UNIVERSIDADE FEEVALE

DIEGO SAMUEL MARMITT

DESENVOLVIMENTO DE *CHECKLIST* PARA AVERIGUAÇÃO DE SEGURANÇA DA TI EM ÓRGÃOS PÚBLICOS: PREVENÇÃO E CONTORNO DE SINISTROS, E CONTROLE DE ACESSO

Novo Hamburgo

2013

DIEGO SAMUEL MARMITT

DESENVOLVIMENTO DE *CHECKLIST* PARA AVERIGUAÇÃO DE SEGURANÇA DA TI EM ÓRGÃOS PÚBLICOS: PREVENÇÃO E CONTORNO DE SINISTROS, E CONTROLE DE ACESSO

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do grau de Bacharel em Ciência da Computação pela Universidade Feevale

Orientador: Prof. Me. Roberto Scheid

Novo Hamburgo

2013

DIEGO SAMUEL MARMITT

Trabalho de conclusão do Curso de Ciência da Computação, com título **Desenvolvimento de *checklist* para averiguação de segurança da TI em órgãos públicos: prevenção e contorno de sinistros, e controle de acesso**, submetido ao corpo docente da Universidade Feevale, como requisito necessário para obtenção do Grau de Bacharel em Ciência da Computação.

Aprovado por:

_____

Roberto Scheid
Professor Orientador

_____

Ricardo Luis Lichtler
Professor Avaliador

_____

Sandra Teresinha Miorelli
Professora Avaliadora

Novo Hamburgo
Junho, 2013

AGRADECIMENTOS

Gostaria de agradecer, primeiramente, a Deus, pela oportunidade de estar concluindo minha graduação.

Agradeço também a minha família, em especial meus pais Mario e Angela. Exemplos supremos de simplicidade, força de vontade e carinho. Incentivadores dos meus estudos, sempre souberam o momento certo de oferecer palavras de apoio.

Aos meus avós, presentes ou em memória, pelos ensinamentos, apoio, carinho, orações e palavras.

Aos meus primos, sem exceção, pela parceria em todos os momentos.

Aos meus amigos, que sempre estiveram presentes, em especial aos que conquistei ao longo destes anos em que estive na Universidade.

Agradeço ainda, a todos os meus colegas de trabalho, que me auxiliaram no crescimento profissional, em especial a Rodrigo Fröhlich e ao amigo Odone Roger's Pfeiff.

Agradecimento com a mesma ênfase e importância ao meu orientador, Mestre Roberto Scheid, um dos melhores professores com quem tive a honra de estudar. Na pessoa dele, também agradeço aos demais Mestres que compartilharam seu conhecimento.

RESUMO

Cada vez mais as empresas estão dependentes das suas informações, bancos de dados e sistemas. Isso se evidencia pelo uso praticamente obrigatório da informática em todos os setores da sociedade. A informação já virou peça fundamental para os negócios, logrando inclusive vantagem competitiva às organizações. Todavia, como praticamente tudo está interconectado e compartilhado, a informação pode estar vulnerável. É prudente que se tomem medidas para garantir a segurança da informação, seja no acesso lógico aos sistemas, ou físico aos locais onde são armazenadas. Também é motivo de atenção o plano de continuidade e a preservação da informação contra sinistros e incidentes naturais. Há algum tempo essa disciplina está em evidência, colaborando para o avanço da proteção dos sistemas. Entretanto, essa não é uma preocupação generalizada entre as organizações. No setor privado, os departamentos de segurança e as políticas de segurança da informação se fazem mais presentes. Contudo, no ambiente público, prefeituras e demais órgãos não tem dado a devida importância à segurança da Tecnologia da Informação (TI), criando um abismo entre as recomendações e o que é de fato implementado para proteção desse que é um dos principais ativos em qualquer empresa, pública ou privada. A proposta deste trabalho é criar um *checklist* (sistema computacional para coleta, armazenamento e análise dos dados) baseado nas melhores práticas e recomendações de segurança da informação. O intuito é de que esse instrumento não exerça apenas um papel avaliativo, mas acima de tudo conscientizador, acerca da importância da segurança da informação. Também, será utilizado como um roteiro de pesquisa, a fim de averiguar a aderência momentânea de órgãos públicos da região do Vale do Rio dos Sinos quanto a alguns requisitos de segurança: prevenção e contorno de sinistros, além de controle físico e lógico a ambientes de armazenamento de dados e sistemas de gestão, respectivamente.

Palavras Chave: Segurança em TI. Avaliação de segurança. Órgão público. Gerenciamento de riscos. ABNT NBR ISO/IEC 27002.

ABSTRACT

Increasingly, companies are dependent on their information, databases and systems. This is evidenced by the almost mandatory use of informatