uma função das quatro lacunas anteriores, isto é:

- *Gap 5* = (f [*gap*1, *gap*2, *gap*3, *gap*4])

Mais tarde, em 1988, os mesmos pesquisadores, criaram uma escala intitulada *Servqual*, objetivando identificar cinco componentes da qualidade dos serviços: tangibilidade, confiabilidade, capacidade de resposta, segurança e empatia. O modelo *Servqual* representou uma ruptura no processo de avaliação de serviços e estimulou um grande número de estudos na área, sendo que muitas outras pesquisas refinaram o modelo conceitual de Parasuraman e seus colaboradores.

Zeithaml et al. (1990) definem a qualidade do serviço, do ponto de vista do cliente como: *"A amplitude da discrepância ou diferença que exista entre as expectativas ou desejos dos clientes e suas percepções".*

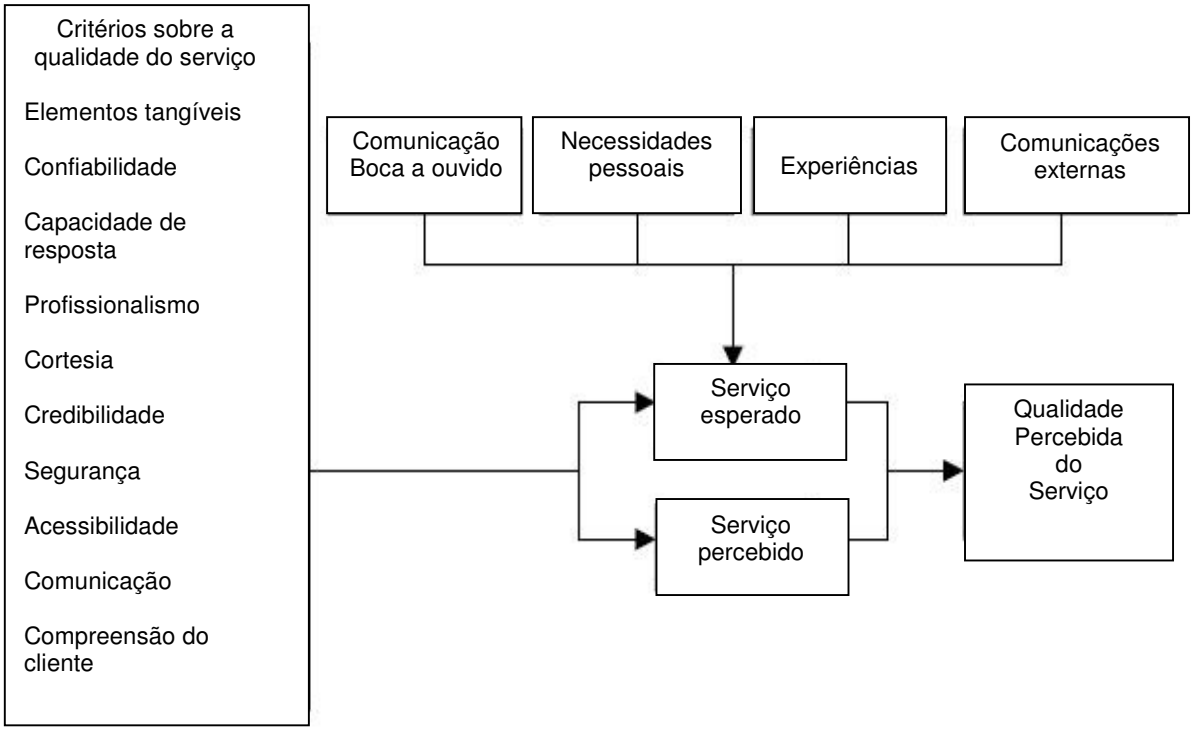


Figura 4: Avaliação do cliente sobre a Qualidade do Serviço
Fonte: Zeithaml, V. A.; Parasuraman, A.; Berry, L. L. ***Delivering Quality Service***. New York: The Free Press, 1990

3.3.2 FORMAÇÃO DE EXPECTATIVAS DO USUÁRIO

Um dos principais pontos deste modelo é a formação das expectativas dos usuários. Essas expectativas são influenciadas seguintes forças:

- **Comunicação informal ("boca-a-boca")** - comunicação sobre produtos, serviços, e desempenho de sistemas, mantida nos contactos informais entre usuários da mesma ou de diferentes organizações.
- **Necessidades pessoais** - necessidades de assistência, suporte ou informações, que os usuários precisam que sejam atendidas pela área de Informática.
- **Experiências passadas** - histórias de sucesso e fracassos envolvendo contactos anteriores com a área de Informática.
- **Informações dos Fornecedores** - influência da propaganda / comunicação dos fornecedores de equipamentos, máquinas e serviços, através de apresentações e contactos de vendas. Na tentativa de vender seus produtos, os fornecedores elevam em demasia as expectativas dos usuários, quando enfatizam somente os possíveis impactos positivos de seus produtos e serviços, esquecendo-se de levantar questões, tais como, compatibilidade, custo e tempo da conversão de sistemas. Na realidade, os fornecedores levantam as expectativas dos potenciais clientes para que eles fiquem insatisfeitos com sua atual infra-estrutura, de forma a ficarem predispostos a comprar novos produtos e soluções. Embora a Informática não tenha muito controle sobre este tipo de comunicação, ela não deve desprezar os seus efeitos sobre a formação das expectativas de seus usuários.
- **Informações da área de Informática** - é evidente que a própria área de Informática pode ser uma poderosa força na moldagem das expectativas dos seus usuários. Os usuários dependem e confiam na sua área de Informática para converter suas necessidades em sistemas e aplicativos. Neste processo, a área de Informática cria uma expectativa sobre como o futuro sistema será e como ele irá se comportar.

3.3.3 *SERVQUAL* - MEDINDO A QUALIDADE DO SERVIÇO

Baseado no conceito da qualidade em serviços e nos dez critérios, encontrados na investigação exploratória realizada, Zeithaml, Parasuraman e Berry iniciaram uma fase de pesquisa quantitativa com a finalidade de desenvolver um instrumento que permitisse medir

as percepções dos clientes sobre a qualidade do serviço, culminando com o desenvolvimento do instrumento de pesquisa denominado "*Servqual*".

O *Servqual* consiste de duas sessões: (1) Uma sessão de expectativas contendo 22 perguntas para determinar as expectativas gerais do cliente com relação ao serviço, e (2) uma sessão de percepção contendo 22 perguntas para medir a avaliação do cliente da categoria de serviço dentro de uma determinada organização.

Dez critérios gerais foram usados pelos clientes para julgar a qualidade do serviço:

- **Elementos tangíveis:** aparência das instalações físicas, equipamentos, pessoal e materiais de comunicação.

- **Confiabilidade:** Habilidade para executar o serviço de forma confiável, precisa e cuidadosa.

- **Capacidade de Resposta:** Disposição de ajudar os clientes e provê-los de um serviço rápido.

- **Profissionalismo:** Posse das habilidades requeridas e conhecimento da execução do serviço.

- **Cortesia:** Atenção, consideração, respeito e amabilidade do pessoal de contato.

- **Credibilidade:** Veracidade, crença, honestidade no serviço que se provê.

- **Segurança:** Inexistência de perigos, riscos e dúvidas.

- **Acessibilidade:** Acessível e fácil de contatar.

- **Comunicação:** Manter os clientes informados utilizando uma linguagem que possam entender, assim como escutá-lo.

- **Compreensão do cliente:** Fazer o esforço de conhecer os clientes e suas necessidades.

Zeithaml *et al.* (1990) argumentam que a colocação dos dez critérios gerais da qualidade do serviço é exaustiva e apropriada para avaliar a qualidade em uma ampla variedade de serviços. Estudos estatísticos posteriores na estruturação do *Servqual*, mostraram uma importante correlação entre os critérios, concluindo que eles podem ser representadas por apenas cinco dimensões. As correlações sugeriram a consolidação dos últimos sete critérios dentro de duas amplas dimensões denominadas *segurança* e *empatia,* os critérios restantes permaneceram sem mudanças, como mostra o quadro abaixo:

	Elementos tangíveis	Confiabilidade	Capacidade de resposta	Segurança	Empatia
Elementos tangíveis					
Confiabilidade					
Capacidade de resposta					
Profissionalismo Cortesia Credibilidade Segurança					
Acessibilidade Comunicação Compreensão do cliente.					

Quadro 2 - Correspondência entre as dimensões do *Servqual* e os dez critérios iniciais de avaliação da Qualidade do Serviço
Fonte: ZEITHAML, V. A.; PARASURAMAN, A.; BERRY L. L. ***Delivering Quality Service***. New York: The Free Press, 1990

As cinco dimensões foram definidas da seguinte maneira:

1. **Elementos tangíveis:** Aparência das instalações físicas, equipamento, pessoal e materiais de comunicação.
2. **Confiabilidade:** Habilidade para realizar o serviço de forma confiável precisa e consistente.

3. Capacidade de resposta: Disposição e vontade para ajudar os clientes e proporcionar o serviço prontamente.

4. Segurança: Conhecimentos e atenção mostrados pelos empregados e suas habilidades para transmitir confiança, segurança e credibilidade.

5. Empatia: Atenção individualizada, facilidade de contato (acesso) e comunicação que as empresas oferecem aos clientes.

Zeithaml et al. (1990) afirmam que o conteúdo dos itens finais que integram as duas novas dimensões, segurança e empatia, também representam as características chaves dos sete critérios anteriormente considerados. Em conseqüência, ainda que o *Servqual* tenha só cinco dimensões diferenciadas, essas incluem todas as facetas dos dez critérios que originalmente foram definidos. Os itens resultantes dos critérios consolidados também fornecem definições concisas desses.

3.3.4 MEDINDO A QUALIDADE DO SERVIÇO DE INFORMAÇÃO

A qualidade dos serviços pode ser medida por ferramentas já desenvolvidas, como o *Servqual* apresentado neste trabalho. Uma vez que o "Gap 5" tenha sido avaliado, os gerentes de Informática podem dirigir sua atenção para os outros 4 (quatro) "gaps" ou forças que influenciam a qualidade dos serviços:

Gap 1 - é a diferença entre a percepção dos gerentes da Informática sobre as expectativas dos usuários e as suas reais expectativas. Infelizmente, não é sempre que estes gerentes entendem o que os usuários querem.

Gap 2 - é diferença entre a percepção dos gerentes em relação às expectativas dos usuários e sua habilidade em traduzi-las para os padrões de qualidade de serviços da Informática. Em outras palavras, os gerentes da Informática podem até saber exatamente o que seus usuários esperam, porém nem sempre são capazes de estabelecer padrões de atendimento e qualidade compatíveis.

Gap 3 - é a diferença entre os padrões de qualidade dos serviços estabelecida para a área de Informática e a qualidade daquilo que é efetivamente entregue pela área aos seus usuários.

Gap 4 - é a diferença entre os serviços efetivamente entregues pela área de Informática e a comunicação (promessas) da própria área.

O trabalho resultou num instrumento para avaliar expectativas e percepções de clientes sobre a qualidade de serviços, chamado *Servqual*. Os tópicos deste instrumento estimam os pontos centrais da questão da qualidade em serviços, uma vez que esses pontos centrais transcendem e independem de específicas funções, áreas ou organizações.

Independentemente do tipo particular de serviço que está sendo avaliado, as 22 questões do instrumento são agrupadas em 5 dimensões de avaliação: Tangíveis, Confiabilidade, Capacidade de Resposta, Segurança e Empatia.

Para cada dimensão, a qualidade dos serviços é calculada pela diferença entre a avaliação da percepção e a da expectativa:

$$G_{\text{dimensão}} = P - E \xrightarrow{\text{onde}} P = \frac{\sum_{1}^{n} pi}{N}, E = \frac{\sum_{1}^{n} ei}{N},$$

$$G_{\text{Total}} = \frac{\sum_{1}^{5} G_{\text{dimensão}}}{5}$$

G = Percepção - Expectativa

3.4 PERCEPÇÃO DE LIDERANÇA

Em 1983, James M. Kouzes e Barry Z. Posner iniciaram um estudo para saber o que as pessoas faziam quando se encontravam em sua melhor fase no tocante à liderança de outras pessoas.

A pesquisa foi conduzida por meio de estudos de casos em que as pessoas contavam suas melhores experiências pessoais de liderança e entrevistas aprofundadas com gerentes de nível médio e alto em organizações dos setores público e privado.

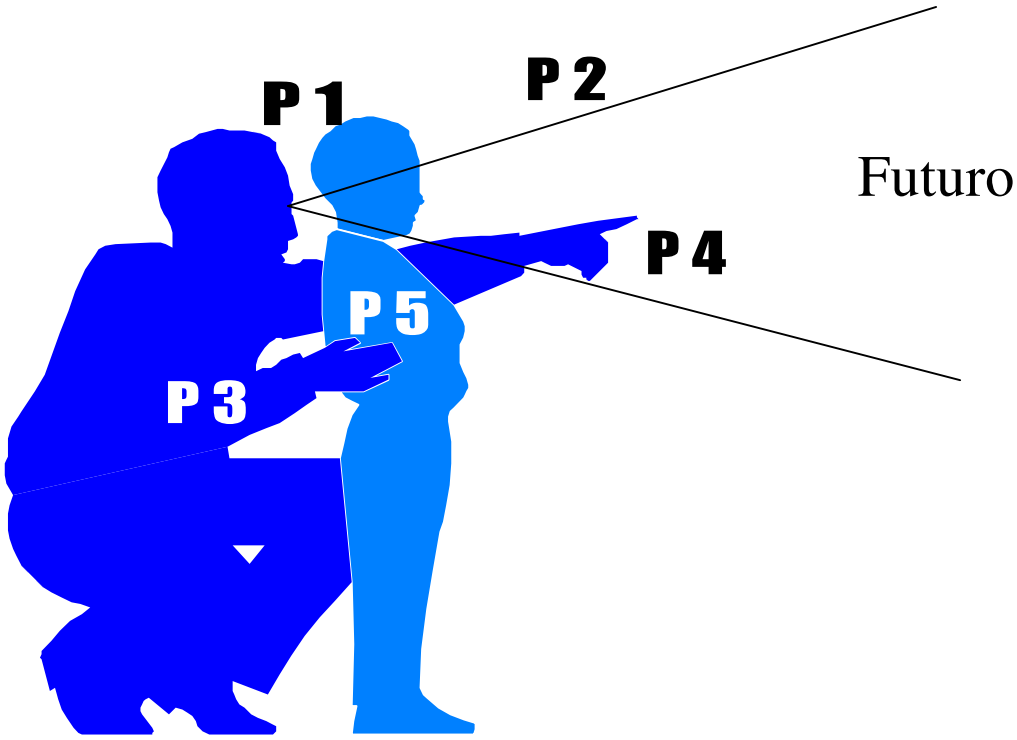
Até 1987, foram coletados mais de 550 estudos de casos das melhores experiências pessoais. Estudos posteriores têm registrado milhares de outros casos incluindo líderes comunitários, estudantes, religiosos e governamentais, além de centenas de outros em cargos não gerenciais (KOUZES e POSNER,1997).

Até 1995, os autores haviam realizado mais de 2500 estudos de caso. Realizaram, ainda, outros 500 estudos de pessoas que responderam a uma versão resumida do questionário de melhores experiências pessoais, e um total de mais de 300 entrevistas aprofundadas (KOUZES e POSNER, 1997).

A partir da análise dos melhores casos pessoais e das entrevistas aprofundadas, foi desenvolvido um modelo de liderança e um instrumento quantitativo - *Leadership Practices Inventory (LPI)* – com vistas a avaliar esta liderança pelos dados coletados.

Kouzes e Posner (2003) citam também, as cinco práticas que podem ser aprendidas e que conduzem à liderança:

- Apontar o caminho.
- Inspirar uma visão compartilhada.
- Desafiar o estabelecido.
- Permitir que os outros ajam.
- Encorajar o coração.



P1 - Prática 1 - O Líder costuma **desafiar as regras**, incentivando as mudanças, envolvendo seus colaboradores neste desafio.
P2 - Prática 2 - O Líder **inspira uma visão compartilhada** em toda a equipe, envolvendo seus colaboradores nesta visão de futuro.
P3 - Prática 3 - O Líder é uma pessoa que **permite que os outros ajam**, isto é, as iniciativas e ações espontâneas são bem aceitas e estimuladas.
P4 - Prática 4 - O Líder **aponta o caminho que deve ser seguido** pela equipe para alcançar melhores níveis de desempenho e relacionamento.
P5 - Prática 5 - O Líder procura **encorajar o coração** de seus subordinados, motivando-os para que enfrentem os obstáculos e desafios do dia-a-dia.

Figura 5 – Práticas de Liderança de KOUZES e POSNER
Fonte: KOUZES, James M. e POSNER, Barry Z. **O desafio da Liderança.** Rio de Janeiro: Campus, 1997.

Em seu papel mais importante, o líder eficaz é aquele capaz de criar condições para o florescimento da liderança em outros, identificando e cultivando líderes potenciais em todos os níveis. Como requisitos, enfrentar riscos, ter persistência para alcançar resultados desafiadores, ter coragem, ser ético, construir novos valores de gestão, fazer com que as pessoas se desenvolvam, ajudar as pessoas a encararem a realidade e mobilizá-las para que façam mudanças, são as responsabilidades do líder neste início de milênio, que ultrapassa tudo o que se falou e esperou dos líderes do passado. Pode se dizer que a função da Liderança Contemporânea não é a de evitar traumas sobre as pessoas, mas sim, minimizá-los e superá-los.

Assim sendo, as organizações necessitam propiciar ambientes qualitativos para facilitar condições adequadas às pessoas em desenvolver as competências tácitas e explícitas

no contexto da competitividade e produtividade pertinentes nas esferas locais e globais. Isto significa reter talentos e estimular as pessoas para compartilharem o conhecimento. Surgem questionamentos de como desenvolver essas competências pessoais no trabalho de equipes, quais seriam as condições ideais para manter a organização numa dinâmica competitiva, e como construir novos valores e dinamizar a cultura organizacional tornando-a flexível e adaptável ao novo cenário.

De acordo com Kouzes e Posner (2003), "A liderança é um relacionamento entre os que aspiram a liderar e os que optam por seguir".

3.4.1 AS CARACTERÍSTICAS MAIS ADMIRADAS DA LIDERANÇA

Conforme os autores, são sete as qualidades que as pessoas "mais procuram e admiram em um líder, alguém cuja direção eles seguiriam de bom grado". O que eles esperam de um líder que seguiriam não porque "têm de seguir", mas sim porque "desejam seguir".

Acredita-se que o indivíduo deve se submeter a diversos testes fundamentais para que as outras pessoas se mostrem dispostas a lhe conceder o título de líder.

Algumas das outras qualidades também aparecem, mas o que as pessoas mais procuram e admiram em um líder tem sido constante. Como os dados mostram claramente, para que as pessoas sigam alguém de bom grado, a maioria dos seguidores precisa acreditar que o líder:

- É honesto
- Tem visão de futuro
- É competente
- É inspirador

O resultado desta pesquisa encontra-se na tabela 3:

Tabela 3. Características dos Líderes Admirados

	Percentual dos Informantes que selecionaram as características		
Característica	Edição de 2002	Edição de 1995	Edição de 1987
HONESTO	88	88	83
TEM VISÃO DE FUTURO	71	75	62
COMPETENTE	66	63	67
INSPIRADOR	65	68	58
Inteligente	47	40	43
Justo	42	49	40
Liberal	40	40	37
Atencioso	35	41	32
Franco	34	33	34
Confiável	34	33	34
Cooperativo	28	28	25
Determinado	24	17	17
Imaginativo	23	28	34
Ambicioso	21	13	21
Corajoso	20	29	27
Zeloso	20	23	26
Maduro	17	13	23
Leal	14	11	11
Autocontrole	8	5	13
Independente	6	5	10

Nota: Esses percentuais representam entrevistados de seis continentes: África. América do Norte. América do Sul. Ásia. Europa e Austrália. A maioria. porém. é dos Estados Unidos. Como pedimos às pessoas que selecionassem sete características. a soma total dá 700%.

Fonte: KOUZES, James M. e POSNER, Barry Z. **O desafio da Liderança.** Rio de Janeiro: Campus, 2003.

3.4.2 AS REGRAS BÁSICAS DA LIDERANÇA

As cinco regras básicas da liderança exemplar e as características dos líderes admirados são perspectivas complementares da mesma questão. Quando dão o melhor de si, os líderes fazem mais do que simplesmente obter resultados. Respondem também à expectativa de seus seguidores, o que enfatiza o argumento de que a liderança é um relacionamento e que esse relacionamento envolve servir a um propósito e servir às pessoas.

Os autores apresentam as seguintes regras:

- **Ser honesto**

O fato de quase 90% dos seguidores desejarem que seus líderes sejam honestos acima de tudo é uma mensagem que os líderes devem internalizar e guardar de cor e salteado.

Ninguém gosta de ser enganado ou iludido. Queremos saber a verdade. Queremos um líder que saiba distinguir o certo do errado. Sim, queremos que nossa equipe vença, mas não queremos ser liderados por uma pessoa que trapaceia para obter a vitória. Queremos que nossos líderes sejam honestos porque sua honestidade é um reflexo de nossa honestidade.

- **Ter visão de futuro**

Por capacidade de *vislumbrar o futuro,* as pessoas não se referem ao poder mágico de um visionário presciente. Ao contrário, a realidade é muito mais sensata: trata-se da capacidade de estabelecer ou escolher o destino para o qual a empresa, órgão governamental, congregação ou comunidade deve caminhar.

- **Ser competente**

A *competência de liderança* refere-se ao histórico do líder e à sua capacidade de fazer o que tem de ser feito. É o tipo de competência que inspira a confiança de que o líder conseguirá guiar a organização inteira, grande ou pequena, na direção certa.

O líder precisa ter a capacidade de extrair o melhor dos outros permitir que os outros ajam.

- **Ser inspirador**

Os líderes inspiradores falam diretamente à nossa necessidade de ter significado e propósito na vida. Além disso, seu otimismo quanto ao futuro dá esperança às pessoas. O entusiasmo e o arrebatamento são essenciais e demonstram o compromisso pessoal do líder em buscar essa meta.

- **Credibilidade, o fator básico**

Ser honesto, capaz de antecipar o futuro, inspirador e competente: essas características têm sido constantes. Mas, acima de tudo, os líderes devem ter credibilidade.

A credibilidade é o alicerce da liderança.

Se não acreditarmos no mensageiro, não acreditaremos na mensagem.

Algumas respostas obtidas:

- "Eles praticam o que pregam."
- "Eles agem de acordo com o que dizem."
- "Seus atos são coerentes com suas palavras."
- "Eles fazem o que dizem que vão fazer."

Essas respostas simplesmente mostraram como a demonstração de um exemplo é essencial para a credibilidade do líder.

3.4.3 O *LEADERSHIP PRACTICES INVENTORY (LPI)*

O LPI - Leadership Practices Inventory - é um instrumento quantitativo que permite avaliar os comportamentos de liderança da pessoa, proporcionando *feedback* para fortalecer sua capacidade de liderança.

Ele contém 30 declarações - seis itens para avaliar cada um dos cinco princípios básicos de liderança - com dois tipos de formulários: um para a própria pessoa e outro para o observador.

O LPI baseia-se nas respostas do Questionário de Melhores Experiências Pessoais de Liderança e entrevistas em profundidade, feitas com gerentes dos níveis médio e alto das organizações em uma variedade de empresas públicas e privadas em todo o mundo.

Com os resultados obtidos dos estudos de caso e as entrevistas em profundidade, foram feitas declarações que descrevem cada uma das várias ações e comportamentos de liderança segundo os cinco princípios básicos da liderança:

Cada princípio contém seis declarações:

Desafiar o Estabelecido
• Procura desafios e oportunidades que testem as habilidades e o talento de cada um • Mantém a equipe atualizada com as principais e mais recentes mudanças da organização • Desafia (questiona) os caminhos existentes para a realização do trabalho • Está atento para inovações que podem melhorar a organização e o projeto • Pergunta "O que nós podemos aprender?" quando as coisas não saem conforme o planejado • Avalia os riscos de novos procedimentos e abordagens quando existe chance de falha
Inspirar uma Visão Compartilhada
• Descreve um futuro que todos desejam criar • Envolve a equipe, tornando único entre líder e liderados os sonhos de futuro • Possui uma comunicação clara, positiva e promissora sobre o futuro da organização • Mostra à equipe como futuro de longo prazo, os objetivos que podem ser alcançados através de uma visão de futuro comum • Olha à frente e para as previsões quanto ao futuro da organização e dos acontecimentos do projeto • É motivador e entusiasta sobre as possibilidades futuras
Permitir que os Outros Ajam
• Envolve a todos no planejamento, decisões e ações que estão ocorrendo ou são necessárias • Trata a todos com dignidade e respeito • Fornece à equipe autoridade para tomar suas próprias decisões • Desenvolve um ambiente de equipe com relações de cooperação entre os participantes • Cria uma atmosfera de confiança mútua entre os participantes da equipe • Possibilita à equipe uma sensação de donos do projeto em que estão trabalhando
Apontar o Caminho
• É claro quanto à forma de pensar sobre liderança • Mantém os projetos orientados dentro dos prazos previstos e as metas planejadas • Dedica tempo e energia para disseminar valores e crenças referentes à organização • Permite que a equipe conheça seus valores e suas crenças sobre a qual a melhor forma de conduzir os projetos e a organização • Apresenta coerência entre a prática e o discurso • Assegura que o trabalho de equipe tem objetivos claros, com etapas e metas bem definidas que sejam de conhecimento de todos
Encorajar o Coração
• Dedica um tempo para comemorar e recompensar as vitórias (objetivos atingidos) com toda a equipe envolvida • Assegura que a equipe é reconhecida por suas contribuições para o sucesso dos projetos • Elogia a equipe quando um trabalho é bem feito • Valoriza os esforços e as contribuições da equipe, dando suporte às atividades • Procura formas de celebrar o sucesso dos projetos • Divulga para o resto da organização os resultados obtidos e a importância da participação de cada membro da equipe

Figura 6: Declarações do LPI segundo os Princípios Básicos da Liderança
Fonte: Adaptado de KOUZES, J. M. e POSNER, B. Z. **O desafio da Liderança**. Rio de Janeiro: Campus, 1997

As declarações foram modificadas ou incluídas, após longas discussões e repetidas sessões de *feedback* com os entrevistados e com peritos em vários assuntos e análises empíricas de vários conjuntos de declarações baseadas em comportamentos.

3.5 PERCEPÇÃO DE SEGUIDORES

Conforme Kelley (1993), podem ser consideradas três impressionantes observações sobre líderes e seguidores:

- Os líderes contribuem, em média, com não mais que 20% do sucesso da maioria das organizações.
- Os seguidores, com os 80% restantes.
- A maioria das pessoas, não importa quão impressionante possa ser sua posição ou salário, passam mais tempo trabalhando como seguidores do que como líderes; isto é, gastamos mais tempo nos dirigindo a outras pessoas do que tendo outras pessoas se dirigindo a nós.

3.5.1 SE HOUVER PESSOAS QUE LIDEREM, OS LÍDERES SEGUIRÃO

Kelley (1993) não se refere às pessoas que sabem como agir sem que lhes seja dito como; às pessoas que agem com inteligência, independência, coragem e um forte senso de ética. Ele está interessado no que separa seguidores exemplares dos que perpetuam os estereótipos negativos.

Acredita que o valor dos seguidores para qualquer organização é enorme. Sem seus exércitos, afinal de contas, Napoleão seria apenas um homem com ambições grandiosas.

Conclui que os seguidores são tão importantes quanto os lideres e, algumas vezes, até mais.

- **O mito da liderança**

Os seguidores não só determinam se alguém será aceito como líder, mas também se esse líder será eficiente. Seguidores eficientes representam um ponto forte para o sucesso de um líder ou de uma organização.

- **O alto preço da veneração dos líderes**

No mínimo, o mito da liderança incita as pessoas a diminuir suas defesas na presença dos líderes. Quando as falhas do líder estão encobertas, os seguidores podem depositar sua confiança nele sem garantias. As pessoas se prestam a abusos a que, de outra forma, não se prestariam. Quando a sociedade confere o poder em favor do mito, isso pode rapidamente gerar a tirania.

Ninguém parece se importar em ser rotulado de líder, e as pessoas também não se importam em rotular seu líder; mas, mesmo falando sobre seus líderes, as pessoas ficam relutantes em ser consideradas seguidores.

- **Por que os mitos dos seguidores satisfazem**

Na verdade, seguidores e líderes representam dois conceitos separados, dois papéis distintos. São dois caminhos para a contribuição em organizações; caminhos complementares, e não competitivos. Nenhum desses dois papéis monopoliza o poder de pensamento, motivação, talento ou ação. Qualquer um deles pode ter como resultado alcançar prêmios ou falhar. Os maiores sucessos requerem que as pessoas em ambos os papéis desempenhem funções de modo excelente. Devemos ter grandes líderes *c* grandes seguidores.

Conta Kelley (1993) que sem os seguidores, pouco é feito; com eles, montanhas podem ser removidas. Os seguidores de Jesus - esses heróis não reconhecidos trabalharam duro para fazer a diferença. Sem eles, Jesus teria sido como muitos de seus contemporâneos, apenas uma outra 'voz que clama no deserto'. Com eles, mudou o curso da história.

Os seguidores, como descobriu, participam com entusiasmo, inteligência e autoconfiança - mas sem brilho - da busca pelos objetivos das organizações. Estão unidos por suas decisões individuais de fazerem um sonho particular ou coletivo tomar-se realidade.

- **Precisamos de seguidores exemplares**

Sem os seguidores, a liderança não tem significado algum e os líderes simplesmente não existem. Sinônimos para seguidores - associados, colegas, co-aventureiros, camaradas, companheiros, cidadãos corporativados, membros, jogadores de um time - não captam o sentido de como líderes e seguidores estão ligados uns aos outros.

A estrutura social depende dos seguidores; sem eles, a sociedade se desfaz. Por isso, a questão não é *se* se deve ter seguidores, mas que *tipo* de seguidores se deseja. Acho que o que se quer são os *bons* seguidores - pessoas que tomam atitudes certas com grande habilidade e realização.

Da democratização global ao coletivismo, a sociedade está se tornando cada vez mais dependente dos seguidores para a obtenção do sucesso. Precisa-se de pessoas não só de boa vontade, mas também capazes de desempenhar bem o seu papel.

3.5.2 IDENTIFICANDO SEU ESTILO DE SEGUIR

Uma vez que a maioria de nós passa a maior parte do tempo no papel de seguidores, é óbvio que o modo como desempenhamos este papel determina, na maior parte das vezes, o quanto estamos satisfeitos com nossa vida profissional diária. As pesquisas mostram que as pessoas que desempenham um bom papel em seu trabalho geralmente se sentem melhor em relação a suas vidas do que as pessoas que não estão felizes com seu desempenho profissional.

Estilo de seguir	**Pontuação para *Pensamento Independente***	***Pontuação para ajuste ativo***
EXEMPLAR	Alto	Alto
ALIENADO	Alto	Baixo
CONFORMISTA	Baixo	Alto
PRAGMÁTICO	Médio	Médio
PASSIVO	Baixo	Baixo

Quadro 3 – Estilos de seguir
Fonte: KELLEY, Robert – **O Poder dos Seguidores.** São Paulo: Siciliano, 1993.

Localizar a posição de cada um nela fornecerá duas vantagens:

- A primeira delas é que se poderá identificar o estilo de seguir.
- A segunda vantagem é que se tem um guia do que se pode fazer para melhorar as habilidades como seguidor. Assim, os resultados do questionário se tornam tanto descritivos quanto prescritivos.

Kelley (1993) demonstra que todos os tipos de seguidores podem ser transformados em seguidores exemplares, que são os ideais para a organização.

3.5.3 - AS HABILIDADES DOS SEGUIDORES EXEMPLARES

Os seguidores exemplares diferem dos outros seguidores, pois têm bom desempenho em ambas as dimensões fundamentais do seguir: por um lado, usam o pensamento crítico, independente, diferentemente do líder ou do grupo. Os líderes e os colegas de trabalho os descrevem como pessoas que 'pensam por si mesmas'. Eles 'são autênticos', são 'inovadores e criativos', 'fazem críticas construtivas' e 'são capazes de enfrentar seus líderes'.

Por outro lado, os seguidores exemplares estão ativamente ajustados à organização e usam seus talentos em prol dela, mesmo quando se vêem frente a frente com futilidades burocráticas ou colegas de trabalho não produtivos. Dizem que eles 'tomam iniciativas', 'assumem seus domínios', 'participam ativamente', 'começam sozinhos na vida', 'apóiam o grupo e o líder', 'são extremamente competentes' e 'vão além da tarefa que lhes é dada'.

Os seguidores exemplares empenham seus talentos, e inclusive seu cérebro, para trabalhar pela organização e seus líderes às vezes complementando os esforços do líder, outras o aliviando de muitas tarefas. Seguidores menos eficientes falham nesta dimensão porque seguem desanimadamente através das mudanças.

Os seguidores exemplares possuem um repertório de habilidades e valores que podem ser tanto aprendidos quanto dados; e que podem ser divididos em três amplas categorias:

- **Habilidades profissionais** - como os seguidores exemplares ajudam com:
    - suas observações e seu empenho
    - sua competência em atividades críticas
    - sua iniciativa em ajudar a organização

- **Habilidades empresariais** - como os seguidores exemplares criam e movimentam uma teia de relações na organização com:
    - membros do grupo
    - redes empresariais
    - líderes

- **Componente de valores** - como os seguidores exemplares usam uma consciência corajosa que guia suas atividades profissionais e relacionamentos na empresa.

3.5.4 A INICIATIVA AO ACRESCENTAR SEU VALOR À ORGANIZAÇÃO

Ao terem suas tarefas sob controle, os seguidores exemplares não ficam apenas observando. Se têm tempo, procuram outras atividades relacionadas à linha mestra e que geralmente se encaixam em três categorias:

- Desenvolver habilidades adicionais.
- Aumentar seu raio de ação nas atividades de linha mestra.
- Patrocinar novas idéias.

Os reais seguidores superam o obsoletismo profissional investindo em pesquisa e desenvolvimento pessoais. Isto significa envolver-se em contínua educação.

Seguidores menos eficientes esperam que o treinamento e o desenvolvimento venham até eles. Se a companhia não se dispuser a pagar um seminário, reclamarão, recusando-se a pagar. Sem atenção paternalista, sua competência diminui. E depois ficam surpresos quando não se lhes dá mais valor.

Os direitos e responsabilidades do seguidor exemplar forjarão muito do futuro dos seguidores.

3.6 SUMÁRIO CONCLUSIVO DO CAPÍTULO

Este capítulo apresentou os referenciais teóricos utilizados como base para as investigações propostas por esta pesquisa.

4 METODOLOGIA

4.1 SUMA DO CAPÍTULO

Este capítulo trata dos procedimentos da metodologia que foi utilizada para elaboração da presente pesquisa, que como já foi citado, teve o objetivo de testar as hipóteses e questões levantadas no presente estudo, fazendo uma avaliação da Percepção de Segurança em Sistemas de Informação e sua relação com a Qualidade Percebida de Serviços, Perfil de Liderança e Perfil dos Seguidores.

4.2 TIPO DE PESQUISA

Existem alguns critérios para a classificação dos tipos de pesquisa e estes variam de acordo com o enfoque dado pelo autor.

Conforme a classificação proposta por Ander-Egg, 1978 (apud LAKATOS e MARCONI, 1999), esta pesquisa pode ser classificada quantos aos fins, como pesquisa aplicada e descritiva.

- **Aplicada -** se caracteriza pelo interesse prático, os resultados são utilizados na solução de problemas que ocorram na realidade.
- **Descritiva -** aborda quatro aspectos: descrição, registro, análises e interpretação do problema; e tem seu objetivo em seu funcionamento no presente.

De acordo com os fundamentos propostos por Marconi e Lakatos (1999), esta dissertação pode ser classificada, quanto aos meios, como:

- **pesquisa de campo** - porque é utilizada com o objeto de conseguir informações ou conhecimentos sobre o problema, para o qual procuramos uma resposta, através de fatos e fenômenos tal como ocorrem espontaneamente, na coleta de dados a eles referentes e no registro de variáveis que se presumem relevantes para analisá-las;

- **exploratória** - porque visa à formulação do problema, com a finalidade de desenvolver hipóteses, aumentar a familiaridade do pesquisador com um ambiente, fato ou fenômeno, para a realização de pesquisas futuras ou modificar e clarificar conceitos.

A pesquisa também apresenta características de pesquisa ação. Segundo Quintella (1994), o objetivo da pesquisa ação é desenvolver novas aptidões com a aplicação direta do estudo ao mundo real.

As características da pesquisa de ação são:

- Ser de natureza prática e diretamente relevante a uma atuação real no mundo do trabalho – Neste modelo, o problema é totalmente prático e a análise feita pode auxiliar as empresas a desenvolverem práticas e programas que poderão promover as habilidades de liderança e de maior conhecimento das necessidades dos clientes.
- Ser de natureza empírica por estar apoiada em observações reais de opinião e de comportamento - As hipóteses e as questões-chave desta pesquisa estão apoiadas nas situações reais que vivem as empresas e nos itens dos questionários utilizados.
- Prover uma estrutura ordenada para resolução de problemas e novos desenvolvimentos - A dissertação está estruturada em hipóteses e questões-chave que são analisadas com base nos questionários respondidos pelas empresas e seus clientes, que nos permitem fazer novas formulações para a realização de uma pesquisa futura.
- Ser flexível e adaptável, permitindo mudanças durante o período de experimentação e sacrificando o conceito de controle sobre variáveis em favor de experimentações locais e inovações nos métodos de investigação e coleta de resultados.

4.3 MÉTODO DE ABORDAGEM

Para esta pesquisa, o foi utilizado o método hipotético-dedutivo. Foi proposto por Karl Popper (1902-94), professor da Universidade de Londres, a quem se associa o

"Racionalismo Critico" que é uma linha do pensamento filosófico que encoraja um estilo de pensar direcionado para problemas concretos, num sentido prático, buscando soluções efetivas.

Também, de acordo com Lakatos e Marconi (1991), o método hipotético-dedutivo se inicia pela percepção de uma lacuna nos conhecimentos, acerca da qual se formulam as hipóteses e, pelo processo de inferência dedutiva, testa a predição da ocorrência de fenômenos abrangidos pela hipótese, como mostra a figura 7.

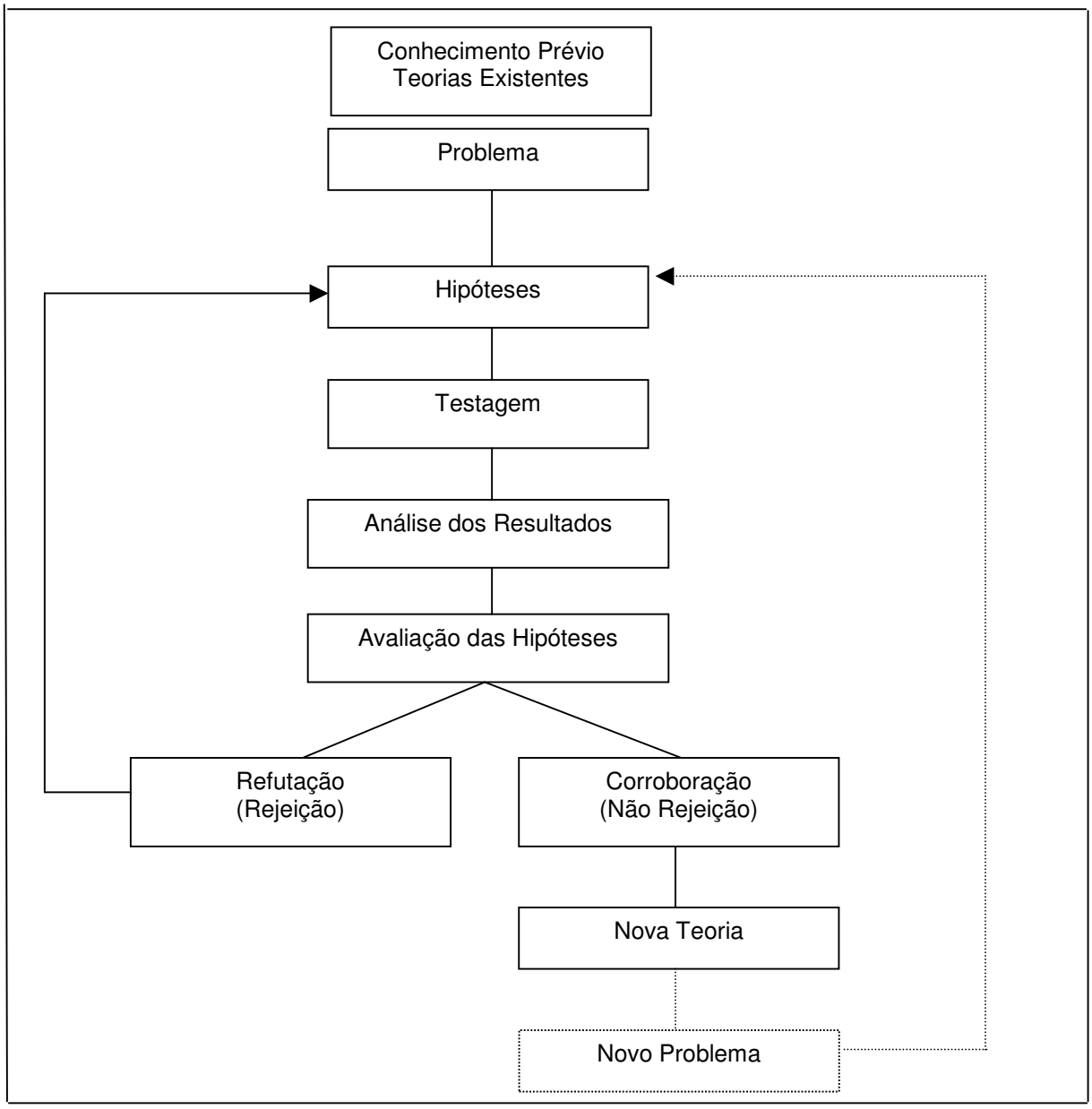


Figura 7: Método hipotético dedutivo segundo Popper
Fonte: Adaptado de Lakatos, E. M. & Marconi, M.A. **Metodologia Científica.** São Paulo: Atlas, 1991**.**

Para o presente trabalho de pesquisa, serão utilizados os métodos monográfico, comparativo e estatístico. Segundo Lakatos e Marconi (1991):

- **O método monográfico** consiste no estudo de determinados indivíduos, profissões, condições e instituições, grupos ou comunidades com a finalidade de obter generalizações.

  Nesta dissertação, serão estudadas a percepção de segurança dos sistemas de informação, a qualidade percebida dos serviços dos sistemas de informação, o perfil de liderança e o perfil dos seguidores, no âmbito das diretorias do Inmetro.

- **O método comparativo** realiza comparações com a finalidade de verificar similaridades e explicar divergências.

  Serão feitas comparações entre as percepções de segurança, de qualidade dos serviços e os perfis de liderança e seguidores, com o intuito de observar as possíveis divergências.

- **O método estatístico** reduz os fenômenos sociais, políticos, econômicos, etc. a termos quantitativos e a manipulação estatística permite comprovar as relações dos fenômenos entre si, e obter generalizações sobre sua natureza, ocorrência ou significado.

  Nesta dissertação, serão utilizadas como população, os usuários de sistemas de informação de cada diretoria do Inmetro, para observar as relações entre segurança da informação, percepções da qualidade do serviço, práticas de liderança e o perfil dos seguidores.

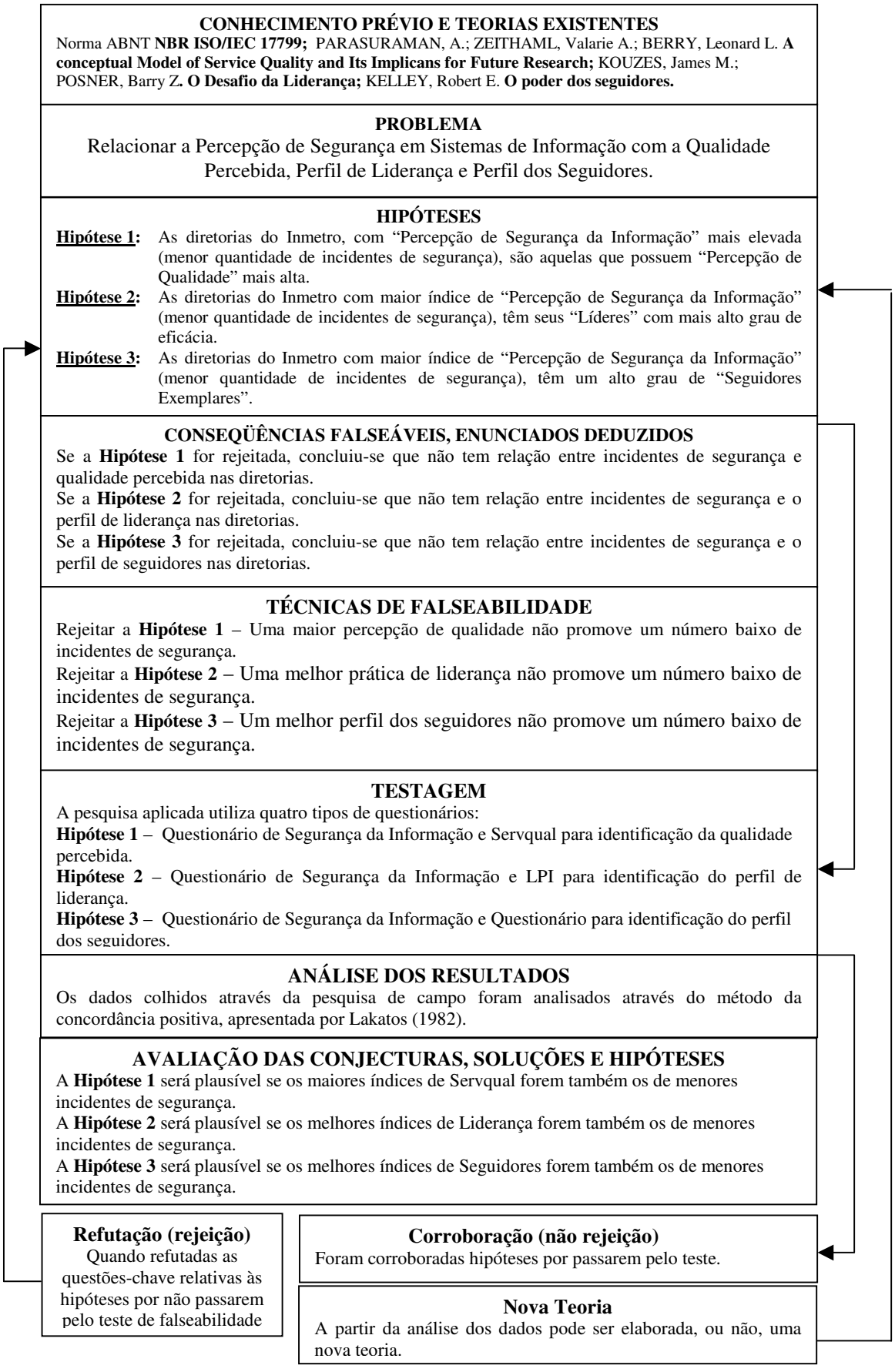


Figura 8 – Aplicação do Método Hipotético-dedutivo ao presente estudo.
Fonte: Elaboração própria, adaptada de Popper (1975).

4.4 ANÁLISE DAS HIPÓTESES

4.4.1 TIPOLOGIA

Segundo a classificação de Selltiz *et al.,* 1967 (apud LAKATOS e MARCONI, 1991), as hipóteses formuladas nesta dissertação podem-se classificar, quanto à freqüência, em hipóteses que podem afirmar que algo é maior, menor ou igual que outras coisas, ao estabelecer relações de diferença.

Segundo a classificação de Goode e Hatt, 1968 (apud LAKATOS e MARCONI, 1991), as hipóteses desta dissertação podem ser classificadas, quanto à ordem crescente de abstração, em hipóteses que se referem a tipos ideais complexos, que visam verificar a existência de relações logicamente derivadas entre uniformidades empíricas.

As hipóteses nesta dissertação foram formuladas para testar as relações (correlação ou não):

- H1 - da percepção de segurança da informação com a percepção de qualidade do serviço;

- H2 - da percepção de segurança da informação com o perfil de liderança;

- H3 – da percepção de segurança da informação com o perfil dos seguidores.

4.4.2 FUNDAMENTAÇÃO

Baseados nos fundamentos das hipóteses propostos por Lakatos e Marconi (1991), as hipóteses desta dissertação podem se fundamentar em:

- Hipóteses que se referem a conjuntos de unidades com mais de um elemento, porque nos referimos ao Inmetro e suas diretorias (unidades) e vários elementos

(segurança da informação, percepção de qualidade, perfil de liderança e perfil de seguidores).

- Hipóteses que se referem a proposições cujas unidades se distribuem probabilisticamente num espaço de variáveis, porque elas podem mudar de uma qualidade deficiente a uma qualidade excelente do serviço.

4.5 VALIDAÇÃO DAS HIPÓTESES

4.5.1 TESTE DE IMPORTÂNCIA

Segundo a importância das hipóteses proposta por Kerlinger, 1980 (apud LAKATOS e MARCONI, 1991), as hipóteses desta dissertação foram formuladas porque elas:

- São instrumentos de trabalho da teoria, pois novas hipóteses podem dela ser deduzidas.
- Podem ser testadas e julgadas como provavelmente verdadeiras ou falsas.
- Constituem instrumentos poderosos para o avanço da ciência, pois sua comprovação requer que se tornem independentes dos valores e opiniões dos indivíduos.
- Dirigem a investigação, indicando ao investigador o que procurar ou o que pesquisar.
- Pelo fato de serem comumente formulações regionais gerais, permitem ao pesquisador deduzir manifestações empíricas específicas, com elas correlacionadas.
- Desenvolvem o conhecimento cientifico, auxiliando ao investigador a confirmar (ou não) sua teoria.
- Incorporam a teoria (ou parte dela) em forma testável ou quase testável.

4.5.2 TESTE DE NECESSIDADE

Segundo a necessidade das hipóteses proposta por Bunge, 1976 (apud LAKATOS e MARCONI, 1991), as hipóteses desta dissertação se fazem necessárias quando:

- Tentamos resumir e generalizar os resultados de nossas investigações.
- Tentamos interpretar generalizações anteriores.
- Tentamos justificar, fundamentando, nossas opiniões.
- Planejamos um experimento ou investigação para a obtenção de mais dados.
- Pretendemos submeter uma "conjectura" a comprovação.

4.6 ALVO DA PESQUISA

Esta pesquisa teve como alvo o Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO, pois ela foi um estudo de caso.

4.6.1 POPULAÇÃO

Neste estudo, a população foi representada pelos funcionários com acesso aos sistemas de informação, dentro das respectivas diretorias do Inmetro, situadas no Rio de Janeiro e em Xerém, Duque de Caxias.

4.6.2 AMOSTRA

Segundo Mattar (1994), há uma grande variedade de tipos de amostras e de planos de amostragem possíveis de se utilizar, mas uma diferenciação fundamental deve ser efetuada entre amostragens probabilísticas e não probabilísticas:

- **Probabilística**: é aquela em que cada elemento da população tem uma chance conhecida e diferente de zero de ser selecionado para compor a amostra.

- **Não probabilística**: é aquela em que a seleção dos elementos da população para compor a amostra depende, ao menos em parte, do julgamento do pesquisador ou do entrevistador no campo. Não há chance conhecida de que um elemento qualquer da população possa fazer parte da amostra.

Para a escolha do processo de amostragem, deve-se levar em conta, dentre outros:

- Tipo de pesquisa;
- Acessibilidade aos elementos da população;
- Disponibilidade ou não de ter os elementos da população em um rol;
- Representatividade desejada ou necessária;
- Oportunidade apresentada pela ocorrência de fatos ou eventos;
- Disponibilidade de tempo;
- Recursos financeiros e humanos.

A amostra empregada neste trabalho pode ser classificada das duas formas. Como uma amostra não-probabilística, quando se buscou incluir na amostra os principais atores do cenário em estudo e que sejam representativos do universo em questão, ou seja, buscou-se respondentes que fossem diretores ou chefes de diretorias. E como amostra probabilística, quando se buscou a inclusão dos usuários dos sistemas, ou seja, os funcionários da diretoria.

Nas diretorias onde o número total de sujeitos da amostra (n) apresentou um tamanho de "$n<30$", e por isso, considerada como uma pequena amostra, o estudo foi baseado nas distribuições amostrais de estatísticas de pequenas amostras, denominado "teoria das pequenas amostras" (SPIEGEL, 1993).

4.7 RESPONDENTES

Foram os seguintes os profissionais selecionados como respondentes:

- Diretores
- Gestores de Sistemas
- Usuários dos sistemas

4.8 INSTRUMENTOS DE MEDIDA UTILIZADOS

Utilizou-se como referencial de medida, os seguintes instrumentos:

- Para avaliação da segurança da informação, um questionário baseado na Norma ABNT NBR ISO/IEC 17799:2001, no CERT.BR e na experiência do autor como Administrador da Rede de Computadores do Inmetro.
- Para avaliação da qualidade do serviço, o questionário extraído de Zeithaml et al. (1990) – *Servqual*
- Para avaliação das práticas de liderança, o questionário apresentado por Kouzes e Posner (1997) - LPI Leadership Practices Inventory
- Para avaliação do perfil dos seguidores, o questionário extraído de Kelley (1993) – O Poder dos Seguidores

4.9 COLETA DE DADOS

A coleta de dados foi realizada através da aplicação de questionários específicos, buscando-se reconhecer se os entrevistados percebem a importância nos aspectos apresentados. O contato inicial deu-se através de e-mail, onde foi solicitada aos participantes a colaboração no desenvolvimento da pesquisa através do preenchimento dos questionários.

Todos os participantes foram informados, na ocasião do contato inicial, que se tratava de uma pesquisa científica com propósitos acadêmicos.

Inicialmente foi realizado um pré-teste sobre o preenchimento dos questionários, com objetivo de checar detalhes como o preenchimento; tabulação de respostas; e críticas a questões, antes do início das entrevistas.

A coleta de dados no campo foi feita em três etapas, a saber:

- A primeira etapa consistiu em pesquisa via e-mail com usuários das diretorias, utilizando o questionário baseado na Norma NBR ISO/IEC 17799 para medir o índice de incidentes de segurança da informação.

- A segunda etapa consistiria de entrevistas com diretores com dupla finalidade. Utilizando o questionário *Servqual*, para medir a qualidade do serviço prestado pelos sistemas de informação e utilizando o questionário LPI para mensurar as práticas de liderança, mas devido a problemas de disponibilidade dos diretores, esta etapa foi prejudicada e descartada.

- A terceira etapa constou de questionários dentro de um "portal web". Utilizando o questionário *Servqual*, para medir a qualidade do serviço percebido dos sistemas de informação, utilizando o questionário LPI para descobrir o perfil da liderança e por fim, um questionário sobre perfil dos seguidores para se medir o índice de seguidores exemplares.

Para facilitar esta pesquisa, a utilização do "portal web" foi fundamental. Nele, os usuários se conectavam para responder as perguntas dos questionários específicos de cada parte da pesquisa, sendo o controle de acessos feito através do logon de cada usuário, impedindo assim, redundância de respostas por parte de um mesmo usuário. O portal foi produzido pelo amigo e analista de sistemas do Inmetro, Gil F. do Almo (2005) e instalado num servidor de informação *web*, com acesso autorizado a todos os usuários da rede do Inmetro. Os dados eram armazenados automaticamente no banco de dados criado para a pesquisa, e somente os questionários respondidos completamente foram levados em consideração.

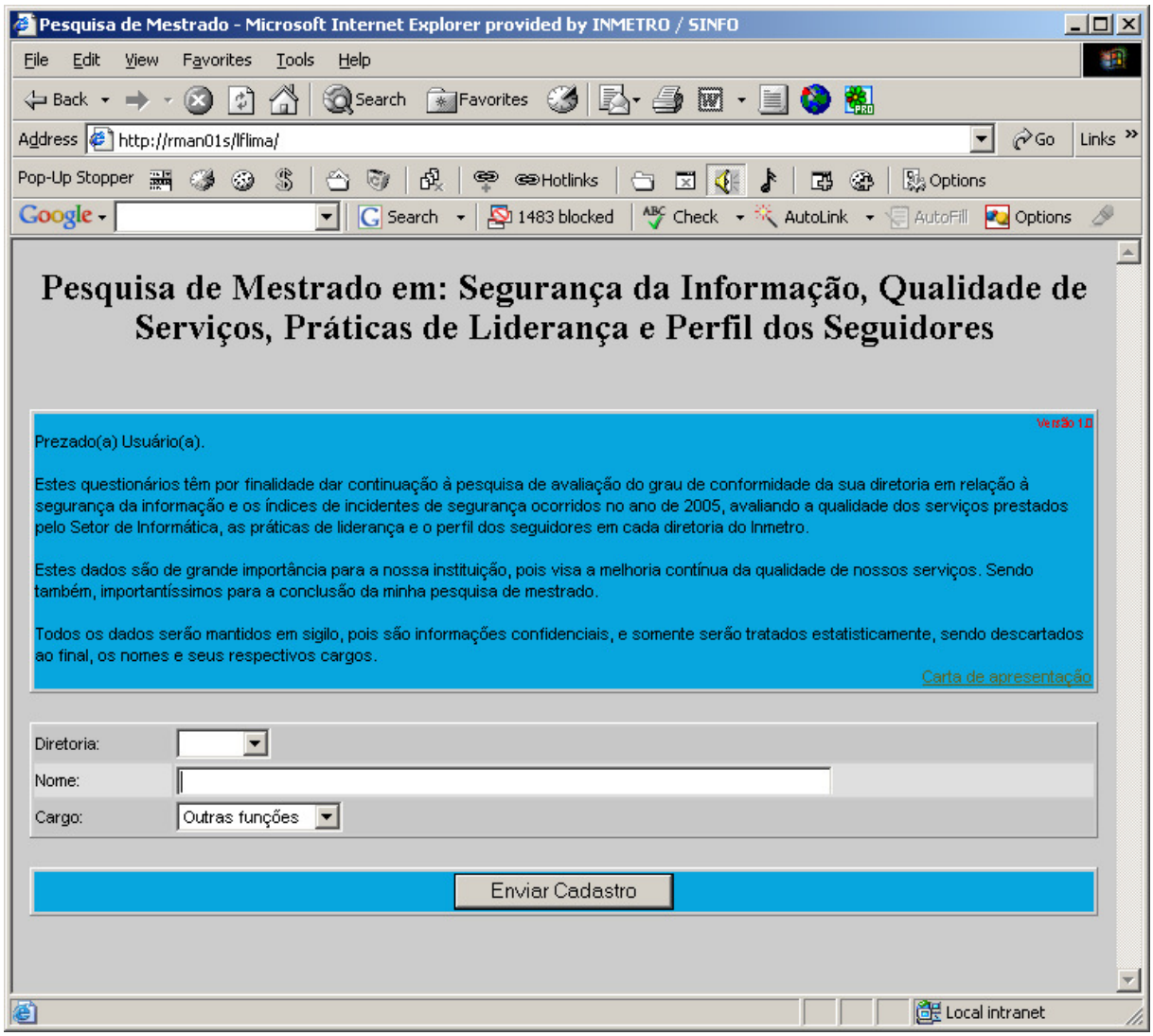


Figura 9: Página inicial do Portal Web da Pesquisa
Fonte: Almo (2005).

4.10 LIMITAÇÕES DO MÉTODO

A amostra disponível para ser utilizada, apesar de ser pequena, reflete a população de usuários de sistemas informatizados que se encaixam na condição definida para análise das hipóteses deste estudo, mas por mais adequado que tenha sido o planejamento e a execução do processo de amostragem, os resultados obtidos a partir de amostras raramente são iguais aos da população, não existindo garantia de que não haja distorção no resultado.

4.11 SUMÁRIO CONCLUSIVO DO CAPÍTULO

Este capítulo apresentou as premissas consideradas válidas para este trabalho de pesquisa, abordando um estudo sobre o tipo da pesquisa, sua classificação, o método de abordagem da pesquisa que é o hipotético-dedutivo baseado nas idéias de Karl Popper. Foram relacionados procedimentos e técnicas, a análise das hipóteses, sua validação, o teste de importância e necessidade. O tratamento estatístico da pesquisa: os alvos da pesquisa, a população, a amostra, os respondentes, o instrumento de medida utilizado, a forma de coleta de dados e as limitações do método.

5 RESULTADOS E ANÁLISE DOS CÁLCULOS

5.1 SUMA DO CAPÍTULO

Este capítulo trata dos resultados encontrados após a tabulação da pesquisa. Serão apresentados gráficos com as estatísticas das hipóteses e suas respectivas questões, e as considerações do autor sobre os resultados encontrados.

5.2 TESTE DAS HIPÓTESES

5.2.1 Hipóteses da pesquisa

- **Hipótese 1:** As diretorias do Inmetro, com "Percepção de Segurança da Informação" mais elevada (menor quantidade de incidentes de segurança), são aquelas que possuem "Percepção de Qualidade" mais alta.

- **Hipótese 2:** As diretorias do Inmetro com maior índice de "Percepção de Segurança da Informação" (menor quantidade de incidentes de segurança), têm seus "Líderes" com mais alto grau de eficácia.

- **Hipótese 3:** As diretorias do Inmetro com maior índice de "Percepção de Segurança da Informação" (menor quantidade de incidentes de segurança), têm um alto grau de "Seguidores Exemplares".

5.3 METODOLOGIA ESTATÍSTICA

O tratamento estatístico foi baseado nas respostas aos questionários de Segurança da Informação, Percepção de Qualidade, Percepção de Liderança e Percepção de Seguidores, na análise das médias (soma das observações divididas pelo número delas), de seus desvios padrões, da distribuição t (STUDENT) para pequenas amostras (n<30) e do coeficiente de correlação, para se determinar a falseabilidade ou não das hipóteses testadas.

Toda a pesquisa foi transcorrida ao nível de confiabilidade de 95%.

O software utilizado para a análise desses dados foi o Microsoft Excel 2000 e suas respectivas ferramentas estatísticas.

5.4 AS AMOSTRAS

Conforme a Norma ABNT 11154, de 1990, as amostras estão iguais ou maiores do que o mínimo permitido (5 itens) para os testes estatísticos aplicados nesta pesquisa.

As amostras foram retiradas aleatoriamente dentro da população finita de usuários dos sistemas de informação dentro de cada diretoria do Inmetro. Em todos os casos, as amostras atenderam aos requisitos da Norma ABNT.

Tabela 4: Quantidades das amostras da pesquisa por diretorias

DIRETORIAS:	POPULAÇÃO:	Amostras Seg. Info.	Amostras *Servqual*	Amostras Liderança	Amostras Seguidores
AUDIN	17	6	7	7	7
CAINT	29	9	6	6	6
CGCRE	76	19	14	14	14
CPLAN	134	35	37	37	37
DIMCI	223	31	17	17	17
DIMEL	111	28	17	17	17
DIRAF	218	20	20	20	20
DQUAL	98	30	21	21	21
GABIN	57	9	14	14	14
PROGE	31	5	7	7	7
Totais:	**994**	**192**	**160**	**160**	**160**

Fonte: Elaboração própria

Pode-se perceber a diferença entre as amostras dos respondentes do questionário de percepção de segurança da informação em relação aos outros. Isso ocorreu basicamente pela forma de resposta a este tipo de questionário, que foi através de documento enviado, em anexo ao e-mail, ou através de malote. Os outros questionários foram respondidos diretamente no portal web.

Abaixo, no gráfico, tem-se a porcentagem de cada espécie de questionário por diretoria:

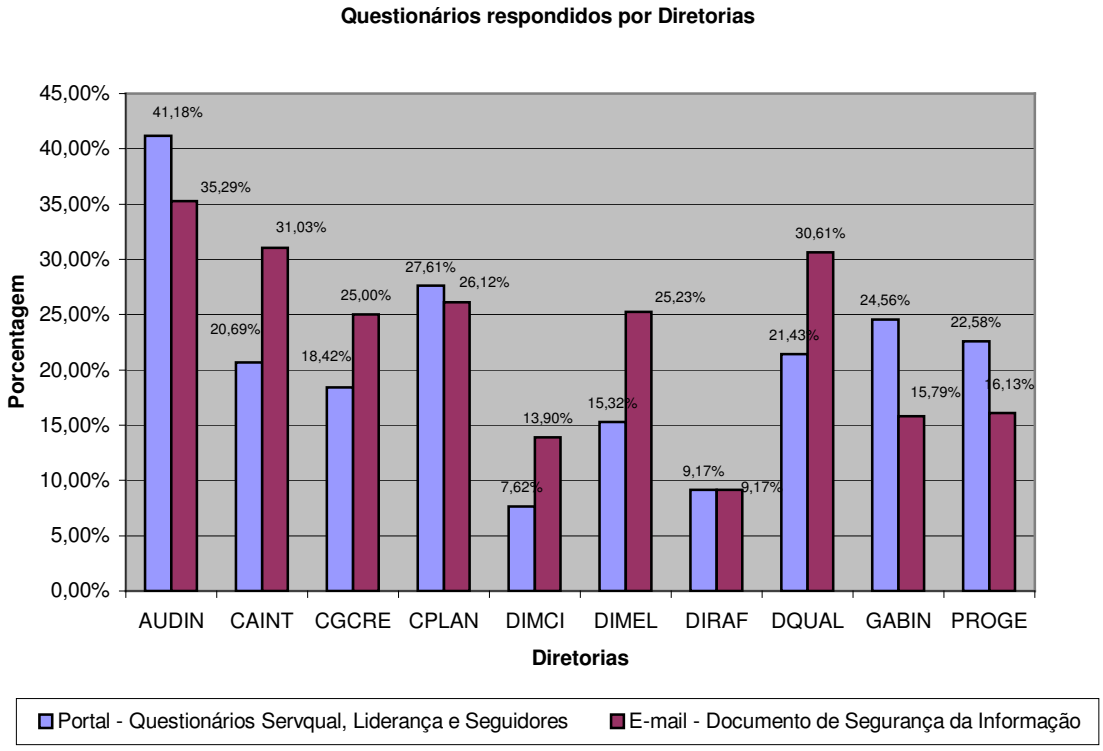


Gráfico 1: Porcentagem dos colaboradores da pesquisa por diretorias
Fonte: Elaboração própria

5.5 APRESENTAÇÃO E DISCUSSÃO DE RESULTADOS

Esta pesquisa fez uma comparação entre as diretorias do Inmetro, para corroborar ou refutar as hipóteses deste estudo.

5.5.1 TESTE DAS HIPÓTESES

Para a análise do resultado final, os testes das hipóteses desta pesquisa, trabalhou-se primeiramente nos cálculos dos índices de Percepção de Segurança da Informação (índice de incidentes de segurança), de Percepção da Qualidade dos Serviços (índice de *Servqual*), de Percepção de Liderança (índice do perfil de liderança) e da Percepção de Seguidores (índice do perfil dos seguidores). Estes índices foram calculados para cada diretoria da instituição, para que posteriormente fosse calculada e testada a respectiva hipótese do estudo.

5.5.2 CÁLCULO DO ÍNDICE DE INCIDENTES E ÍNDICE DE SEGURANÇA DA INFORMAÇÃO

Para este cálculo, foram tabulados os resultados da pesquisa obtida através das respostas, por meio de amostras aleatórias dos usuários, ao questionário de Segurança da Informação, dentro de cada diretoria. O questionário foi composto de perguntas sobre o conhecimento da Norma ABNT NBR ISO/IEC 17799, perguntas sobre os tipos de incidentes de segurança que ocorreram nas respectivas diretorias, no ano de 2005, e por perguntas sobre a quantidade total (estimada) ocorrida de incidentes de segurança neste período por diretoria.

Para fins desta pesquisa, para o cálculo do índice de incidentes de segurança, somente foram levadas em conta as respostas da quantidade de incidentes ocorridos. As outras respostas servem para ilustrar esta pesquisa e para iniciar, se alguém tiver interesse, um novo estudo posterior a este.

Os dados foram tratados estatisticamente pela distribuição **t** (distribuição de STUDENT), para pequenas amostras (n<30), mas de acordo com Anderson et al. (2003) ela não se restringe às pequenas amostras, podendo ser utilizada com o intuito de corroborar ou refutar as hipóteses de teste da média da população.

Conforme a Norma ABNT NBR 10536, sobre terminologia em estatística:

- ***Distribuição t – Distribuição de Student*** - Distribuição de um quociente de variáveis aleatórias independentes, cujo numerador é uma variável aleatória normal padronizada e o denominador é a raiz quadrada positiva do

quociente entre uma variável aleatória X^2 e o seu numero de graus de liberdade.

Conforme Anderson et al. (2003, p. 297):

- ***Distribuição t – Distribuição de Student*** – A distribuição não está restrita à situação de pequena amostra. Ela é aplicável sempre que a população é normal ou próxima à normal e sempre que o desvio-padrão da amostra é usado para estimar o desvio-padrão da população.

Após o teste de corroboração ou refutação da média, calculou-se o índice de segurança da informação (ISI), que é o inverso da média encontrada de incidentes de segurança em cada diretoria no ano de 2005, sendo esta, a forma de posicionar as unidades organizacionais em ordem de melhor percepção de segurança da informação.

5.5.2.1 AUDIN

Esta diretoria apresentou os seguintes resultados:

- Em relação ao conhecimento da Norma ABNT NBR ISO/IEC 17799, sobre Segurança da Informação, apresentou-se desta forma:

Tabela 5: Perguntas quanto ao conhecimento da Norma ABNT NBR ISO/IEC 17799.

QUESTÕES:	SIM	NÃO
1. Você muda sua senha periodicamente?	50,00%	50,00%
2. Você utiliza senha forte (caracteres alfanuméricos, especiais e mínimo de 8 ‘oito’ dígitos)?	50,00%	50,00%
3. Você anota sua senha em papel?	0,00%	100,00%
4. Você bloqueia sua estação de trabalho (computador) ao se afastar dela?	83,33%	16,67%
5. Você permite que alguém utilize sua senha para acesso a rede?	0,00%	100,00%
6. Você utiliza a opção de "scan" completo do antivírus, todos os dias?	33,33%	66,67%
7. Você monitora regularmente seu computador para reportar algo “suspeito”?	100,00%	0,00%
8. Você tem conhecimento sobre Segurança da Informação?	50,00%	50,00%
9. Você tem treinamento sobre Segurança da Informação?	0,00%	100,00%
10. Sua diretoria já teve algum incidente de segurança?	83,33%	16,67%
11. Sua diretoria tem algum plano de Segurança da Informação?	0,00%	100,00%

Fonte: Elaboração própria

Analisando as respostas pode-se notar que metade dos usuários muda periodicamente suas senhas, utilizam senhas “fortes” e têm conhecimento sobre Segurança da Informação. Trinta e três por cento deles forçam a opção de passar o antivírus por completo. Todos monitoram seus computadores para reportar algo suspeito e não anotam suas senhas em papel, nem permitem o acesso de outras pessoas com as suas senhas. Essa diretoria não tem nenhum plano de Segurança da Informação e também não treina seus usuários para este fim. Por fim, oitenta e três por cento dos usuários reportaram algum incidente de segurança.

- Em relação aos tipos de incidentes ocorridos nesta diretoria no ano de 2005:

Tabela 6: Freqüência dos diferentes tipos de incidente de Segurança da Informação

Quais os tipos de incidentes de segurança que ocorreram em sua diretoria, no ano de 2005?		
	Freq.	%
a) acesso interno indevido (utilização da sua senha por terceiros)	1	14,29%
b) roubo de dados	0	0,00%
c) ataque de vírus, worms e trojans	1	14,29%
d) ataque de hacker externo	0	0,00%
e) perda dos dados	0	0,00%
f) fraude bancária	4	57,14%
g) modificação nos sistemas corporativos	0	0,00%
h) uso abusivo da rede (envio de spam, tentativas de ataque a outros computadores)	0	0,00%
i) instalação de programas maliciosos (spywares, malwares)	0	0,00%
j) não sei dizer	1	14,29%

Fonte: Elaboração própria

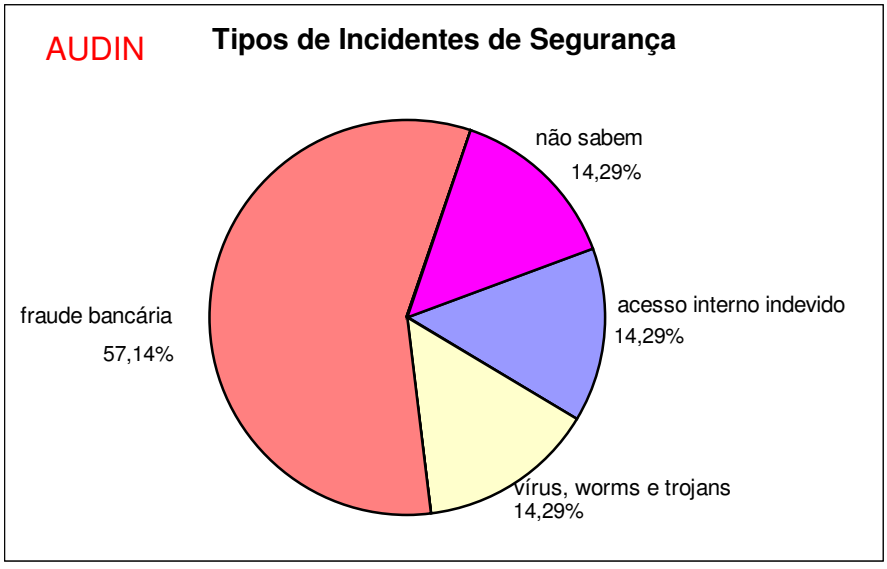


Gráfico 2: Tipos de Incidentes de Segurança da Informação
Fonte: Elaboração própria

Tem-se cinqüenta e sete por cento de usuários reportando “fraude bancária” como o principal incidente de segurança, seguidos por ataque de vírus, worms e trojans. Não souberam informar quatorze por cento dos respondentes.

- Em relação à quantidade de incidentes de segurança ocorridos no ano de 2005:

Tabela 7: Dados estatísticos da diretoria

Diretoria	Amostra:	Incidentes:	Média:	Desvio Padrão	Índice de Segurança
AUDIN	6	25	4,167	3,764	0,240

Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  $\bar{x}$ = 4,167

  s = 3,764

  n = 6

  ν = n –1 = 5

  $t_\alpha = t_{0,05}$ = 2,015

  t = (4,167 – 0) / (3,764 / √ 6) = 2,712

Logo:

t = 2,712 > $t_\alpha = t_{0,05}$ = 2,015 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Segurança da Informação = 1 / $\bar{x}$ = 1 / 4,167 = 0,240

5.5.2.2 CAINT

Esta diretoria apresentou os seguintes resultados:

- Em relação ao conhecimento da Norma ABNT NBR ISO/IEC 17799, sobre Segurança da Informação, apresentou-se desta forma:

Tabela 8: Perguntas quanto ao conhecimento da Norma ABNT NBR ISO/IEC 17799:

QUESTÕES:	SIM	NÃO
1. Você muda sua senha periodicamente?	22,22%	77,78%
2. Você utiliza senha forte (caracteres alfanuméricos, especiais e mínimo de 8 'oito' dígitos)?	55,56%	44,44%
3. Você anota sua senha em papel?	0,00%	100,00%
4. Você bloqueia sua estação de trabalho (computador) ao se afastar dela?	55,56%	44,44%
5. Você permite que alguém utilize sua senha para acesso a rede?	11,11%	88,89%
6. Você utiliza a opção de "scan" completo do antivírus, todos os dias?	22,22%	77,78%
7. Você monitora regularmente seu computador para reportar algo "suspeito"?	66,67%	33,33%
8. Você tem conhecimento sobre Segurança da Informação?	55,56%	44,44%
9. Você tem treinamento sobre Segurança da Informação?	0,00%	100,00%
10. Sua diretoria já teve algum incidente de segurança?	25,00%	75,00%
11. Sua diretoria tem algum plano de Segurança da Informação?	12,50%	87,50%

Fonte: Elaboração própria

Analisando as respostas pode-se notar que somente vinte e dois por cento dos usuários mudam periodicamente suas senhas e forçam a opção de passar o antivírus por completo. Cinqüenta e cinco por cento utilizam senhas "fortes", bloqueiam suas estações ao sair dela e têm conhecimento sobre Segurança da Informação. Sessenta e seis por cento monitoram seus computadores para reportar algo suspeito. Eles não anotam suas senhas em papel, mas onze por cento permitem o acesso de outras pessoas com as suas senhas. Essa diretoria não tem nenhum plano de Segurança da Informação para oitenta e sete por cento e também não treina seus usuários para este fim. Por fim, setenta e cinco por cento dos usuários reportaram algum incidente de segurança.

- Em relação aos tipos de incidentes ocorridos nesta diretoria no ano de 2005:

Tabela 9: Freqüência dos diferentes tipos de incidente de Segurança da Informação

Quais os tipos de incidentes de segurança que ocorreram em sua diretoria, no ano de 2005?		
	Freq.	%
a) acesso interno indevido (utilização da sua senha por terceiros)	0	0,00%
b) roubo de dados	0	0,00%
c) ataque de vírus, worms e trojans	6	35,29%
d) ataque de hacker externo	1	5,88%
e) perda dos dados	2	11,76%
f) fraude bancária	0	0,00%
g) modificação nos sistemas corporativos	0	0,00%
h) uso abusivo da rede (envio de spam, tentativas de ataque a outros computadores)	3	17,65%
i) instalação de programas maliciosos (spywares, malwares)	4	23,53%
j) não sei dizer	1	5,88%

Fonte: Elaboração própria

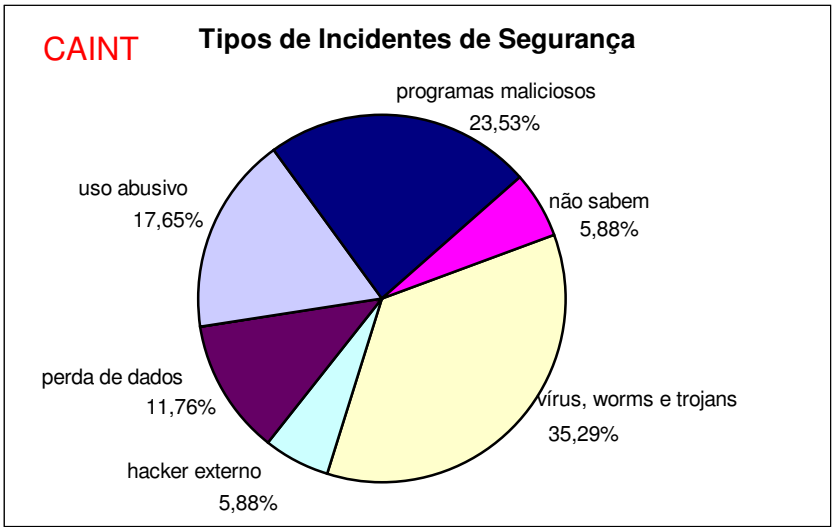


Gráfico 3: Tipos de Incidentes de Segurança da Informação
Fonte: Elaboração própria

Tem-se trinta e cinco por cento de usuários reportando "vírus, worms e trojans" como o principal incidente de segurança, seguidos por instalação de "programas maliciosos". Não souberam informar, quase seis por cento dos respondentes.

- Em relação à quantidade de incidentes de segurança ocorridos no ano de 2005:

Tabela 10: Dados estatísticos da diretoria

Diretoria	Amostra:	Incidentes:	Média:	Desvio Padrão	Índice de Segurança
CAINT	9	1155	128,333	134,094	0,008

Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  $\bar{x}$ = 128,333

  s = 134,09

  n = 9

  ν = n –1 = 8

  $t_\alpha = t_{0,05}$ = 1,860

  t = (128,333 – 0) / (134,09 / √ 9) = 2,871

Logo:

t = 2,871 > $t_\alpha = t_{0,05}$ = 1,860 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Segurança da Informação = 1 / $\bar{x}$ = 1 / 128,333 = 0,008

5.5.2.3 CGCRE

Esta diretoria apresentou os seguintes resultados:

- Em relação ao conhecimento da Norma ABNT NBR ISO/IEC 17799, sobre Segurança da Informação, apresentou-se desta forma:

Tabela 11: Perguntas quanto ao conhecimento da Norma ABNT NBR ISO/IEC 17799:

QUESTÕES:	SIM	NÃO
1. Você muda sua senha periodicamente?	10,53%	89,47%
2. Você utiliza senha forte (caracteres alfanuméricos, especiais e mínimo de 8 'oito' dígitos)?	21,05%	78,95%
3. Você anota sua senha em papel?	0,00%	100,00%
4. Você bloqueia sua estação de trabalho (computador) ao se afastar dela?	57,89%	42,11%
5. Você permite que alguém utilize sua senha para acesso a rede?	21,05%	78,95%
6. Você utiliza a opção de "scan" completo do antivírus, todos os dias?	15,79%	84,21%
7. Você monitora regularmente seu computador para reportar algo "suspeito"?	63,16%	36,84%
8. Você tem conhecimento sobre Segurança da Informação?	42,11%	57,89%
9. Você tem treinamento sobre Segurança da Informação?	0,00%	100,00%
10. Sua diretoria já teve algum incidente de segurança?	66,67%	33,33%
11. Sua diretoria tem algum plano de Segurança da Informação?	6,67%	93,33%

Fonte: Elaboração própria

Analisando as respostas pode-se notar que somente dez por cento dos usuários mudam periodicamente suas senhas. Quinze por cento forçam a opção de passar o antivírus por completo. Vinte e um por cento utilizam senhas "fortes". Quase sessenta por cento bloqueiam suas estações ao sair dela e monitoram seus computadores para reportar algo suspeito. Eles não anotam suas senhas em papel, mas vinte e um por cento permitem o acesso de outras pessoas com as suas senhas. Essa diretoria não tem nenhum plano de Segurança da Informação para noventa e três por cento e também não treina seus usuários para este fim. Por fim, sessenta e seis por cento dos usuários reportaram algum incidente de segurança.

- Em relação aos tipos de incidentes ocorridos nesta diretoria no ano de 2005:

Tabela 12: Freqüência dos diferentes tipos de incidente de Segurança da Informação

Quais os tipos de incidentes de segurança que ocorreram em sua diretoria, no ano de 2005?		
	Freq.	%
a) acesso interno indevido (utilização da sua senha por terceiros)	0	0,00%
b) roubo de dados	1	2,86%
c) ataque de vírus, worms e trojans	10	28,57%
d) ataque de hacker externo	0	0,00%
e) perda dos dados	6	17,14%
f) fraude bancária	4	11,43%
g) modificação nos sistemas corporativos	0	0,00%
h) uso abusivo da rede (envio de spam, tentativas de ataque a outros computadores)	6	17,14%
i) instalação de programas maliciosos (spywares, malwares)	3	8,57%
j) não sei dizer	5	14,29%

Fonte: Elaboração própria

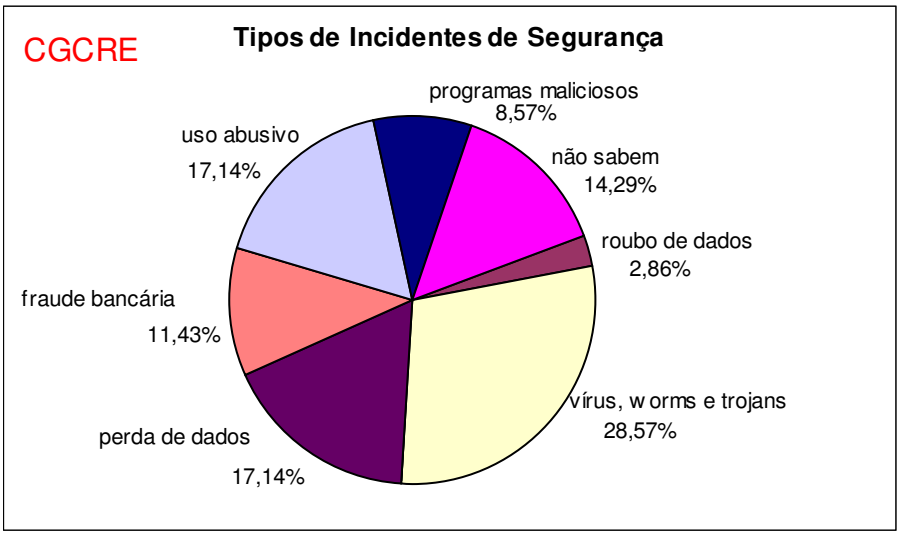


Gráfico 4: Tipos de Incidentes de Segurança da Informação
Fonte: Elaboração própria

Tem-se vinte e nove por cento de usuários reportando "vírus, worms e trojans" como o principal incidente de segurança, seguidos por "perda de dados" e "uso abusivo" da rede. Não souberam informar, quase quinze por cento dos respondentes.

- Em relação à quantidade de incidentes de segurança ocorridos no ano de 2005:

Tabela 13: Dados estatísticos da diretoria

Diretoria	Amostra:	Incidentes:	Média:	Desvio Padrão	Índice de Segurança
CGCRE	19	510	26,842	66,817	0,037

Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\bar{x}$ = 26,842

s = 66,817

n = 19

ν = n –1 = 18

$t_\alpha = t_{0,05} = 1,734$

t = (26,842 – 0) / (66,817 / √ 19) = 1,751

Logo:

t = 1,751 > $t_\alpha = t_{0,05} = 1,734$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Segurança da Informação = $1 / \bar{x} = 1 / 26,842 = 0,037$

5.5.2.4 CPLAN

Esta diretoria apresentou os seguintes resultados:

- Em relação ao conhecimento da Norma ABNT NBR ISO/IEC 17799, sobre Segurança da Informação, apresentou-se desta forma:

Tabela 14: Perguntas quanto ao conhecimento da Norma ABNT NBR ISO/IEC 17799:

QUESTÕES:	SIM	NÃO
1. Você muda sua senha periodicamente?	31,43%	68,57%
2. Você utiliza senha forte (caracteres alfanuméricos, especiais e mínimo de 8 'oito' dígitos)?	48,57%	51,43%
3. Você anota sua senha em papel?	8,57%	91,43%
4. Você bloqueia sua estação de trabalho (computador) ao se afastar dela?	64,71%	35,29%
5. Você permite que alguém utilize sua senha para acesso a rede?	20,00%	80,00%
6. Você utiliza a opção de "scan" completo do antivírus, todos os dias?	14,29%	85,71%
7. Você monitora regularmente seu computador para reportar algo "suspeito"?	68,57%	31,43%
8. Você tem conhecimento sobre Segurança da Informação?	62,86%	37,14%
9. Você tem treinamento sobre Segurança da Informação?	14,29%	85,71%
10. Sua diretoria já teve algum incidente de segurança?	72,73%	27,27%
11. Sua diretoria tem algum plano de Segurança da Informação?	54,55%	45,45%

Fonte: Elaboração própria

Analisando as respostas pode-se notar que trinta e um por cento dos usuários mudam periodicamente suas senhas. Quatorze por cento forçam a opção de passar o antivírus por completo. Quase metade dos usuários utiliza senhas "fortes". Cerca de dois terços deles bloqueiam suas estações ao sair dela e monitoram seus computadores para reportar algo suspeito. Oito por cento anotam suas senhas em papel e vinte por cento permitem o acesso de

outras pessoas com as suas senhas. Essa diretoria tem um plano de Segurança da Informação para cinqüenta e cinco por cento e também treina seus usuários para este fim para oitenta e cinco por cento dos respondentes. Por fim, setenta e dois por cento dos usuários reportaram algum incidente de segurança.

- Em relação aos tipos de incidentes ocorridos nesta diretoria no ano de 2005:

Tabela 15: Freqüência dos diferentes tipos de incidente de Segurança da Informação

Quais os tipos de incidentes de segurança que ocorreram em sua diretoria, no ano de 2005?		
	Freq.	%
a) acesso interno indevido (utilização da sua senha por terceiros)	6	6,59%
b) roubo de dados	1	1,10%
c) ataque de vírus, worms e trojans	20	21,98%
d) ataque de hacker externo	5	5,49%
e) perda dos dados	9	9,89%
f) fraude bancária	16	17,58%
g) modificação nos sistemas corporativos	0	0,00%
h) uso abusivo da rede (envio de spam, tentativas de ataque a outros computadores)	14	15,38%
i) instalação de programas maliciosos (spywares, malwares)	17	18,68%
j) não sei dizer	3	3,30%

Fonte: Elaboração própria

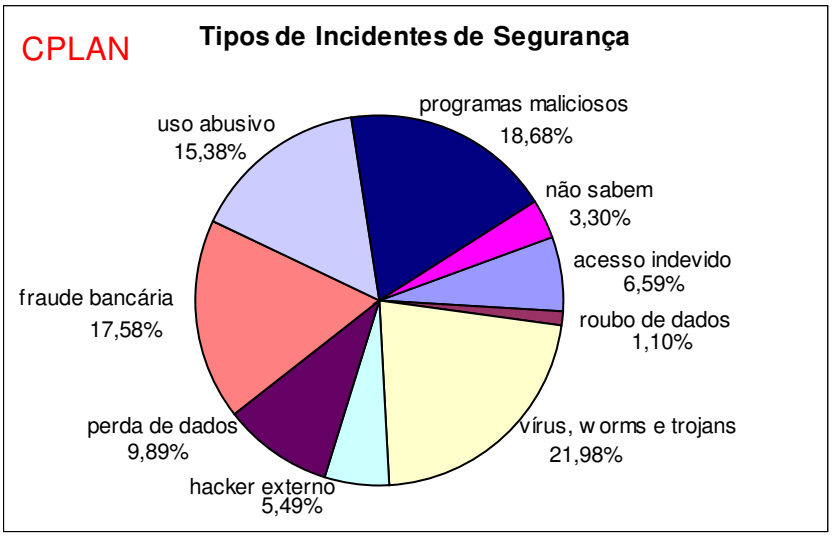


Gráfico 5: Tipos de Incidentes de Segurança da Informação
Fonte: Elaboração própria

Tem-se vinte e dois por cento de usuários reportando "vírus, worms e trojans" como o principal incidente de segurança, seguidos por instalação de "programas maliciosos" e "fraude bancária". Não souberam informar somente três por cento dos respondentes.

- Em relação à quantidade de incidentes de segurança ocorridos no ano de 2005:

Tabela 16: Dados estatísticos da diretoria

Diretoria	Amostra:	Incidentes:	Média:	Desvio Padrão	Índice de Segurança
CPLAN	35	1870	53,429	96,678	0,019

Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**v**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  $\bar{x}$ = 53,429

  s = 96,678

  n = 35

  ν = n –1 = 34

  $t_\alpha = t_{0,05}$ = 1,689

  t = (96,678 – 0) / (96,678 / √ 35) = 3,269

Logo:

t = 3,269 > $t_\alpha = t_{0,05}$ = 1,689 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Segurança da Informação = 1 / $\bar{x}$ = 1 / 53,429 = 0,019

5.5.2.5 DIMCI

Esta diretoria apresentou os seguintes resultados:

- Em relação ao conhecimento da Norma ABNT NBR ISO/IEC 17799, sobre Segurança da Informação, apresentou-se desta forma:

Tabela 17: Perguntas quanto ao conhecimento da Norma ABNT NBR ISO/IEC 17799:

QUESTÕES:	SIM	NÃO
1. Você muda sua senha periodicamente?	19,35%	80,65%
2. Você utiliza senha forte (caracteres alfanuméricos, especiais e mínimo de 8 'oito' dígitos)?	64,52%	35,48%
3. Você anota sua senha em papel?	6,45%	93,55%
4. Você bloqueia sua estação de trabalho (computador) ao se afastar dela?	41,94%	58,06%
5. Você permite que alguém utilize sua senha para acesso a rede?	12,90%	87,10%
6. Você utiliza a opção de "scan" completo do antivírus, todos os dias?	23,33%	76,67%
7. Você monitora regularmente seu computador para reportar algo "suspeito"?	51,61%	48,39%
8. Você tem conhecimento sobre Segurança da Informação?	51,61%	48,39%
9. Você tem treinamento sobre Segurança da Informação?	3,23%	96,77%
10. Sua diretoria já teve algum incidente de segurança?	70,37%	29,63%
11. Sua diretoria tem algum plano de Segurança da Informação?	22,22%	77,78%

Fonte: Elaboração própria

Analisando as respostas nota-se que menos de vinte por cento dos usuários mudam periodicamente suas senhas. Vinte e três por cento forçam a opção de passar o antivírus por completo. Quase sessenta e cinco por cento dos usuários utilizam senhas "fortes". Quarenta e dois por cento deles bloqueiam suas estações ao sair dela e metade monitora seus computadores para reportar algo suspeito. Seis por cento anotam suas senhas em papel e treze por cento permitem o acesso de outras pessoas com as suas senhas. Essa diretoria não tem nenhum plano de Segurança da Informação para setenta e sete por cento e também treina seus usuários para este fim para noventa e seis por cento dos respondentes. Por fim, setenta por cento dos usuários reportaram algum incidente de segurança.

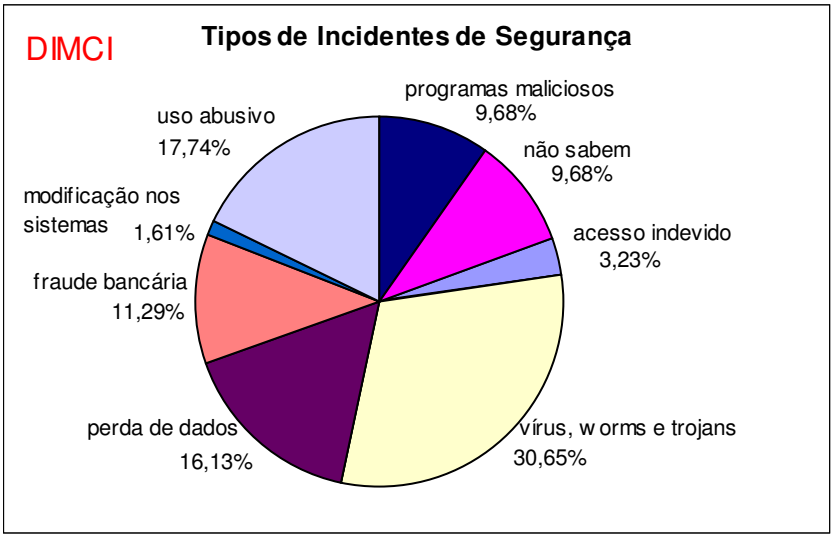
- Em relação aos tipos de incidentes ocorridos nesta diretoria no ano de 2005:

Tabela 18: Freqüência dos diferentes tipos de incidente de Segurança da Informação

Quais os tipos de incidentes de segurança que ocorreram em sua diretoria, no ano de 2005?		
	Freq.	%
a) acesso interno indevido (utilização da sua senha por terceiros)	2	3,23%
b) roubo de dados	0	0,00%
c) ataque de vírus, worms e trojans	19	30,65%
d) ataque de hacker externo	0	0,00%
e) perda dos dados	10	16,13%
f) fraude bancária	7	11,29%
g) modificação nos sistemas corporativos	1	1,61%
h) uso abusivo da rede (envio de spam, tentativas de ataque a outros computadores)	11	17,74%
i) instalação de programas maliciosos (spywares, malwares)	6	9,68%
j) não sei dizer	6	9,68%

Fonte: Elaboração própria

Gráfico 6: Tipos de Incidentes de Segurança da Informação
Fonte: Elaboração própria



Percebe-se trinta por cento de usuários reportando "vírus, worms e trojans" como o principal incidente de segurança, seguidos por "uso abusivo" da rede e "perda de dados". Não souberam informar quase dez por cento dos respondentes.

- Em relação à quantidade de incidentes de segurança ocorridos no ano de 2005:

Tabela 19: Dados estatísticos da diretoria

Diretoria	Amostra:	Incidentes:	Média:	Desvio Padrão	Índice de Segurança
DIMCI	31	1120	36,129	88,475	0,028

Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\bar{x}$ = 36,129

s = 88,475

n = 31

ν = n –1 = 30

$t_\alpha = t_{0,05} = 1,697$

t = (36,129 – 0) / (88,475 / √ 31) = 2,274

Logo:

t = 2,274 > $t_\alpha = t_{0,05} = 1,697$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Segurança da Informação = $1 / \bar{x} = 1 / 36,129 = 0,028$

5.5.2.6 DIMEL

Esta diretoria apresentou os seguintes resultados:

- Em relação ao conhecimento da Norma ABNT NBR ISO/IEC 17799, sobre Segurança da Informação, apresentou-se desta forma:

Tabela 20: Perguntas quanto ao conhecimento da Norma ABNT NBR ISO/IEC 17799:

QUESTÕES:	SIM	NÃO
1. Você muda sua senha periodicamente?	10,71%	89,29%
2. Você utiliza senha forte (caracteres alfanuméricos, especiais e mínimo de 8 'oito' dígitos)?	42,86%	57,14%
3. Você anota sua senha em papel?	10,71%	89,29%
4. Você bloqueia sua estação de trabalho (computador) ao se afastar dela?	35,71%	64,29%
5. Você permite que alguém utilize sua senha para acesso a rede?	39,29%	60,71%
6. Você utiliza a opção de "scan" completo do antivírus, todos os dias?	3,57%	96,43%
7. Você monitora regularmente seu computador para reportar algo "suspeito"?	53,57%	46,43%
8. Você tem conhecimento sobre Segurança da Informação?	42,86%	57,14%
9. Você tem treinamento sobre Segurança da Informação?	7,14%	92,86%
10. Sua diretoria já teve algum incidente de segurança?	68,00%	32,00%
11. Sua diretoria tem algum plano de Segurança da Informação?	13,64%	86,36%

Fonte: Elaboração própria

Analisando as respostas nota-se que somente dez por cento dos usuários mudam periodicamente suas senhas. Apenas três por cento forçam a opção de passar o antivírus por completo. Quarenta e dois por cento dos usuários utilizam senhas "fortes". Trinta e cinco por cento deles bloqueiam suas estações ao sair dela e metade monitora seus computadores para reportar algo suspeito. Dez por cento anotam suas senhas em papel e quase quarenta por cento

permitem o acesso de outras pessoas com as suas senhas. Essa diretoria não tem nenhum plano de Segurança da Informação para oitenta e seis por cento e também não treina seus usuários para este fim para noventa e três por cento dos respondentes. Por fim, quase setenta por cento dos usuários reportaram algum incidente de segurança.

- Em relação aos tipos de incidentes ocorridos nesta diretoria no ano de 2005:

Tabela 21: Freqüência dos diferentes tipos de incidente de Segurança da Informação

Quais os tipos de incidentes de segurança que ocorreram em sua diretoria, no ano de 2005?		
	Freq.	%
a) acesso interno indevido (utilização da sua senha por terceiros)	4	6,67%
b) roubo de dados	0	0,00%
c) ataque de vírus, worms e trojans	16	26,67%
d) ataque de hacker externo	2	3,33%
e) perda dos dados	5	8,33%
f) fraude bancária	10	16,67%
g) modificação nos sistemas corporativos	0	0,00%
h) uso abusivo da rede (envio de spam, tentativas de ataque a outros computadores)	11	18,33%
i) instalação de programas maliciosos (spywares, malwares)	6	10,00%
j) não sei dizer	6	10,00%

Fonte: Elaboração própria

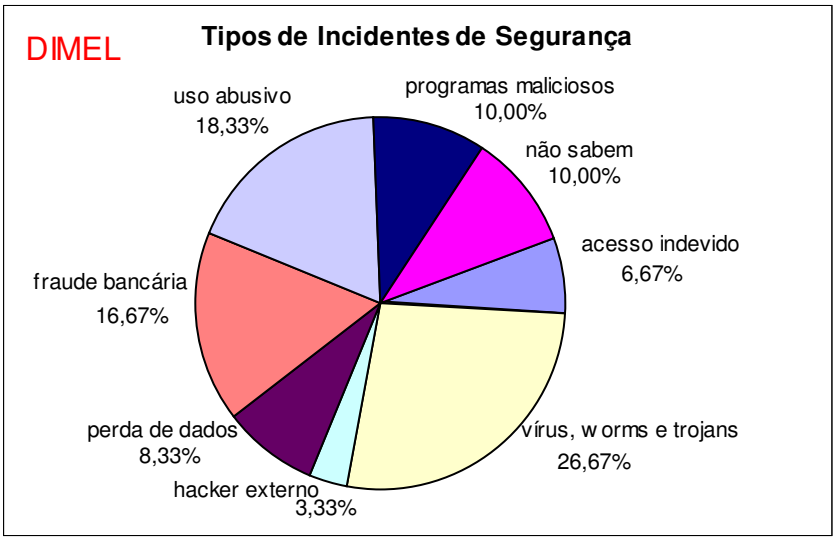


Gráfico 7: Tipos de Incidentes de Segurança da Informação
Fonte: Elaboração própria

Percebe-se quase trinta por cento de usuários reportando “vírus, worms e trojans” como o principal incidente de segurança, seguidos por “uso abusivo” da rede e “fraude bancária”. Não souberam informar dez por cento dos respondentes.

- Em relação à quantidade de incidentes de segurança ocorridos no ano de 2005:

Tabela 22: Dados estatísticos da diretoria

Diretoria	Amostra:	Incidentes:	Média:	Desvio Padrão	Índice de Segurança
DIMEL	28	680	24,286	63,577	0,041

Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  $\bar{x}$ = 24,286

  s = 63,577

  n = 28

  ν = n –1 = 27

  $t_\alpha = t_{0,05}$ = 1,703

  t = (24,286 – 0) / (63,577 / √ 28) = 2,021

Logo:

t = 2,021 > $t_\alpha = t_{0,05}$ = 1,703 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Segurança da Informação = 1 / $\bar{x}$ = 1 / 24,286 = 0,041

5.5.2.7 DIRAF

Esta diretoria apresentou os seguintes resultados:

- Em relação ao conhecimento da Norma ABNT NBR ISO/IEC 17799, sobre Segurança da Informação, apresentou-se desta forma:

Tabela 23: Perguntas quanto ao conhecimento da Norma ABNT NBR ISO/IEC 17799:

QUESTÕES:	SIM	NÃO
1. Você muda sua senha periodicamente?	10,00%	90,00%
2. Você utiliza senha forte (caracteres alfanuméricos, especiais e mínimo de 8 'oito' dígitos)?	45,00%	55,00%
3. Você anota sua senha em papel?	10,00%	90,00%
4. Você bloqueia sua estação de trabalho (computador) ao se afastar dela?	55,00%	45,00%
5. Você permite que alguém utilize sua senha para acesso a rede?	25,00%	75,00%
6. Você utiliza a opção de "scan" completo do antivírus, todos os dias?	15,00%	85,00%
7. Você monitora regularmente seu computador para reportar algo "suspeito"?	55,00%	45,00%
8. Você tem conhecimento sobre Segurança da Informação?	55,00%	45,00%
9. Você tem treinamento sobre Segurança da Informação?	10,00%	90,00%
10. Sua diretoria já teve algum incidente de segurança?	56,25%	43,75%
11. Sua diretoria tem algum plano de Segurança da Informação?	21,43%	78,57%

Fonte: Elaboração própria

Analisando as respostas pode-se notar que somente dez por cento dos usuários mudam periodicamente suas senhas. Quinze por cento forçam a opção de passar o antivírus por completo. Quarenta e cinco por cento utilizam senhas "fortes". Cinqüenta e cinco por cento bloqueiam suas estações ao sair dela e monitoram seus computadores para reportar algo suspeito. Noventa por cento dos usuários não anotam suas senhas em papel, mas vinte e cinco por cento permitem o acesso de outras pessoas com as suas senhas. Essa diretoria não tem nenhum plano de Segurança da Informação para setenta e oito por cento dos usuários e para noventa por cento, também não há treinamento para este fim. Por fim, cinqüenta e seis por cento dos usuários reportaram algum incidente de segurança.

- Em relação aos tipos de incidentes ocorridos nesta diretoria no ano de 2005:

Tabela 24: Freqüência dos diferentes tipos de incidente de Segurança da Informação

Quais os tipos de incidentes de segurança que ocorreram em sua diretoria, no ano de 2005?		
	Freq.	%
a) acesso interno indevido (utilização da sua senha por terceiros)	2	4,65%
b) roubo de dados	0	0,00%
c) ataque de vírus, worms e trojans	10	23,26%
d) ataque de hacker externo	0	0,00%
e) perda dos dados	4	9,30%
f) fraude bancária	7	16,28%
g) modificação nos sistemas corporativos	1	2,33%
h) uso abusivo da rede (envio de spam, tentativas de ataque a outros computadores)	7	16,28%
i) instalação de programas maliciosos (spywares, malwares)	4	9,30%
j) não sei dizer	8	18,60%

Fonte: Elaboração própria

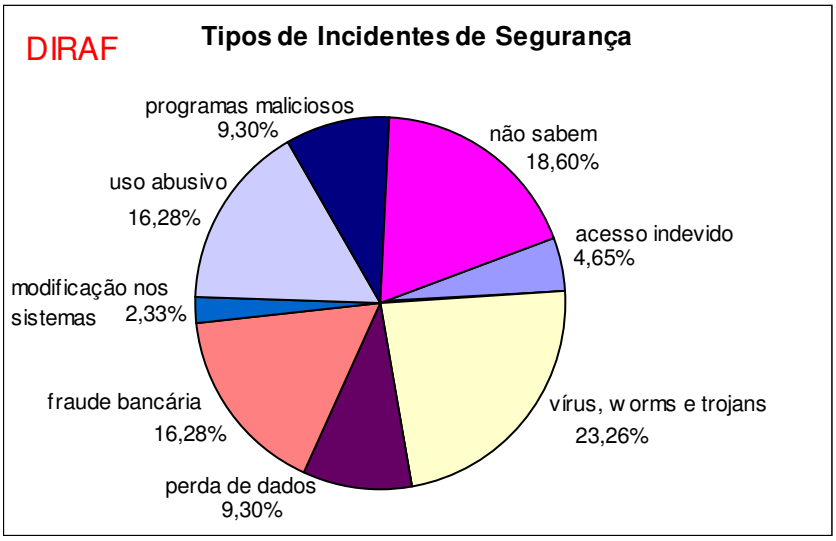


Gráfico 8: Tipos de Incidentes de Segurança da Informação
Fonte: Elaboração própria

Tem-se vinte e três por cento de usuários reportando "vírus, worms e trojans" como o principal incidente de segurança, seguidos por "fraude bancária" e "uso abusivo" da rede. Não souberam informar, mais de dezoito por cento dos respondentes.

- Em relação à quantidade de incidentes de segurança ocorridos no ano de 2005:

Tabela 25: Dados estatísticos da diretoria

Diretoria	Amostra:	Incidentes:	Média:	Desvio Padrão	Índice de Segurança
DIRAF	20	1035	51,750	107,340	0,019

Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  $\bar{x}$ = 51,750

  s = 107,340

  n = 20

  ν = n –1 = 19

  $t_\alpha = t_{0,05}$ = 1,729

  t = (51,750 – 0) / (107,340 / √ 20) = 2,156

Logo:

t = 2,156 > $t_\alpha = t_{0,05}$ = 1,729 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Segurança da Informação = 1 / $\bar{x}$ = 1 / 51,750 = 0,019

5.5.2.8 DQUAL

Esta diretoria apresentou os seguintes resultados:

- Em relação ao conhecimento da Norma ABNT NBR ISO/IEC 17799, sobre Segurança da Informação, apresentou-se desta forma:

Tabela 26: Perguntas quanto ao conhecimento da Norma ABNT NBR ISO/IEC 17799:

QUESTÕES:	SIM	NÃO
1. Você muda sua senha periodicamente?	0,00%	100,00%
2. Você utiliza senha forte (caracteres alfanuméricos, especiais e mínimo de 8 'oito' dígitos)?	33,33%	66,67%
3. Você anota sua senha em papel?	3,33%	96,67%
4. Você bloqueia sua estação de trabalho (computador) ao se afastar dela?	43,33%	56,67%
5. Você permite que alguém utilize sua senha para acesso a rede?	36,67%	63,33%
6. Você utiliza a opção de "scan" completo do antivírus, todos os dias?	17,24%	82,76%
7. Você monitora regularmente seu computador para reportar algo "suspeito"?	23,33%	76,67%
8. Você tem conhecimento sobre Segurança da Informação?	23,33%	76,67%
9. Você tem treinamento sobre Segurança da Informação?	3,33%	96,67%
10. Sua diretoria já teve algum incidente de segurança?	58,33%	41,67%
11. Sua diretoria tem algum plano de Segurança da Informação?	0,00%	100,00%

Fonte: Elaboração própria

Analisando as respostas observa-se que nenhum usuário muda periodicamente sua senha. Dezessete por cento forçam a opção de passar o antivírus por completo. Trinta e três por cento utilizam senhas "fortes". Quarenta e três por cento bloqueiam suas estações ao sair dela e somente vinte e três por cento monitoram seus computadores para reportar algo suspeito. Noventa e seis por cento dos usuários não anotam suas senhas em papel, mas trinta e seis por cento permitem o acesso de outras pessoas com as suas senhas. Essa diretoria não tem nenhum plano de Segurança da Informação para todos os usuários e para noventa e seis por cento, também não há treinamento para este fim. Por fim, cinqüenta e oito por cento dos usuários reportaram algum incidente de segurança.

- Em relação aos tipos de incidentes ocorridos nesta diretoria no ano de 2005:

Tabela 27: Freqüência dos diferentes tipos de incidente de Segurança da Informação

Quais os tipos de incidentes de segurança que ocorreram em sua diretoria, no ano de 2005?		
	Freq.	%
a) acesso interno indevido (utilização da sua senha por terceiros)	4	7,55%
b) roubo de dados	1	1,89%
c) ataque de vírus, worms e trojans	12	22,64%
d) ataque de hacker externo	1	1,89%
e) perda dos dados	3	5,66%
f) fraude bancária	9	16,98%
g) modificação nos sistemas corporativos	0	0,00%
h) uso abusivo da rede (envio de spam, tentativas de ataque a outros computadores)	9	16,98%
i) instalação de programas maliciosos (spywares, malwares)	7	13,21%
j) não sei dizer	7	13,21%

Fonte: Elaboração própria

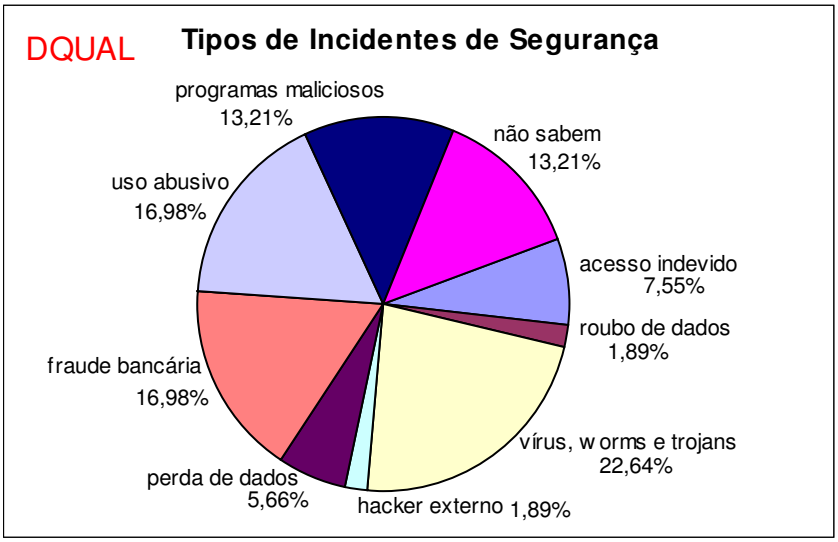


Gráfico 9: Tipos de Incidentes de Segurança da Informação
Fonte: Elaboração própria

Tem-se vinte e três por cento de usuários reportando "vírus, worms e trojans" como o principal incidente de segurança, seguidos por "fraude bancária" e "uso abusivo" da rede. Não souberam informar, mais de treze por cento dos respondentes.

- Em relação à quantidade de incidentes de segurança ocorridos no ano de 2005:

Tabela 28: Dados estatísticos da diretoria

Diretoria	Amostra:	Incidentes:	Média:	Desvio Padrão	Índice de Segurança
DQUAL	30	695	23,167	59,704	0,043

Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\bar{x}$ = 23,167

s = 59,704

n = 30

ν = n –1 = 29

$t_\alpha = t_{0,05} = 1,699$

t = (23,167 – 0) / (59,704 / √ 30) = 2,125

Logo:

t = 2,125 > $t_\alpha = t_{0,05} = 1,699$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Segurança da Informação = $1 / \bar{x} = 1 / 23,167 = 0,043$

5.5.2.9 GABIN

Esta diretoria apresentou os seguintes resultados:

- Em relação ao conhecimento da Norma ABNT NBR ISO/IEC 17799, sobre Segurança da Informação, apresentou-se desta forma:

Tabela 29: Perguntas quanto ao conhecimento da Norma ABNT NBR ISO/IEC 17799:

QUESTÕES:	SIM	NÃO
1. Você muda sua senha periodicamente?	22,22%	77,78%
2. Você utiliza senha forte (caracteres alfanuméricos, especiais e mínimo de 8 'oito' dígitos)?	11,11%	88,89%
3. Você anota sua senha em papel?	11,11%	88,89%
4. Você bloqueia sua estação de trabalho (computador) ao se afastar dela?	33,33%	66,67%
5. Você permite que alguém utilize sua senha para acesso a rede?	22,22%	77,78%
6. Você utiliza a opção de "scan" completo do antivírus, todos os dias?	0,00%	100,00%
7. Você monitora regularmente seu computador para reportar algo "suspeito"?	66,67%	33,33%
8. Você tem conhecimento sobre Segurança da Informação?	44,44%	55,56%
9. Você tem treinamento sobre Segurança da Informação?	0,00%	100,00%
10. Sua diretoria já teve algum incidente de segurança?	33,33%	66,67%
11. Sua diretoria tem algum plano de Segurança da Informação?	0,00%	100,00%

Fonte: Elaboração própria

Analisando as respostas nota-se que vinte e dois por cento dos usuários mudam periodicamente suas senhas. Nenhum usuário força a opção de passar o antivírus por completo. Somente onze por cento dos usuários utilizam senhas "fortes". Trinta e três por cento deles bloqueiam suas estações ao sair dela e sessenta e seis por cento monitoram seus computadores para reportar algo suspeito. Onze por cento anotam suas senhas em papel e

vinte e dois por cento permitem o acesso de outras pessoas com as suas senhas. Essa diretoria não tem nenhum plano de Segurança da Informação para todos os usuários e também não treina seus usuários para este fim para cem por cento dos respondentes. Por fim, trinta e três por cento dos usuários reportaram algum incidente de segurança.

- Em relação aos tipos de incidentes ocorridos nesta diretoria no ano de 2005:

Tabela 30: Freqüência dos diferentes tipos de incidente de Segurança da Informação

Quais os tipos de incidentes de segurança que ocorreram em sua diretoria, no ano de 2005?		
	Freq.	%
a) acesso interno indevido (utilização da sua senha por terceiros)	0	0,00%
b) roubo de dados	0	0,00%
c) ataque de vírus, worms e trojans	4	30,77%
d) ataque de hacker externo	1	7,69%
e) perda dos dados	1	7,69%
f) fraude bancária	1	7,69%
g) modificação nos sistemas corporativos	0	0,00%
h) uso abusivo da rede (envio de spam, tentativas de ataque a outros computadores)	1	7,69%
i) instalação de programas maliciosos (spywares, malwares)	3	23,08%
j) não sei dizer	2	15,38%

Fonte: Elaboração própria

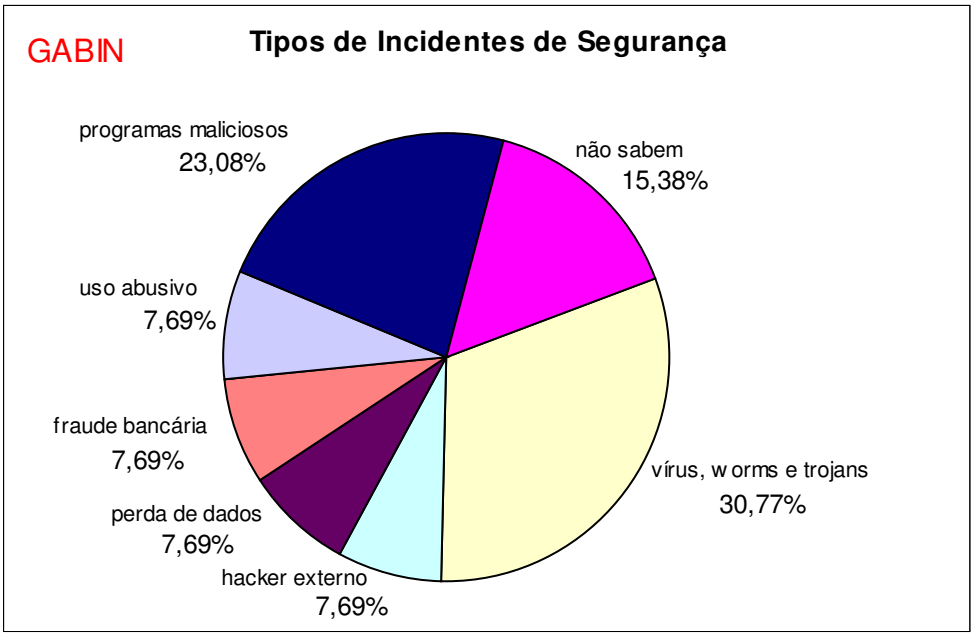


Gráfico 10: Tipos de Incidentes de Segurança da Informação
Fonte: Elaboração própria

Percebe-se trinta por cento de usuários reportando "vírus, worms e trojans" como o principal incidente de segurança, seguidos por instalação de "programas maliciosos". Não souberam informar quinze por cento dos respondentes.

- Em relação à quantidade de incidentes de segurança ocorridos no ano de 2005:

Tabela 31: Dados estatísticos da diretoria

Diretoria	Amostra:	Incidentes:	Média:	Desvio Padrão	Índice de Segurança
GABIN	9	40	4,444	5,833	0,225

Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\bar{x}$ = 4,444

s = 5,833

n = 9

ν = n –1 = 8

$t_\alpha = t_{0,05}$ = 1,860

t = (4,444 – 0) / (5,833 / √ 9) = 2,286

Logo:

t = 2,286 > $t_\alpha = t_{0,05}$ = 1,860 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Segurança da Informação = 1 / $\bar{x}$ = 1 / 4,444 = 0,225

5.5.2.10 PROGE

Esta diretoria apresentou os seguintes resultados:

- Em relação ao conhecimento da Norma ABNT NBR ISO/IEC 17799, sobre Segurança da Informação, apresentou-se desta forma:

Tabela 32: Perguntas quanto ao conhecimento da Norma ABNT NBR ISO/IEC 17799:

QUESTÕES:	SIM	NÃO
1. Você muda sua senha periodicamente?	40,00%	60,00%
2. Você utiliza senha forte (caracteres alfanuméricos, especiais e mínimo de 8 'oito' dígitos)?	40,00%	60,00%
3. Você anota sua senha em papel?	40,00%	60,00%
4. Você bloqueia sua estação de trabalho (computador) ao se afastar dela?	60,00%	40,00%
5. Você permite que alguém utilize sua senha para acesso a rede?	20,00%	80,00%
6. Você utiliza a opção de "scan" completo do antivírus, todos os dias?	20,00%	80,00%
7. Você monitora regularmente seu computador para reportar algo "suspeito"?	20,00%	80,00%
8. Você tem conhecimento sobre Segurança da Informação?	0,00%	100,00%
9. Você tem treinamento sobre Segurança da Informação?	0,00%	100,00%
10. Sua diretoria já teve algum incidente de segurança?	25,00%	75,00%
11. Sua diretoria tem algum plano de Segurança da Informação?	0,00%	100,00%

Fonte: Elaboração própria

Analisando as respostas percebe-se que quarenta por cento dos usuários mudam periodicamente suas senhas. Vinte por cento dos usuários forçam a opção de passar o antivírus por completo. Quarenta por cento dos usuários utilizam senhas "fortes". Sessenta por cento deles bloqueiam suas estações ao sair dela, mas somente vinte por cento monitoram seus computadores para reportar algo suspeito. Quarenta por cento anotam suas senhas em papel e vinte por cento permitem o acesso de outras pessoas com as suas senhas. Essa diretoria não tem nenhum plano de Segurança da Informação para todos os usuários e também não treina seus usuários para este fim para cem por cento dos respondentes. Por fim, vinte e cinco por cento dos usuários reportaram algum incidente de segurança.

- Em relação aos tipos de incidentes ocorridos nesta diretoria no ano de 2005:

Tabela 33: Freqüência dos diferentes tipos de incidente de Segurança da Informação

Quais os tipos de incidentes de segurança que ocorreram em sua diretoria, no ano de 2005?		
	Freq.	%
a) acesso interno indevido (utilização da sua senha por terceiros)	0	0,00%
b) roubo de dados	0	0,00%
c) ataque de vírus, worms e trojans	3	37,50%
d) ataque de hacker externo	0	0,00%
e) perda dos dados	0	0,00%
f) fraude bancária	2	25,00%
g) modificação nos sistemas corporativos	0	0,00%
h) uso abusivo da rede (envio de spam, tentativas de ataque a outros computadores)	2	25,00%
i) instalação de programas maliciosos (spywares, malwares)	0	0,00%
j) não sei dizer	1	12,50%

Fonte: Elaboração própria

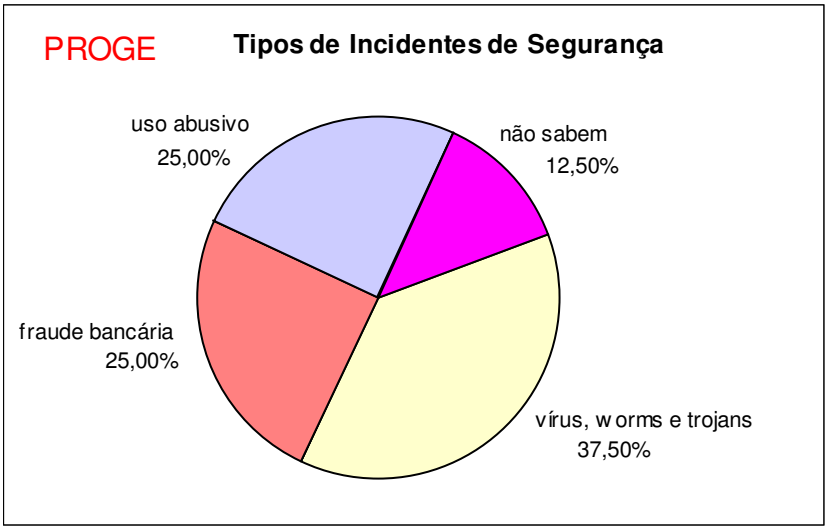


Gráfico 11: Tipos de Incidentes de Segurança da Informação
Fonte: Elaboração própria

Observa-se quase quarenta por cento de usuários reportando "vírus, worms e trojans" como o principal incidente de segurança, seguidos por "fraude bancária" e "uso abusivo" da rede. Não souberam informar doze por cento dos respondentes.

- Em relação à quantidade de incidentes de segurança ocorridos no ano de 2005:

Tabela 34: Dados estatísticos da diretoria

Diretoria	Amostra:	Incidentes:	Média:	Desvio Padrão	Índice de Segurança
PROGE	5	85	17,000	12,550	0,059

Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**v**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

$\alpha = 0,05$

$\bar{x} = 17,000$

$s = 12,550$

$n = 5$

$\nu = n - 1 = 4$

$t_\alpha = t_{0,05} = 2,132$

$t = (17,000 - 0) / (12,550 / \sqrt{5}) = 3,029$

Logo:

$t = 3,029 > t_\alpha = t_{0,05} = 2,132$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Segurança da Informação = $1 / \bar{x} = 1 / 17,000 = 0,059$

5.5.2.11 RESULTADO DO ÍNDICE DE SEGURANÇA DA INFORMAÇÃO

Após o término dos cálculos e teste de corroboração ou refutação da média, tem-se o índice de segurança da informação, como a forma de posicionar as unidades organizacionais em ordem de melhor percepção de segurança da informação. Abaixo, são apresentados os resultados e as respectivas colocações das diretorias do Inmetro, na parte da pesquisa relativa a percepção de segurança da informação:

Tabela 35: Índices de Segurança da Informação das diretorias

Ordem:	Diretorias:	Índice:
1	AUDIN	0,240
2	GABIN	0,225
3	PROGE	0,059
4	DQUAL	0,043
5	DIMEL	0,041
6	CGCRE	0,037
7	DIMCI	0,028
8	DIRAF	0,019
9	CPLAN	0,019
10	CAINT	0,008

Fonte: Elaboração própria

Pode-se perceber que mesmo as duas melhores diretorias, não possuem valores altos de índice, indicando que a instituição como um todo, ainda tem problemas em relação a Segurança da Informação.

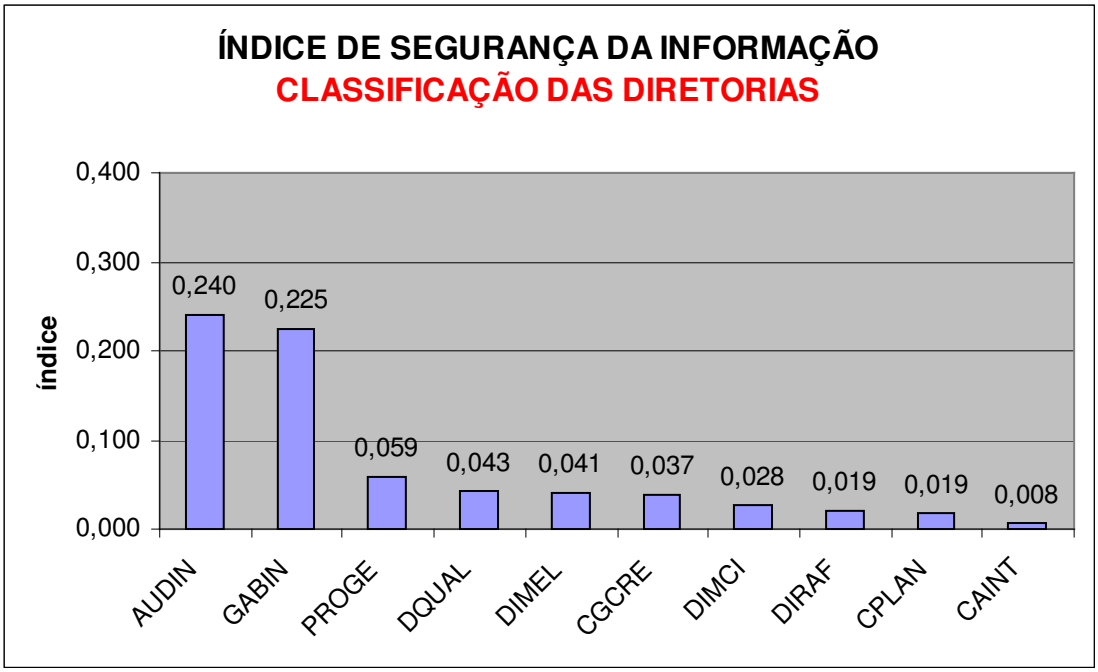


Gráfico 12: Índice de Segurança da Informação – Classificação das Diretorias
Fonte: Elaboração própria

5.5.3 CÁLCULO DO ÍNDICE DE PERCEPÇÃO DA QUALIDADE

Para este cálculo, foram tabulados os resultados da pesquisa obtida através das respostas, por meio de amostras aleatórias dos usuários, ao questionário *Servqual*, dentro de cada diretoria. O questionário foi disponibilizado através de um "portal web", de forma a facilitar aos usuários respondê-lo, como também, facilitar a tabulação das respostas, sendo essas armazenadas diretamente no banco de dados da pesquisa.

Dimensões de Avaliação	**Declarações**
Elementos Tangíveis	1. O setor de informática deve ter equipamentos e sistemas de última geração. 2. Suas instalações físicas devem ser visualmente atraentes. 3. Seus funcionários têm boa aparência - bem vestidos, limpos e organizados. 4. Tem elementos materiais relacionados com o serviço (folhetos, manuais, etc.) que são visualmente atraentes.
Confiabilidade	5. Quando promete fazer algo para uma certa data, ele faz. 6. Quando os usuários têm um problema, o setor de informática mostra um sincero interesse em resolvê-lo. 7. Este serviço é confiável - ajudando quando precisamos dele. 8. Ele entrega seus serviços nas datas em que promete fazer. 9. Ele se esforça para ter um histórico de trabalho sem erros.
Capacidade de Resposta	10. Ele diz aos usuários exatamente quando os serviços serão executados. 11. Seus funcionários dão pronto atendimento aos usuários. 12. Seus funcionários estão sempre dispostos a ajudar os usuários. 13. Seus funcionários nunca estão muito ocupados para atender às solicitações dos usuários.
Segurança	14. O comportamento dos funcionários inspira confiança aos usuários. 15. Os usuários se sentem seguros em suas transações com os funcionários deste setor. 16. Seus funcionários são sempre educados com os usuários. 17. Seus funcionários têm formação e conhecimento para realizar seu trabalho bem feito.
Empatia	18. Este setor dá aos seus usuários atendimento individual. 19. Este setor trabalha nos horários mais convenientes para seus usuários. 20. Este setor tem funcionários que dão atendimento personalizado aos seus usuários. 21. Este setor tem sempre em mente o interesse de seus usuários. 22. Os funcionários deste setor entendem as necessidades específicas de seus usuários.

Quadro 4: Correspondência entre as Dimensões Servqual e seus respectivos itens.
Fonte: Elaboração própria, adaptado de Zeithaml, V. A.; Parasuraman, A.; Berry L. L. ***Delivering Quality Service***. New York: The Free Press, 1990.

Para fins desta pesquisa, para o cálculo do índice de percepção da qualidade, somente foi levado em conta, o "Gap 5" do modelo de Parasuraman et al. (1990), ou seja, a diferença total da percepção e da expectativa da qualidade dos serviços prestados pelos sistemas da informação do Inmetro. As outras respostas servem para ilustrar esta pesquisa e para iniciar, se alguém tiver interesse, um futuro estudo além deste.

Os dados foram tratados estatisticamente pela distribuição **t** (distribuição de Student), para pequenas amostras (n<30), mas de acordo com Anderson et al. (2003) ela não se restringe às pequenas amostras, podendo ser utilizada com o intuito de corroborar ou refutar as hipóteses de teste da diferença entre duas médias da população, para comprovar ou não, a existência do "gap".

Após o teste de corroboração ou refutação das diferenças entre as duas médias, calculou-se o índice de percepção da qualidade, sendo esta, a forma de posicionar as unidades organizacionais em ordem de melhor percepção de qualidade.

5.5.3.1 AUDIN

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste *Servqual*, sobre a Qualidade dos Serviços dos Sistemas da Informação, apresentou-se desta forma:

Tabela 36: Teste *Servqual* quanto à qualidade dos serviços prestados pelos sistemas da informação.

Dimensão	Percepção	Expectativa	Gap 5	Importância
Tangibilidade	4,39	5,89	-1,50	14,71%
Confiabilidade	4,09	5,94	-1,86	24,43%
Capacidade de Resposta	4,14	5,68	-1,54	24,14%
Segurança	4,86	6,11	-1,25	21,00%
Empatia	4,71	5,91	-1,20	15,71%
Médias:	**4,44**	**5,91**	**-1,47**	**100,00%**

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos “gaps”, onde se mostra a “empatia” como sendo a dimensão com a menor distância da expectativa desses usuários, tendo a mesma, o menor hiato (gap) e a “confiabilidade” a dimensão de maior diferença entre a percepção e a expectativa da qualidade do serviço prestado:

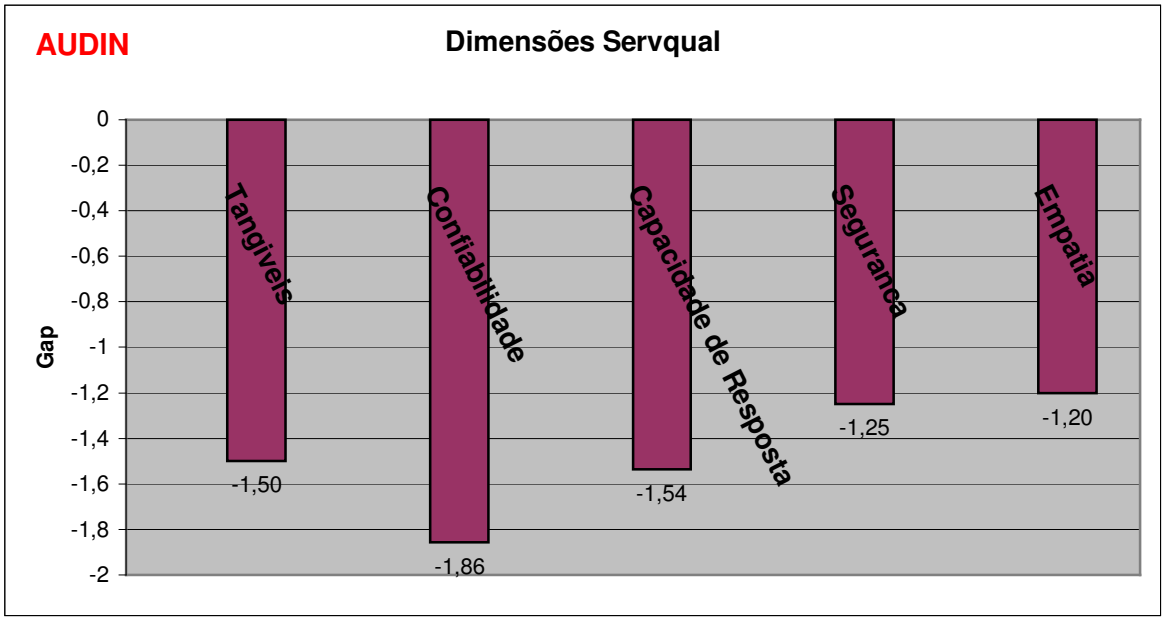


Gráfico 13: Dimensões *Servqual*
Fonte: Elaboração própria

- Em relação à importância dada para cada dimensão, esta diretoria se apresenta da seguinte forma:

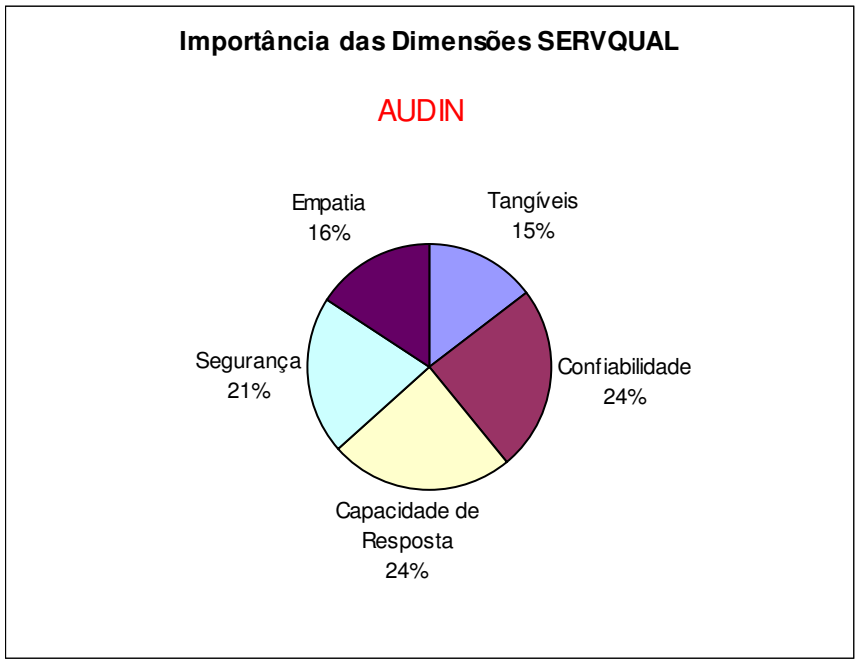


Gráfico 14: Importância das dimensões *Servqual*
Fonte: Elaboração própria

Observa-se que a dimensão "confiabilidade" foi a que teve a maior importância para os usuários desta diretoria, sendo seguida pela "capacidade de resposta", com quase a mesma importância.

- Teste de hipótese da diferença entre duas médias da população – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{e} - \mu_{p} = 0$
- H_1: $\mu_{e} - \mu_{p} \neq 0$

Onde:

μ_e = média da população das expectativas dos usuários;

μ_p = média da população das percepções dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{(\bar{x}_e - \bar{x}_p) - (\mu_e - \mu_p)}{\sqrt{s^2\left(\frac{1}{n_e} + \frac{1}{n_p}\right)}}$$

Onde:

$\bar{x}_e$ = média da amostra das expectativas;

$\bar{x}_p$ = média da amostra das percepções;

n_e = tamanho da amostra das expectativas;

n_p = tamanho da amostra das percepções;

s^2 = variância das amostras;

$$s^2 = \frac{(n_e - 1)s_e^2 + (n_p - 1)s_p^2}{n_e + n_p - 2}$$

Onde:

$n_e + n_p - 2$ = graus de liberdade (**ν**);

s_e = desvio padrão da amostra das expectativas;

s_p = desvio padrão da amostra das percepções;

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "$n_e + n_p - 2$" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\bar{x}_e$ = 5,910 $\bar{x}_p$ = 4,440

$s_e = 1{,}355$ $s_p = 1{,}460$

$n_e = 7$ $n_p = 7$

$\nu = n_e + n_p - 2 = 12$

$t_\alpha = t_{0{,}05} = 1{,}782$

$s^2 = ((7-1)*(1{,}355\text{^}2)+(7-1)*(1{,}460\text{^}2))/12 = 1{,}984$

$t = ((5{,}910 - 4{,}440) - 0) / \sqrt{((1{,}984)*((1/7)+(1/7))} = 2{,}276$

Logo:

$t = 2{,}276 > t_\alpha = t_{0{,}05} = 1{,}782$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a existência do "gap". Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a diferença entre as médias das populações é igual a zero.

Concluindo:

Índice de Percepção da Qualidade = -1,47

5.5.3.2 CAINT

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste *Servqual*, sobre a Qualidade dos Serviços dos Sistemas da Informação, apresentou-se desta forma:

Tabela 37: Teste *Servqual* quanto à qualidade dos serviços prestados pelos sistemas da informação.

Dimensão	Percepção	Expectativa	Gap 5	Importância
Tangibilidade	3,75	5,29	-1,54	10,83%
Confiabilidade	5,30	6,37	-1,07	32,50%
Capacidade de Resposta	4,46	5,75	-1,29	21,67%
Segurança	5,04	6,67	-1,63	15,83%
Empatia	5,00	6,30	-1,30	19,17%
Médias:	**4,71**	**6,08**	**-1,37**	**100,00%**

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos "gaps", onde se mostra a "confiabilidade" como sendo a dimensão com a menor distância da expectativa desses usuários, tendo a mesma, o menor hiato (gap) e a "segurança" a dimensão de maior diferença entre a percepção e a expectativa da qualidade do serviço prestado:

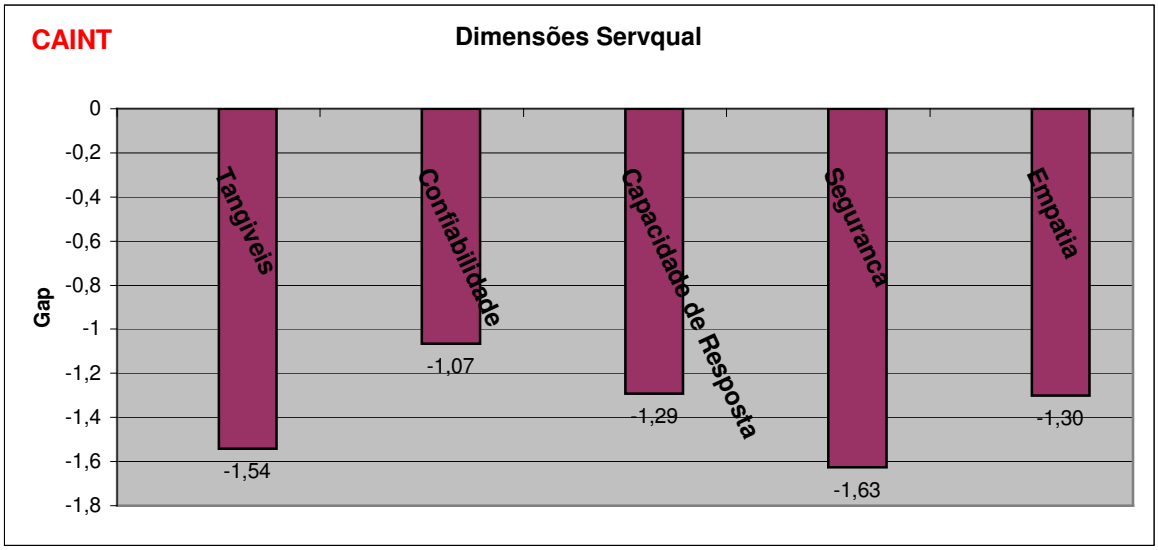


Gráfico 15: Dimensões *Servqual*
Fonte: Elaboração própria

- Em relação à importância dada para cada dimensão, esta diretoria se apresenta da seguinte forma:

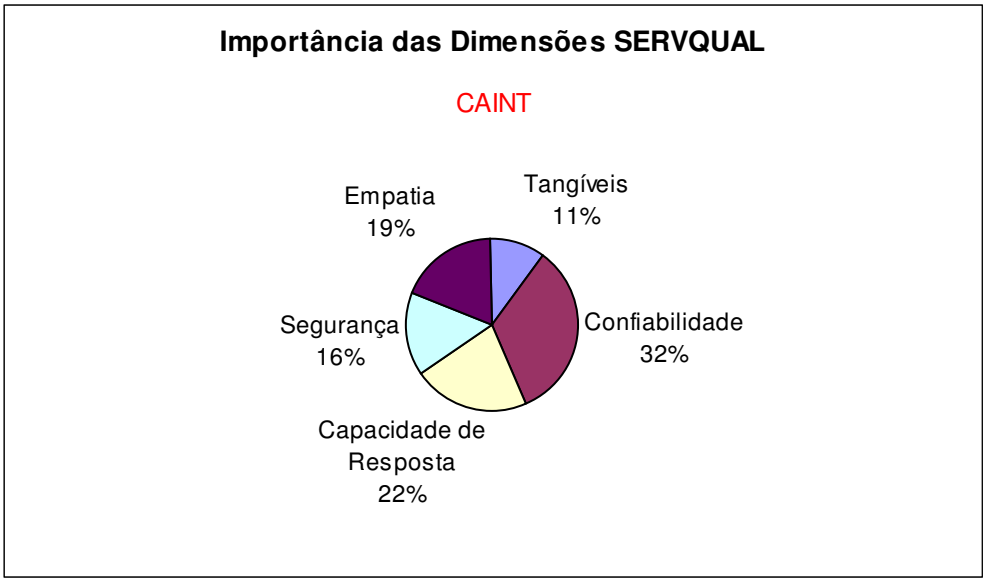


Gráfico 16: Importância das dimensões *Servqual*
Fonte: Elaboração própria

Observa-se que a dimensão “confiabilidade” foi a que teve a maior importância para os usuários desta diretoria, sendo seguida pela “capacidade de resposta”, com uma porcentagem um pouco menor de importância.

- Teste de hipótese da diferença entre duas médias da população – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{e} - \mu_{p} = 0$
- H_1: $\mu_{e} - \mu_{p} \neq 0$

Onde:

μ_{e} = média da população das expectativas dos usuários;

μ_{p} = média da população das percepções dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{(\bar{x}_e - \bar{x}_p) - (\mu_e - \mu_p)}{\sqrt{s^2\left(\frac{1}{n_e} + \frac{1}{n_p}\right)}}$$

Onde:

$\bar{x}_e$ = média da amostra das expectativas;

$\bar{x}_p$ = média da amostra das percepções;

n_e = tamanho da amostra das expectativas;

n_p = tamanho da amostra das percepções;

s^2 = variância das amostras;

$$s^2 = \frac{(n_e - 1)s_e^2 + (n_p - 1)s_p^2}{n_e + n_p - 2}$$

Onde:

$n_e + n_p - 2$ = graus de liberdade (**ν**);

s_e = desvio padrão da amostra das expectativas;

s_p = desvio padrão da amostra das percepções;

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "$n_e + n_p - 2$" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\overline{x}_e$ = 6,100 $\overline{x}_p$ = 4,750

s_e = 1,050 s_p = 1,410

n_e = 6 n_p = 6

ν = $n_e + n_p - 2$ = 10

t_α = $t_{0,05}$ = 1,812

s^2 = ((6–1)*(1,050^2)+(6-1)*(1,410^2))/10 = 1,545

t = ((6,100 – 4,750) – 0) / √ ((1,545)*((1/6)+(1/6)) = 1,969

Logo:

t = 1,969 > t_α = $t_{0,05}$ = 1,812 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a existência do "gap". Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a diferença entre as médias das populações é igual a zero.

Concluindo:

Índice de Percepção da Qualidade = -1,37

5.5.3.3 CGCRE

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste *Servqual*, sobre a Qualidade dos Serviços dos Sistemas da Informação, apresentou-se desta forma:

Tabela 38: Teste *Servqual* quanto à qualidade dos serviços prestados pelos sistemas da informação.

Dimensão	Percepção	Expectativa	Gap 5	Importância
Tangibilidade	3,43	4,80	-1,38	10,57%
Confiabilidade	4,70	6,26	-1,56	30,64%
Capacidade de Resposta	3,91	6,02	-2,11	21,71%
Segurança	5,23	6,36	-1,13	24,57%
Empatia	4,47	5,81	-1,34	12,50%
Médias:	**4,35**	**5,85**	**-1,50**	**100,00%**

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos "gaps", onde se mostra a "segurança" como sendo a dimensão com a menor distância da expectativa desses usuários, tendo a mesma, o menor hiato (gap) e a "capacidade de resposta" a dimensão de maior diferença entre a percepção e a expectativa da qualidade do serviço prestado:

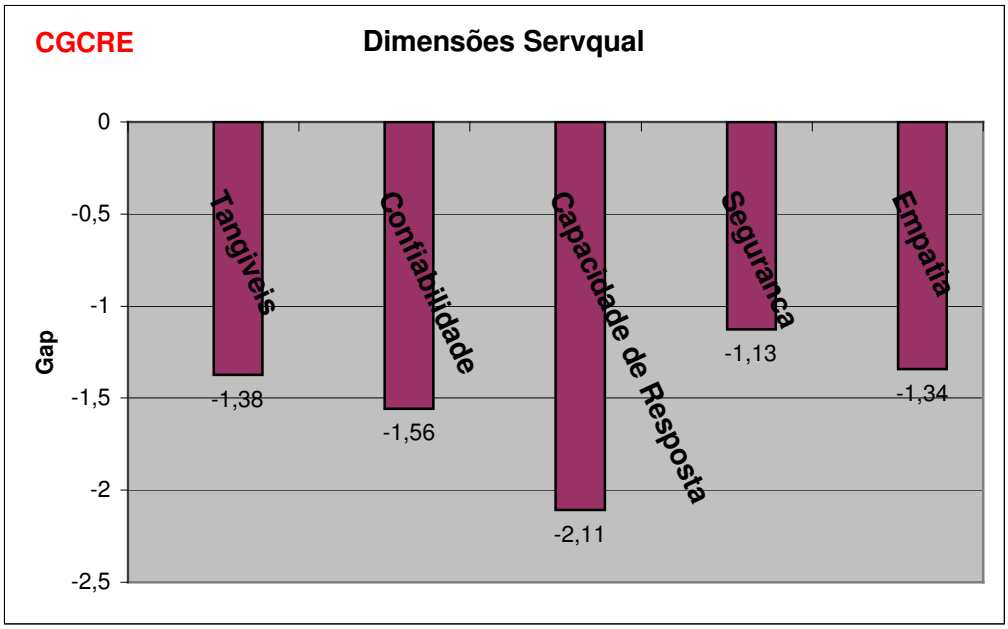


Gráfico 17: Dimensões *Servqual*
Fonte: Elaboração própria

- Em relação à importância dada para cada dimensão, esta diretoria se apresenta da seguinte forma:

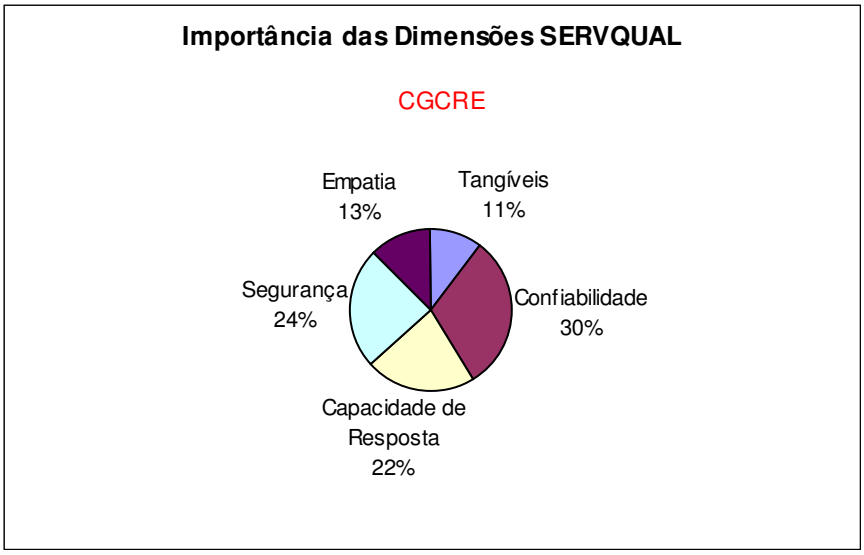


Gráfico 18: Importância das dimensões *Servqual*
Fonte: Elaboração própria

Observa-se que a dimensão "confiabilidade" foi a que teve a maior importância para os usuários desta diretoria, sendo seguida pela "segurança", com uma porcentagem um pouco menor de importância.

- Teste de hipótese da diferença entre duas médias da população – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{e} - \mu_{p} = 0$
- H_1: $\mu_{e} - \mu_{p} \neq 0$

Onde:

μ_e = média da população das expectativas dos usuários;

μ_p = média da população das percepções dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{(\overline{x}_e - \overline{x}_p) - (\mu_e - \mu_p)}{\sqrt{s^2\left(\frac{1}{n_e} + \frac{1}{n_p}\right)}}$$

Onde:

$\overline{x}_e$ = média da amostra das expectativas;

$\overline{x}_p$ = média da amostra das percepções;

n_e = tamanho da amostra das expectativas;

n_p = tamanho da amostra das percepções;

s^2 = variância das amostras;

$$s^2 = \frac{(n_e - 1)s_e^2 + (n_p - 1)s_p^2}{n_e + n_p - 2}$$

Onde:

$n_e + n_p - 2$ = graus de liberdade (**ν**);

s_e = desvio padrão da amostra das expectativas;

s_p = desvio padrão da amostra das percepções;

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "$n_e + n_p - 2$" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

$\alpha = 0,05$

$\bar{x}_e = 5,870$ $\bar{x}_p = 4,370$

$s_e = 1,980$ $s_p = 2,078$

$n_e = 14$ $n_p = 14$

$\nu = n_e + n_p - 2 = 26$

$t_\alpha = t_{0,05} = 1,706$

s^2 = ((14–1)*(1,980^2)+(14-1)*(2,078^2))/26 = 4,119

t = ((5,870 – 4,370) – 0) / √ ((4,119)*((1/14)+(1/14)) = 2,753

Logo:

t = 2,753 > $t_\alpha = t_{0,05}$ = 1,706 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a existência do "gap". Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a diferença entre as médias das populações é igual a zero.

Concluindo:

Índice de Percepção da Qualidade = -1,50

5.5.3.4 CPLAN

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste *Servqual*, sobre a Qualidade dos Serviços dos Sistemas da Informação, apresentou-se desta forma:

Tabela 39: Teste *Servqual* quanto à qualidade dos serviços prestados pelos sistemas da informação.

Dimensão	Percepção	Expectativa	Gap 5	Importância
Tangibilidade	3,90	5,59	-1,69	17,14%
Confiabilidade	5,42	6,38	-0,97	27,05%
Capacidade de Resposta	4,84	6,08	-1,24	20,14%
Segurança	5,69	6,39	-0,70	19,49%
Empatia	5,21	6,05	-0,84	16,19%
Médias:	**5,01**	**6,10**	**-1,09**	**100,00%**

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos "gaps", onde se mostra a "segurança" como sendo a dimensão com a menor distância da expectativa desses usuários, tendo a mesma, o menor hiato (gap) e a "tangibilidade" a dimensão de maior diferença entre a percepção e a expectativa da qualidade do serviço prestado:

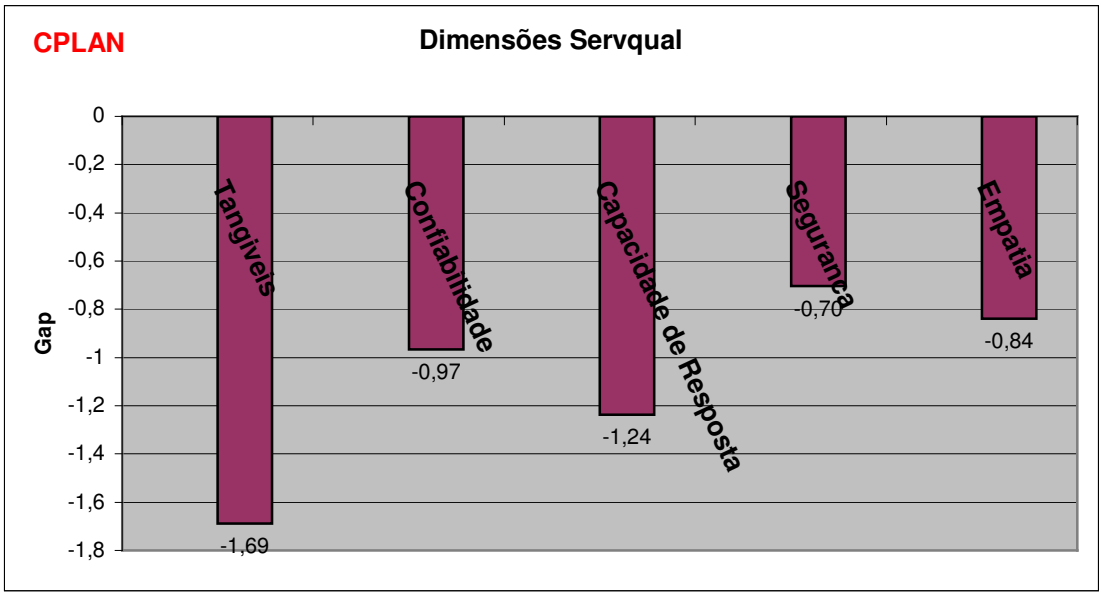


Gráfico 19: Dimensões *Servqual*
Fonte: Elaboração própria

- Em relação à importância dada para cada dimensão, esta diretoria se apresenta da seguinte forma:

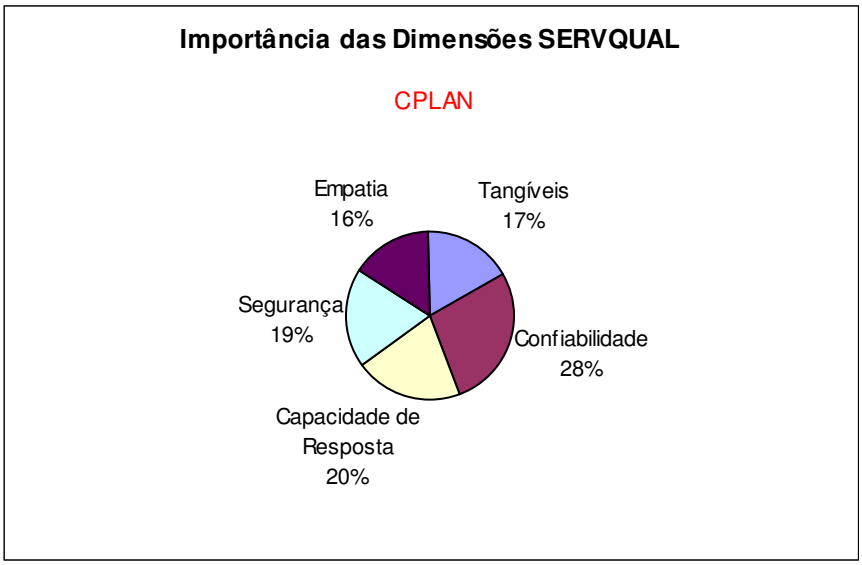


Gráfico 20: Importância das dimensões *Servqual*
Fonte: Elaboração própria

Observa-se que a dimensão "confiabilidade" foi a que teve a maior importância para os usuários desta diretoria, sendo seguida pela "capacidade de resposta", com uma porcentagem um pouco menor de importância.

- Teste de hipótese da diferença entre duas médias da população – Pequena amostra

Hipótese de nulidade da média:

- $H_0: \mu_{e} - \mu_{p} = 0$
- $H_1: \mu_{e} - \mu_{p} \neq 0$

Onde:

μ_e = média da população das expectativas dos usuários;

μ_p = média da população das percepções dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{(\bar{x}_e - \bar{x}_p) - (\mu_e - \mu_p)}{\sqrt{s^2\left(\frac{1}{n_e} + \frac{1}{n_p}\right)}}$$

Onde:

$\bar{x}_e$ = média da amostra das expectativas;

$\bar{x}_p$ = média da amostra das percepções;

n_e = tamanho da amostra das expectativas;

n_p = tamanho da amostra das percepções;

s^2 = variância das amostras;

$$s^2 = \frac{(n_e - 1)s_e^2 + (n_p - 1)s_p^2}{n_e + n_p - 2}$$

Onde:

$n_e + n_p - 2$ = graus de liberdade (**ν**);

s_e = desvio padrão da amostra das expectativas;

s_p = desvio padrão da amostra das percepções;

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "$n_e + n_p - 2$" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\bar{x}_e$ = 6,110 $\bar{x}_p$ = 5,040

$s_e = 1{,}230$ $\quad$ $s_p = 1{,}670$

$n_e = 37$ $\quad$ $n_p = 37$

$\nu = n_e + n_p - 2 = 72$

$t_\alpha = t_{0{,}05} = 1{,}668$

$s^2 = ((37-1)*(1{,}230\text{^}2)+(37-1)*(1{,}670\text{^}2))/72 = 2{,}151$

$t = ((6{,}110 - 5{,}040) - 0) / \sqrt{((2{,}151)*((1/37)+(1/37))} = 3{,}561$

Logo:

$t = 3{,}561 > t_\alpha = t_{0{,}05} = 1{,}668$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a existência do "gap". Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a diferença entre as médias das populações é igual a zero.

Concluindo:

Índice de Percepção da Qualidade = -1,09

5.5.3.5 DIMCI

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste *Servqual*, sobre a Qualidade dos Serviços dos Sistemas da Informação, apresentou-se desta forma:

Tabela 40: Teste *Servqual* quanto à qualidade dos serviços prestados pelos sistemas da informação.

Dimensão	Percepção	Expectativa	Gap 5	Importância
Tangibilidade	3,88	5,24	-1,35	13,18%
Confiabilidade	4,18	6,35	-2,18	27,35%
Capacidade de Resposta	3,99	6,03	-2,04	20,29%
Segurança	4,84	6,22	-1,38	21,53%
Empatia	4,38	5,64	-1,26	17,65%
Médias:	**4,25**	**5,89**	**-1,64**	**100,00%**

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos "gaps", onde se mostra a "empatia" como sendo a dimensão com a menor distância da expectativa desses usuários, tendo a mesma, o menor hiato (gap) e a "confiabilidade" a dimensão de maior diferença entre a percepção e a expectativa da qualidade do serviço prestado:

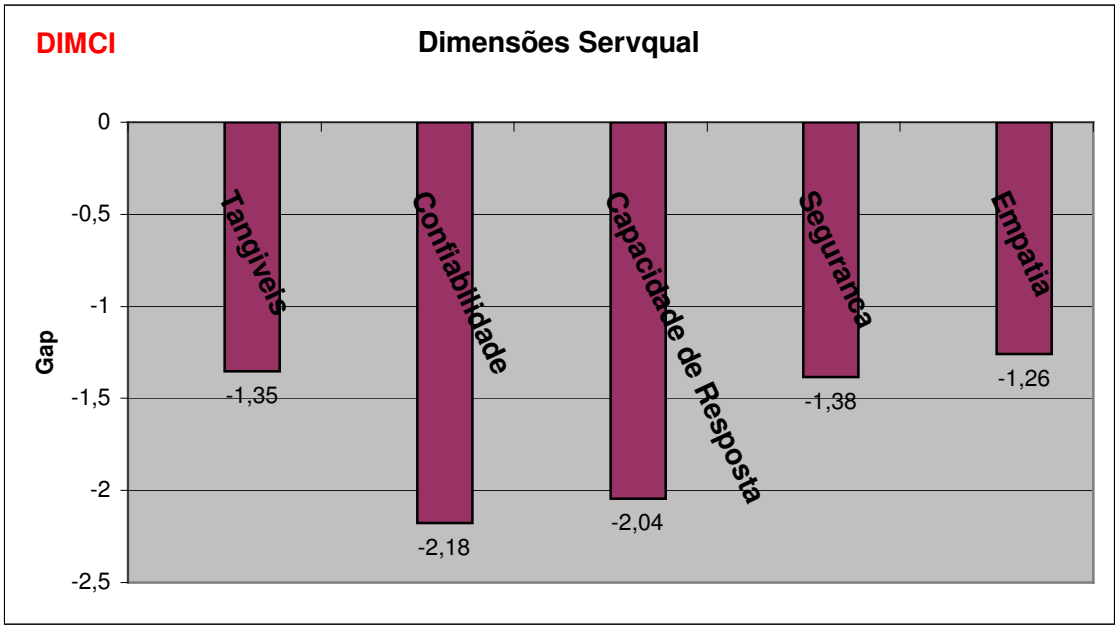


Gráfico 21: Dimensões *Servqual*
Fonte: Elaboração própria

- Em relação à importância dada para cada dimensão, esta diretoria se apresenta da seguinte forma:

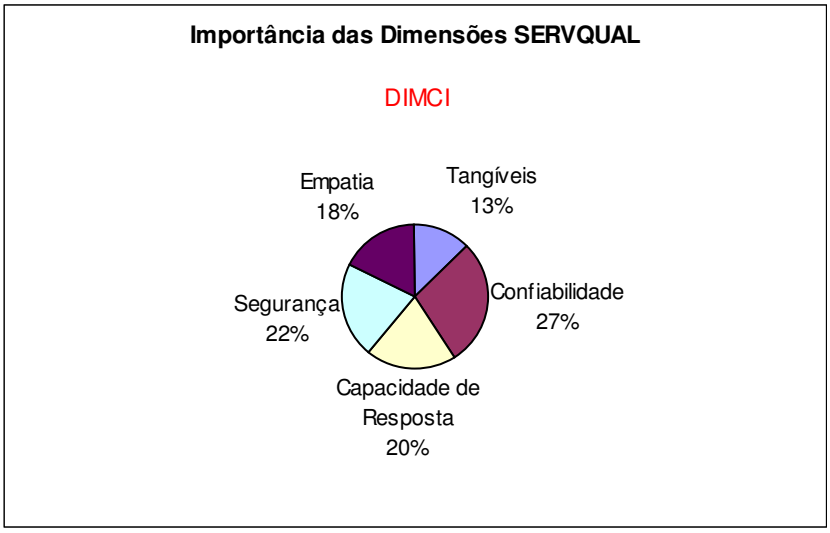


Gráfico 22: Importância das dimensões *Servqual*
Fonte: Elaboração própria

Observa-se que a dimensão “confiabilidade” foi a que teve a maior importância para os usuários desta diretoria, sendo seguida pela “segurança”, com uma porcentagem um pouco menor de importância.

- Teste de hipótese da diferença entre duas médias da população – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{e} - \mu_{p} = 0$
- H_1: $\mu_{e} - \mu_{p} \neq 0$

Onde:

μ_{e} = média da população das expectativas dos usuários;

μ_{p} = média da população das percepções dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{(\bar{x}_e - \bar{x}_p) - (\mu_e - \mu_p)}{\sqrt{s^2\left(\frac{1}{n_e} + \frac{1}{n_p}\right)}}$$

Onde:

$\bar{x}_e$ = média da amostra das expectativas;

$\bar{x}_p$ = média da amostra das percepções;

n_e = tamanho da amostra das expectativas;

n_p = tamanho da amostra das percepções;

s^2 = variância das amostras;

$$s^2 = \frac{(n_e - 1)s_e^2 + (n_p - 1)s_p^2}{n_e + n_p - 2}$$

Onde:

$n_e + n_p - 2$ = graus de liberdade (**ν**);

s_e = desvio padrão da amostra das expectativas;

s_p = desvio padrão da amostra das percepções;

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α= índice t, para α = 0,05, com "$n_e + n_p - 2$" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\overline{x}_e$ = 5,900 $\overline{x}_p$ = 4,250

s_e = 1,803 s_p = 1,887

n_e = 17 n_p = 17

ν = $n_e + n_p - 2$ = 32

t_α = $t_{0,05}$ = 1,693

s^2 = ((17–1)*(1,803^2)+(17-1)*(1,887^2))/32 = 3,406

t = ((5,900 – 4,250) – 0) / √ ((3,406)*((1/17)+(1/17)) = 3,502

Logo:

t = 3,502 > t_α = $t_{0,05}$ = 1,693 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a existência do "gap". Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a diferença entre as médias das populações é igual a zero.

Concluindo:

Índice de Percepção da Qualidade = -1,64

5.5.3.6 DIMEL

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste *Servqual*, sobre a Qualidade dos Serviços dos Sistemas da Informação, apresentou-se desta forma:

Tabela 41: Teste *Servqual* quanto à qualidade dos serviços prestados pelos sistemas da informação.

Dimensão	Percepção	Expectativa	Gap 5	Importância
Tangibilidade	3,97	5,87	-1,90	11,47%
Confiabilidade	4,44	6,45	-2,01	31,29%
Capacidade de Resposta	3,75	6,29	-2,54	21,76%
Segurança	5,15	6,50	-1,35	20,18%
Empatia	4,73	6,25	-1,52	15,29%
Médias:	**4,41**	**6,27**	**-1,86**	**100,00%**

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos "gaps", onde se mostra a "segurança" como sendo a dimensão com a menor distância da expectativa desses usuários, tendo a mesma, o menor hiato (gap) e a "capacidade de resposta" a dimensão de maior diferença entre a percepção e a expectativa da qualidade do serviço prestado:

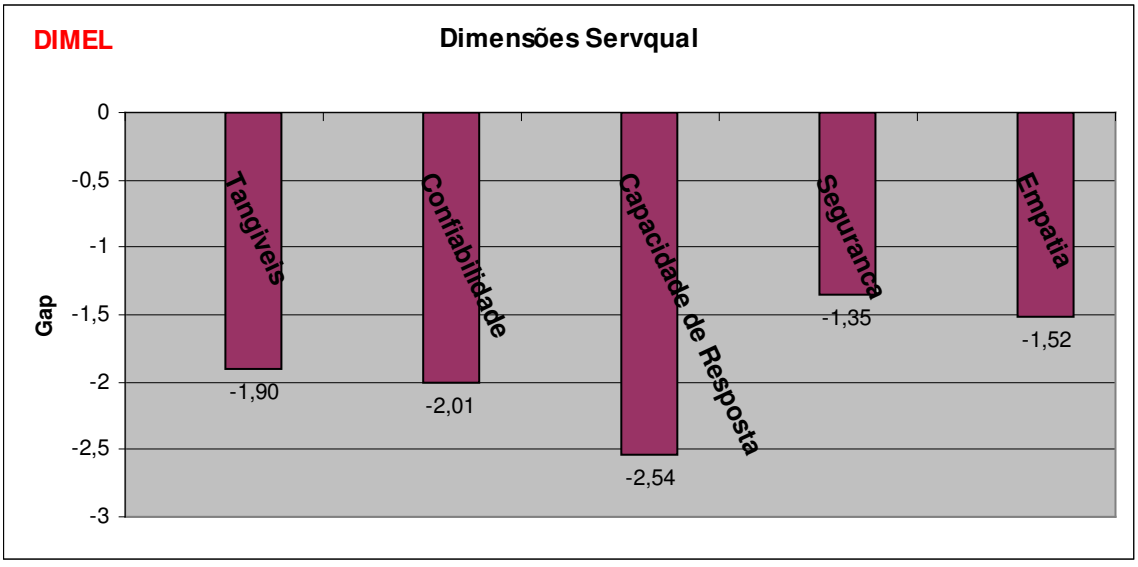


Gráfico 23: Dimensões *Servqual*
Fonte: Elaboração própria

- Em relação à importância dada para cada dimensão, esta diretoria se apresenta da seguinte forma:

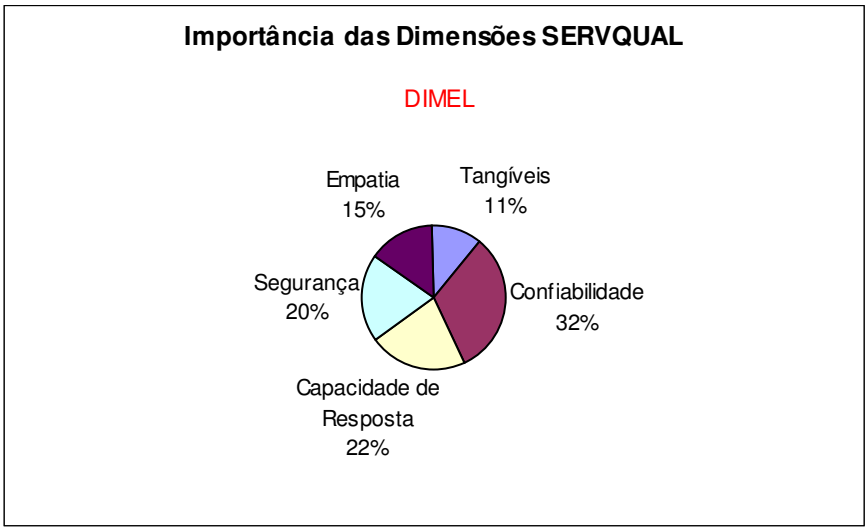


Gráfico 24: Importância das dimensões *Servqual*
Fonte: Elaboração própria

Observa-se que a dimensão "confiabilidade" foi a que teve a maior importância para os usuários desta diretoria, sendo seguida pela "capacidade de resposta", com uma porcentagem um pouco menor de importância.

- Teste de hipótese da diferença entre duas médias da população – Pequena amostra

Hipótese de nulidade da média:

- $H_0: \mu_{e} - \mu_{p} = 0$
- $H_1: \mu_{e} - \mu_{p} \neq 0$

Onde:

μ_e = média da população das expectativas dos usuários;

μ_p = média da população das percepções dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{(\overline{x}_e - \overline{x}_p) - (\mu_e - \mu_p)}{\sqrt{s^2\left(\frac{1}{n_e} + \frac{1}{n_p}\right)}}$$

Onde:

$\overline{x}_e$ = média da amostra das expectativas;

$\overline{x}_p$ = média da amostra das percepções;

n_e = tamanho da amostra das expectativas;

n_p = tamanho da amostra das percepções;

s^2 = variância das amostras;

$$s^2 = \frac{(n_e - 1)s_e^2 + (n_p - 1)s_p^2}{n_e + n_p - 2}$$

Onde:

$n_e + n_p - 2$ = graus de liberdade (**ν**);

s_e = desvio padrão da amostra das expectativas;

s_p = desvio padrão da amostra das percepções;

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "$n_e + n_p - 2$" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\overline{x}_e$ = 6,280 $\overline{x}_p$ = 4,730

$s_e = 1{,}114$ $s_p = 1{,}796$

$n_e = 17$ $n_p = 17$

$\nu = n_e + n_p - 2 = 32$

$t_\alpha = t_{0{,}05} = 1{,}693$

$s^2 = ((17–1)*(1{,}114\text{^}2)+(17\text{-}1)*(1{,}796\text{^}2))/32 = 2{,}233$

$t = ((6{,}280 – 4{,}730) – 0\ ) / \sqrt{}\ ((2{,}233)*((1/17)+(1/17)) = 3{,}372$

Logo:

$t = 3{,}372 > t_\alpha = t_{0{,}05} = 1{,}693$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a existência do "gap". Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a diferença entre as médias das populações é igual a zero.

Concluindo:

Índice de Percepção da Qualidade = -1,86

5.5.3.7 DIRAF

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste *Servqual*, sobre a Qualidade dos Serviços dos Sistemas da Informação, apresentou-se desta forma:

Tabela 42: Teste *Servqual* quanto à qualidade dos serviços prestados pelos sistemas da informação.

Dimensão	Percepção	Expectativa	Gap 5	Importância
Tangibilidade	4,01	6,01	-2,00	15,10%
Confiabilidade	5,04	6,42	-1,38	24,75%
Capacidade de Resposta	4,61	5,94	-1,33	22,25%
Segurança	5,64	6,53	-0,89	19,00%
Empatia	5,01	6,16	-1,15	18,90%
Médias:	**4,86**	**6,21**	**-1,35**	**100,00%**

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos "gaps", onde se mostra a "segurança" como sendo a dimensão com a menor distância da expectativa desses usuários, tendo a mesma, o menor hiato (gap) e a "tangibilidade" a dimensão de maior diferença entre a percepção e a expectativa da qualidade do serviço prestado:

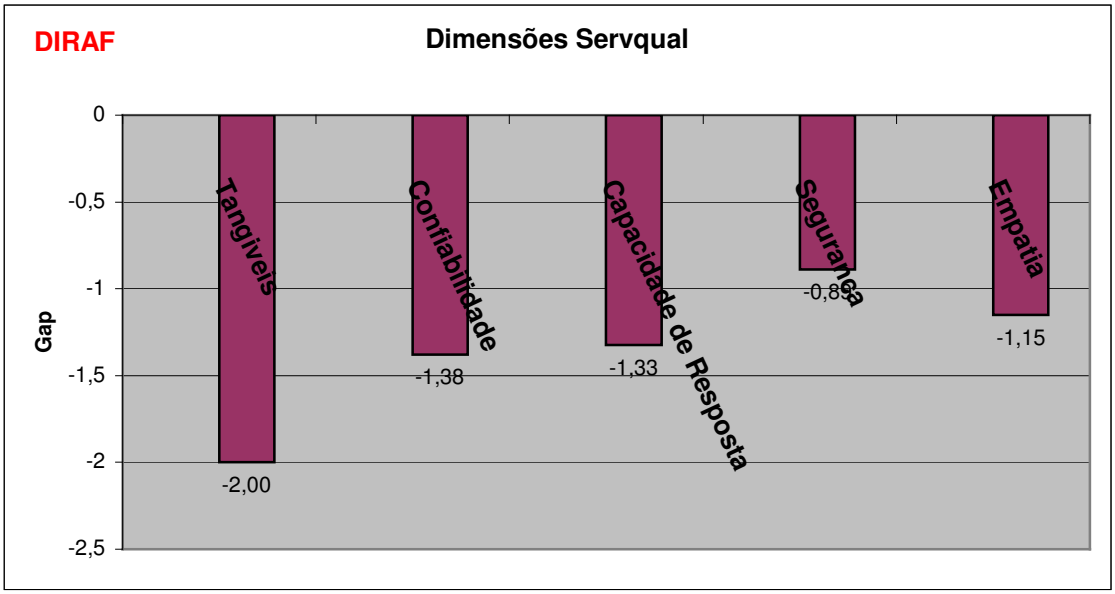


Gráfico 25: Dimensões *Servqual*
Fonte: Elaboração própria

- Em relação à importância dada para cada dimensão, esta diretoria se apresenta da seguinte forma:

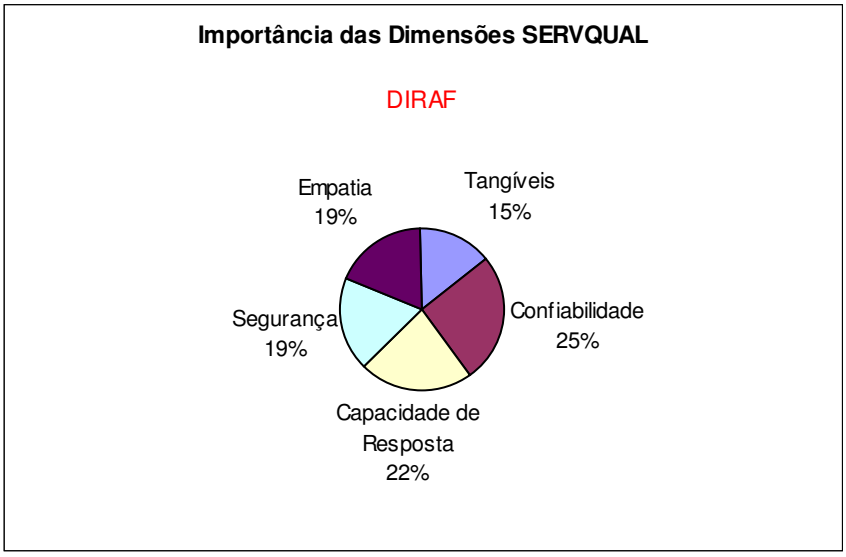


Gráfico 26: Importância das dimensões *Servqual*
Fonte: Elaboração própria

Observa-se que a dimensão “confiabilidade” foi a que teve a maior importância para os usuários desta diretoria, sendo seguida pela “capacidade de resposta”, com uma porcentagem um pouco menor de importância.

- Teste de hipótese da diferença entre duas médias da população – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{e} - \mu_{p} = 0$
- H_1: $\mu_{e} - \mu_{p} \neq 0$

Onde:

μ_e = média da população das expectativas dos usuários;

μ_p = média da população das percepções dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{(\bar{x}_e - \bar{x}_p) - (\mu_e - \mu_p)}{\sqrt{s^2\left(\frac{1}{n_e} + \frac{1}{n_p}\right)}}$$

Onde:

$\bar{x}_e$ = média da amostra das expectativas;

$\bar{x}_p$ = média da amostra das percepções;

n_e = tamanho da amostra das expectativas;

n_p = tamanho da amostra das percepções;

s^2 = variância das amostras;

$$s^2 = \frac{(n_e - 1)s_e^2 + (n_p - 1)s_p^2}{n_e + n_p - 2}$$

Onde:

$n_e + n_p - 2$ = graus de liberdade (**ν**);

s_e = desvio padrão da amostra das expectativas;

s_p = desvio padrão da amostra das percepções;

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α= índice t, para α = 0,05, com "$n_e + n_p - 2$" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\overline{x}_e$ = 6,220 $\overline{x}_p$ = 5,010

s_e = 1,071 s_p = 1,727

n_e = 20 n_p = 20

ν = $n_e + n_p - 2$ = 38

t_α = $t_{0,05}$ = 1,686

s^2 = ((20–1)*(1,071^2)+(20-1)*(1,727^2))/38 = 2,064

t = ((6,220 – 5,010) – 0) / √ ((2,064)*((1/20)+(1/20)) = 2,912

Logo:

t = 2,912 > t_α = $t_{0,05}$ = 1,686 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a existência do "gap". Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a diferença entre as médias das populações é igual a zero.

Concluindo:

Índice de Percepção da Qualidade = -1,35

5.5.3.8 DQUAL

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste *Servqual*, sobre a Qualidade dos Serviços dos Sistemas da Informação, apresentou-se desta forma:

Tabela 43: Teste *Servqual* quanto à qualidade dos serviços prestados pelos sistemas da informação.

Dimensão	Percepção	Expectativa	Gap 5	Importância
Tangibilidade	3,87	5,55	-1,68	11,25%
Confiabilidade	5,19	6,50	-1,31	28,00%
Capacidade de Resposta	5,04	6,10	-1,06	23,75%
Segurança	5,67	6,32	-0,65	20,25%
Empatia	4,98	5,75	-0,77	16,75%
Médias:	**4,95**	**6,04**	**-1,10**	**100,00%**

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos "gaps", onde se mostra a "segurança" como sendo a dimensão com a menor distância da expectativa desses usuários, tendo a mesma, o menor hiato (gap) e a "tangibilidade" a dimensão de maior diferença entre a percepção e a expectativa da qualidade do serviço prestado:

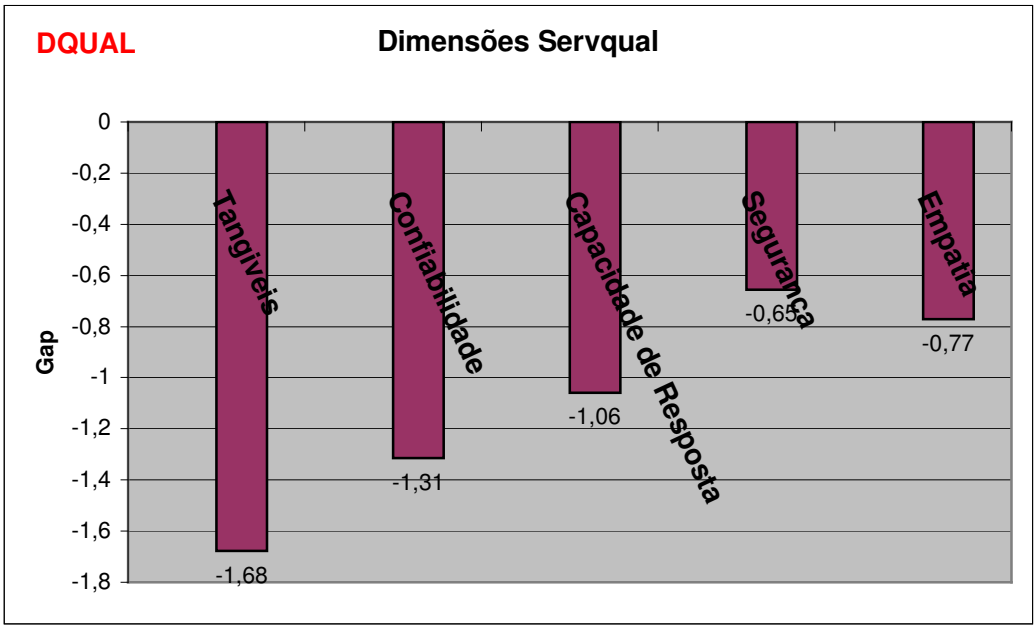


Gráfico 27: Dimensões *Servqual*
Fonte: Elaboração própria

- Em relação à importância dada para cada dimensão, esta diretoria se apresenta da seguinte forma:

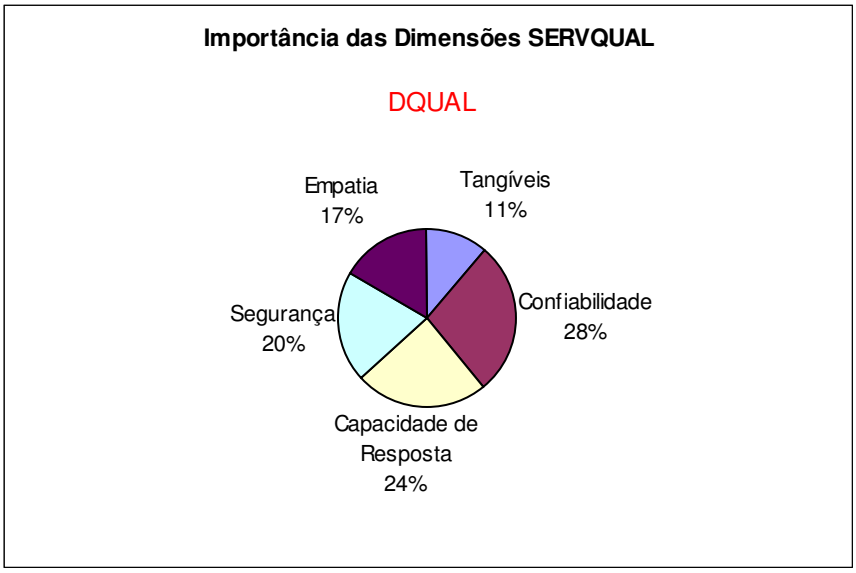


Gráfico 28: Importância das dimensões *Servqual*
Fonte: Elaboração própria

Observa-se que a dimensão "confiabilidade" foi a que teve a maior importância para os usuários desta diretoria, sendo seguida pela "capacidade de resposta", com uma porcentagem um pouco menor de importância.

- Teste de hipótese da diferença entre duas médias da população – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{e} - \mu_{p} = 0$
- H_1: $\mu_{e} - \mu_{p} \neq 0$

Onde:

μ_e = média da população das expectativas dos usuários;

μ_p = média da população das percepções dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{(\overline{x}_e - \overline{x}_p) - (\mu_e - \mu_p)}{\sqrt{s^2\left(\frac{1}{n_e} + \frac{1}{n_p}\right)}}$$

Onde:

$\overline{x}_e$ = média da amostra das expectativas;

$\overline{x}_p$ = média da amostra das percepções;

n_e = tamanho da amostra das expectativas;

n_p = tamanho da amostra das percepções;

s^2 = variância das amostras;

$$s^2 = \frac{(n_e - 1)s_e^2 + (n_p - 1)s_p^2}{n_e + n_p - 2}$$

Onde:

$n_e + n_p - 2$ = graus de liberdade (**ν**);

s_e = desvio padrão da amostra das expectativas;

s_p = desvio padrão da amostra das percepções;

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α= índice t, para α = 0,05, com "$n_e + n_p - 2$" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

$\alpha = 0,05$

$\overline{x}_e = 6,050$ $\overline{x}_p = 4,980$

$s_e = 1,460$ $s_p = 1,571$

$n_e = 21$ $n_p = 21$

$\nu = n_e + n_p - 2 = 40$

$t_\alpha = t_{0,05} = 1,684$

s^2 = ((21–1)*(1,460^2)+(21-1)*(1,571^2))/40 = 2,300

t = ((6,050 – 4,980) – 0) / √ ((2,300)*((1/21)+(1/21)) = 2,766

Logo:

t = 2,766 > $t_\alpha = t_{0,05}$ = 1,684 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a existência do "gap". Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a diferença entre as médias das populações é igual a zero.

Concluindo:

Índice de Percepção da Qualidade = -1,10

5.5.3.9 GABIN

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste *Servqual*, sobre a Qualidade dos Serviços dos Sistemas da Informação, apresentou-se desta forma:

Tabela 44: Teste *Servqual* quanto à qualidade dos serviços prestados pelos sistemas da informação.

Dimensão	Percepção	Expectativa	Gap 5	Importância
Tangibilidade	4,32	5,80	-1,48	12,21%
Confiabilidade	6,10	6,63	-0,53	30,00%
Capacidade de Resposta	5,68	6,50	-0,82	23,21%
Segurança	6,14	6,68	-0,54	18,43%
Empatia	5,93	6,56	-0,63	16,14%
Médias:	**5,63**	**6,43**	**-0,80**	**100,00%**

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos "gaps", onde se mostra a "confiabilidade" como sendo a dimensão com a menor distância da expectativa desses usuários, tendo a mesma, o menor hiato (gap) e a "tangibilidade" a dimensão de maior diferença entre a percepção e a expectativa da qualidade do serviço prestado:

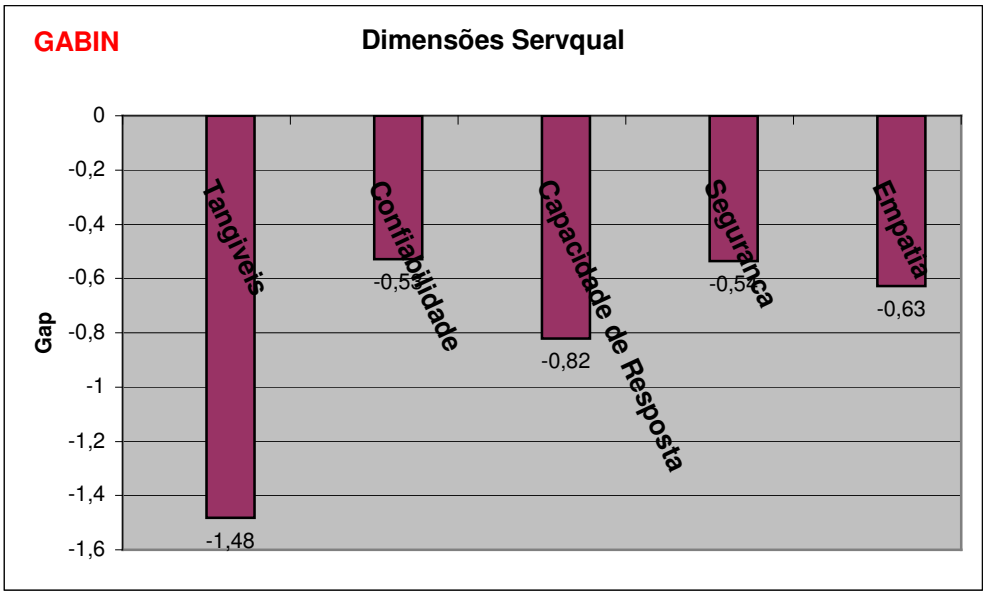


Gráfico 29: Dimensões *Servqual*
Fonte: Elaboração própria

- Em relação à importância dada para cada dimensão, esta diretoria se apresenta da seguinte forma:

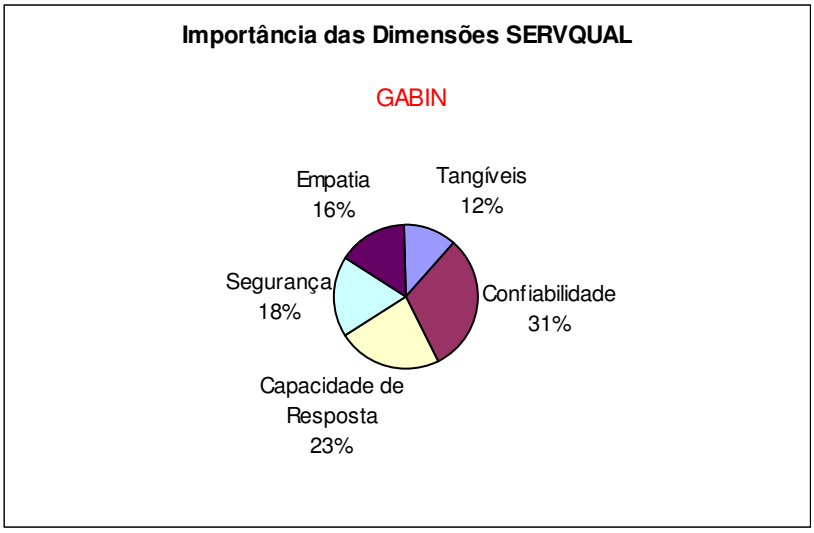


Gráfico 30: Importância das dimensões *Servqual*
Fonte: Elaboração própria

Observa-se que a dimensão "confiabilidade" foi a que teve a maior importância para os usuários desta diretoria, sendo seguida pela "capacidade de resposta", com uma porcentagem um pouco menor de importância.

- Teste de hipótese da diferença entre duas médias da população – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{e} - \mu_{p} = 0$
- H_1: $\mu_{e} - \mu_{p} \neq 0$

Onde:

μ_e = média da população das expectativas dos usuários;

μ_p = média da população das percepções dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{(\bar{x}_e - \bar{x}_p) - (\mu_e - \mu_p)}{\sqrt{s^2\left(\frac{1}{n_e} + \frac{1}{n_p}\right)}}$$

Onde:

$\bar{x}_e$ = média da amostra das expectativas;

$\bar{x}_p$ = média da amostra das percepções;

n_e = tamanho da amostra das expectativas;

n_p = tamanho da amostra das percepções;

s^2 = variância das amostras;

$$s^2 = \frac{(n_e - 1)s_e^2 + (n_p - 1)s_p^2}{n_e + n_p - 2}$$

Onde:

$n_e + n_p - 2$ = graus de liberdade (**ν**);

s_e = desvio padrão da amostra das expectativas;

s_p = desvio padrão da amostra das percepções;

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "$n_e + n_p - 2$" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\bar{x}_e$ = 6,450 $\bar{x}_p$ = 5,670

$s_e = 1{,}090$ $\quad$ $s_p = 1{,}390$

$n_e = 14$ $\quad$ $n_p = 14$

$\nu = n_e + n_p - 2 = 26$

$t_\alpha = t_{0{,}05} = 1{,}706$

$s^2 = ((14–1)*(1{,}090\text{^}2)+(14\text{-}1)*(1{,}390\text{^}2))/26 = 1{,}560$

$t = ((6{,}450 – 5{,}670) – 0) / \sqrt{}((1{,}560)*((1/14)+(1/14)) = 1{,}750$

Logo:

$t = 1{,}750 > t_\alpha = t_{0{,}05} = 1{,}706$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a existência do "gap". Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a diferença entre as médias das populações é igual a zero.

Concluindo:

Índice de Percepção da Qualidade = -0,80

5.5.3.10 PROGE

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste *Servqual*, sobre a Qualidade dos Serviços dos Sistemas da Informação, apresentou-se desta forma:

Tabela 45: Teste *Servqual* quanto à qualidade dos serviços prestados pelos sistemas da informação.

Dimensão	Percepção	Expectativa	Gap 5	Importância
Tangibilidade	3,21	5,36	-2,14	10,71%
Confiabilidade	4,37	5,69	-1,31	25,00%
Capacidade de Resposta	3,79	5,50	-1,71	22,86%
Segurança	4,79	5,75	-0,96	21,43%
Empatia	4,11	5,49	-1,37	20,00%
Médias:	**4,05**	**5,56**	**-1,50**	**100,00%**

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos "gaps", onde se mostra a "segurança" como sendo a dimensão com a menor distância da expectativa desses usuários, tendo a mesma, o menor hiato (gap) e a "tangibilidade" a dimensão de maior diferença entre a percepção e a expectativa da qualidade do serviço prestado:

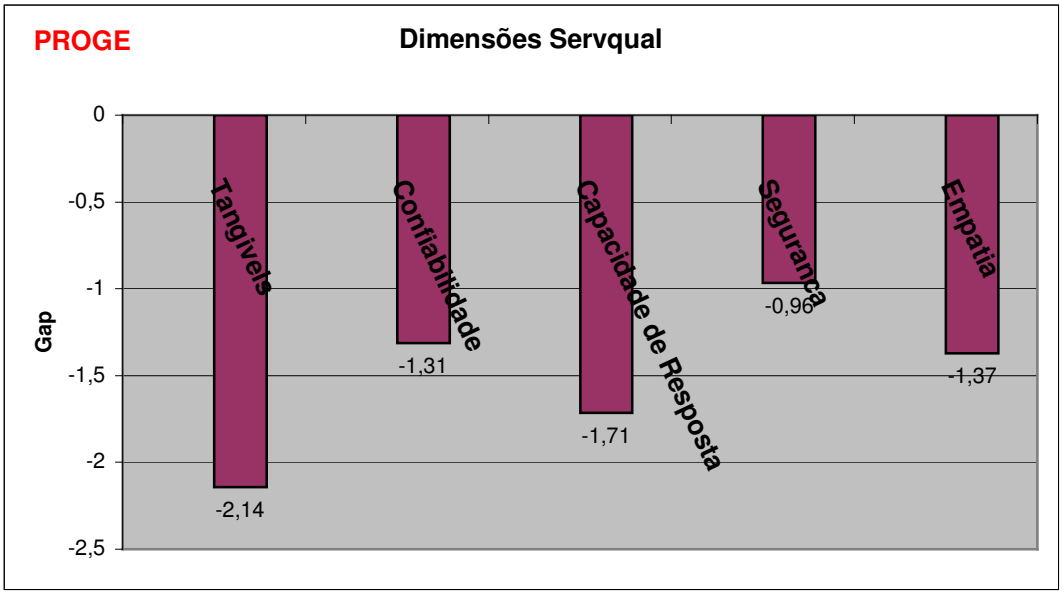


Gráfico 31: Dimensões *Servqual*
Fonte: Elaboração própria

- Em relação à importância dada para cada dimensão, esta diretoria se apresenta da seguinte forma:

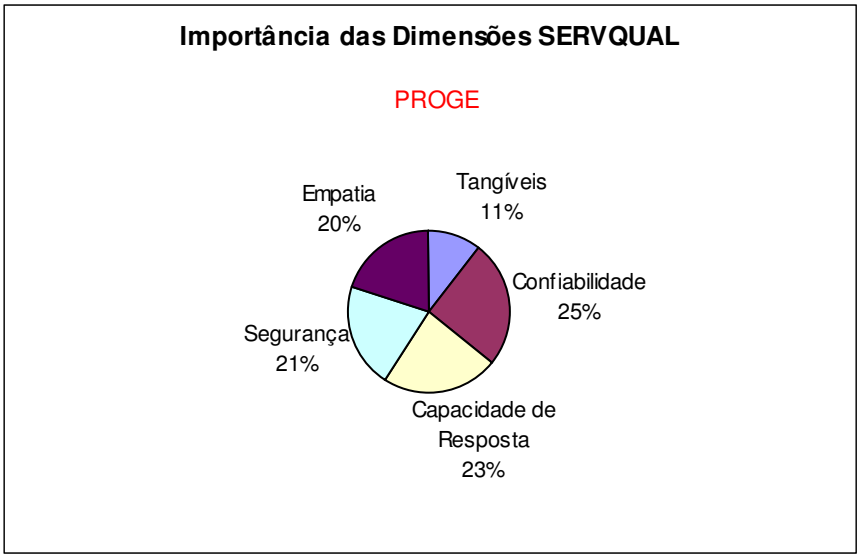


Gráfico 32: Importância das dimensões *Servqual*
Fonte: Elaboração própria

Observa-se que a dimensão “confiabilidade” foi a que teve a maior importância para os usuários desta diretoria, sendo seguida pela “capacidade de resposta”, com uma porcentagem um pouco menor de importância.

- Teste de hipótese da diferença entre duas médias da população – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{e} - \mu_{p} = 0$
- H_1: $\mu_{e} - \mu_{p} \neq 0$

Onde:

μ_{e} = média da população das expectativas dos usuários;

μ_{p} = média da população das percepções dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{(\bar{x}_e - \bar{x}_p) - (\mu_e - \mu_p)}{\sqrt{s^2\left(\frac{1}{n_e} + \frac{1}{n_p}\right)}}$$

Onde:

$\bar{x}_e$ = média da amostra das expectativas;

$\bar{x}_p$ = média da amostra das percepções;

n_e = tamanho da amostra das expectativas;

n_p = tamanho da amostra das percepções;

s^2 = variância das amostras;

$$s^2 = \frac{(n_e - 1)s_e^2 + (n_p - 1)s_p^2}{n_e + n_p - 2}$$

Onde:

$n_e + n_p - 2$ = graus de liberdade (**ν**);

s_e = desvio padrão da amostra das expectativas;

s_p = desvio padrão da amostra das percepções;

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α= índice t, para α = 0,05, com "$n_e + n_p - 2$" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\overline{x}_e$ = 5,560 $\overline{x}_p$ = 4,070

s_e = 2,370 s_p = 2,370

n_e = 7 n_p = 7

ν = $n_e + n_p - 2$ = 12

t_α = $t_{0,05}$ = 1,782

s^2 = ((7–1)*(2,370^2)+(7-1)*(2.370^2))/12 = 5,617

t = ((5,560 – 4,070) – 0) / √ ((5,617)*((1/7)+(1/7)) = 1,811

Logo:

t = 1,811 > t_α = $t_{0,05}$ = 1,782 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a existência do "gap". Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a diferença entre as médias das populações é igual a zero.

Concluindo:

Índice de Percepção da Qualidade = -1,50

5.5.3.11 RESULTADO DO ÍNDICE DE PERCEPÇÃO DA QUALIDADE

Após o término dos cálculos e teste de corroboração ou refutação da média, tem-se o índice de percepção de qualidade, como a forma de posicionar as unidades organizacionais em ordem de melhor percepção de qualidade. Abaixo, são apresentados os resultados e as respectivas colocações das diretorias do Inmetro, na parte da pesquisa relativa a percepção de qualidade de serviços:

Tabela 46: Índice de percepção de qualidade nas diretorias

Ordem:	Diretoria:	GAP
1	GABIN	-0,80
2	CPLAN	-1,09
3	DQUAL	-1,10
4	DIRAF	-1,35
5	CAINT	-1,37
6	AUDIN	-1,47
7	CGCRE	-1,50
8	PROGE	-1,50
9	DIMCI	-1,64
10	DIMEL	-1,86

Fonte: Elaboração própria

Pode-se perceber que mesmo as duas piores diretorias, não possuem valores altos de gap, indicando que a instituição como um todo tem uma boa percepção da qualidade dos serviços prestados pelos sistemas de informação.

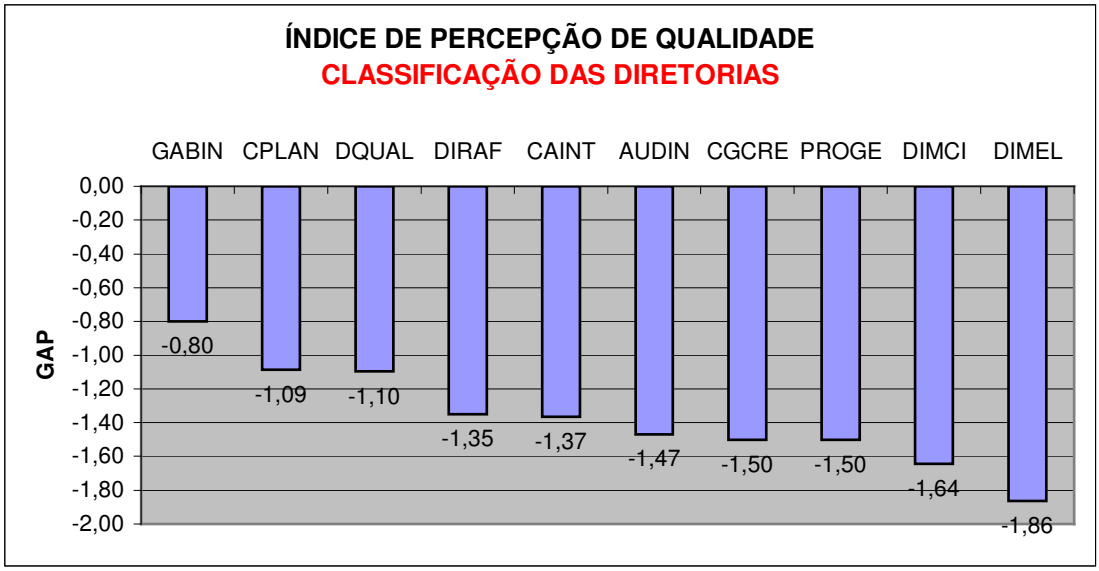


Gráfico 33: Classificação das Diretorias em relação à Percepção da Qualidade
Fonte: Elaboração própria

5.5.4 CÁLCULO DO ÍNDICE DE PERCEPÇÃO DA LIDERANÇA

Para este cálculo, foram tabulados os resultados da pesquisa obtida através das respostas, por meio de amostras aleatórias dos usuários, ao questionário LPI de práticas de liderança, dentro de cada diretoria. O questionário foi disponibilizado através de um "portal web" (Anexo D), de forma a facilitar aos usuários respondê-lo, como também, facilitar a tabulação das respostas, sendo essas armazenadas diretamente no banco de dados da pesquisa.

Para fins desta pesquisa, para o cálculo do índice de percepção da liderança, não foi levada em consideração a auto-avaliação pelos diretores do Inmetro, que por diversos motivos, não foram possíveis de conseguir. Essas respostas poderão fazer parte de uma nova pesquisa e para iniciar, se alguém tiver interesse, um futuro estudo além deste.

Os dados foram tratados estatisticamente pela distribuição t (distribuição de Student), para pequenas amostras (n<30), mas de acordo com Anderson et al. (2003) ela não se restringe às pequenas amostras, podendo ser utilizada com o intuito de corroborar ou refutar as hipóteses de teste da média da população. Este tratamento estatístico baseou-se na análise das respostas dos questionários utilizando a Média Aritmética (*Me*), isto é, "a soma das observações dividida pelo número delas". As questões do teste foram separadas pelos Princípios de Liderança e os resultados das respostas foram transcritos nas tabelas, onde a

soma das médias representa o resultado (mínimo = 0 ponto e máximo = 60 pontos) do Princípio de Liderança em análise, conforme ilustração abaixo:

Princípios de Liderança e respectivos itens:	Médias:	Soma das Médias:
Desafiar o Estabelecido		
1. Procura desafios e oportunidades que testem as habilidades e o talento de cada um	x	
6. Mantém a equipe atualizada com as principais e mais recentes mudanças da organização	x	
11. Desafia (questiona) os caminhos existentes para a realização do trabalho	x	
16. Está atento para inovações que podem melhorar a organização e o projeto	x	∑x
21. Pergunta "O que nós podemos aprender?" quando as coisas não saem conforme o planejado	x	
26. Avalia os riscos de novos procedimentos e abordagens quando existe chance de falha	x	
Inspirar uma Visão Compartilhada		
2. Descreve um futuro que todos desejam criar	x	
7. Envolve a equipe, tornando único entre líder e liderados os sonhos de futuro	x	
12. Possui uma comunicação clara, positiva e promissora sobre o futuro da organização	x	
17. Mostra à equipe como futuro de longo prazo, os objetivos que podem ser alcançados através de uma visão de futuro comum	x	∑x
22. Olha à frente e para as previsões quanto ao futuro da organização e dos acontecimentos do projeto	x	
27. É motivador e entusiasta sobre as possibilidades futuras	x	
Permitir que os Outros Ajam		
3. Envolve a todos no planejamento, decisões e ações que estão ocorrendo ou são necessárias	x	
8. Trata a todos com dignidade e respeito	x	
13. Fornece à equipe autoridade para tomar suas próprias decisões	x	∑x
18. Desenvolve um ambiente de equipe com relações de cooperação entre os participantes	x	
23. Cria uma atmosfera de confiança mútua entre os participantes da equipe	x	
28. Possibilita à equipe uma sensação de donos do projeto em que estão trabalhando	x	
Apontar o Caminho		
4. É claro quanto à forma de pensar sobre liderança	x	
9. Mantém os projetos orientados dentro dos prazos previstos e as metas planejadas	x	
14. Dedica tempo e energia para disseminar valores e crenças referentes à organização	x	
19. Permite que a equipe conheça seus valores e suas crenças sobre a qual a melhor forma de conduzir os projetos e a organização	x	∑x
24. Apresenta coerência entre a prática e o discurso	x	
29. Assegura que o trabalho de equipe tem objetivos claros, com etapas e metas bem definidas que sejam de conhecimento de todos	x	
Encorajar o Coração		
5. Dedica um tempo para comemorar e recompensar as vitórias (objetivos atingidos) com toda a equipe envolvida	x	
10. Assegura que a equipe é reconhecida por suas contribuições para o sucesso dos projetos	x	
15. Elogia a equipe quando um trabalho é bem feito	x	
20. Valoriza os esforços e as contribuições da equipe, dando suporte às atividades	x	∑x
25. Procura formas de celebrar o sucesso dos projetos	x	
30. Divulga para o resto da organização os resultados obtidos e a importância da participação de cada membro da equipe	x	

Quadro 5: Correspondência entre os Princípios de Liderança, seus respectivos itens e os cálculos das somas das médias.
Fonte: Elaboração própria.

Após o teste de corroboração ou refutação da média, calculou-se o índice de percepção de liderança (a média total dos Princípios de Liderança), sendo esta, a forma de posicionar as unidades organizacionais em ordem de melhor percepção de liderança das diretorias.

5.5.4.1 AUDIN

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Liderança (LPI), apresentou-se desta forma:

Tabela 47: Teste LPI quanto ao perfil de liderança.

PRINCÍPIOS DE LIDERANÇA	Soma das médias	Índice de liderança
Desafiar o Estabelecido	53,000	
Inspirar uma Visão Compartilhada	53,000	
Permitir que os Outros Ajam	54,600	**53,720**
Apontar o Caminho	51,600	
Encorajar o Coração	56,400	

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos princípios de liderança, onde se mostra como o principal princípio, "Encorajar o Coração", seguido por "Permitir que os Outros Ajam". Sendo "Apontar o Caminho", o princípio mais fraco da liderança da diretoria.

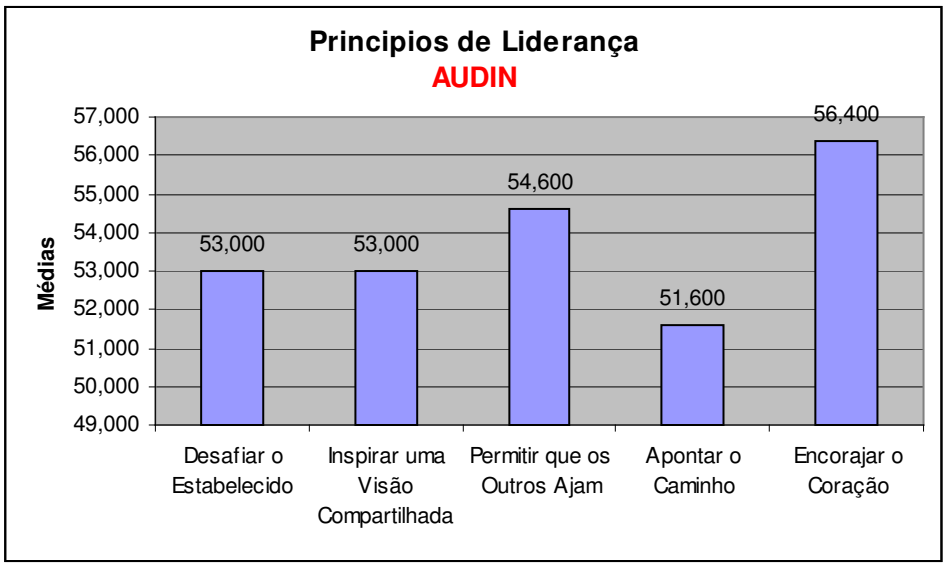


Gráfico 34: Princípios de Liderança
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para $\alpha = 0,05$, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

$\alpha = 0,05$

$\bar{x}$ = 8,953

s = 1,547

n = 5

ν = n –1 = 4

$t_\alpha = t_{0,05} = 2,132$

t = (8,953 – 0) / (1,547 / √ 5) = 12,940

Logo:

t = 12,940 > $t_\alpha = t_{0,05} = 2,132$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Liderança = 53,720

5.5.4.2 CAINT

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Liderança (LPI), apresentou-se desta forma:

Tabela 48: Teste LPI quanto ao perfil de liderança.

PRINCÍPIOS DE LIDERANÇA	Soma das médias	Índice de liderança
Desafiar o Estabelecido	44,800	
Inspirar uma Visão Compartilhada	45,800	
Permitir que os Outros Ajam	45,200	**44,880**
Apontar o Caminho	43,200	
Encorajar o Coração	45,400	

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos princípios de liderança, onde se mostra como o principal princípio, "Inspirar uma Visão Compartilhada", seguido por "Encorajar o Coração". Sendo "Apontar o Caminho", o princípio mais fraco da liderança da diretoria.

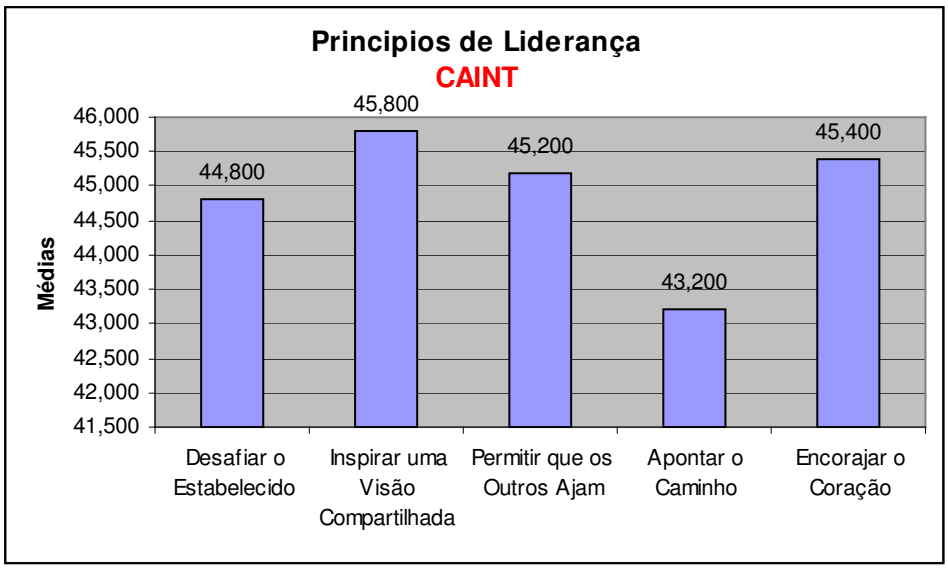


Gráfico 35: Princípios de Liderança
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para $\alpha = 0,05$, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

$\alpha = 0,05$

$\bar{x} = 7,480$

$s = 2,399$

n = 5

$\nu = n - 1 = 4$

$t_\alpha = t_{0,05} = 2,132$

$t = (7,480 - 0) / (2,399 / \sqrt{5}) = 6,972$

Logo:

$t = 6{,}972 > t_{\alpha} = t_{0{,}05} = 2{,}132$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Liderança = 44,880

5.5.4.3 CGCRE

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Liderança (LPI), apresentou-se desta forma:

Tabela 49: Teste LPI quanto ao perfil de liderança.

PRINCÍPIOS DE LIDERANCA	Soma das medias	Indice de lideranca
Desafiar o Estabelecido	39,615	40,862
Inspirar uma Visão Compartilhada	40,154	
Permitir que os Outros Ajam	43,385	
Apontar o Caminho	40,769	
Encorajar o Coração	40,385	

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos princípios de liderança, onde se mostra como o principal princípio, “Permitir que os Outros Ajam”, seguido por “Apontar o Caminho”. Sendo “Desafiar o Estabelecido”, o princípio mais fraco da liderança da diretoria.

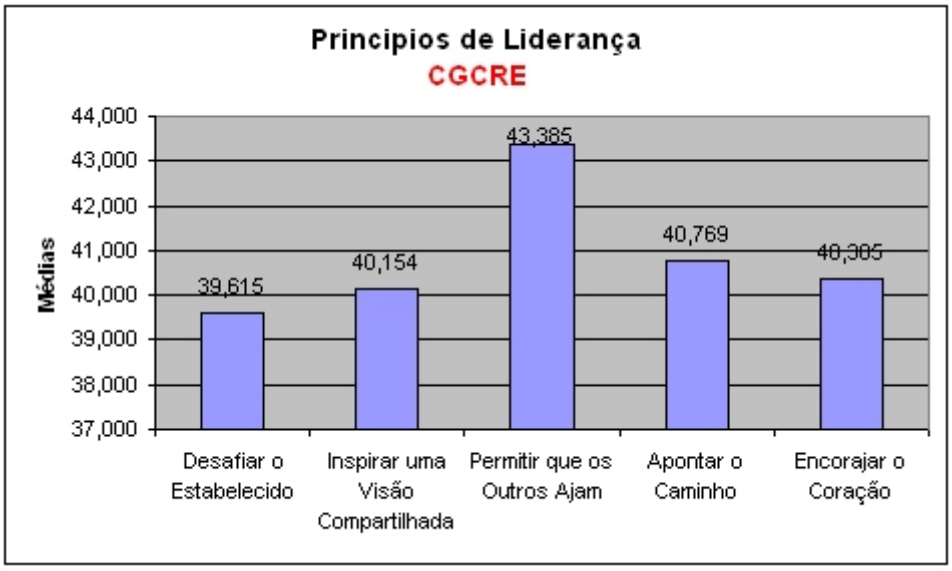


Gráfico 36: Princípios de Liderança
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  $\bar{x}$ = 6,810

  s = 2,745

  n = 13

  ν = n –1 = 12

  $t_\alpha = t_{0,05}$ = 1,782

  t = (6,810 – 0) / (2,745 / √ 13) = 8,944

Logo:

t = 8,944 > $t_\alpha = t_{0,05}$ = 1,782 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Liderança = 40,862

5.5.4.4 CPLAN

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Liderança (LPI), apresentou-se desta forma:

Tabela 50: Teste LPI quanto ao perfil de liderança.

PRINCÍPIOS DE LIDERANÇA	Soma das médias	Índice de liderança
Desafiar o Estabelecido	38,919	
Inspirar uma Visão Compartilhada	36,676	
Permitir que os Outros Ajam	40,054	**38,259**
Apontar o Caminho	38,162	
Encorajar o Coração	37,486	

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos princípios de liderança, onde se mostra como o principal princípio, "Permitir que os Outros Ajam", seguido por "Desafiar o Estabelecido". Sendo "Inspirar uma Visão Compartilhada", o princípio mais fraco da liderança da diretoria.

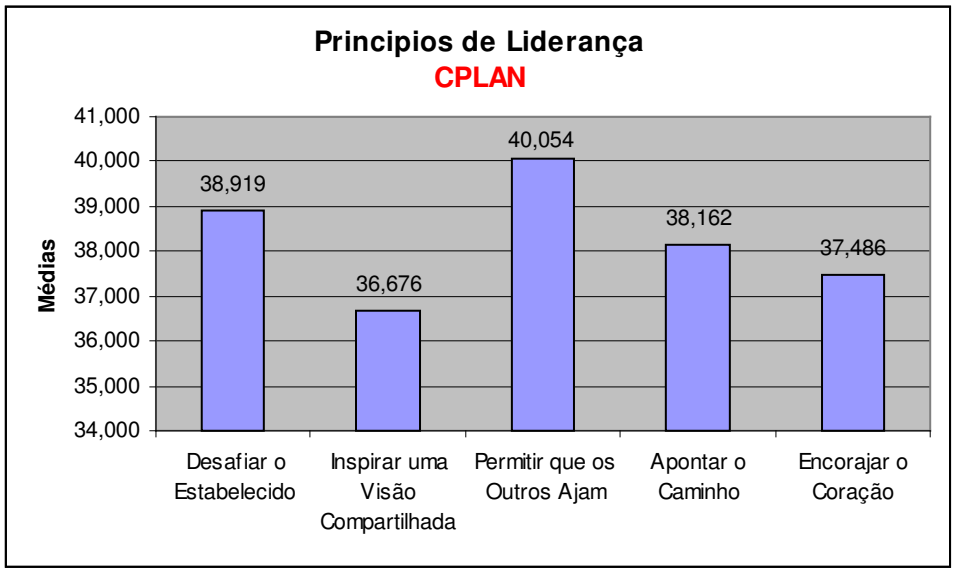


Gráfico 37: Princípios de Liderança
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para $\alpha = 0,05$, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

$\alpha = 0,05$

$\bar{x} = 6,377$

s = 3,098

n = 37

ν = n –1 = 36

$t_\alpha = t_{0,05} = 1,692$

t = (6,377 – 0) / (3,098 / √ 37) = 12,521

Logo:

t = 12,521 > $t_\alpha = t_{0,05} = 1,692$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Liderança = 38,259

5.5.4.5 DIMCI

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Liderança (LPI), apresentou-se desta forma:

Tabela 51: Teste LPI quanto ao perfil de liderança.

PRINCÍPIOS DE LIDERANÇA	Soma das médias	Índice de liderança
Desafiar o Estabelecido	39,176	
Inspirar uma Visão Compartilhada	39,588	
Permitir que os Outros Ajam	40,471	**38,882**
Apontar o Caminho	36,882	
Encorajar o Coração	38,294	

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos princípios de liderança, onde se mostra como o principal princípio, “Permitir que os Outros Ajam”, seguido por “Inspirar uma Visão Compartilhada”. Sendo “Apontar o Caminho”, o princípio mais fraco da liderança da diretoria.

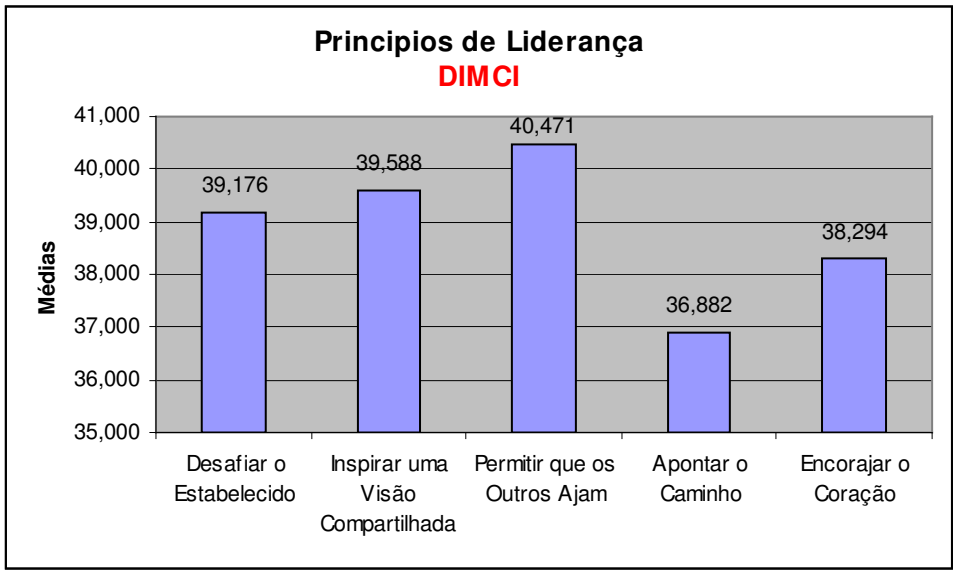


Gráfico 38: Princípios de Liderança
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  $\bar{x}$ = 6,480

  s = 2,704

  n = 17

  ν = n –1 = 16

  $t_\alpha = t_{0,05}$ = 1,746

  t = (6,480 – 0) / (2,704 / √ 17) = 9,882

Logo:

t = 9,882 > $t_\alpha = t_{0,05}$ = 1,746 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Liderança = 38,882

5.5.4.6 DIMEL

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Liderança (LPI), apresentou-se desta forma:

Tabela 52: Teste LPI quanto ao perfil de liderança.

PRINCÍPIOS DE LIDERANÇA	Soma das médias	Índice de liderança
Desafiar o Estabelecido	31,471	
Inspirar uma Visão Compartilhada	31,235	
Permitir que os Outros Ajam	30,235	**30,400**
Apontar o Caminho	30,412	
Encorajar o Coração	28,647	

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos princípios de liderança, onde se mostra como o principal princípio, "Desafiar o Estabelecido", seguido por "Inspirar uma Visão Compartilhada". Sendo "Encorajar o Coração", o princípio mais fraco da liderança da diretoria.

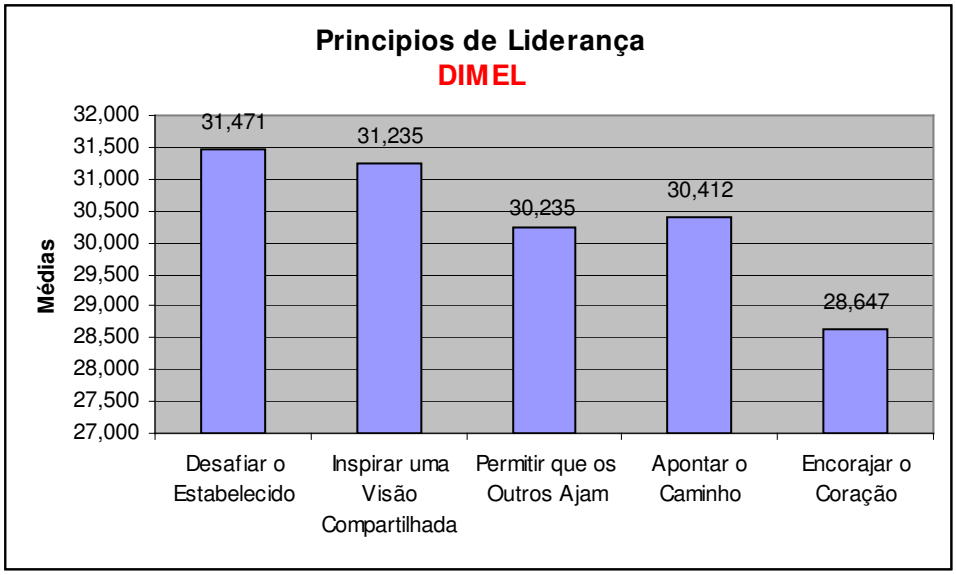


Gráfico 39: Princípios de Liderança
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\bar{x}$ = 5,067

s = 3,047

$n = 17$

$\nu = n - 1 = 16$

$t_\alpha = t_{0,05} = 1,746$

$t = (5,067 - 0) / (3,047 / \sqrt{17}) = 6,856$

Logo:

$t = 6,856 > t_\alpha = t_{0,05} = 1,746$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Liderança = 30,400

5.5.4.7 DIRAF

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Liderança (LPI), apresentou-se desta forma:

Tabela 53: Teste LPI quanto ao perfil de liderança.

PRINCÍPIOS DE LIDERANÇA	Soma das médias	Índice de liderança
Desafiar o Estabelecido	45,438	
Inspirar uma Visão Compartilhada	43,875	
Permitir que os Outros Ajam	49,625	**46,300**
Apontar o Caminho	45,500	
Encorajar o Coração	47,063	

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos princípios de liderança, onde se mostra como o principal princípio, “Permitir que os Outros Ajam”, seguido por “Encorajar o Coração”. Sendo “Inspirar uma Visão Compartilhada”, o princípio mais fraco da liderança da diretoria.

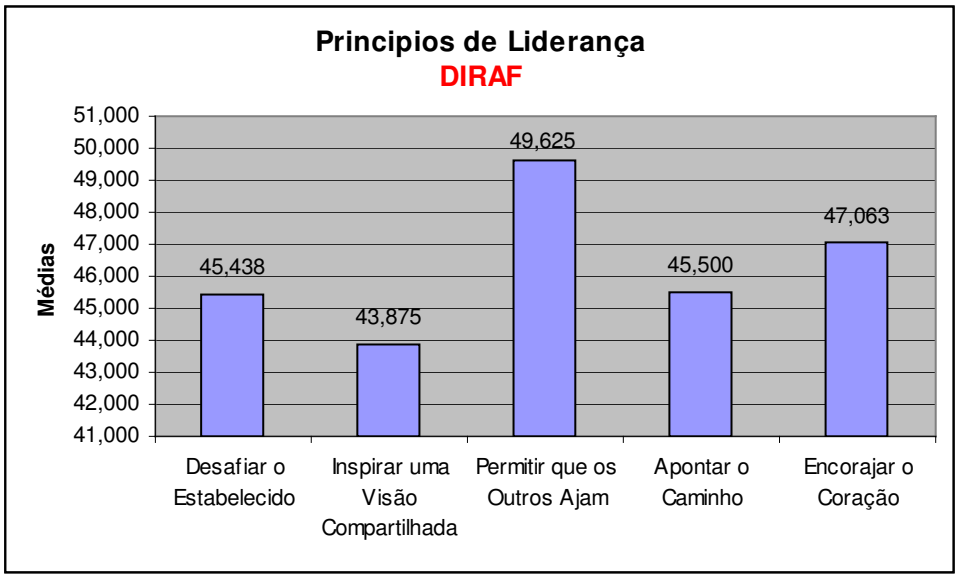


Gráfico 40: Princípios de Liderança
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\bar{x}$ = 7,717

s = 2,243

n = 16

ν = n –1 = 15

$t_\alpha = t_{0,05} = 1,753$

t = (7,717 – 0) / (2,243 / √ 16) = 13,762

Logo:

t = 13,762 > $t_\alpha = t_{0,05} = 1,753$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Liderança = 46,300

5.5.4.8 DQUAL

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Liderança (LPI), apresentou-se desta forma:

Tabela 54: Teste LPI quanto ao perfil de liderança.

PRINCÍPIOS DE LIDERANÇA	Soma das médias	Índice de liderança
Desafiar o Estabelecido	44,600	
Inspirar uma Visão Compartilhada	42,550	
Permitir que os Outros Ajam	41,550	**42,510**
Apontar o Caminho	41,350	
Encorajar o Coração	42,500	

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos princípios de liderança, onde se mostra como o principal princípio, "Desafiar o Estabelecido", seguido por "Inspirar uma Visão Compartilhada". Sendo "Apontar o Caminho", o princípio mais fraco da liderança da diretoria.

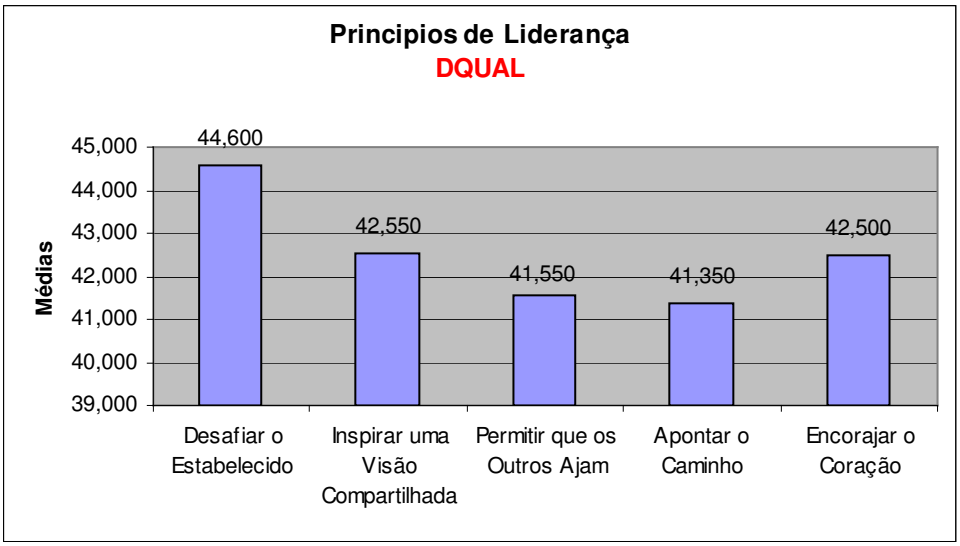


Gráfico 41: Princípios de Liderança
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para $\alpha = 0,05$, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

$\alpha = 0,05$

$\bar{x}$ = 7,085

s = 2,199

$n = 20$

$\nu = n - 1 = 19$

$t_\alpha = t_{0,05} = 1,729$

$t = (7,085 - 0) / (2,199 / \sqrt{20}) = 14,409$

Logo:

$t = 14,409 > t_\alpha = t_{0,05} = 1,729$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Liderança = 42,510

5.5.4.9 GABIN

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Liderança (LPI), apresentou-se desta forma:

Tabela 55: Teste LPI quanto ao perfil de liderança.

PRINCÍPIOS DE LIDERANÇA	Soma das médias	Índice de liderança
Desafiar o Estabelecido	41,583	
Inspirar uma Visão Compartilhada	43,750	
Permitir que os Outros Ajam	42,333	**41,650**
Apontar o Caminho	42,000	
Encorajar o Coração	38,583	

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos princípios de liderança, onde se mostra como o principal princípio, “Inspirar uma Visão Compartilhada”, seguido por “Permitir que os Outros Ajam”. Sendo “Encorajar o Coração”, o princípio mais fraco da liderança da diretoria.

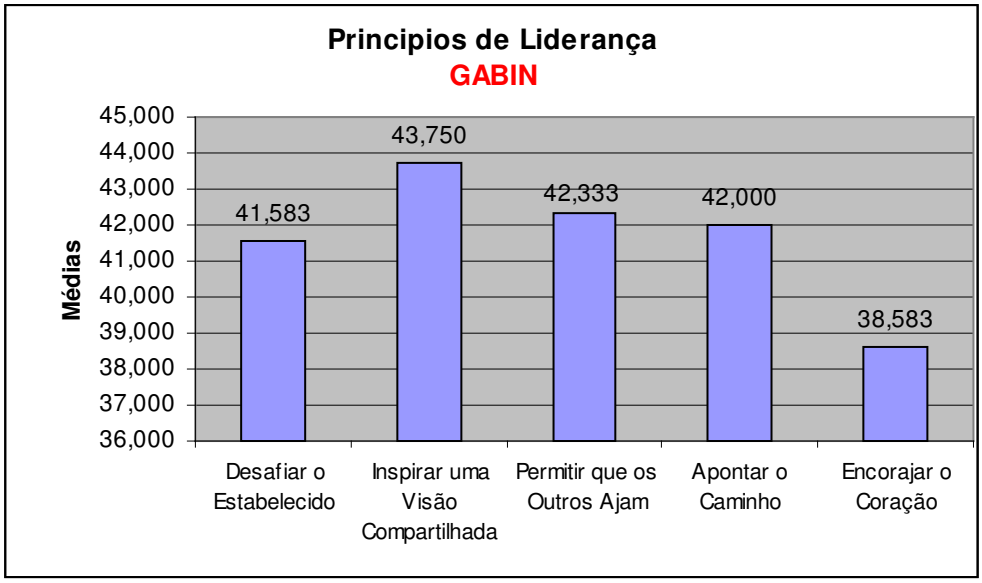


Gráfico 42: Princípios de Liderança
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\bar{x}$ = 6,942

s = 3,176

n = 12

ν = n –1 = 11

$t_\alpha = t_{0,05}$ = 1,796

t = (6,942 – 0) / (3,176 / √ 12) = 7,571

Logo:

t = 7,571 > $t_\alpha = t_{0,05}$ = 1,796 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Liderança = 41,650

5.5.4.10 PROGE

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Liderança (LPI), apresentou-se desta forma:

Tabela 56: Teste LPI quanto ao perfil de liderança.

PRINCÍPIOS DE LIDERANÇA	Soma das médias	Índice de liderança
Desafiar o Estabelecido	46,143	
Inspirar uma Visão Compartilhada	46,571	
Permitir que os Outros Ajam	46,000	**45,829**
Apontar o Caminho	45,286	
Encorajar o Coração	45,143	

Fonte: Elaboração própria

Abaixo, pode-se observar o gráfico dos princípios de liderança, onde se mostra como o principal princípio, "Inspirar uma Visão Compartilhada", seguido por "Desafiar o Estabelecido". Sendo "Encorajar o Coração", o princípio mais fraco da liderança da diretoria.

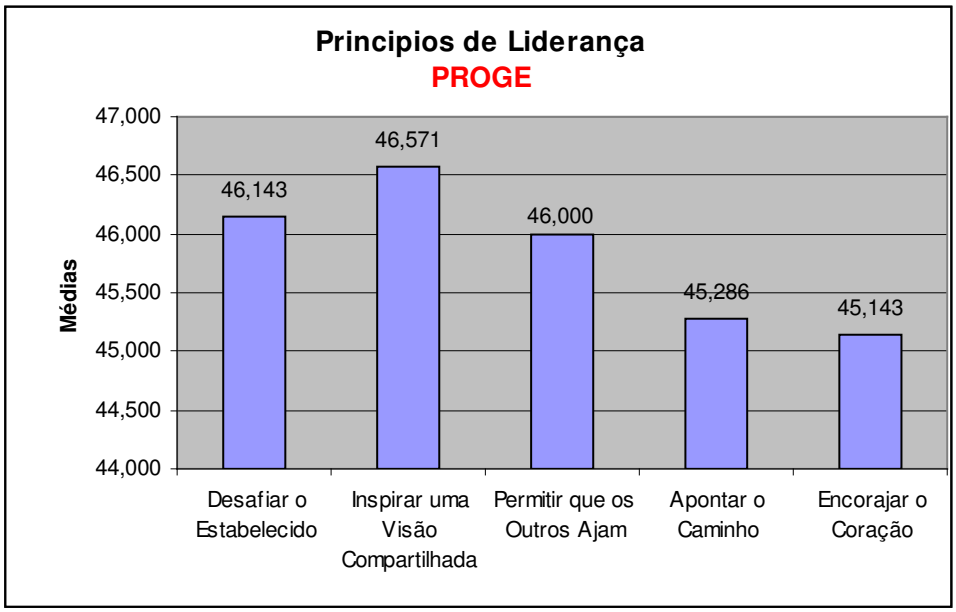


Gráfico 43: Princípios de Liderança
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

α = 0,05

$\bar{x}$ = 7,638

s = 2,428

$n = 7$

$\nu = n - 1 = 6$

$t_\alpha = t_{0,05} = 1{,}943$

$t = (7{,}638 - 0) / (2{,}428 / \sqrt{7}) = 8{,}322$

Logo:

$t = 8{,}322 > t_\alpha = t_{0,05} = 1{,}943$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Liderança = 45,829

5.5.4.11 RESULTADO DO ÍNDICE DE PERCEPÇÃO DA LIDERANÇA

Após o término dos cálculos e teste de corroboração ou refutação da média, tem-se o índice de percepção de liderança, como a forma de posicionar as unidades organizacionais em ordem das melhores práticas de liderança. Abaixo, são apresentados os resultados e as respectivas colocações das diretorias do Inmetro, na parte da pesquisa relativa a percepção de liderança:

Tabela 57: Índice de percepção de liderança nas diretorias

Ordem:	Diretoria:	Índice:
1	AUDIN	53,720
2	DIRAF	46,300
3	PROGE	45,829
4	CAINT	44,880
5	DQUAL	42,510
6	GABIN	41,650
7	CGCRE	40,862
8	DIMCI	38,882
9	CPLAN	38,260
10	DIMEL	30,400

Fonte: Elaboração própria

Pode-se perceber que algumas diretorias possuem valores altos de percepção de liderança, indicando que seus diretores têm as melhores práticas de liderança como premissas de suas administrações.

Tabela 58: Princípios de Liderança – Diretorias do Inmetro

PRINCÍPIOS DE LIDERANÇA (Médias)	AUDIN	CAINT	CGCRE	CPLAN	DIMCI	DIMEL	DIRAF	DQUAL	GABIN	PROGE
Desafiar o Estabelecido	53,000	44,800	39,615	38,919	39,176	31,471	45,438	44,600	41,583	46,143
Inspirar uma Visão Compartilhada	53,000	45,800	40,154	36,676	39,588	31,235	43,875	42,550	43,750	46,571
Permitir que os Outros Ajam	54,600	45,200	43,385	40,054	40,471	30,235	49,625	41,550	42,333	46,000
Apontar o Caminho	51,600	43,200	40,769	38,162	36,882	30,412	45,500	41,350	42,000	45,286
Encorajar o Coração	56,400	45,400	40,385	37,486	38,294	28,647	47,063	42,500	38,583	45,143
Média total:	53,720	44,880	40,862	38,260	38,882	30,400	46,300	42,510	41,650	45,829

Fonte: Elaboração própria

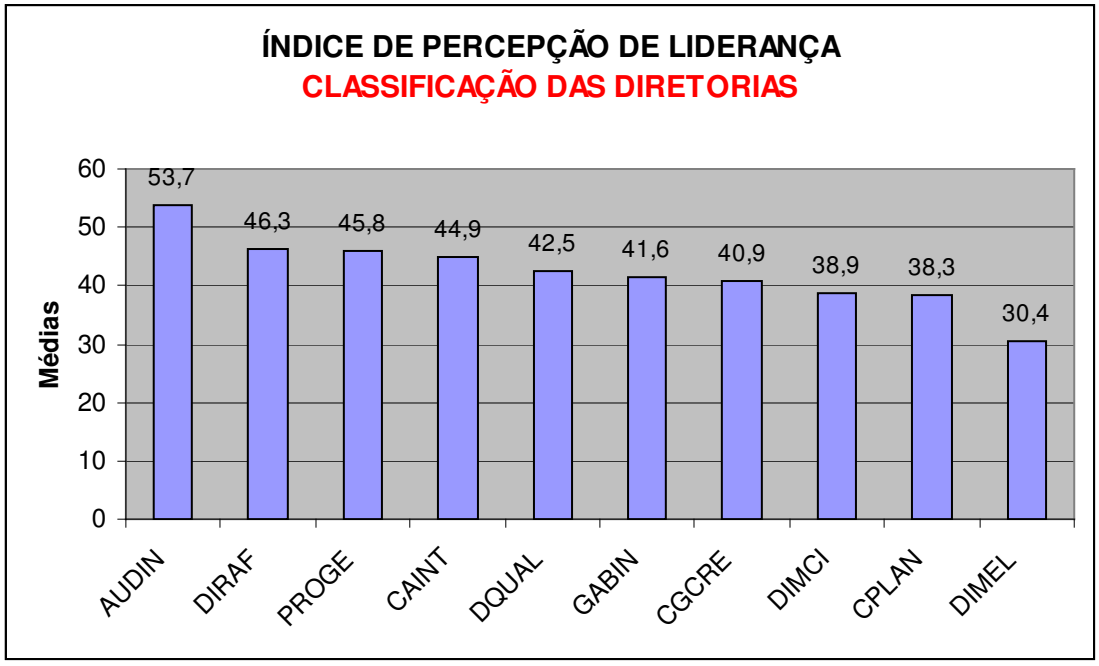


Gráfico 44: Classificação das Diretorias em relação ao Perfil da Liderança.
Fonte: Elaboração própria

5.5.5 CÁLCULO DO ÍNDICE DE PERCEPÇÃO DE SEGUIDORES

Para este cálculo, foram tabulados os resultados da pesquisa obtida através das respostas, por meio de amostras aleatórias dos usuários, ao questionário sobre perfil de seguidores (anexo E, pág. 282), dentro de cada diretoria. O questionário foi disponibilizado através de um "portal web", de forma a facilitar aos usuários respondê-lo, como também, facilitar a tabulação das respostas, sendo essas armazenadas diretamente no banco de dados da pesquisa.

Os seguidores exemplares diferem dos outros seguidores, pois têm bom desempenho em ambas as dimensões fundamentais do seguir: por um lado, usam o pensamento crítico, independente, diferentemente do líder ou do grupo. Por outro lado, os seguidores exemplares estão ativamente ajustados à organização e usam seus talentos em prol dela. Os seguidores exemplares empenham seus talentos, e inclusive seu cérebro, para trabalhar pela organização.

Para fins desta pesquisa, para o cálculo do índice de percepção de seguidores, somente o índice de seguidores exemplares será levado em conta. Essas respostas poderão fazer parte de uma nova pesquisa e para iniciar, se alguém tiver interesse, um futuro estudo além deste.

Os dados foram tratados estatisticamente pela distribuição **t** (distribuição de Student), para pequenas amostras ($n<30$), mas de acordo com Anderson et al. (2003) ela não se restringe às pequenas amostras, podendo ser utilizada com o intuito de corroborar ou refutar as hipóteses de teste da média da população.

Após o teste de corroboração ou refutação da média, calculou-se o índice de percepção de seguidores (a proporção de seguidores exemplares em relação ao total da amostra), sendo esta, a forma de posicionar as unidades organizacionais em ordem de melhor percepção de seguidores das diretorias.

5.5.5.1 AUDIN

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Seguidores, apresentou-se desta forma:

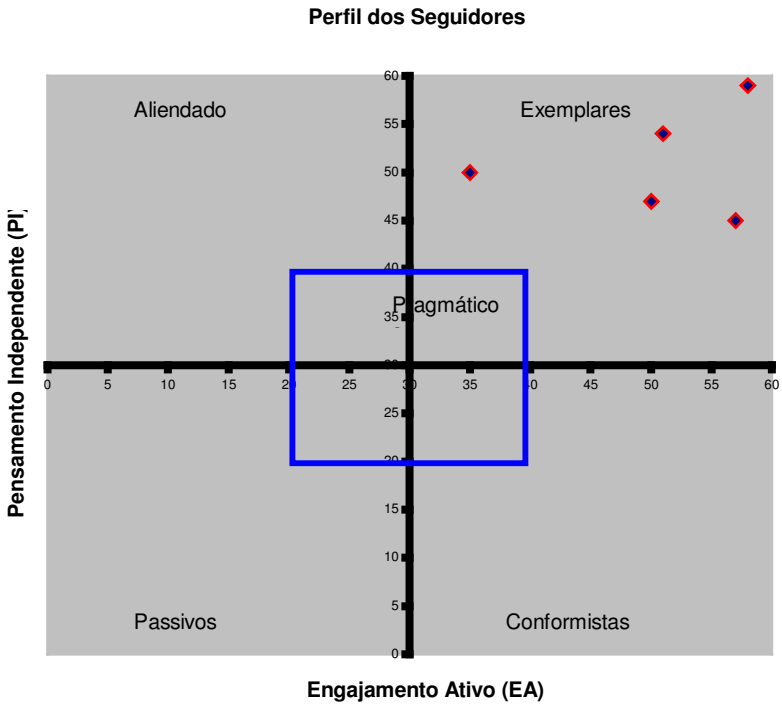


Gráfico 45: Teste de perfil de seguidores.
Fonte: Elaboração própria

Observa-se no gráfico dos tipos de seguidores, que esta diretoria teve na amostra dos respondentes, todos com perfil de seguidor “exemplar”.

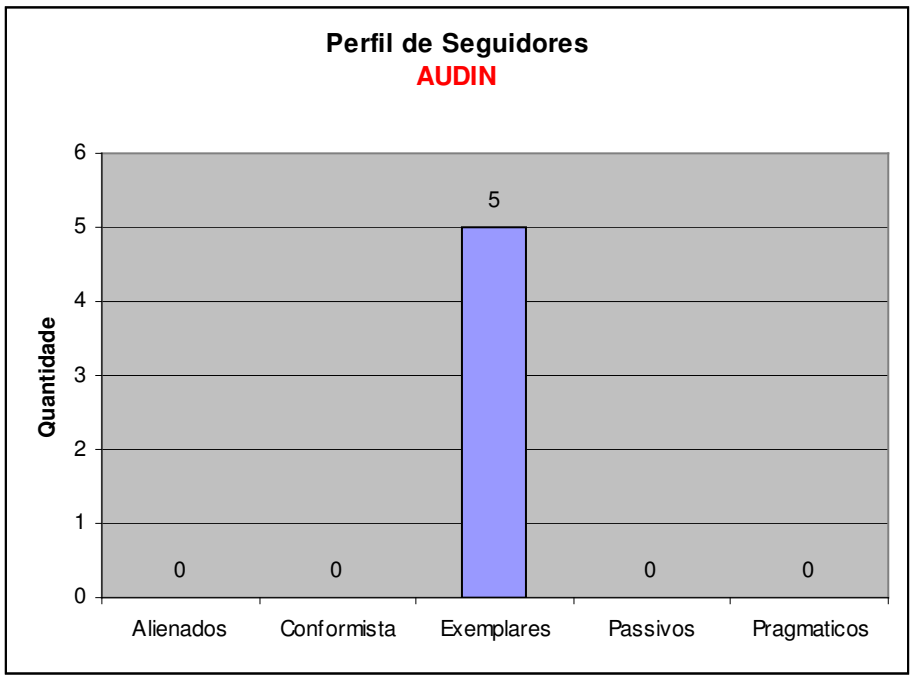


Gráfico 46: Tipos e quantidade de perfis dos seguidores
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para $\alpha = 0,05$, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

$\alpha = 0,05$

$\bar{x}$ = 5,060

s = 1,413

n = 5

ν = n –1 = 4

$t_\alpha = t_{0,05} = 2,132$

t = (5,060 – 0) / (1,413 / √ 5) = 8,008

Logo:

t = 8,008 > $t_\alpha = t_{0,05} = 2,132$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Seguidores = (seg. exemplares) / n = 5 / 5 = 1,000

5.5.5.2 CAINT

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Seguidores, apresentou-se desta forma:

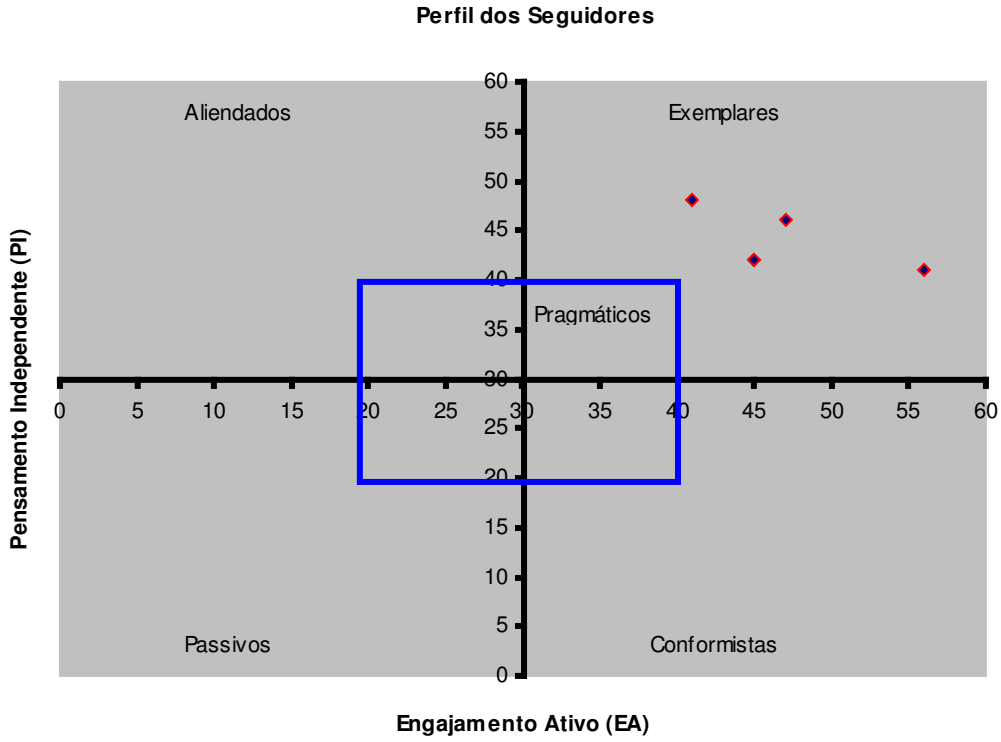


Gráfico 47: Teste de perfil de seguidores.
Fonte: Elaboração própria

Observa-se no gráfico dos tipos de seguidores, que esta diretoria teve na amostra dos respondentes, todos com perfil de seguidor "exemplar".

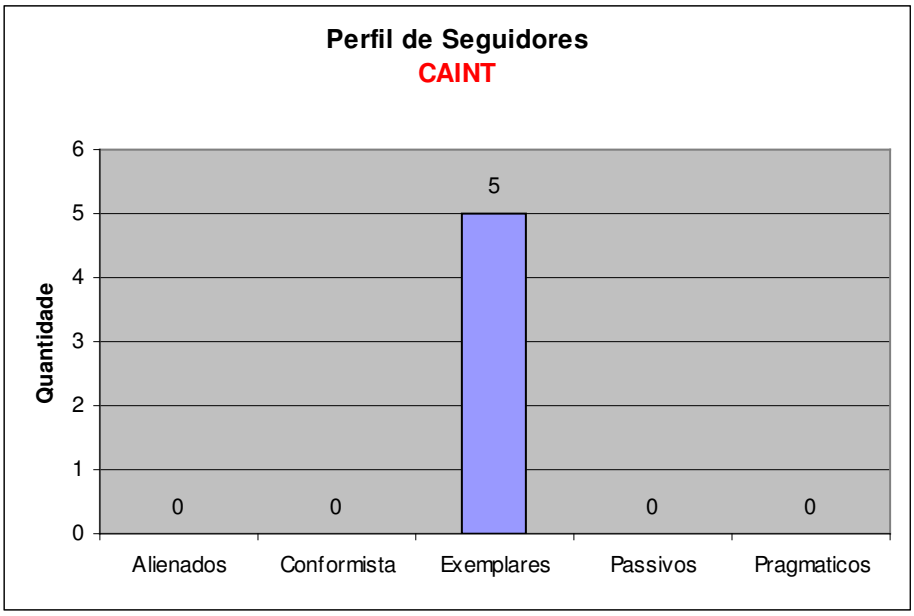


Gráfico 48: Tipos e quantidade de perfis dos seguidores
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para $\alpha = 0,05$, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

$\alpha = 0,05$

$\bar{x} = 4,530$

s = 1,058

n = 5

ν = n –1 = 4

$t_\alpha = t_{0,05} = 2,132$

t = (4,530 – 0) / (1,058 / √ 5) = 9,570

Logo:

t = 9,570 > $t_\alpha = t_{0,05} = 2,132$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Seguidores = (seg. exemplares) / n = 5 / 5 = 1,000

5.5.5.3 CGCRE

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Seguidores, apresentou-se desta forma:

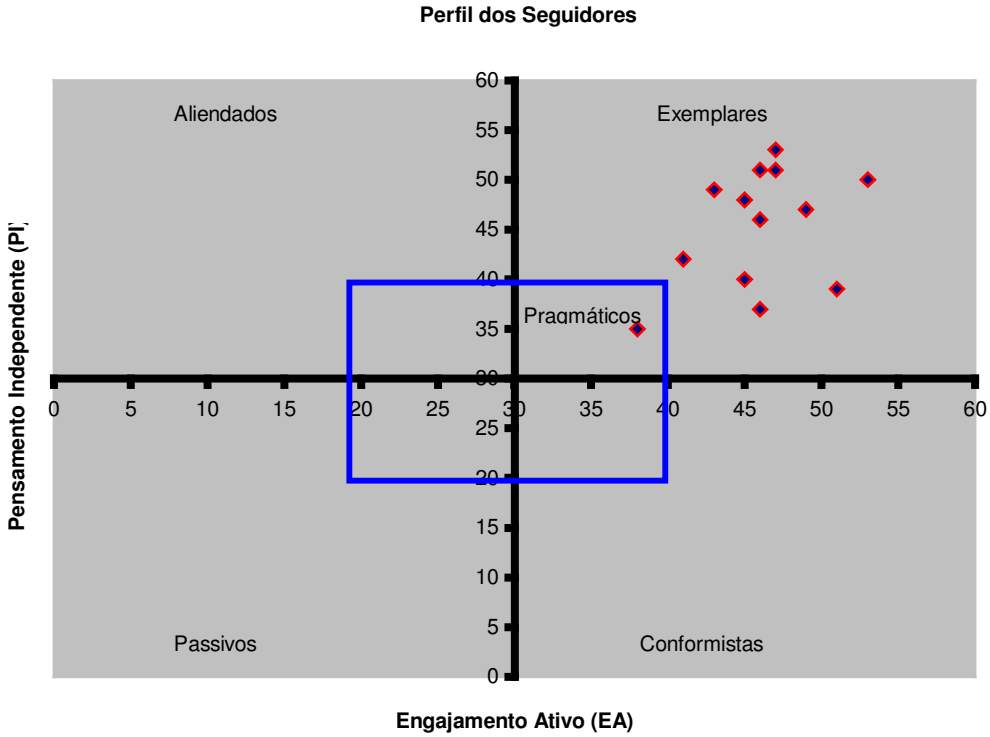


Gráfico 49: Teste de perfil de seguidores.
Fonte: Elaboração própria

Observa-se no gráfico dos tipos de seguidores, que esta diretoria teve na amostra dos respondentes, a grande maioria com perfil de seguidor "exemplar". Apenas um foi considerado seguidor "pragmático".

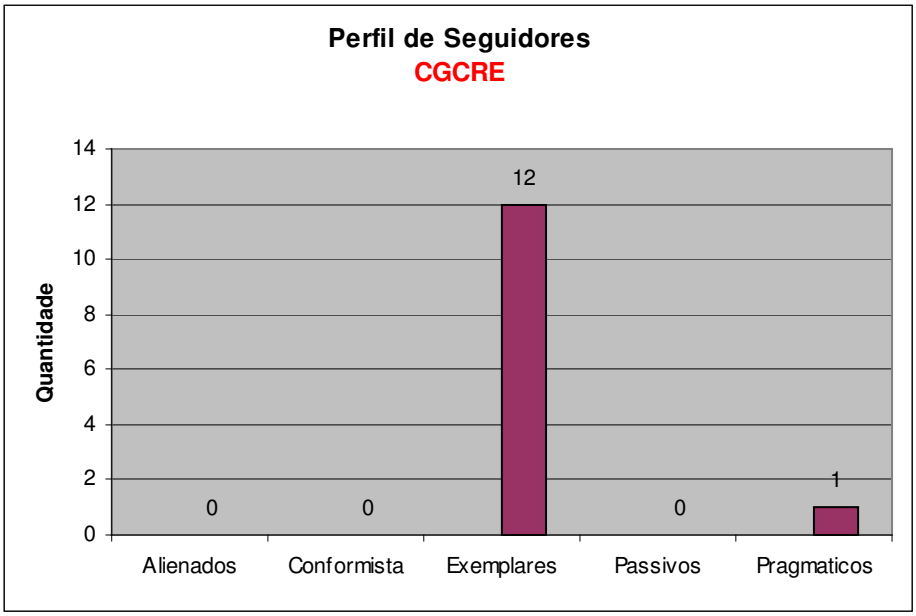


Gráfico 50: Tipos e quantidade de perfis dos seguidores
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para $\alpha = 0,05$, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

$\alpha = 0,05$

$\bar{x}$ = 4,558

s = 1,406

n = 13

ν = n –1 = 12

$t_\alpha = t_{0,05}$ = 1,782

t = (4,558 – 0) / (1,406 / √ 13) = 11,686

Logo:

t = 11,686 > $t_\alpha = t_{0,05}$ = 1,782 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Seguidores = (seg. exemplares) / n = 12 / 13 = 0,923

5.5.5.4 CPLAN

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Seguidores, apresentou-se desta forma:

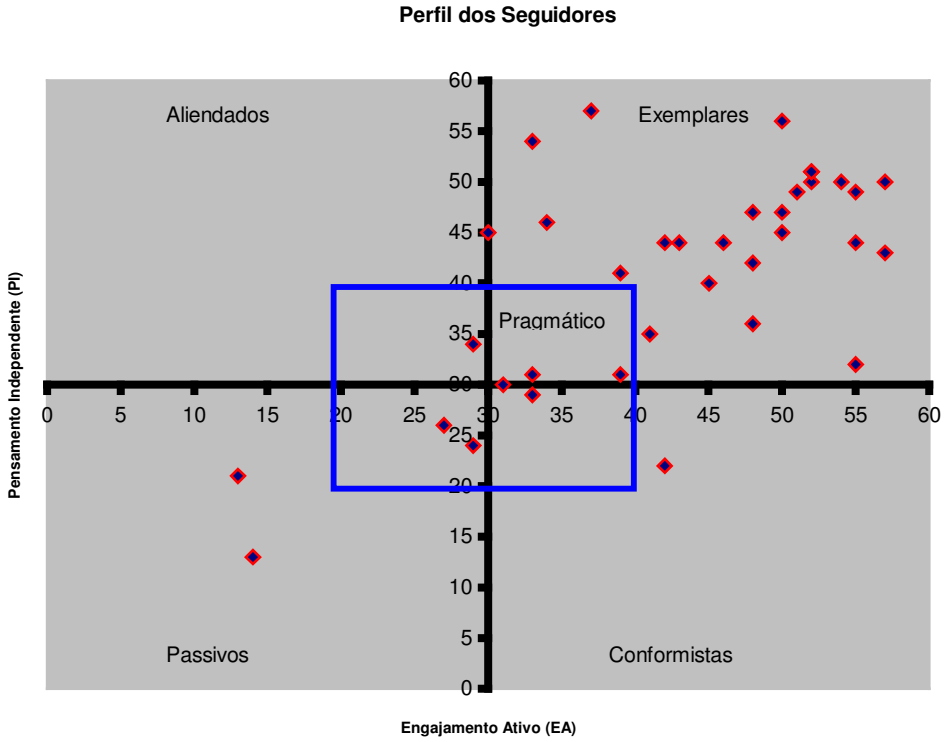


Gráfico 51: Teste de perfil de seguidores.
Fonte: Elaboração própria

Observa-se no gráfico dos tipos de seguidores, que esta diretoria teve na amostra dos respondentes, uma maior distribuição pelos tipos de seguidores, mas ainda, a grande maioria com perfil de seguidor "exemplar".

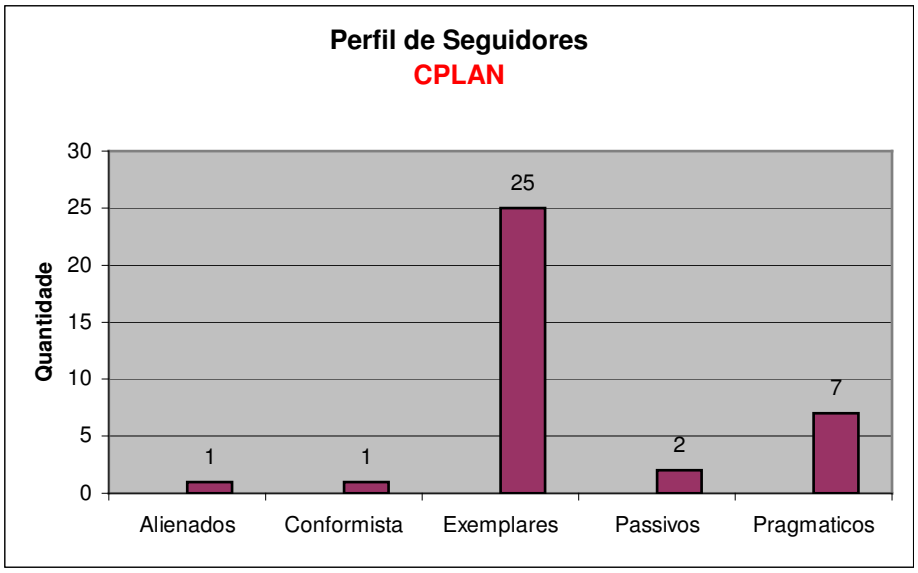


Gráfico 52: Tipos e quantidade de perfis dos seguidores
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para $\alpha = 0,05$, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

$\alpha = 0,05$

$\bar{x}$ = 4,121

s = 1,733

n = 36

ν = n –1 = 35

$t_\alpha = t_{0,05} = 1,673$

t = (4,121 – 0) / (1,733 / √ 36) = 14,263

Logo:

t = 14,263 > $t_\alpha = t_{0,05} = 1,673$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Seguidores = (seg. exemplares) / n = 25 / 36 = 0,694

5.5.5.5 DIMCI

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Seguidores, apresentou-se desta forma:

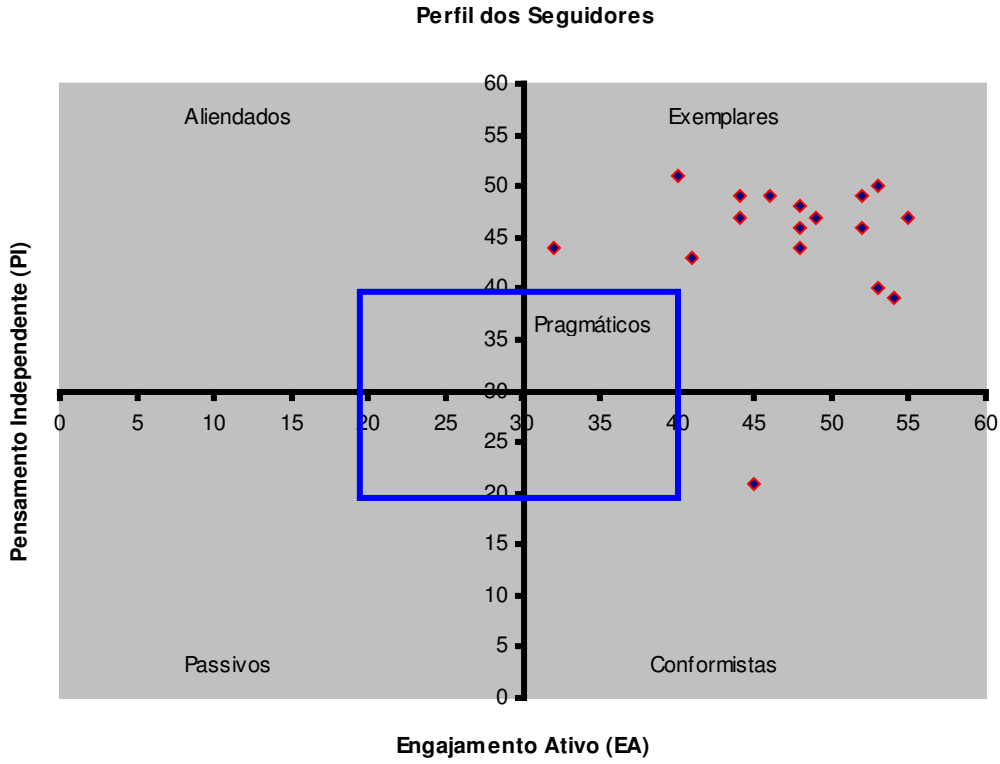


Gráfico 53: Teste de perfil de seguidores.
Fonte: Elaboração própria

Observa-se no gráfico dos tipos de seguidores, que esta diretoria teve na amostra dos respondentes, a grande maioria com perfil de seguidor "exemplar". E apenas um seguidor "conformista".

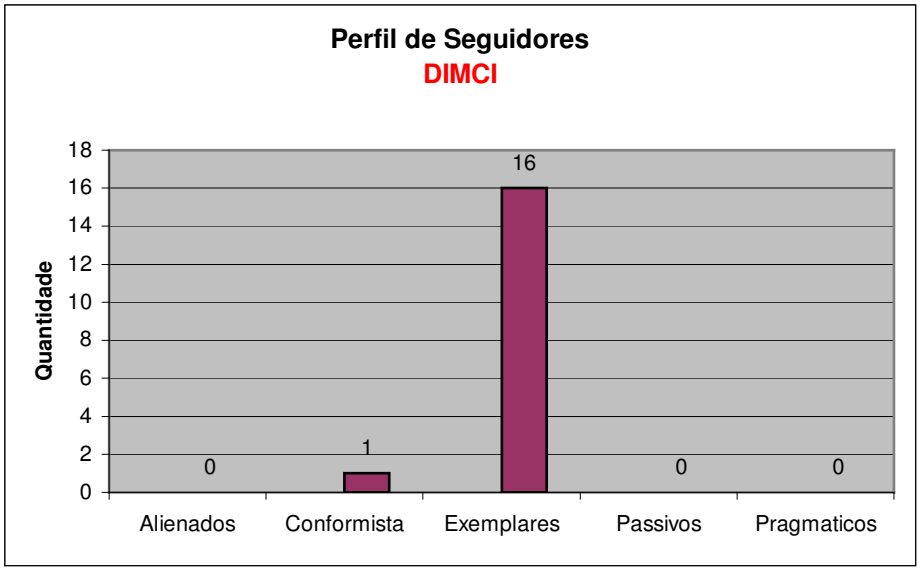


Gráfico 54: Tipos e quantidade de perfis dos seguidores
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para $\alpha = 0,05$, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

$\alpha = 0,05$

$\bar{x}$ = 4,600

s = 1,323

n = 17

ν = n –1 = 16

$t_\alpha = t_{0,05}$ = 1,746

t = (4,600 – 0) / (1,323 / √ 17) = 14,333

Logo:

t = 14,333 > $t_\alpha = t_{0,05}$ = 1,746 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Seguidores = (seg. exemplares) / n = 16 / 17 = 0,941

5.5.5.6 DIMEL

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Seguidores, apresentou-se desta forma:

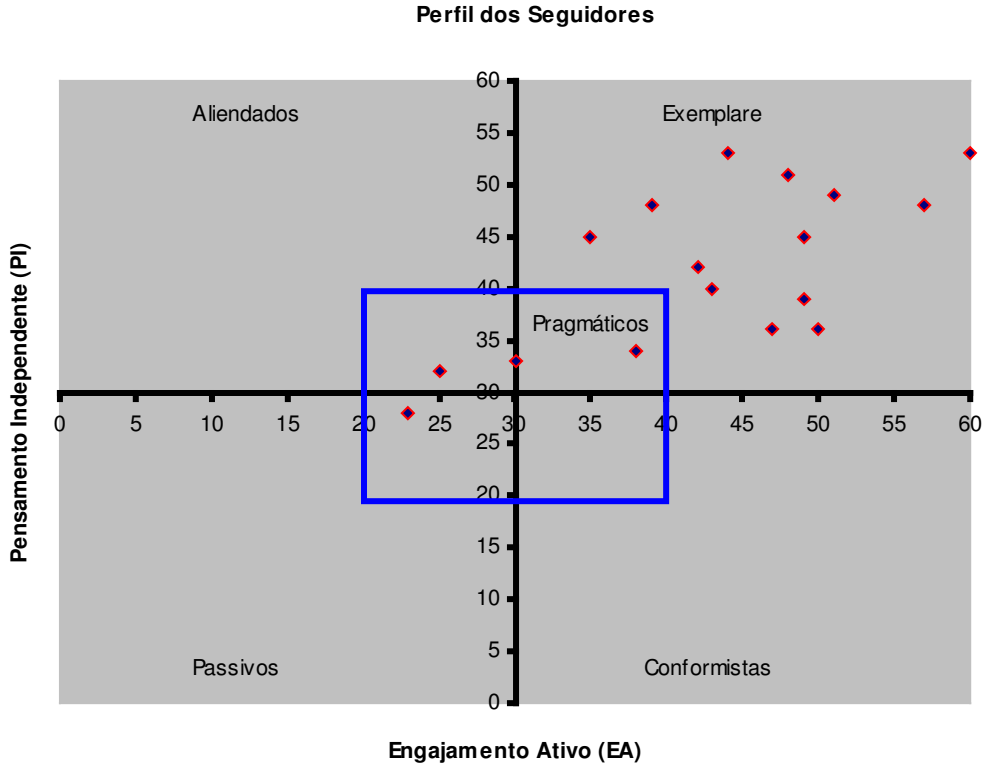


Gráfico 55: Teste de perfil de seguidores.
Fonte: Elaboração própria

Observa-se no gráfico dos tipos de seguidores, que esta diretoria teve na amostra dos respondentes, a grande maioria com perfil de seguidor "exemplar". E quatro seguidores "pragmáticos".

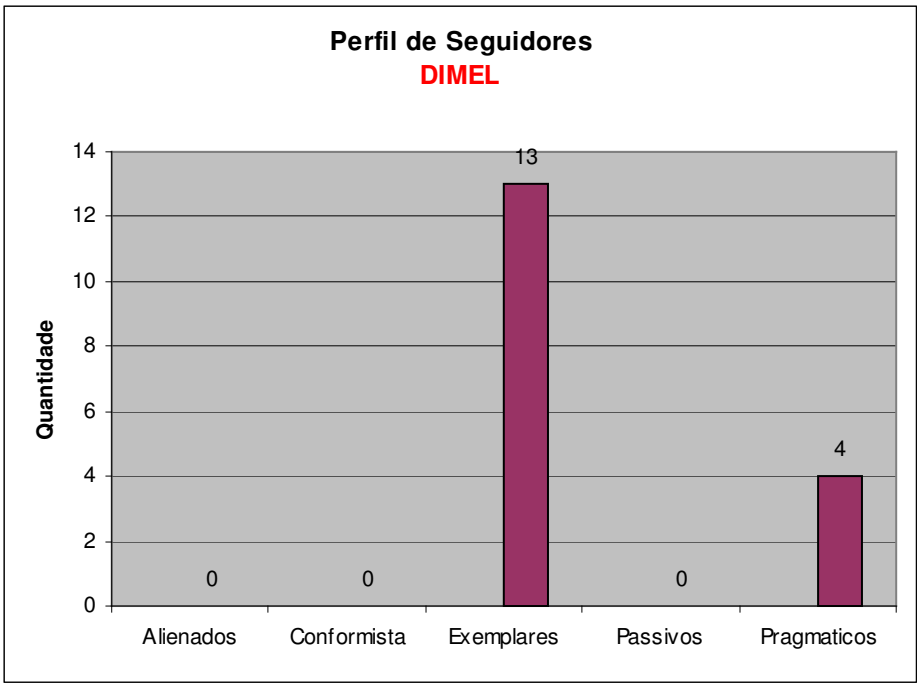


Gráfico 56: Tipos e quantidade de perfis dos seguidores
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  $\bar{x}$ = 4,241

  s = 1,599

  n = 17

  ν = n –1 = 16

  $t_\alpha = t_{0,05}$ = 1,746

  t = (4,241 – 0) / (1,599 / √ 17) = 10,939

Logo:

t = 10,939 > $t_\alpha = t_{0,05}$ = 1,746 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Seguidores = (seg. exemplares) / n = 13 / 17 = 0,765

5.5.5.7 DIRAF

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Seguidores, apresentou-se desta forma:

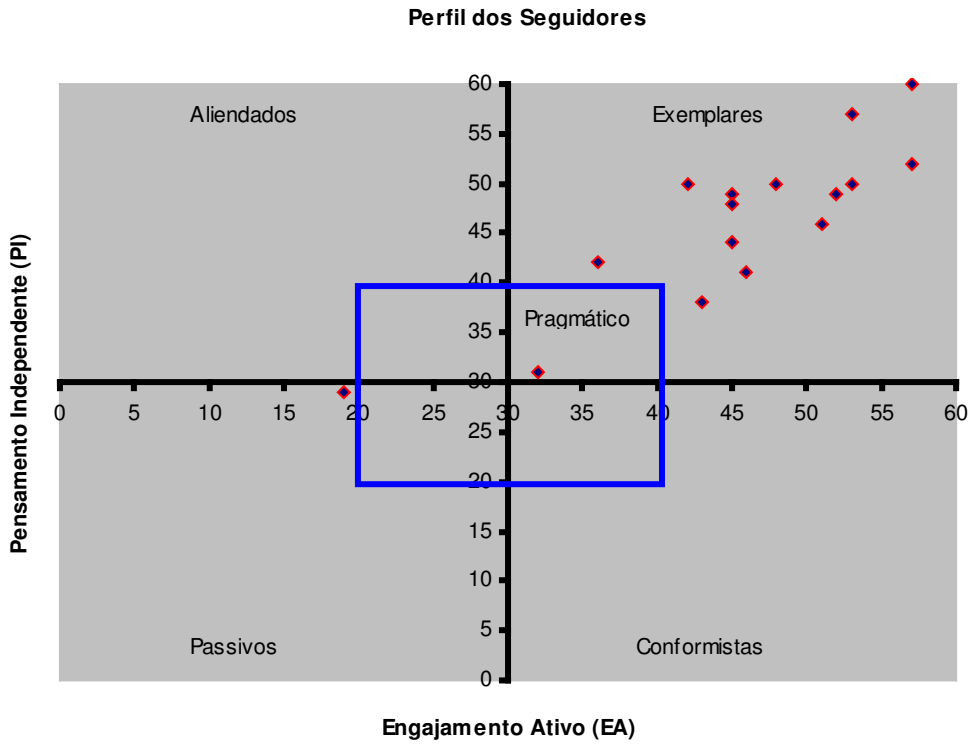


Gráfico 57: Teste de perfil de seguidores.
Fonte: Elaboração própria

Observa-se no gráfico dos tipos de seguidores, que esta diretoria teve na amostra dos respondentes, a grande maioria com perfil de seguidor “exemplar”. Um seguidor “passivo” e um seguidor “pragmático”.

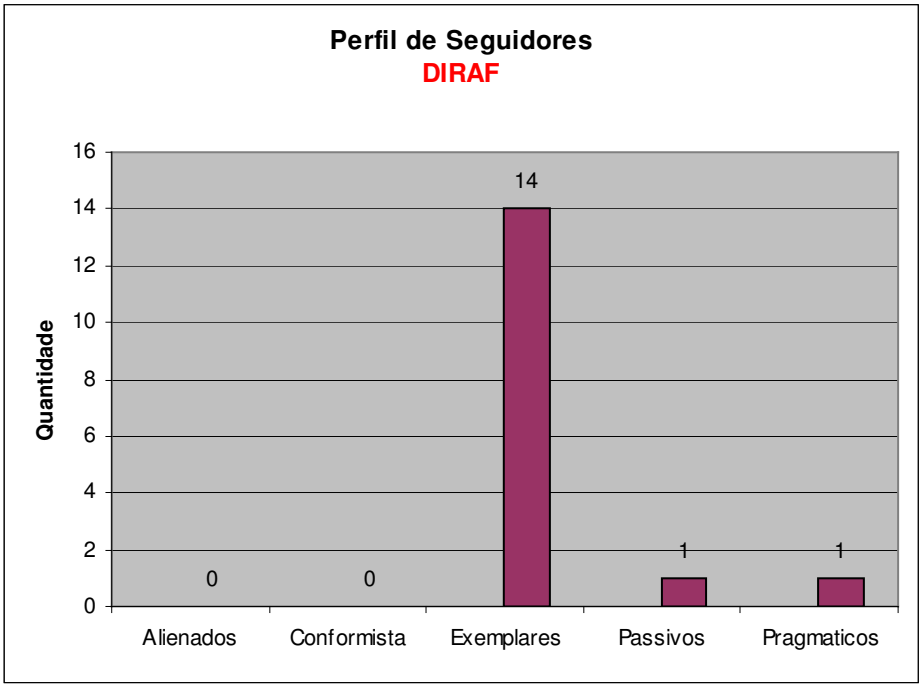


Gráfico 58: Tipos e quantidade de perfis dos seguidores
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  $\bar{x}$ = 4,563

  s = 1,424

  n = 16

  ν = n –1 = 15

  $t_\alpha = t_{0,05}$ = 1,753

  t = (4,563 – 0) / (1,424 / √ 16) = 12,817

Logo:

t = 12,817 > $t_\alpha = t_{0,05}$ = 1,753 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Seguidores = (seg. exemplares) / n = 14 / 16 = 0,875

5.5.5.8 DQUAL

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Seguidores, apresentou-se desta forma:

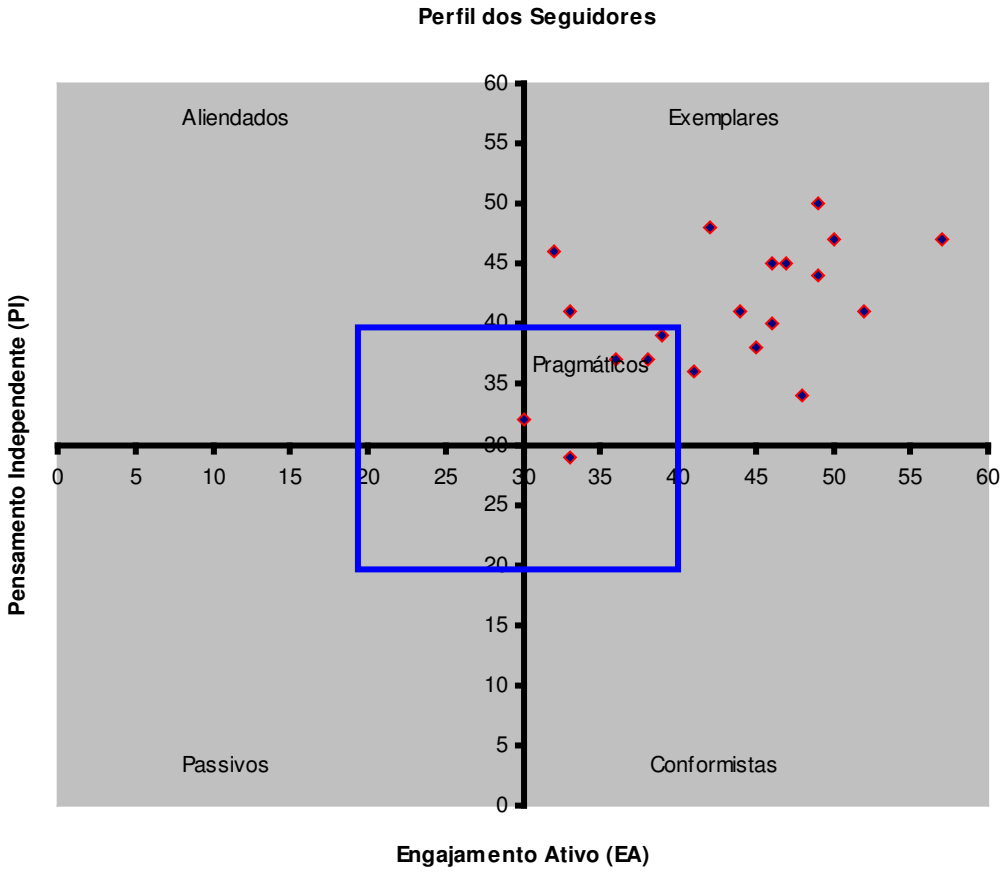


Gráfico 59: Teste de perfil de seguidores.
Fonte: Elaboração própria

Observa-se no gráfico dos tipos de seguidores, que esta diretoria teve na amostra dos respondentes, a grande maioria com perfil de seguidor "exemplar". E cinco seguidores "pragmáticos".

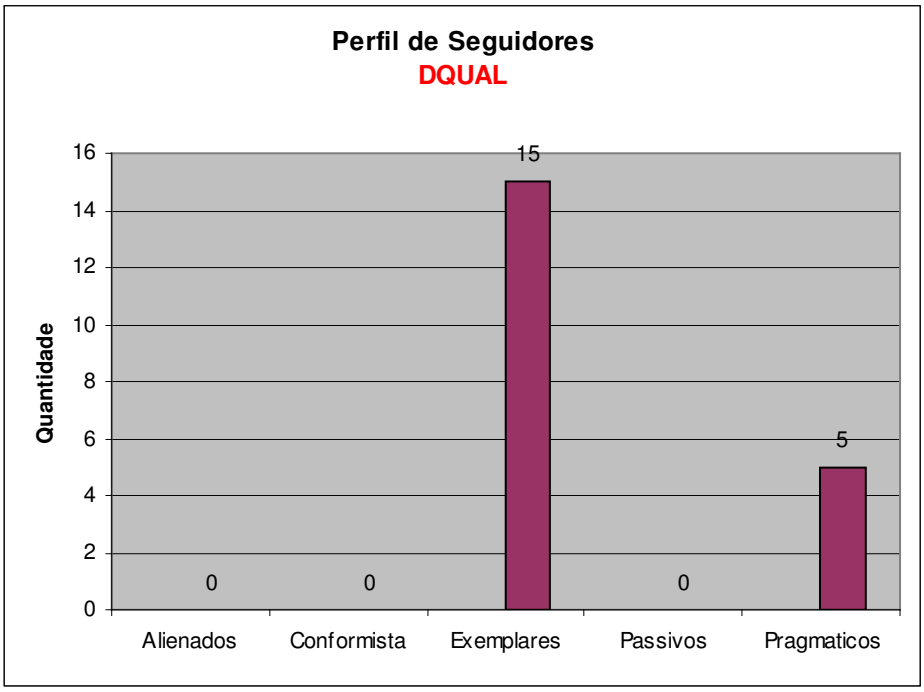


Gráfico 60: Tipos e quantidade de perfis dos seguidores
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  $\bar{x}$ = 4,185

  s = 1,444

  n = 20

  ν = n –1 = 19

  $t_\alpha = t_{0,05}$ = 1,729

  t = (4,185 – 0) / (1,444 / √ 20) = 12,958

Logo:

t = 12,958 > $t_\alpha = t_{0,05}$ = 1,729 ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Seguidores = (seg. exemplares) / n = 15 / 20 = 0,750

5.5.5.9 GABIN

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Seguidores, apresentou-se desta forma:

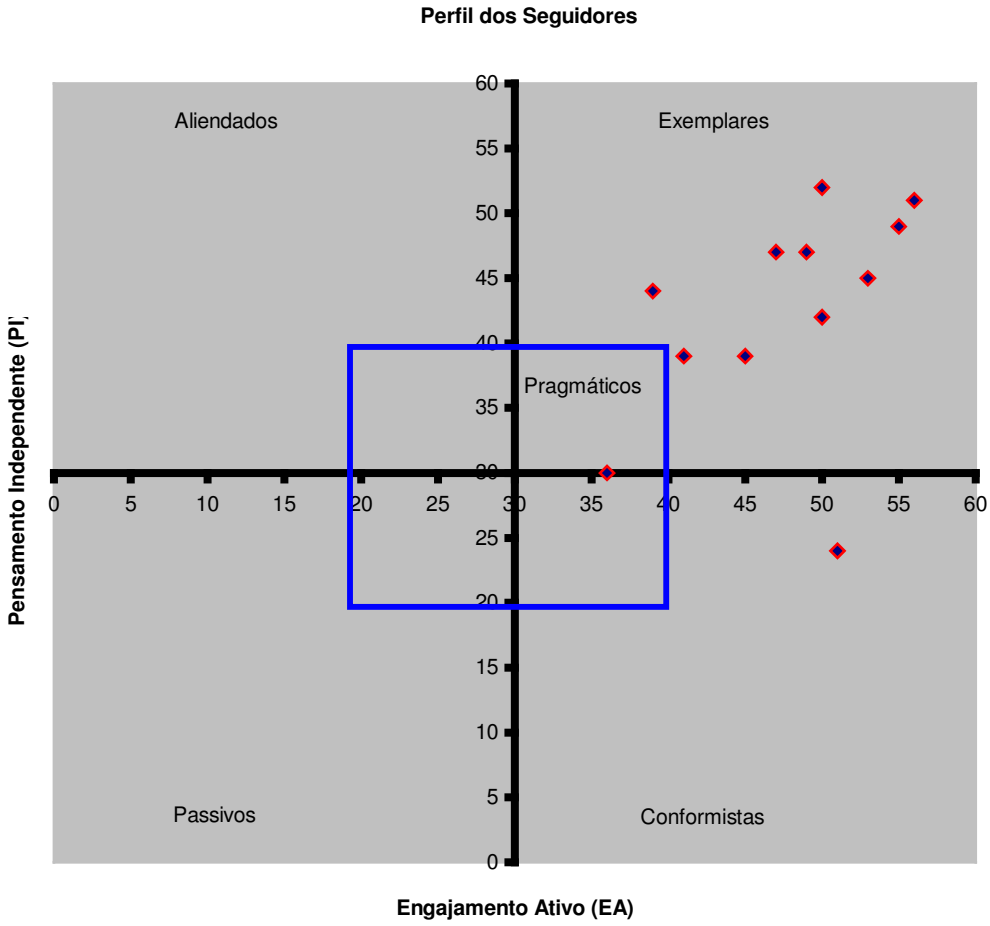


Gráfico 61: Teste de perfil de seguidores.
Fonte: Elaboração própria

Observa-se no gráfico dos tipos de seguidores, que esta diretoria teve na amostra dos respondentes, a grande maioria com perfil de seguidor "exemplar". Um seguidor "conformista" e um seguidor "pragmático".

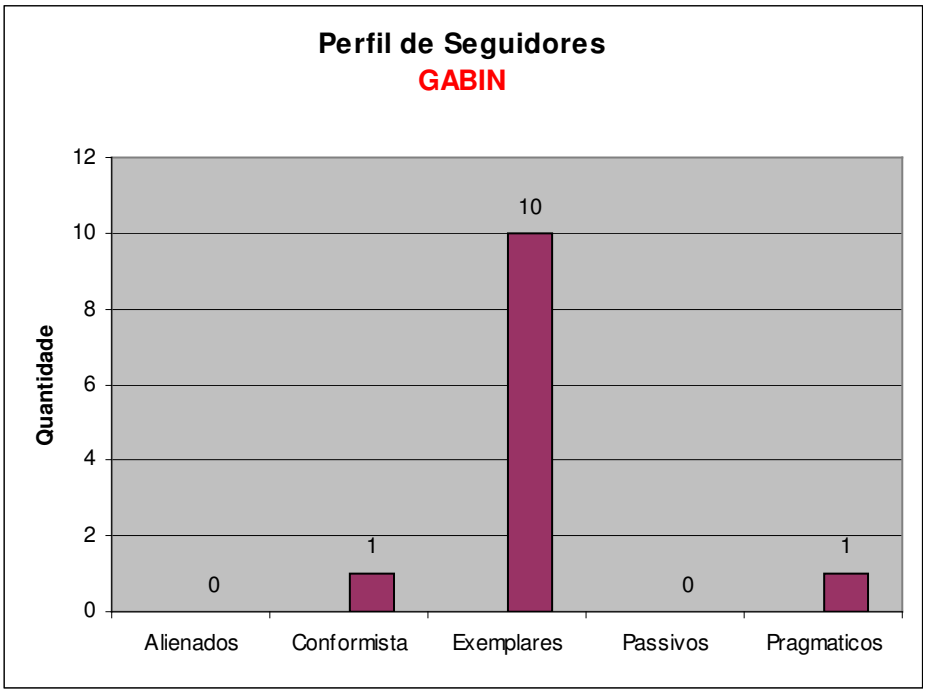


Gráfico 62: Tipos e quantidade de perfis dos seguidores
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  $\bar{x}$ = 4,504

  s = 1,560

  n = 12

  ν = n –1 = 11

  $t_\alpha = t_{0,05} = 1,796$

  t = (4,504 – 0) / (1,560 / √ 12) = 9,999

Logo:

t = 9,999 > $t_\alpha = t_{0,05} = 1,796$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Seguidores = (seg. exemplares) / n = 10 / 12 = 0,833

5.5.5.10 PROGE

Esta diretoria apresentou os seguintes resultados:

- Em relação ao teste do Perfil de Seguidores, apresentou-se desta forma:

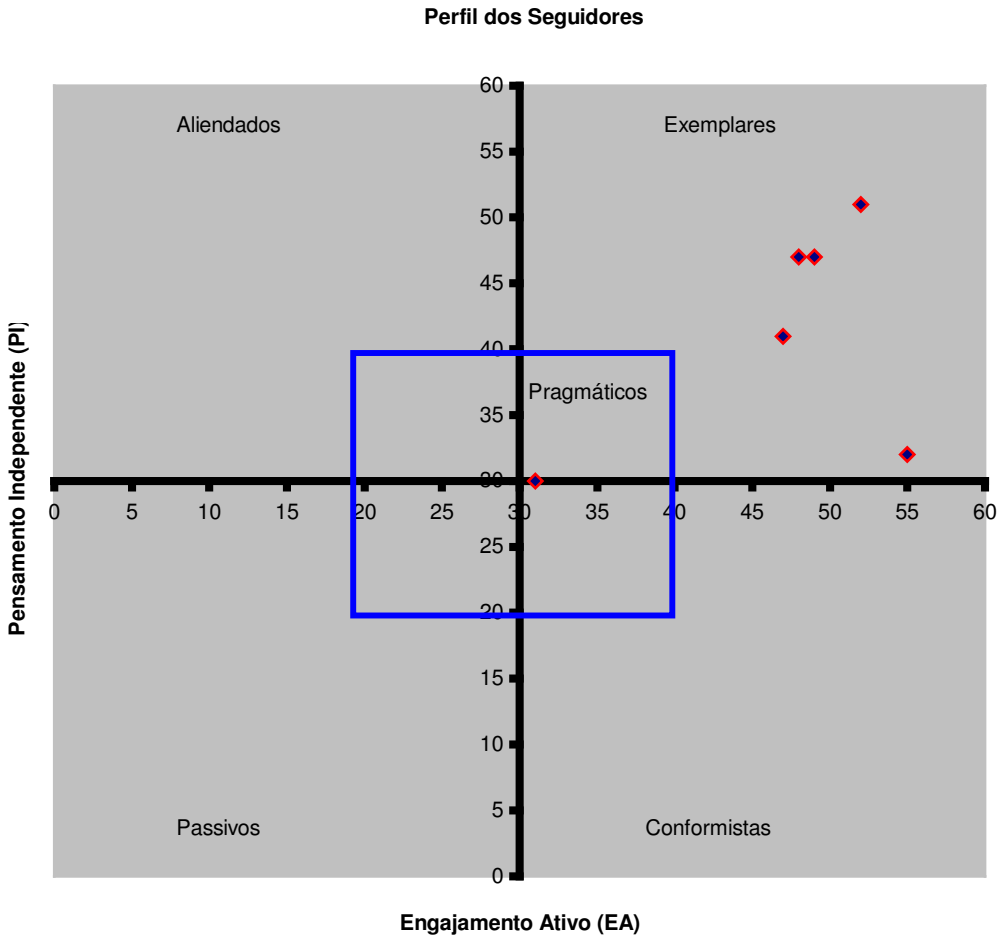


Gráfico 63: Teste de perfil de seguidores.
Fonte: Elaboração própria

Observa-se no gráfico dos tipos de seguidores, que esta diretoria teve na amostra dos respondentes, a grande maioria com perfil de seguidor "exemplar". Um seguidor "conformista" e um seguidor "pragmático".

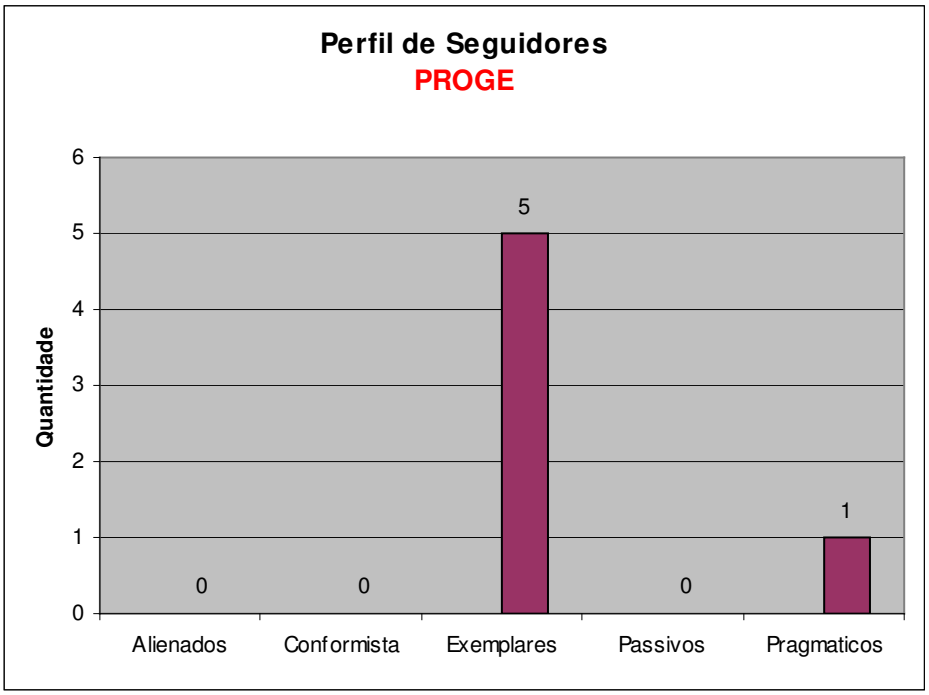


Gráfico 64: Tipos e quantidade de perfis dos seguidores
Fonte: Elaboração própria

- Teste de Hipótese da Média da População – Pequena amostra

Hipótese de nulidade da média:

- H_0: $\mu_{\circ} = 0$
- H_1: $\mu_{\circ} \neq 0$

Onde:

$\mu_{\circ}$ = média da população dos usuários;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\bar{x} - \mu_o}{s / \sqrt{n}}$$

Onde:

$\bar{x}$ = média da amostra;

s = desvio padrão da amostra

n = tamanho da amostra

$$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$$

Onde:

$n-1$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-1" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  $\bar{x}$ = 4,417

  s = 1,470

  n = 6

  ν = n –1 = 5

  $t_\alpha = t_{0,05} = 2,015$

  t = (4,417 – 0) / (1,470 / √ 6) = 7,359

Logo:

t = 7,359 > $t_\alpha = t_{0,05} = 2,015$ ➔ Rejeitar H_0

Pode-se então rejeitar H_0 ao nível de 5% de significância e corroborar a média da amostra. Isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população é igual a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Concluindo:

Índice de Percepção de Seguidores = (seg. exemplares) / n = 5 / 6 = 0,833

5.5.5.11 RESULTADO DO ÍNDICE DE PERCEPÇÃO DE SEGUIDORES

Após o término dos cálculos e teste de corroboração ou refutação da média, tem-se o índice de percepção de seguidores, como a forma de posicionar as unidades organizacionais em ordem dos melhores perfis de seguidores. Abaixo, são apresentados os resultados e as respectivas colocações das diretorias do Inmetro, na parte da pesquisa relativa a percepção de seguidores:

Tabela 59: Índice de percepção de seguidores nas diretorias

Ordem:	Diretoria:	Índice:
1	AUDIN	1,000
2	CAINT	1,000
3	DIMCI	0,941
4	CGCRE	0,923
5	DIRAF	0,875
6	GABIN	0,833
7	PROGE	0,833
8	DIMEL	0,765
9	DQUAL	0,750
10	CPLAN	0,694

Fonte: Elaboração própria

Pode-se perceber que algumas diretorias possuem valores altos de percepção de seguidores, indicando que seus usuários têm, na sua maioria, os melhores perfis de seguidores. Sendo esse dado de grande importância para a instituição.

Tabela 60: Princípios de Seguidores – Diretorias do Inmetro

PERFIL DE SEGUIDORES	AUDIN	CAINT	CGCRE	CPLAN	DIMCI	DIMEL	DIRAF	DQUAL	GABIN	PROGE
Alienados				1						
Conformistas				1	1				1	
Exemplares	5	5	12	25	16	13	14	15	10	5
Passivos				2			1			
Pragmáticos			1	7		4	1	5	1	1

Fonte: Elaboração própria

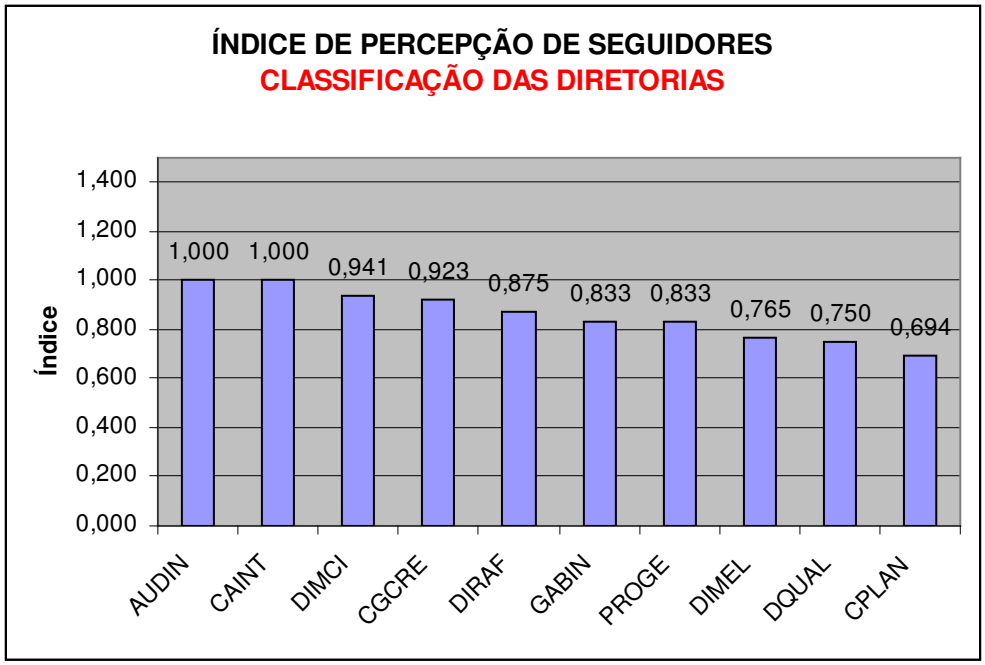


Gráfico 65: Classificação das Diretorias em relação ao Perfil da Liderança.
Fonte: Elaboração própria

5.5.6 TESTAGEM DAS HIPÓTESES PRINCIPAIS

É freqüente a procura da existência ou não de relações entre duas ou mais variáveis aleatórias. A verificação da existência e do grau de relação entre variáveis é objeto do estudo da correlação.

Nesta pesquisa testa-se a relação entre Percepção de Segurança da Informação, Percepção de Qualidade, Percepção de Liderança e Percepção de Seguidores, com a intenção de corroborar ou rejeitar estas relações entre as percepções estudadas aqui.

Conforme Ehlers (2005), as correlações estão tabuladas em correlações bem fortes, fortes, moderada, fraca e bem fraca, de acordo com sua colocação na tabela dos valores de correlação. Dando assim, uma forma de classificar as relações entre as variáveis testadas.

Tabela 61: Tabela de Interpretação de Correlação

Tabela de Interpretação de Correlação	
Valor da Correlação	Interpretação
0,00 a 0,19	Uma correlação bem fraca
0,20 a 0,39	Uma correlação fraca
0,40 a 0,69	Uma correlação moderada
0,70 a 0,89	Uma correlação forte
0,90 a 1,00	Uma correlação bem forte

Fonte: EHLERS, Ricardo S. **Introdução à Estatística**, 2. ed, Curitiba: UFPR, 2005.

Para testar estas hipóteses utiliza-se o coeficiente de correlação de Pearson, a significância destas correlações e o teste **t** de Student, para identificar em que medida a variação em uma variável está associada pela variação em outra variável.

O coeficiente de correlação de Pearson (τ) é definido como:

$$\tau = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}}$$

A significância (s_τ) de (τ) é definido como:

$$s_\tau = \sqrt{\frac{1 - \tau^2}{n - 2}}$$

E o teste **t** para correlação e significância é definido como:

$$t = \frac{\tau}{s_\tau}$$

5.5.6.1 TESTE DA HIPÓTESE 1

- **Hipótese 1:** As diretorias do Inmetro, com "Percepção de Segurança da Informação" mais elevada (menor quantidade de incidentes de segurança), são aquelas que possuem "Percepção de Qualidade" mais alta.

  - **Questão 1:** Qual é o índice de incidentes de segurança da informação nestas diretorias?

  - **Questão 2:** Qual é o grau de satisfação (percepção de qualidade) dos clientes do Sistema de Informação destas diretorias?

Tabela 62: Comparação das Diretorias em relação à Percepção de Segurança da Informação e a Percepção da Qualidade

Hipótese 1	Questão 1	Questão 2
Diretorias	**Índ. Seg. Info**	**Índ. Perc. Qual.**
AUDIN	**0,240**	**-1,47**
GABIN	**0,225**	**-0,80**
PROGE	**0,059**	**-1,50**
DQUAL	**0,043**	**-1,10**
DIMEL	**0,041**	**-1,86**
CGCRE	**0,037**	**-1,50**
DIMCI	**0,028**	**-1,64**
CPLAN	**0,019**	**-1,09**
DIRAF	**0,019**	**-1,35**
CAINT	**0,008**	**-1,37**

Fonte: Elaboração própria

O coeficiente de correlação entre as variáveis é de:

$\tau = 0{,}329$ ➔ indica correlação fraca

- Teste de significância da correlação:

  Hipótese de nulidade do coeficiente de correlação:

  - H_0: $\tau = 0$
  - H_1: $\tau \neq 0$

Onde:

τ = coeficiente de correlação entre as percepções de segurança da informação e percepção de qualidade;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0,05$) para testar a hipótese nula.

$$t = \frac{\tau}{s_\tau}$$

Onde:

τ = coeficiente de correlação**;**

s_τ = significância da correlação;

$$\tau = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}}$$

Onde:

$\bar{x}$ = média da amostra de percepção de segurança;

$\bar{y}$ = média da amostra de percepção de qualidade;

$$s_\tau = \sqrt{\frac{1 - \tau^2}{n - 2}}$$

Onde:

$n - 2$ = graus de liberdade (**v**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t **,** para $\alpha = 0,05$, com "n-2" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

$\alpha = 0,05$

$\tau = 0,329$

$s_\tau = 0,334$

$\nu = n - 2 = 8$

$t_\alpha = t_{0,05} = 1,860$

$t = 0,986$

Logo:

$t = 0,986 < t_\alpha = t_{0,05} = 1,860$ ➔ Não rejeitar H_0

Concluindo:

Não se pode rejeitar H_0 ao nível de 5%, não confirmando a existência de correlação significativa. As evidências são insuficientes para concluir que a relação significante existe. Portanto, apesar da ocorrência de uma correlação fraca entre a percepção de segurança da informação e a percepção de qualidade, esta correlação não pode ser classificada como significante.

5.5.6.2 TESTE DA HIPÓTESE 2

- **<u>Hipótese 2</u>:** As diretorias do Inmetro com maior índice de "Percepção de Segurança da Informação" (menor quantidade de incidentes de segurança), têm seus "Líderes" com mais alto grau de eficácia.

  - **Questão 1:** Qual é o índice de incidentes de segurança da informação nestas diretorias?

  - **Questão 2:** Os líderes (diretores/gerentes) destas diretorias do Inmetro têm alto grau de eficácia (percepção de liderança)?

Tabela 63: Comparação das Diretorias em relação à Percepção de Segurança da Informação e a Percepção de Liderança

Hipótese 2	Questão 1	Questão 2
Diretorias	**Índ. Seg. Info**	**Índ. Perc. Lid.**
AUDIN	**0,240**	**53,720**
GABIN	**0,225**	**41,650**
PROGE	**0,059**	**45,829**
DQUAL	**0,043**	**42,510**
DIMEL	**0,041**	**30,400**
CGCRE	**0,037**	**40,862**
DIMCI	**0,028**	**38,882**
CPLAN	**0,019**	**38,260**
DIRAF	**0,019**	**46,300**
CAINT	**0,008**	**44,880**

Fonte: Elaboração própria

O coeficiente de correlação entre as variáveis é de:

$\tau = 0{,}459$ ➔ indica correlação moderada

- Teste de significância da correlação:

Hipótese de nulidade do coeficiente de correlação:

- H_0: $\tau = 0$
- H_1: $\tau \neq 0$

Onde:

τ = coeficiente de correlação entre as percepções de segurança da informação e percepção de qualidade;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% ($\alpha = 0{,}05$) para testar a hipótese nula.

$$t = \frac{\tau}{s_\tau}$$

Onde:

τ = coeficiente de correlação;

s_τ = significância da correlação;

$$\tau = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}}$$

Onde:

$\bar{x}$ = média da amostra de percepção de segurança;

$\bar{y}$ = média da amostra de percepção de qualidade;

$$s_\tau = \sqrt{\frac{1 - \tau^2}{n - 2}}$$

Onde:

$n - 2$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-2" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  τ = 0,459

  s_τ = 0,314

  ν = n –2 = 8

  $t_\alpha = t_{0,05}$ = 1,860

  t = 1,460

Logo:

t = 1,460 < $t_\alpha = t_{0,05}$ = 1,860 ➔ Não rejeitar H_0

Concluindo:

Não se pode rejeitar H_0 ao nível de 5%, não confirmando a existência de correlação significativa. As evidências são insuficientes para concluir que a relação significante existe. Portanto, apesar da ocorrência de uma correlação moderada entre a percepção de segurança da informação e a percepção de liderança, esta correlação não pode ser classificada como significante.

5.5.6.3 TESTE DA HIPÓTESE 3

- **Hipótese 3:** As diretorias do Inmetro com maior índice de "Percepção de Segurança da Informação" (menor quantidade de incidentes de segurança), têm um alto grau de "Seguidores Exemplares" (Percepção dos Seguidores).

  - **Questão 1:** Qual é o índice de incidentes de segurança da informação nestas diretorias?

  - **Questão 2:** Qual o grau de "Seguidores Exemplares" destas diretorias?

Tabela 64: Comparação das Diretorias em relação à Percepção de Segurança da Informação e a Percepção de Seguidores

Hipótese 3	Questão 1	Questão 2
Diretorias	Índ. Seg. Info	Índ. Perc. Seg.
AUDIN	0,240	1,000
GABIN	0,225	0,833
PROGE	0,059	0,833
DQUAL	0,043	0,750
DIMEL	0,041	0,765
CGCRE	0,037	0,923
DIMCI	0,028	0,941
CPLAN	0,019	0,694
DIRAF	0,019	0,875
CAINT	0,008	1,000

Fonte: Elaboração própria

O coeficiente de correlação entre as variáveis é de:

τ = 0,235 ➔ indica correlação fraca

- Teste de significância da correlação:

Hipótese de nulidade do coeficiente de correlação:

- H_0: $\tau = 0$
- H_1: $\tau \neq 0$

Onde:

τ = coeficiente de correlação entre as percepções de segurança da informação e percepção de qualidade;

- Prova estatística:

Emprega-se a distribuição **t** (distribuição de Student), para pequenas amostras (n<30), com nível de significância de 5% (α = 0,05) para testar a hipótese nula.

$$t = \frac{\tau}{s_\tau}$$

Onde:

τ = coeficiente de correlação**;**

s_τ = significância da correlação;

$$\tau = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}}$$

Onde:

$\bar{x}$ = média da amostra de percepção de segurança;

$\bar{y}$ = média da amostra de percepção de qualidade;

$$s_\tau = \sqrt{\frac{1-\tau^2}{n-2}}$$

Onde:

$n-2$ = graus de liberdade (**ν**)

Rejeitar H_0 se $t > t_\alpha$

Onde:

t_α = índice t, para α = 0,05, com "n-2" graus de liberdade, encontrado na tabela do Anexo G.

- Cálculos:

  α = 0,05

  τ = 0,235

  s_τ = 0,344

  ν = n –2 = 8

  $t_\alpha = t_{0,05}$ = 1,860

  t = 0,684

Logo:

t = 0,684 < $t_\alpha = t_{0,05}$ = 1,860 ➔ Não rejeitar H_0

Concluindo:

Não se pode rejeitar H_0 ao nível de 5%, não confirmando a existência de correlação significativa. As evidências são insuficientes para concluir que a relação significante existe. Portanto, apesar da ocorrência de uma correlação fraca entre a percepção de segurança da informação e a percepção de seguidores, esta correlação não pode ser classificada como significante.

5.6 SUMÁRIO CONCLUSIVO DO CAPÍTULO

Neste capítulo, os resultados obtidos com a pesquisa de campo foram tabulados e analisados. As amostras foram consideradas válidas para representar as populações da pesquisa em questão. Os resultados apresentaram confiabilidade estatística suficiente para corroboração ou refutação das hipóteses, mas provavelmente não representaram a realidade diária do trabalho nas diretorias, pois existiu a possibilidade dos respondentes terem mascarados seus sentimentos na hora de responder os questionários da pesquisa. As análises e comentários serão vistos na conclusão da dissertação.

6 CONCLUSÕES E RECOMENDAÇÕES

6.1 SUMA DO CAPÍTULO

Neste capítulo são apresentadas as conclusões e sugestões para novas pesquisas no futuro. As conclusões a seguir apresentam as respostas para as hipóteses e questões feitas no Capítulo 1.

6.2 CONCLUSÕES

6.2.1 O PROBLEMA

O objetivo deste projeto é estudar a Percepção de Segurança em Sistemas de Informação e sua relação com a Qualidade Percebida (*Servqual*), Perfil de Liderança (*Leadership*) e Perfil dos Seguidores (*Followership*).

Esta pesquisa tem o intuito de começar um estudo de caso (Caso Inmetro), dando início para pesquisas posteriores e mais aprofundadas, sobre o comportamento do elo mais fraco da segurança da informação: o fator humano. Sobre como os índices de incidentes de segurança da informação estão relacionados com os índices da qualidade de serviços dos sistemas de informação, com a percepção de liderança e a percepção dos seguidores.

6.2.2 SOLUÇÃO DO PROBLEMA

Para solucionar este problema, foram tabulados os dados respondidos pelos usuários de sistemas de informação de cada diretoria do Inmetro. Foi realizado um tratamento estatístico das respostas aos questionários de Segurança da Informação, Percepção de Qualidade, Percepção de Liderança e Percepção de Seguidores, para a análise das médias, de

seus desvios padrões, da distribuição t (Student) e do coeficiente de correlação, para se determinar a falseabilidade ou não das hipóteses testadas, sendo a pesquisa completamente transcorrida ao nível de confiabilidade de 95%.

O software utilizado para a análise desses dados foi o Microsoft Excel 2000 e suas respectivas ferramentas estatísticas.

6.2.3 VERIFICAÇÃO DAS HIPÓTESES

A metodologia aplicada se baseia no teste de falseabilidade das hipóteses levantadas, por meio do método da hipótese nula, ou seja, pela aplicação de um teste estatístico adequado à natureza das variáveis e da amostra analisada, de forma a corroborar ou rejeitar as hipóteses.

Desta forma, para cada hipótese, para cada diretoria, foram testadas estatisticamente todos os resultados desta pesquisa.

6.2.3.1 HIPÓTESE 1

As diretorias do Inmetro, com "Percepção de Segurança da Informação" mais elevada (menor quantidade de incidentes de segurança), são aquelas que possuem "Percepção de Qualidade" mais alta.

- **Questão 1:** Qual é o índice de incidentes de segurança da informação nestas diretorias?

Para responder esta questão, foram utilizados os seguintes referenciais teóricos:

- Norma ABNT NBR ISO/IEC 17799
- Pesquisa de Segurança da Módulo
- Pesquisa de Segurança do CERT.BR
- Conhecimento e Formação do Autor em Análise de Sistemas e Segurança da Informação

Os dados foram tratados estatisticamente pela distribuição **t** (distribuição de Student), para pequenas amostras (n<30), utilizada com o intuito de corroborar ou refutar as hipóteses de teste da média da população. Após o teste de corroboração ou refutação da média, calculou-se o índice de segurança da informação (ISI), que é o inverso da média encontrada de incidentes de segurança em cada diretoria no ano de 2005, sendo esta, a forma de posicionar as unidades organizacionais em ordem de melhor percepção de segurança da informação.

Todos os testes rejeitaram suas hipóteses nulas e corroboraram as médias das amostras de cada diretoria, isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a média da população seja igual a zero. Pode-se utilizar a média de cada amostra como estimativa da média populacional.

Tabela 65: Índices de Segurança da Informação das diretorias

Ordem:	Diretorias:	Índice:
1	AUDIN	0,240
2	GABIN	0,225
3	PROGE	0,059
4	DQUAL	0,043
5	DIMEL	0,041
6	CGCRE	0,037
7	DIMCI	0,028
8	DIRAF	0,019
9	CPLAN	0,019
10	CAINT	0,008

Fonte: Elaboração própria

Pode-se perceber que mesmo as diretorias mais bem colocadas, não possuem valores altos de índice, indicando que a instituição como um todo, ainda tem problemas em relação à Segurança da Informação.

- **Questão 2:** Qual é o grau de satisfação dos clientes do Sistema de Informação destas diretorias?

Para responder esta questão, os dados foram tabulados dos resultados da pesquisa obtida através das respostas, por meio de amostras aleatórias dos usuários, ao questionário

Servqual, dentro de cada diretoria. Para fins desta pesquisa, para o cálculo do índice de percepção da qualidade, somente foi levado em conta, o "Gap 5" do modelo de Parasuraman et al.(1990), ou seja, a diferença total da percepção e da expectativa da qualidade dos serviços prestados pelos sistemas da informação do Inmetro. As outras respostas servem para ilustrar esta pesquisa e para iniciar, se alguém tiver interesse, um futuro estudo além deste. Foi utilizado como referencial teórico PARASURAMAN, A.; ZEITHAML, Valarie A.; BERRY, Leonard L. **A conceptual Model of Service Quality and Its Implicans for Future Research.**

Os dados foram tratados estatisticamente pela distribuição **t** (distribuição de Student), que foi utilizada com o intuito de corroborar ou refutar as hipóteses de teste da diferença entre duas médias da população, para comprovar ou não, a existência do "gap".

Após o teste de corroboração ou refutação das diferenças entre as duas médias, calculou-se o índice de percepção da qualidade, sendo esta, a forma de posicionar as unidades organizacionais em ordem de melhor percepção de qualidade. Todos os testes rejeitaram suas hipóteses nulas e corroboraram as diferenças entre as médias das amostras de cada diretoria, isto é, não há evidências suficientes, ao nível de confiança de 95%, de que a diferença entre as médias da população seja igual a zero. Pode-se utilizar diferença das médias de cada amostra como estimativa das diferenças das médias da população. Os "gaps" ficam assim, validados.

Tabela 66: Índice de percepção de qualidade nas diretorias

Ordem:	Diretoria:	GAP
1	GABIN	-0,80
2	CPLAN	-1,09
3	DQUAL	-1,10
4	DIRAF	-1,35
5	CAINT	-1,37
6	AUDIN	-1,47
7	CGCRE	-1,50
8	PROGE	-1,50
9	DIMCI	-1,64
10	DIMEL	-1,86

Fonte: Elaboração própria

Pode-se perceber que mesmo as duas piores diretorias, não possuem valores altos de gap, indicando que a instituição como um todo, tem uma boa percepção da qualidade dos serviços prestados pelos sistemas de informação.

- **Testagem da Hipótese 1:**

Os resultados das questões 1 e 2 foram comparados para corroborar ou refutar a relação entre as percepções de segurança da informação e as percepções de qualidade de serviços. Para esta comparação estatística foram utilizados o coeficiente de correlação de Pearson, a significância destas correlações e o teste **t** de Student, para identificar em que medida a variação em uma variável está associada pela variação em outra variável.

Após os testes, chegou-se ao resultado de coeficiente "τ = 0,329"; o que indica uma correlação fraca, mas não se pode rejeitar a hipótese nula ao nível de 5%, não confirmando a existência de correlação significativa. As evidências são insuficientes para concluir que a relação significante existe. Portanto, apesar da ocorrência de uma correlação fraca entre a percepção de segurança da informação e a percepção de qualidade, esta correlação não pode ser classificada como significante.

6.2.3.2 HIPÓTESE 2

As diretorias do Inmetro com maior índice de "Percepção de Segurança da Informação" (menor quantidade de incidentes de segurança), têm seus "Líderes" com mais alto grau de eficácia.

- **Questão 1:** Qual é o índice de incidentes de segurança da informação nestas diretorias?

Vide o item 6.2.4.1 HIPÓTESE 1, Questão 1.

- **Questão 2:** Os líderes (diretores/gerentes) destas diretorias do Inmetro têm alto grau de eficácia?

Para responder esta questão, os dados foram tabulados dos resultados da pesquisa obtida através das respostas, por meio de amostras aleatórias dos usuários, ao questionário

LPI para práticas de liderança, dentro de cada diretoria. Nesta pesquisa foi utilizado o referencial teórico de KOUZES, James M.; POSNER, Barry Z**. O Desafio da Liderança.**

Para fins desta pesquisa, para o cálculo do índice de percepção da liderança, não foi levada em consideração a auto-avaliação dos diretores do Inmetro, que por diversos motivos, não foram possíveis de conseguir.

Os dados foram tratados estatisticamente pela distribuição t (distribuição de Student), com o intuito de corroborar ou refutar as hipóteses de teste da média da população. Após o teste de corroboração ou refutação da média, calculou-se o índice de percepção de liderança (a média total dos princípios de liderança), sendo esta, a forma de posicionar as unidades organizacionais em ordem de melhor percepção de liderança das diretorias.

Todos os testes rejeitaram suas hipóteses nulas e corroboraram as médias das amostras de cada diretoria, isto é, não há evidências suficientes, ao nível de confiança de 95%, de que as médias da população sejam iguais a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Abaixo, são apresentados os resultados e as respectivas colocações das diretorias do Inmetro, na parte da pesquisa relativa a percepção de liderança:

Tabela 67: Índice de percepção de liderança nas diretorias

Ordem:	Diretoria:	Índice:
1	AUDIN	53,720
2	DIRAF	46,300
3	PROGE	45,829
4	CAINT	44,880
5	DQUAL	42,510
6	GABIN	41,650
7	CGCRE	40,862
8	DIMCI	38,882
9	CPLAN	38,260
10	DIMEL	30,400

Fonte: Elaboração própria

Pode-se perceber que algumas diretorias possuem valores altos de percepção de liderança, indicando que seus diretores têm as melhores práticas de liderança como premissas de suas administrações.

- **Testagem da Hipótese 2:**

Os resultados das questões 1 e 2 foram comparados para corroborar ou refutar a relação entre as percepções de segurança da informação e as percepções de qualidade de serviços. Para esta comparação estatística foram utilizados o coeficiente de correlação de Pearson, a significância destas correlações e o teste **t** de Student, para identificar em que medida a variação em uma variável está associada pela variação em outra variável.

Após os testes, chegou-se ao resultado de coeficiente "τ = 0,459"; o que indica uma correlação moderada, mas não se pode rejeitar a hipótese nula ao nível de 5%, não confirmando a existência de correlação significativa. As evidências são insuficientes para concluir que a relação significante existe. Portanto, apesar da ocorrência de uma correlação moderada entre a percepção de segurança da informação e a percepção de liderança, esta correlação não pode ser classificada como significante.

6.2.3.3 HIPÓTESE 3

As diretorias do Inmetro com maior índice de "Percepção de Segurança da Informação" (menor quantidade de incidentes de segurança), têm um alto grau de "Seguidores Exemplares".

- **Questão 1:** Qual é o índice de incidentes de segurança da informação nestas diretorias?

Vide o item 6.2.4.1 HIPÓTESE 1, Questão 1.

- **Questão 2:** Qual o grau de "Seguidores Exemplares" destas diretorias?

Para responder esta questão, os dados foram tabulados dos resultados da pesquisa obtida através das respostas, por meio de amostras aleatórias dos usuários, ao questionário de perfil dos seguidores, dentro de cada diretoria. Para fins desta pesquisa, para o cálculo do índice de percepção dos seguidores, foi utilizado o referencial teórico de KELLEY, Robert E. **O poder dos seguidores:** como criar os verdadeiros líderes**.**

Os dados foram tratados estatisticamente pela distribuição t (distribuição de Student), com o intuito de corroborar ou refutar as hipóteses de teste da média da população. Após o

teste de corroboração ou refutação da média, calculou-se o índice de percepção de seguidores (número de seguidores exemplares divididos pelo tamanho da amostra), sendo esta, a forma de posicionar as unidades organizacionais em ordem de melhor percepção de seguidores das diretorias.

Todos os testes rejeitaram suas hipóteses nulas e corroboraram as médias das amostras de cada diretoria, isto é, não há evidências suficientes, ao nível de confiança de 95%, de que as médias da população sejam iguais a zero. Pode-se utilizar a média da amostra como estimativa da média populacional.

Abaixo, são apresentados os resultados e as respectivas colocações das diretorias do Inmetro, na parte da pesquisa relativa a percepção de seguidores:

Tabela 68: Índice de percepção de seguidores nas diretorias

Ordem:	Diretoria:	Índice:
1	AUDIN	1,000
2	CAINT	1,000
3	DIMCI	0,941
4	CGCRE	0,923
5	DIRAF	0,875
6	GABIN	0,833
7	PROGE	0,833
8	DIMEL	0,765
9	DQUAL	0,750
10	CPLAN	0,694

Fonte: Elaboração própria

Pode-se perceber que algumas diretorias possuem valores altos de percepção de seguidores, indicando que seus usuários têm, na sua maioria, os melhores perfis de seguidores. Sendo esse dado de grande importância para a instituição.

- **Testagem da Hipótese 3:**

Os resultados das questões 1 e 2 foram comparados para corroborar ou refutar a relação entre as percepções de segurança da informação e as percepções de qualidade de serviços. Para esta comparação estatística foram utilizados o coeficiente de correlação de Pearson, a significância destas correlações e o teste **t** de Student, para identificar em que medida a variação em uma variável está associada pela variação em outra variável.

Após os testes, chegou-se ao resultado de coeficiente "τ = 0,235"; o que indica uma correlação fraca, mas não se pode rejeitar a hipótese nula ao nível de 5%, não confirmando a existência de correlação significativa. As evidências são insuficientes para concluir que a relação significante existe. Portanto, apesar da ocorrência de uma correlação fraca entre a percepção de segurança da informação e a percepção de seguidores, esta correlação não pode ser classificada como significante.

6.2.4 VALIDAÇÃO DAS HIPÓTESES

Tabela 69: Validação das hipóteses

Validação das hipóteses		
Hipóteses	**Questões-chave**	**Validação da hipótese**
Hipótese I As diretorias do Inmetro, com "Percepção de Segurança da Informação" mais elevada (menor quantidade de incidentes de segurança), são aquelas que possuem "Percepção de Qualidade" mais alta. **Não pode ser considerada plausível**	1) Qual é o índice de incidentes de segurança da informação nestas diretorias?	AUDIN 0,240 GABIN 0,225 PROGE 0,059 DQUAL 0,043 DIMEL 0,041 CGCRE 0,037 DIMCI 0,028 DIRAF 0,019 CPLAN 0,019 CAINT 0,008
	2) Qual é o grau de satisfação dos clientes do Sistema de Informação destas diretorias?	GABIN -0,80 CPLAN -1,09 DQUAL -1,10 DIRAF -1,35 CAINT -1,37 AUDIN -1,47 CGCRE -1,50 PROGE -1,50 DIMCI -1,64 DIMEL -1,86
	➔ Existe ralação entre os índices de segurança da informação e o índice de percepção de qualidade?	→ Coeficiente de correlação: **"τ = 0,329"**; o que indica uma correlação fraca, mas não se pode rejeitar a hipótese nula ao nível de 5%, não confirmando a existência de correlação significativa. As evidências são insuficientes para concluir que a relação significante existe.

Hipóteses	Questões-chave	Validação da hipótese
Hipótese II As diretorias do Inmetro com maior índice de "Percepção de Segurança da Informação" (menor quantidade de incidentes de segurança), têm seus "Líderes" com mais alto grau de eficácia. **Não pode ser considerada plausível**	1) Qual é o índice de incidentes de segurança da informação nestas diretorias?	AUDIN 0,240 GABIN 0,225 PROGE 0,059 DQUAL 0,043 DIMEL 0,041 CGCRE 0,037 DIMCI 0,028 DIRAF 0,019 CPLAN 0,019 CAINT 0,008
	2) Os líderes (diretores/gerentes) destas diretorias do Inmetro têm alto grau de eficácia?	AUDIN 53,720 DIRAF 46,300 PROGE 45,829 CAINT 44,880 DQUAL 42,510 GABIN 41,650 CGCRE 40,862 DIMCI 38,882 CPLAN 38,260 DIMEL 30,400
	➔ Existe ralação entre os índices de segurança da informação e o índice de percepção de liderança?	→ Coeficiente de correlação: **"τ = 0,459"**; o que indica uma correlação moderada, mas não se pode rejeitar a hipótese nula ao nível de 5%, não confirmando a existência de correlação significativa. As evidências são insuficientes para concluir que a relação significante existe.

Hipóteses	Questões-chave	Validação da hipótese
Hipótese III As diretorias do Inmetro com maior índice de "Percepção de Segurança da Informação" (menor quantidade de incidentes de segurança), têm um alto grau de "Seguidores Exemplares". **Não pode ser considerada plausível**	1) Qual é o índice de incidentes de segurança da informação nestas diretorias?	AUDIN 0,240 GABIN 0,225 PROGE 0,059 DQUAL 0,043 DIMEL 0,041 CGCRE 0,037 DIMCI 0,028 DIRAF 0,019 CPLAN 0,019 CAINT 0,008
	2) Qual o grau de "Seguidores Exemplares" destas diretorias?	AUDIN 1,000 CAINT 1,000 DIMCI 0,941 CGCRE 0,923 DIRAF 0,875 GABIN 0,833 PROGE 0,833 DIMEL 0,765 DQUAL 0,750 CPLAN 0,694

	➔ Existe ralação entre os índices de segurança da informação e o índice de percepção de seguidores?	→ Coeficiente de correlação: **"τ = 0,235"**; o que indica uma correlação fraca, mas não se pode rejeitar a hipótese nula ao nível de 5%, não confirmando a existência de correlação significativa. As evidências são insuficientes para concluir que a relação significante existe.

Fonte: Elaboração própria

6.3 CONCLUSÃO FINAL

Ao final desta pesquisa chega-se à conclusão que existe uma relação entre as percepções de segurança da informação, percepções de qualidade, percepções de liderança e percepções de seguidores, entre as diretorias do Inmetro. Esta relação tem correlações fracas e moderadas, mas elas não podem ser classificadas como significantes ao nível de 5%.

Com estes dados, observa-se que a Instituição tem de melhorar seus níveis de percepção de segurança da informação e de percepção de liderança. Os sistemas de informação devem melhorar a qualidade dos serviços, para melhor atender as expectativas dos usuários das diretorias.

No aspecto de seguidores exemplares, as diretorias, e a instituição num todo, estariam bem servidas pelo seu quadro funcional, mas observou-se que, estranhamente, a quantidade de seguidores exemplares foi muito alta. Existiu neste ponto, uma grande possibilidade que as respostas estivessem mascaradas de alguma forma, seja pela impaciência dos respondentes, seja pelo receio de responder sinceramente o que pensava, ou por quaisquer outros motivos. Da mesma forma, os dados do perfil de liderança também tiveram, possivelmente, uma discrepância com a realidade dos fatos.

Notou-se um baixo índice de segurança da informação em todas as diretorias do Inmetro, o que denota uma falta de conhecimento ou de vontade na aplicação das normas de segurança por parte dos usuários em geral. Constatou-se uma falta da política de segurança da informação das diretorias e a não existência de treinamentos sobre o assunto. É evidente a não conformidade das diretorias, e dos usuários da instituição como um todo, em relação à Norma ABNT NBR ISO/IEC 17799.

6.4 RECOMENDAÇÕES

Os resultados aqui apresentados não são definitivos. Estudos posteriores se tornam necessários, inclusive estendendo-os a todos os funcionários e a outros serviços da organização, para verificar a confirmação destes resultados.

Espera-se que futuros pesquisadores interessem-se pela continuidade e atualização deste trabalho, contribuindo para o progresso do conhecimento científico e para o desenvolvimento e melhoria contínua do Inmetro.

Sugere-se, para novos estudos sobre o tema, um maior cuidado com as amostras, com o referencial teórico e os instrumentos da pesquisa, e até, com a metodologia, pois os resultados apresentados pareceram estar distorcidos da realidade, provavelmente por causa da forma como os usuários responderam aos questionários.

Recomenda-se, acima de tudo:

- campanhas internas de marketing e treinamento dos usuários sobre segurança da informação;
- aumento do cumprimento das normas pelas diretorias e pela instituição, com o intuito de elevar o nível de conformidade às normas e decretos sobre segurança da informação;
- adoção de políticas de segurança da informação mais severas;
- e por fim, a criação de uma diretoria, ou de um departamento de segurança da informação, ligado diretamente a presidência da organização.

REFERÊNCIAS

ALMO, Gil Fonseca do. **Portal web**. Disponível em **http://rman01s.inmetro.gov.br/lflima**. Acesso em dezembro de 2005.

ALVARADO, Williams O. **Qualidade em serviços liderança gerencial nas empresas de informática.** Dissertação (Mestrado em Engenharia de Produção), Universidade Federal Fluminense, Niterói, 2001.

ALVES, Gustavo Alberto. **Segurança da Informação:** Uma Visão Inovadora da Gestão. Rio de Janeiro: Ciência Moderna, 2006.

ANDERSON, David R.; SWEENEY, D.; WILLIANS, Thomas A**. Estatística Aplicada à Administração e Economia.** 2. ed. São Paulo: Pioneira Thomson Learning. 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799:** Tecnologia da informação - Código de prática para a gestão da segurança da informação**.** Rio de Janeiro, 2001.

_____. **NBR 11154:** Interpretação Estatística de Dados. Rio de Janeiro, 1990.

_____. **NBR 10536:** Estatística. Rio de Janeiro, 1988.

BOGADO, Sávio Domingos Coube. **Análise da Competitividade e Tecnologia de Informação das Empresas de Refrigerantes**. Dissertação (Mestrado em Engenharia de Produção). Universidade Federal Fluminense, Niterói, 2003.

CAUBIT, Rosangela. **A Aplicação de um Modelo de Gestão de Segurança da Informação e a sua Influência na Percepção de Competitividade no Setor de Telecomunicações e Informática.** Dissertação (Mestrado em Sistemas de Gestão), Universidade Federal Fluminense, Niterói, 2003.

CERT. Disponível em: http://www.cert.org. Acesso em: setembro de 2005.

CERT.BR. Disponível em: http://www.cert.br. Acesso em: setembro de 2005.

COSTA, Jeffrey H.; **Avaliando Treinamentos em Vendas: Um estudo da qualidade dos serviços prestados por organizações de *Call Center*, percebida por clientes da indústria de telecomunicações.** Dissertação (Mestrado em Sistemas de Gestão), Universidade Federal Fluminense, Niterói, 2004.

COX, William. **The Most Critical Security Issue.** Disponível em: http://www.giac.org/practical/gsec/William_Cox_GSEC.pdf. Acesso em: outubro de 2005.

EHLERS, Ricardo S**. Introdução à Estatística.** 2. ed. Curitiba: Depto. Estatística da Universidade Federal do Paraná, 2005.

FERNANDES, Edite Manuela da G. P.; **Estatística Aplicada**. Braga – Portugal: Universidade do Minho, 1999.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 1991.

KELLEY, Robert. **O Poder dos Seguidores:** Como criar os verdadeiros líderes**.** São Paulo: Siciliano, 1993.

KISSER, Scott. **A Hardware Based Firewall Option for the SOHO.** Disponível em: http://www.giac.org/certified_professionals/practicals/gsec/0303.php. Acesso em outubro de 2005.

KOUZES, James M.; POSNER, Barry Z. **Leadership Practices Inventory [LPI]:** Participant's Workbook. San Francisco: Jossey - Bass/Pfeiffer, 1997.

_____. **O Desafio da Liderança**. Rio de Janeiro: Campus, 2003.

LAKATOS, E. M., MARCONI**,** M.A. **Metodologia científica**. 2. ed. São Paulo: Atlas, 1991.

_____. **Fundamentos da metodologia científica.** São Paulo: Atlas, 1993.

_____. **Técnicas de pesquisa**: planejamento e execução de pesquisas, amostragens e técnicas de pesquisas, elaboração, análise e interpretação de dados. 4. ed. São Paulo: Atlas, 1999.

_____. **Metodologia do trabalho científico**. 5. ed. São Paulo: Atlas, 2001.

MATTAR, F. N. **Pesquisa *de Marketing*:** Metodologia, Planejamento, Execução, Análise. 2. ed. São Paulo: Atlas, 1994.

MÓDULO. Disponível em: http://www.modulo.com.br. Acesso em: setembro de 2005.

MOREIRA, Sérgio Dias. **Percepção da Qualidade e uso competitivo de Tecnologia de Informação em Empresas Têxteis e de Confecção de *"Jeanswear"***. Dissertação (Mestrado em Sistemas de Gestão), Universidade Federal Fluminense, Niterói, 2004.

PARASURAMAN, A.; ZEITHAML, Valarie A.; BERRY, Leonard L. **A conceptual Model of Service Quality and Its Implicans for Future Research**. *Journal of Marketing*, Fall, 1985.

_____. **Delivering Quality Service**. New York: The Free Press, 1990.

POPPER, Karl S.**, A lógica da pesquisa científica.** 2 ed. São Paulo: Cultrix, 1975.

QUINTELLA, Heitor M**. Fatores humanos e tecnológicos da competitividade.** Projeto de Pesquisa - Departamento de Engenharia Civil, Universidade Federal Fluminense, Niterói, 1997.

_____. Um método de orientação de mestrandos: relatório interno. Niterói: Universidade Federal Fluminense, 1999. Apostila.

_____; COSTA, J. H.; FREITAS, M. **Liderança e Qualidade Percebida: Relação entre os dois fatores em *Call Centers* de empresas de telecomunicações**. Tendências do trabalho, Rio de Janeiro, v. 367, n. Mar, p. 30-34, 2005.

_____; SILVA, R. K. **Qualidade e Liderança na Prestação de Serviços: Uma Avaliação Usando Escala *SERVQUAL* e *LPI***. Relatórios de Pesquisa em Engenharia de Produção UFF, Niterói, v. 6, n. 4, p. 1-16, 2006.

RABENER, Joseph. Do you need a security assessment? Disponível em: **http://www.giac.org/practical/gsec/Joseph_Rabener_GSEC.pdf**. Acesso em outubro de 2005.

ROCHA, Henrique**. Fatores Críticos de Sucesso de start up de veículos e a qualidade (CMMI) no desenvolvimento de produtos no sul fluminense.** Dissertação (Mestrado em Engenharia de Produção), Universidade Federal Fluminense, Niterói, 2005.

SANS INSTITUTE. Disponível em: http://www.sans.org. Acesso em setembro de 2005.

SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO. Departamento de Serviços de Rede. **Guia de Referência para a Segurança da Informação:** Usuário Final. Brasília: Ministério do Planejamento, Orçamento e Gestão, 2005.

SÊMOLA, Marcos. **Gestão da Segurança da Informação – Uma Visão Executiva.** Rio de Janeiro: Campus, 2003.

SPIEGEL, Murray R**. Estatística.** 3. ed. São Paulo: Makron Books, 1993.

TOLEDO, Roberto Farias. **Maturidade CMM, Qualidade de Processos Six Sigma e a Relação com a Qualidade Percebida para Cliente: Estudo de Caso Xerox**. Dissertação (Mestrado em Sistemas de Gestão), Universidade Federal Fluminense, Niterói, 2005.

US-CERT. Disponível em: http://www.us-cert.gov. Acesso em: setembro de 2005.

GLOSSÁRIO

Antivírus	Programa utilizado para eliminar vírus eletrônicos de computadores contaminados.
Aplicação	Programa, ou conjunto de programas que realizam uma determinada função.
Ataque	Ação que constitui uma tentativa deliberada e não autorizada para acessar/manipular informações, ou tornar um sistema não confiável, ou indisponível, violando assim a política de segurança. Um ataque bem sucedido que resulte no acesso ou manipulação de informações, de forma não autorizada, é chamado de invasão.
Ataque de Negação de Serviço	Ataque que consiste em impedir o acesso autorizado a recursos de um sistema, seja através de uma grande sobrecarga no processamento de dados de um sistema computacional, da saturação de um ponto de acesso através de um grande tráfego de dados para uma rede, ou da indisponibilização de um ou mais serviços desse sistema.
Ativo	Ativo é tudo que manipula direta ou indiretamente uma informação, inclusive a própria informação, dentro de uma organização. É esse ativo que deve ser protegido contra ameaças para que o negócio funcione corretamente.
Autenticação	Procedimento utilizado na identificação de usuários, dispositivos ou processos, e que é pré-requisito para o acesso aos recursos de um sistema.
Autorização	É o direito ou permissão de acesso a um recurso de um sistema.
Crackers	São os hackers do mal. Eles assim como os hackers, sabem muito, só que usam esse conhecimento para prejudicar o patrimônio dos outros, ao contrário dos hackers, que apenas olham e inclusive chegam a dizer os bugs de segurança para os administradores de sistema. A imprensa em geral confunde os crackers chamando-os de hackers.
Denial of service	Ver “ataque de negação de serviço”.
Direito de Acesso	É a permissão dada a uma entidade para acessar e manipular Informações presentes em um sistema.
Firewall	Sistema ou combinação de sistemas que protege a fronteira entre duas ou mais redes de computadores contra ataques externos. Funciona filtrando as informações e permitindo ou proibindo certos tipos de acesso, de acordo com uma política de segurança pré-estabelecida.

Fraude	Crimes relacionados a computadores envolvendo deliberada alteração, falsificação ou divulgação de dados com a intenção de obter algo de valor (normalmente ganho monetário).
Fraude Bancária	Acesso a um computador ou uma rede de computadores do sistema bancário, ou fingindo ser deste sistema, que é envolvido na realização de ato ou série de atos fraudulentos, com a manipulação imprópria de dados de entrada; saída ou resultados; aplicações; arquivos de dados; operações de computador; comunicações; ou hardware de computador ou software de sistemas.
Hacker	Pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, com o intuito de acesso a determinado ambiente para proveito próprio ou de terceiros. Dependendo dos objetivos da ação, podem ser chamados de *Cracker*, *Lammer* ou *BlackHat.*
Hardware	É todo o equipamento físico dos sistemas de informação, como por exemplo: computador, monitor, nobreak, etc.
IDS	*Intrusion Detection System*, sistema de detecção de intrusão. Consiste no monitoramento e análise de eventos em sistemas computacionais, com o propósito de detectar e prover alertas sobre tentativas de acesso não autorizado a recursos destes sistemas.
Incidente de Segurança	Um incidente de segurança é caracterizado por qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas computacionais ou de redes de computadores. Tentativas de obter acesso não autorizado a sistemas ou dados, ataques de negação de serviço, uso ou acesso não autorizado a um sistema e desrespeito à política de segurança ou à política de uso aceitável de uma instituição são exemplos de incidentes de segurança.
Invasão	Evento ou combinação de eventos que constituem um incidente de segurança em que um invasor ou um código malicioso obtém acesso a um sistema, ou a recursos de um sistema, de forma não autorizada.
Invasor	Indivíduo responsável pela realização de uma invasão.
IPS	*Intrusion Prevention System,* sistema de prevenção de intrusão. Consiste no monitoramento e análise de eventos em sistemas computacionais, com o propósito de prevenir e detectar tentativas de acesso não autorizado a recursos destes sistemas.
Logon	Nome de usuário, nome no qual você será identificado pelo computador, junto com uma senha. É o processo seguro de entrada num sistema de informação.
Malware	Do inglês "*malicious software*" (software malicioso). Veja *software* malicioso.

Mecanismo de Controle de Acesso	São mecanismos de hardware ou software, procedimentos operacionais ou gerenciais usados para detectar e prevenir os sistemas computacionais contra acessos não autorizados.
Política de Segurança	Atribui direitos e responsabilidades aos indivíduos que lidam com os recursos computacionais de uma instituição e com as informações neles armazenadas. Define as atribuições de cada indivíduo em relação à segurança dos recursos com os quais trabalha. Qualquer evento que resulte no descumprimento da política de segurança é considerado um incidente de segurança.
Proxy	Um servidor proxy é usado como um funil, para as conexões de uma rede. Um servidor proxy para a internet, por exemplo, somente ele precisa ter um acesso para se conectar com a internet, todos os outros computadores aparecerão como se fossem o proxy (com o mesmo IP). Por isso também pode ser utilizado para acesso anônimo.
Risco	Pode ser entendido como tudo aquilo que pode afetar os negócios e impedir que se alcance os objetivos.
Servidor *Web*	Computador encarregado de prover serviços web.
Sistema de Informação	30Sistema de Informação é o conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens; que possibilitam a agregação dos recursos de informática e telecomunicações de maneira integrada.
Software	Em uma forma bastante resumida, é qualquer programa que você tenha em seu computador.
Software Malicioso	Programa, ou parte de um programa de computador, projetado especificamente para atentar contra a segurança de um sistema computacional, normalmente através de exploração de alguma vulnerabilidade desse sistema.
Spam	Toda a mensagem comercial/propaganda não solicitada, tanto para listas como para o seu e-mail pessoal. O principal contra argumento deles é que as propagandas também são recebidos pelo correio normal. O que eles esquecem é que nos correios, eles pagam para nós recebermos. Nos e-mails nós pagamos para receber.
Spyware	Termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

Trojan	Também conhecido como “cavalo de tróia” ou “*trojan horse*”, é um programa de computador com função aparentemente ou realmente útil, que contém as funções (escondidas) adicionais e que explora secretamente as autorizações legítimas do processo, provocando perda da segurança.
Vírus	Um programa de computador com capacidade de se multiplicar em outros programas, exatamente como um "vírus biológico". Os vírus de computador quase sempre tem capacidade destrutiva. Pode ser desde uma brincadeirinha como adicionar um pequeno texto em todos os arquivos “.txt”, até apagar a flash bios do computador. A melhor forma de se proteger dos vírus é manter o seu antivírus sempre atualizado, embora isso, não seja garantia total de proteção.
Wireless	Conexão sem fio.
Worm	Espécie de vírus eletrônico que se instala em micros ocupando espaço e causando lentidão no sistema.

ANEXOS

ANEXO A - Carta de Apresentação

Ministério da Educação e do Desporto
Universidade Federal Fluminense
Centro Tecnológico

Niterói, 20 de dezembro de 2005.

Prezados Senhores,

A UFF – Universidade Federal Fluminense, sob a coordenação do Prof. Heitor Luiz Murat de Meirelles Quintella D.Sc., está realizando um Projeto de Pesquisa sobre a Competitividade das Empresas Brasileira, sob o título ‘‘Fatores Humanos e Tecnológicos da Competitividade’’.

Este Projeto está sendo conduzido por um grupo de pesquisadores – mestrandos, mestres e doutores – que vem realizando há cinco anos várias pesquisas em empresas e instituições brasileiras, como é o caso do Inmetro.

A metodologia utilizada neste Projeto já foi testada em diversas empresas de grande expressão na indústria brasileira através da Fundação Getúlio Vargas e, em 250 empresas de diversos segmentos da indústria nos Estados Unidos, através de pesquisa conduzida por Joseph Pine da Harvard University.

É nossa intenção analisar em 2005 a competitividade nas instituições no Brasil, focando seu relacionamento com as ferramentas de gestão estratégica associada à Segurança da Informação, Percepção de Qualidade, Percepção de Liderança e Percepção dos Seguidores, através de um trabalho de dissertação de mestrado que está sendo desenvolvido por Luiz Fernando F. de M. Lima, um dos pesquisadores deste Projeto.

Acreditamos que além de trazer uma contribuição significativa para o Projeto, a pesquisa da gestão estratégica associada à Segurança da Informação, Percepção de Qualidade, Percepção de Liderança e Percepção dos Seguidores, resultará em trabalho de grande utilidade para as instituições que estão focando seu futuro em estratégia.

Para tal, estamos encaminhando questionários sobre **‘‘Percepção de Segurança da Informação, Percepção de Qualidade, Percepção de Liderança e Percepção dos Seguidores’’**, que acreditamos não exigir mais do que 15 minutos para ser respondido.

Contamos com a sua colaboração em nos devolver o questionário com a máxima brevidade possível, desejavelmente até 10 de janeiro de 2006, porque existe um prazo determinado para a conclusão da dissertação e sua defesa até 08 de março de 2006, e diversas etapas deverão ser cumpridas, após o recebimento dos questionários até a finalização do trabalho.

O endereço para resposta é:

INMETRO

Rua Santa Alexandrina, 416 – 4º andar

Rio Comprido – Rio de Janeiro - RJ – CEP: 20261-232

A/C: Luiz Fernando F. de M. Lima

Telefones: +55 21 2563-2932

Para responder por e-mail, encaminhar para: <lflima@inmetro.gov.br>

Todos os dados informados serão tratados com total confidencialidade pelo pesquisador e pela Universidade, devendo-se destacar que os resultados serão apresentados de forma global para o Inmetro, sem qualquer possibilidade de identificação de informações especificas de cada respondente participante da pesquisa.

Após a conclusão da pesquisa e sua homologação pela UFF, caso seja do interesse da empresa participante na pesquisa, teremos o maior prazer em enviar cópia do trabalho.

A participação de cada pessoa entrevistada é vital para o sucesso do trabalho e para que cheguemos a um cenário fidedigno sobre a gestão estratégica no Brasil, portanto, contamos com a sua adesão ao nosso trabalho e com o máximo de subsídios que possam nos fornecer.

Qualquer dúvida quanto aos questionários ou outras informações sobre o trabalho, não hesitem em contactar o Luiz Fernando F. de M. Lima no endereço acima mencionado.

Desde já, agradecemos a sua participação.

Atenciosamente,

Prof. Heitor Luiz Murat de Meirelles Quintella D.Sc.
Certified Management Consultant – Líder de Pesquisa

Departamento de Engenharia de Produção - UFF

ANEXO B - Questionário de Percepção de Segurança da Informação

Prezado(a) usuário(a).

Este questionário tem por finalidade avaliar o grau de conformidade da sua diretoria em relação à segurança da informação e os índices de incidentes de segurança ocorridos no ano de 2005.

Estes dados são de grande importância para a nossa instituição, pois visa à melhoria contínua da qualidade de nossos serviços.

Todos os dados serão mantidos em sigilo, pois são informações confidenciais, e somente serão tratados estatisticamente, sendo descartados ao final, os nomes e suas respectivas lotações nas diretorias.

Nome: _____

Diretoria: _____

Cargo: _____

a) Perguntas quanto ao conhecimento da Norma NBR ISO/IEC 17799:

	SIM	NÃO
1. Você muda sua senha periodicamente?		
2. Você utiliza senha forte (caracteres alfanuméricos, especiais e mínimo de 8 ‘oito’ dígitos)?		
3. Você anota sua senha em papel?		
4. Você bloqueia sua estação de trabalho (computador) ao se afastar dela?		
5. Você permite que alguém utilize sua senha para acesso a rede?		
6. Você utiliza a opção de "scan" completo do antivírus, todos os dias?		
7. Você monitora regularmente seu computador para reportar algo “suspeito”?		
8. Você tem conhecimento sobre Segurança da Informação?		
9. Você tem treinamento sobre Segurança da Informação?		
10. Sua diretoria já teve algum incidente de segurança?		
11. Sua diretoria tem algum plano de Segurança da Informação?		

b) Perguntas relativas a incidentes de Segurança da Informação:

12. Quais os tipos de incidentes de segurança que ocorreram em sua diretoria, no ano de 2005?

( ) acesso interno indevido (utilização da sua senha por terceiros)
( ) roubo de dados
( ) ataque de vírus, worms e trojans
( ) ataque de hacker externo
( ) perda dos dados
( ) fraude bancária

( ) modificação nos sistemas corporativos
( ) uso abusivo da rede (envio de spam, tentativas de ataque a outros computadores)
( ) instalação de programas maliciosos (spywares, malwares)
( ) não sei dizer

13. Qual é a quantidade total (estimada) ocorrida de incidentes de segurança neste período? Marque apenas uma resposta:

( ) nenhum
( ) de 1 a 5
( ) de 6 a 10
( ) de 11 a 15
( ) de 16 a 20
( ) de 21 a 25
( ) de 26 a 30
( ) de 31 a 35
( ) de 36 a 40
( ) de 41 a 45
( ) de 46 a 50
( ) de 51 a 60
( ) de 61 a 70
( ) de 71 a 80
( ) de 81 a 90
( ) de 91 a 100
( ) de 101 a 150
( ) de 151 a 200
( ) de 200 a 300

Obrigado pela sua colaboração.

ANEXO C - Questionários de Qualidade Percebida de Serviços – *Servqual*

Prezado(a) usuário(a).

Estes questionários têm por finalidade avaliar a qualidade dos serviços prestados pelo Setor de Informática e seus Sistemas de Informação.

Estes dados são de grande importância para a nossa instituição, pois visa à melhoria contínua da qualidade de nossos serviços.

Todos os dados serão mantidos em sigilo, pois são informações confidenciais, e somente serão tratados estatisticamente, sendo descartados ao final, os nomes e suas respectivas lotações nas diretorias.

Nome: _____

Diretoria: _____

Cargo: _____

Questionário 1:

AVALIAÇÃO DA EXPECTATIVA EM RELAÇÃO A UM SERVIÇO DE INFORMÁTICA IDEAL

INSTRUÇÕES: Baseado em sua experiência como usuário, responda este questionário pensando em um **Serviço de Informática ideal**, capaz de prestar serviços de excelente qualidade. Mostre o quanto você concorda (ou discorda) com cada uma das afirmações abaixo. Se você concorda fortemente com a afirmação, marque o "7". Caso discorde fortemente, marque o "1". Para opiniões menos extremas, marque qualquer uma das pontuações da escala.

	Características de um Serviço de Informática Ideal	**Discordo Concordo**						
E01	O setor de informática deve ter equipamentos e sistemas de última geração.	1	2	3	4	5	6	7

E02	Suas instalações físicas devem ser visualmente atraentes.	1	2	3	4	5	6	7
E03	Seus funcionários têm boa aparência - bem vestidos, limpos e organizados.	1	2	3	4	5	6	7
E04	Tem elementos materiais relacionados com o serviço (folhetos, manuais, etc.) que são visualmente atraentes.	1	2	3	4	5	6	7
E05	Quando promete fazer algo para uma certa data, ele faz.	1	2	3	4	5	6	7
E06	Quando os usuários têm um problema, o setor de informática mostra um sincero interesse em resolvê-lo.	1	2	3	4	5	6	7
E07	Este serviço é confiável - ajudando quando precisamos dele.	1	2	3	4	5	6	7
E08	Ele entrega seus serviços nas datas em que promete fazer.	1	2	3	4	5	6	7
E09	Ele se esforça para ter um histórico de trabalho sem erros.	1	2	3	4	5	6	7
E10	Ele diz aos usuários exatamente quando os serviços serão executados.	1	2	3	4	5	6	7
E11	Seus funcionários dão pronto atendimento aos usuários.	1	2	3	4	5	6	7
E12	Seus funcionários estão sempre dispostos a ajudar os usuários.	1	2	3	4	5	6	7
E13	Seus funcionários nunca estão muito ocupados para atender às solicitações dos usuários.	1	2	3	4	5	6	7

E14	O comportamento dos funcionários inspira confiança aos usuários.	1	2	3	4	5	6	7
E15	Os usuários se sentem seguros em suas transações com os funcionários deste setor.	1	2	3	4	5	6	7
E16	Seus funcionários são sempre educados com os usuários.	1	2	3	4	5	6	7
E17	Seus funcionários têm formação e conhecimento para realizar seu trabalho bem feito.	1	2	3	4	5	6	7
E18	Este setor dá aos seus usuários atendimento individual.	1	2	3	4	5	6	7
E19	Este setor trabalha nos horários mais convenientes para seus usuários.	1	2	3	4	5	6	7
E20	Este setor tem funcionários que dão atendimento personalizado aos seus usuários.	1	2	3	4	5	6	7
E21	Este setor tem sempre em mente o interesse de seus usuários.	1	2	3	4	5	6	7
E22	Os funcionários deste setor entendem as necessidades específicas de seus usuários.	1	2	3	4	5	6	7

Questionário 2:

AVALIAÇÃO DA QUALIDADE DOS SERVIÇOS DE INFORMÁTICA DO INMETRO

INSTRUÇÕES: O conjunto de questões abaixo se relaciona com seus sentimentos em relação à **área de Informática do Inmetro**. Para cada questão, mostre o quanto você acredita que o seu departamento de Informática atende a característica descrita. Novamente aqui, marque "7" quando concordar fortemente que sua Informática tem aquela característica, e marque "1" quando achar que ela não tem. Você pode marcar os outros valores para mostrar valores intermediários.

	CARACTERÍSTICAS DO SERVIÇO DE INFORMÁTICA - INMETRO	**Discordo**						**Concordo**
P01	O setor tem equipamentos e sistemas de última geração.	1	2	3	4	5	6	7
P02	Suas instalações físicas são visualmente atraentes.	1	2	3	4	5	6	7
P03	Os funcionários da Informática têm boa aparência - bem vestidos, limpos e organizados.	1	2	3	4	5	6	7
P04	Tem elementos materiais relacionados com o serviço (folhetos, manuais, etc.) que são visualmente atraentes.	1	2	3	4	5	6	7
P05	Quando a Informática promete fazer alguma coisa para uma determinada data, ela faz.	1	2	3	4	5	6	7
P06	Quando os usuários têm um problema, a Informática mostra sincero interesse em resolvê-lo.	1	2	3	4	5	6	7
P07	A Informática é confiável - ajuda quando precisamos dela.	1	2	3	4	5	6	7

P08	A Informática entrega seus serviços nas datas que prometeu.	1	2	3	4	5	6	7
P09	A Informática se esforça para manter um histórico de trabalho sem erros.	1	2	3	4	5	6	7
P10	A Informática diz aos usuários exatamente quando seus serviços serão executados.	1	2	3	4	5	6	7
P11	Os funcionários da Informática dão pronto atendimento aos usuários.	1	2	3	4	5	6	7
P12	Os funcionários da Informática estão sempre dispostos a ajudar os usuários.	1	2	3	4	5	6	7
P13	Os funcionários da Informática nunca estão ocupados para atender às solicitações dos usuários.	1	2	3	4	5	6	7
P14	O comportamento dos funcionários inspira confiança aos usuários.	1	2	3	4	5	6	7
P15	Os usuários se sentem seguros em suas transações com os funcionários da Informática.	1	2	3	4	5	6	7
P16	Os funcionários da Informática são sempre educados com os usuários.	1	2	3	4	5	6	7
P17	Os funcionários da Informática têm formação e conhecimento para realizar seu trabalho bem feito.	1	2	3	4	5	6	7
P18	A Informática dá atenção individualizada aos usuários.	1	2	3	4	5	6	7

P19	A Informática trabalha nos horários mais convenientes para seus usuários.	1	2	3	4	5	6	7
P20	A Informática tem funcionários que dão atenção personalizada aos usuários.	1	2	3	4	5	6	7
P21	A Informática tem sempre em mente os interesses dos seus usuários.	1	2	3	4	5	6	7
P22	Os funcionários da Informática entendem as necessidades específicas dos usuários.	1	2	3	4	5	6	7

Questionário 3:

A lista a seguir inclui cinco características que correspondem ao setor de informática e seus serviços prestados. Gostaríamos de conhecer quanta importância tem para você, cada uma dessas características quando avalia a qualidade do serviço de informática.

Por favor, distribua um total de 100 pontos entre as cinco características de acordo com a importância que têm para você de cada uma dessas características: quanto mais importante considere que são essas características, mais pontos deverá assinalar-lhe. Por favor, assegure-se de que os pontos assinalados às cinco características somem 100.

1. Aparência das instalações físicas, equipamentos, pessoal e material de comunicação que utiliza um setor de informática.		pontos
2. Habilidade de um setor de informática para realizar o serviço prometido de forma confiável, precisa e consistente.		pontos
3. Disposição de um setor de informática para proporcionar o serviço prontamente e auxiliar os clientes.		pontos
4. Conhecimentos e trato amável dos empregados de um setor de informática e habilidade para transmitir confiança, segurança e credibilidade.		pontos
5. Atenção individualizada, facilidade de contato (acesso) e comunicação que um setor de informática dá a seus clientes.		pontos
Total de pontos assinalados	100	pontos

ANEXO D - Questionários de Percepção de Liderança

QUESTIONÁRIOS SOBRE PERCEPÇÃO DE LIDERANÇA

Prezado(a) usuário(a).

Estes questionários têm por finalidade avaliar a práticas de liderança em cada diretoria do Inmetro.

Estes dados são de grande importância para a nossa instituição, pois visa à melhoria contínua da qualidade de nossos serviços.

Todos os dados serão mantidos em sigilo, pois são informações confidenciais, e somente serão tratados estatisticamente, sendo descartados ao final, os nomes e suas respectivas lotações nas diretorias.

Nome: _____

Diretoria: _____

Cargo: _____

Questionário de auto-avaliação do líder:

Baseado na sua experiência como líder dentro da sua diretoria, por favor, indique-nos até que ponto você considera que realiza estas práticas de liderança descritas em cada declaração.

A escala traz a seguinte variação:

1. Muito raramente ou nunca...
2. ...
3. ...
4. ...
5. Às vezes...
6. ...
7. ...

8. ...

9. ...

10. Muito freqüentemente ou sempre...

Também neste caso marque a opção que você considere que melhor represente suas convicções a respeito.

Não há respostas certas ou erradas. Nós só estamos interessados no número que reflete com precisão sua prática de liderança dentro da sua organização.

	Você:	1	2	3	4	5	6	7	8	9	10
L01	Procura desafios e oportunidades que testem as habilidades e o talento de cada um.										
L02	Descreve um futuro que é desejado de ser criado por todos.										
L03	Envolve a todos no planejamento, decisões e ações que estão ocorrendo ou são necessárias.										
L04	É claro quanto à forma de pensar sobre liderança.										
L05	Dedica um tempo para comemorar e recompensar as vitórias (objetivos atingidos) com toda a equipe envolvida.										
L06	Mantém a equipe atualizada com as principais e mais recentes mudanças da organização.										
L07	Envolve a equipe, tornando os sonhos de futuro único entre líder e os liderados.										
L08	Trata a todos com dignidade e respeito.										
L09	Mantém os projetos orientados dentro dos prazos previstos e as metas planejadas.										
L10	Assegura que a equipe é reconhecida por suas contribuições para o sucesso dos projetos.										
L11	Desafia (questiona) os caminhos existentes para a realização do										

	trabalho.										
L12	Possui uma comunicação clara, positiva e promissora sobre o futuro da organização.										
L13	Fornece à equipe autoridade para tomar suas próprias decisões.										
L14	Dedica tempo e energia para disseminar valores e crenças referentes à organização.										
L15	Elogia a equipe quando um trabalho é bem feito.										
L16	Está atento para inovações que podem melhorar a organização e o projeto.										
L17	Mostra à equipe como futuro de longo prazo, os objetivos que podem ser alcançados através de uma visão de futuro comum.										
L18	Desenvolve um ambiente de equipe com relações de cooperação entre os participantes.										
L19	Permite que a equipe conheça seus valores e suas crenças para a qual a melhor forma de conduzir os projetos e a organização.										
L20	Valoriza os esforços e as contribuições da equipe, dando suporte às atividades.										
L21	Pergunta "o que nós podemos aprender?" Quando as coisas não saem conforme o planejado.										
L22	Olha à frente e para as previsões quanto ao futuro da organização e dos acontecimentos do projeto.										
L23	Cria uma atmosfera de confiança mútua entre os participantes da equipe.										
L24	Apresenta coerência entre a prática e o discurso.										
L25	Procura formas de celebrar o sucesso dos projetos.										
L26	Avalia os riscos de novos procedimentos e abordagens quando existe chance de falha.										
L27	É motivador e entusiasta sobre as possibilidades futuras.										
L28	Possibilita à equipe uma sensação de donos do projeto em que estão trabalhando.										

L29	Assegura que o trabalho de equipe tem objetivos claros, com etapas e metas bem definidas que sejam de conhecimento de todos.										
L30	Divulga para o resto da organização os resultados obtidos e a importância da participação de cada membro da equipe.										

Questionário de alter avaliação do líder:

Baseado na sua vivência com o líder de sua diretoria, por favor, indique-nos até que ponto você considera que ele realiza estas práticas de liderança descritas em cada declaração.

A escala traz a seguinte variação:

1 Muito raramente ou nunca...

2 ...

3 ...

4 ...

5 Às vezes...

6 ...

7 ...

8 ...

9 ...

10 Muito freqüentemente ou sempre...

Também neste caso marque a opção que você considere que melhor represente suas convicções a respeito.

Não há respostas certas ou erradas. Nós só estamos interessados no número que reflete com precisão sua prática de liderança dentro da sua organização.

	Seu líder:	1	2	3	4	5	6	7	8	9	10
L01	Procura desafios e oportunidades que testem as habilidades e o talento de cada um.										
L02	Descreve um futuro que é desejado de ser criado por todos.										
L03	Envolve a todos no planejamento, decisões e ações que estão ocorrendo ou são necessárias.										
L04	É claro quanto à forma de pensar										

	sobre liderança.										
L05	Dedica um tempo para comemorar e recompensar as vitórias (objetivos atingidos) com toda a equipe envolvida.										
L06	Mantém a equipe atualizada com as principais e mais recentes mudanças da organização.										
L07	Envolve a equipe, tornando os sonhos de futuro único entre líder e os liderados.										
L08	Trata a todos com dignidade e respeito.										
L09	Mantém os projetos orientados dentro dos prazos previstos e as metas planejadas.										
L10	Assegura que a equipe é reconhecida por suas contribuições para o sucesso dos projetos.										
L11	Desafia (questiona) os caminhos existentes para a realização do trabalho.										
L12	Possui uma comunicação clara, positiva e promissora sobre o futuro da organização.										
L13	Fornece à equipe autoridade para tomar suas próprias decisões.										
L14	Dedica tempo e energia para disseminar valores e crenças referentes à organização.										
L15	Elogia a equipe quando um trabalho é bem feito.										
L16	Está atento para inovações que podem melhorar a organização e o projeto.										
L17	Mostra à equipe como futuro de longo prazo, os objetivos que podem ser alcançados através de uma visão de futuro comum.										
L18	Desenvolve um ambiente de equipe com relações de cooperação entre os participantes.										
L19	Permite que a equipe conheça seus valores e suas crenças para a qual a melhor forma de conduzir os projetos e a organização.										
L20	Valoriza os esforços e as contribuições da equipe, dando suporte às atividades.										

L21	Pergunta "o que nós podemos aprender?" Quando as coisas não saem conforme o planejado.										
L22	Olha à frente e para as previsões quanto ao futuro da organização e dos acontecimentos do projeto.										
L23	Cria uma atmosfera de confiança mútua entre os participantes da equipe.										
L24	Apresenta coerência entre a prática e o discurso.										
L25	Procura formas de celebrar o sucesso dos projetos.										
L26	Avalia os riscos de novos procedimentos e abordagens quando existe chance de falha.										
L27	É motivador e entusiasta sobre as possibilidades futuras.										
L28	Possibilita à equipe uma sensação de donos do projeto em que estão trabalhando.										
L29	Assegura que o trabalho de equipe tem objetivos claros, com etapas e metas bem definidas que sejam de conhecimento de todos.										
L30	Divulga para o resto da organização os resultados obtidos e a importância da participação de cada membro da equipe.										

Obrigado.

ANEXO E - Questionários de Percepção de Seguidores

QUESTIONÁRIOS SOBRE PERCEPÇÃO DE SEGUIDORES

Prezado(a) usuário(a).

Estes questionários têm por finalidade avaliar as práticas dos seguidores em cada diretoria do Inmetro.

Estes dados são de grande importância para a nossa instituição, pois visa à melhoria contínua da qualidade de nossos serviços.

Todos os dados serão mantidos em sigilo, pois são informações confidenciais, e somente serão tratados estatisticamente, sendo descartados ao final, os nomes e suas respectivas lotações nas diretorias.

Nome: _____

Diretoria: _____

Cargo: _____

Para cada questão, use a escala abaixo para indicar até que ponto o item descreve você. Pense numa situação específica de um seguidor, mas típica, e em como você agiria.

0 Raramente...
1 ...
2 ...
3 Às vezes
4 ...
5 ...
6 Quase sempre...

Também neste caso marque a opção que você considere que melhor represente suas convicções a respeito.

Não há respostas certas ou erradas. Nós só estamos interessados no número que reflete com precisão sua prática de liderança dentro da sua organização.

		0	1	2	3	4	5	6
S01	Seu trabalho o ajuda a desempenhar algum objetivo social ou sonho pessoal que seja importante para você?							
S02	Seus objetivos de trabalho pessoais estão em harmonia com os objetivos prioritários da organização?							
S03	Você está altamente comprometido e motivado por seu trabalho e por sua organização, dando a eles suas melhores idéias e desempenho?							
S04	Seu entusiasmo atinge e motiva seus colegas de trabalho?							
S05	Em vez de esperar ou meramente aceitar o que o líder lhe diz, você identifica pessoalmente quais as atividades da organização que são as mais críticas para atingir os objetivos prioritários da mesma?							
S06	Você desenvolve ativamente sua competência nas atividades críticas de modo que você se torne mais valioso para o líder e para a organização?							
S07	Ao iniciar um novo serviço ou uma nova incumbência você rapidamente registra uma série de sucessos em tarefas que são importantes para o líder?							
S08	O líder pode lhe conferir uma tarefa difícil sem ter de lhe fornecer constante supervisão, pois sabe que você encontrará um meio de desempenhá-la bem, e que você 'preenche as expectativas' se for necessário?							
S09	Você toma a iniciativa de procurar pelas tarefas que estão além e acima de seu cargo e desempenhá-las bem?							
S10	Quando você não é o líder de um projeto grupal, ainda assim contribui em alta escala, freqüentemente fazendo mais do que lhe é incumbido?							
S11	Você cria e patrocina, independentemente, idéias novas que irão contribuir significativamente com os objetivos do líder ou da organização?							
S12	Você tenta resolver problemas difíceis (técnicos ou referentes à organização), em vez de recorrer ao líder para que o faça por você?							
S13	Você ajuda seus colegas de trabalho, fazendo-os parecer bons, mesmo quando não conseguem nenhum crédito?							

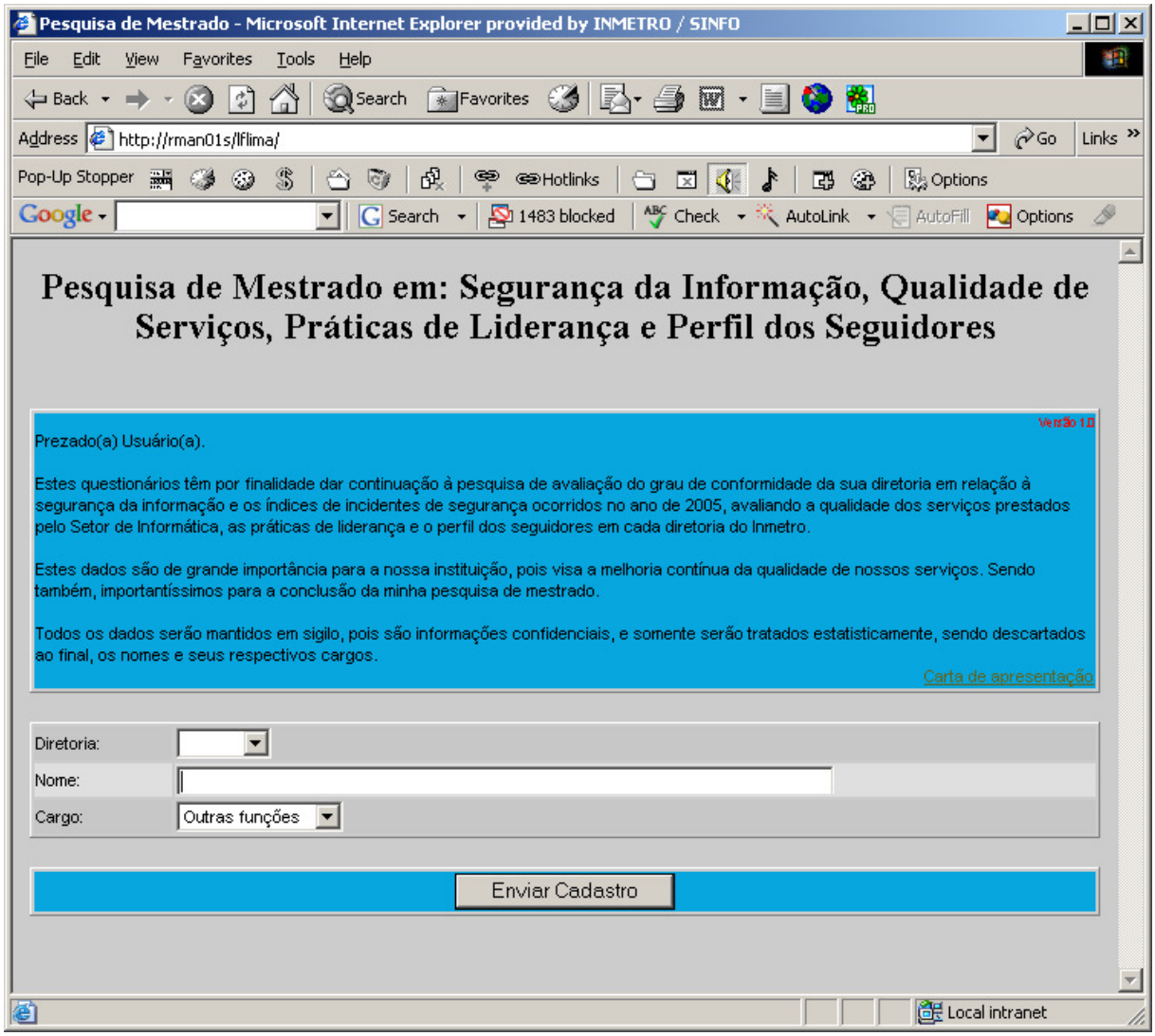
S14	Você ajuda o líder ou o grupo a ver tanto o potencial mais elevado quanto os piores riscos de idéias e planejamentos, passando por 'advogado do diabo' se necessário?							
S15	Você compreende as necessidades do líder, seus objetivos e constrangimentos, e trabalha duro para ajudar a atingí-los?							
S16	Você, enérgica e honestamente, reconhece suas forças e fraquezas, em vez de adiar essa avaliação?							
S17	Você habitualmente questiona a sabedoria existente nas decisões do líder, em vez de simplesmente fazer o que lhe é mandado?							
S18	Quando o líder lhe pede para que faça algo que seja contrário a suas preferências pessoais ou profissionais, você diz 'não' em vez de 'sim'?							
S19	Você age de acordo com seus próprios padrões éticos, em vez de fazê-lo de acordo com os padrões do líder ou do grupo?							
S20	Você focaliza seus objetivos em atividades importantes, mesmo que isso possa entrar em conflito com seu grupo e provocar represálias do líder?							

Obrigado.

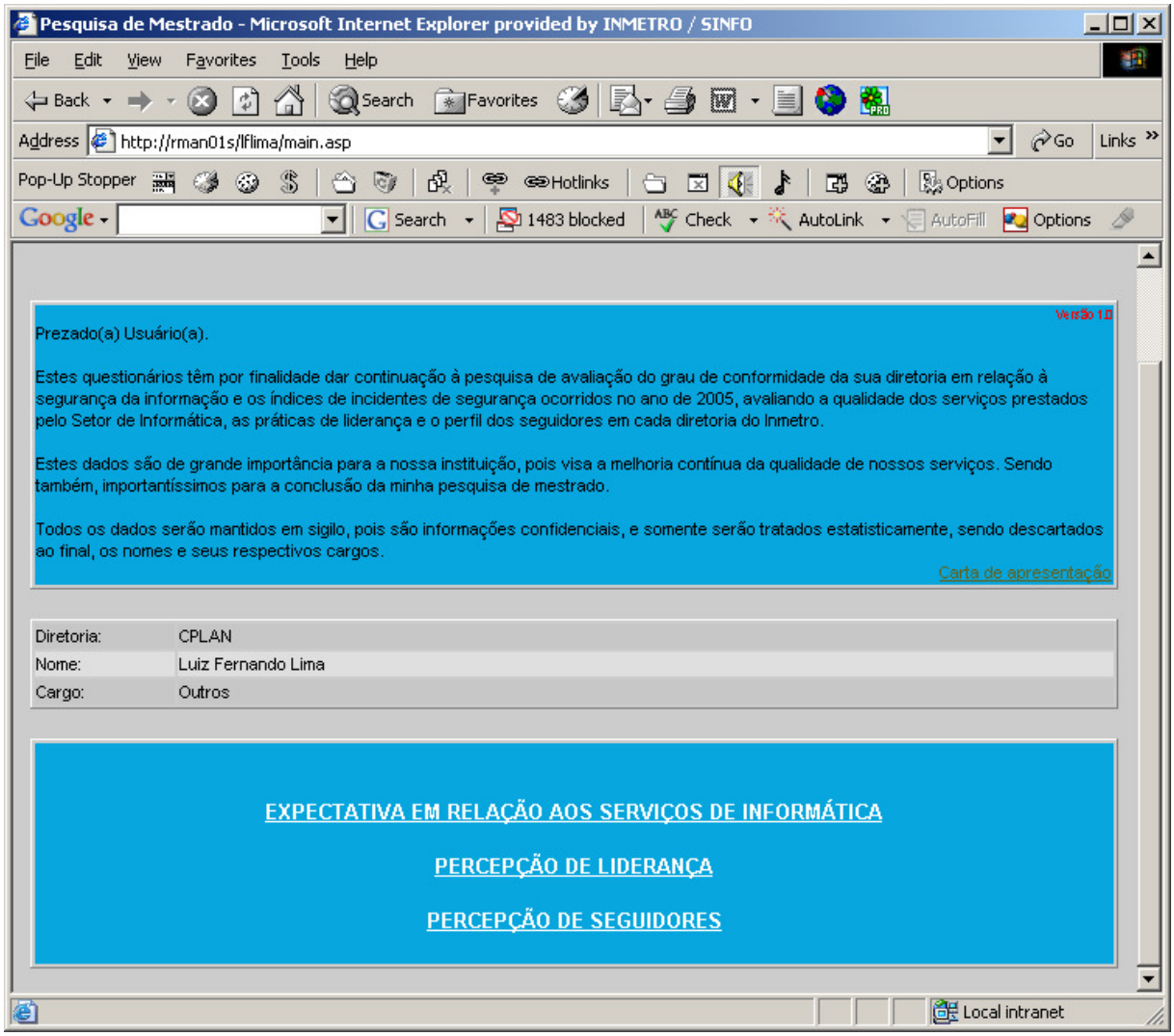
ANEXO F - Portal Web para Respostas aos Questionários

Para facilitar a pesquisa, foi utilizado um “portal web”, onde os usuários se conectavam para responder as perguntas dos questionários específicos de cada parte da pesquisa. O controle de acessos foi feito através do logon de cada usuário, impedindo assim, redundância de respostas por parte de um mesmo usuário. Os dados eram armazenados automaticamente no banco de dados criado para a pesquisa, e somente os questionários respondidos completamente eram levados em conta.

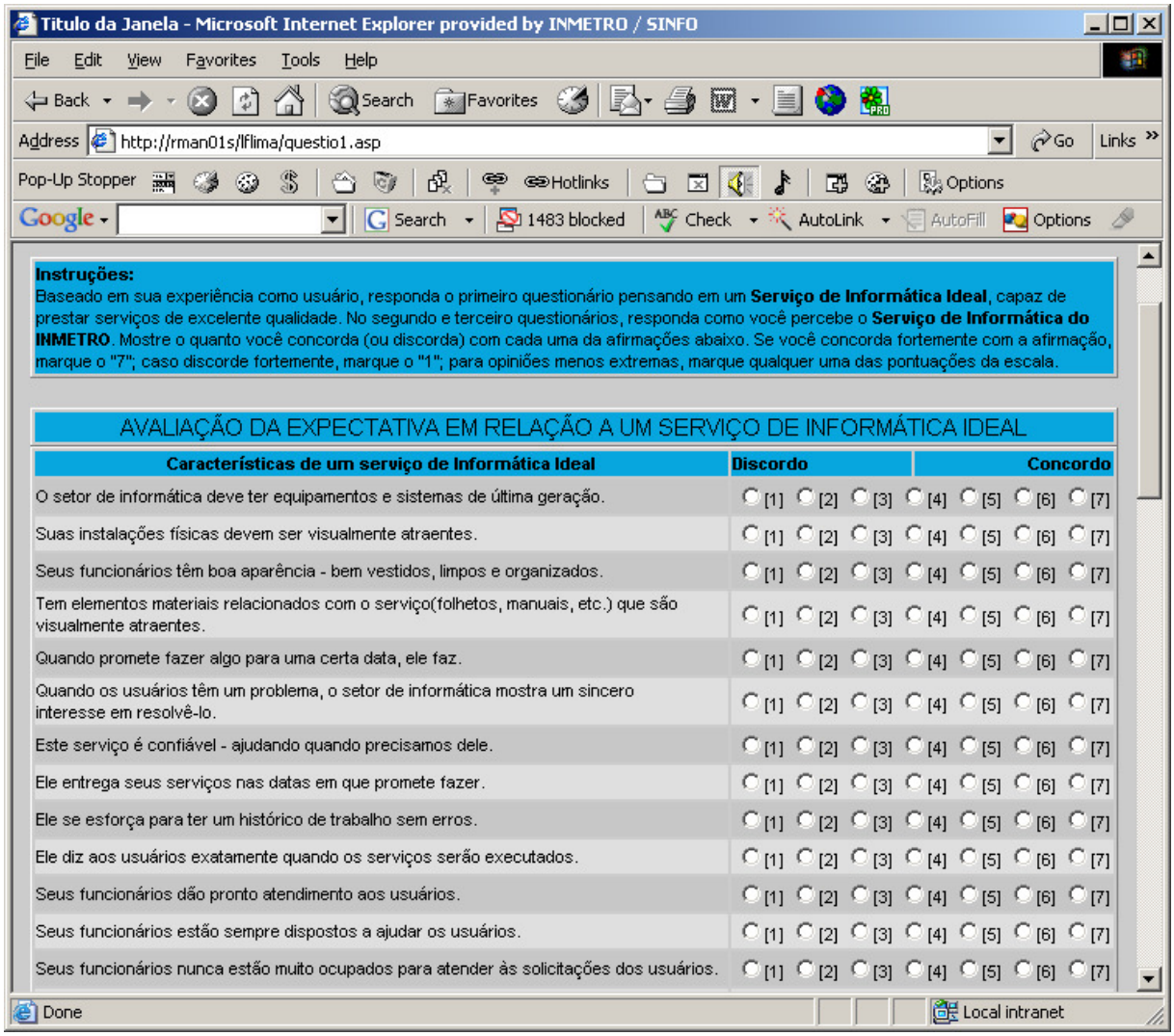
Página inicial do portal da pesquisa



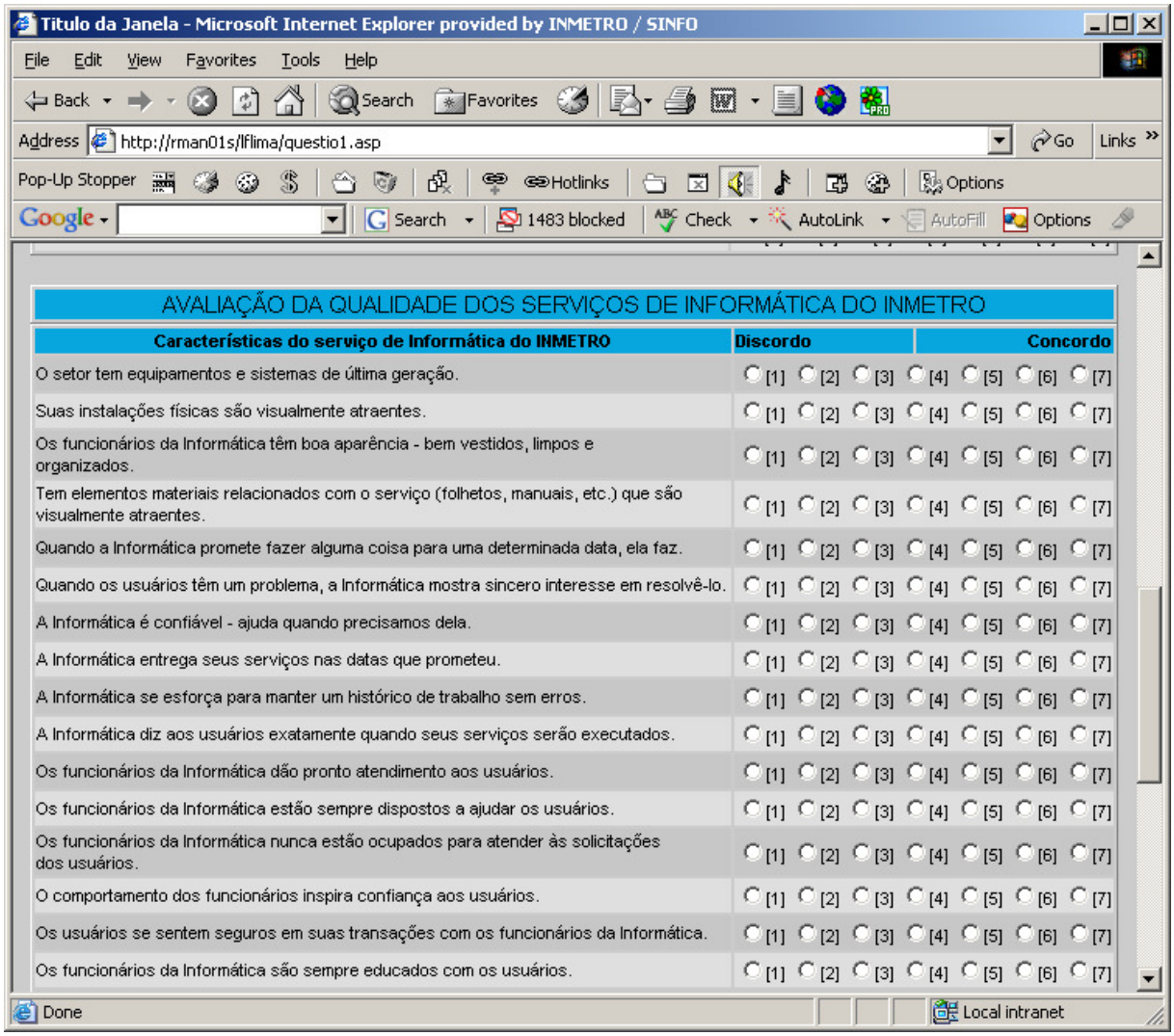
Segunda página do portal da pesquisa



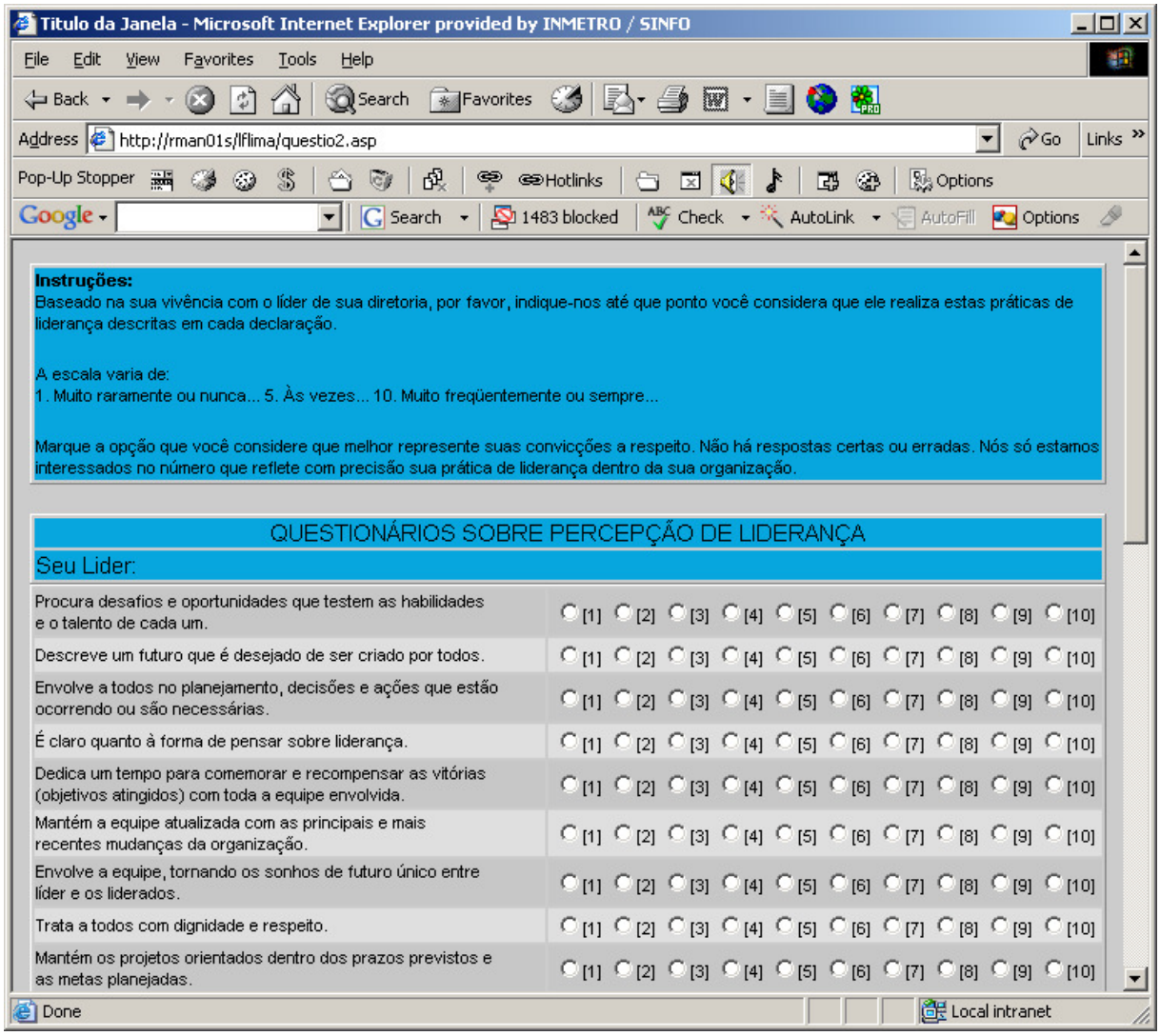
Terceira página do portal da pesquisa



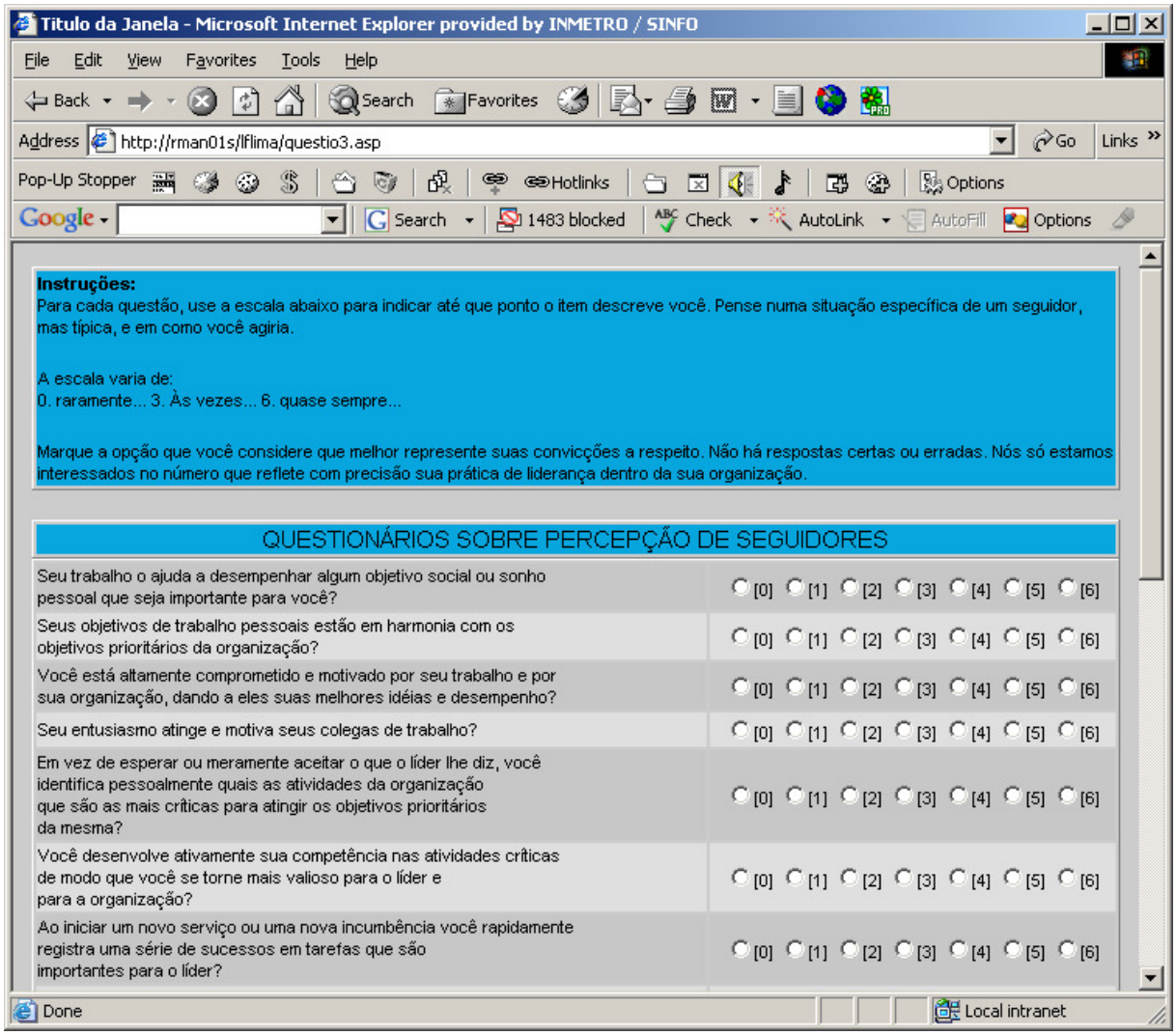
Quarta página do portal da pesquisa



Quinta página do portal da pesquisa



Sexta página do portal da pesquisa



ANEXO G - Tabela da Distribuição t – Distribuição de Student

Distribuição **t**

TABELA 8.3	TABELA DA DISTRIBUIÇÃO t PARA ÁREAS NA EXTREMIDADE SUPERIOR				
Graus de Liberdade	Área da Extremidade Superior Sombreada				
	0,1	0,05	0,025	0,01	0,005
1	3,078	6,314	12,706	31,821	63,657
2	1,886	2,920	4,303	6,965	9,925
3	1,638	2,353	3,182	4,541	5,841
4	1,533	2,132	2,776	3,747	4,604
5	1,476	2,015	2,571	3,365	4,032
6	1,440	1,943	2,447	3,143	3,707
7	1,415	1,895	2,365	2,998	3,499
8	1,397	1,860	2,306	2,896	3,355
9	1,383	1,833	2,262	2,821	3,250
10	1,372	1,812	2,228	2,764	3,169
11	1,363	1,796	2,201	2,718	3,106
12	1,356	1,782	2,179	2,681	3,055
13	1,350	1,771	2,160	2,650	3,012
14	1,345	1,761	2,145	2,624	2,977
15	1,341	1,753	2,131	2,602	2,947
16	1,337	1,746	2,120	2,583	2,921
17	1,333	1,740	2,110	2,567	2,898
18	1,330	1,734	2,101	2,552	2,878
19	1,328	1,729	2,093	2,539	2,861
20	1,325	1,725	2,086	2,528	2,845
21	1,323	1,721	2,080	2,518	2,831
22	1,321	1,717	2,074	2,508	2,819
23	1,319	1,714	2,069	2,500	2,807
24	1,318	1,711	2,064	2,492	2,797
25	1,316	1,708	2,060	2,485	2,787
26	1,315	1,706	2,056	2,479	2,779
27	1,314	1,703	2,052	2,473	2,771
28	1,313	1,701	2,048	2,467	2,763
29	1,311	1,699	2,045	2,462	2,756
30	1,310	1,697	2,042	2,457	2,750
40	1,303	1,684	2,021	2,423	2,704
60	1,296	1,671	2,000	2,390	2,660
120	1,289	1,658	1,980	2,358	2,617
∞	1,282	1,645	1,960	2,326	2,576

Fonte: Anderson et al. **Estatística Aplicada à Administração e Economia.** São Paulo: Pioneira Thomson Learning, 2003.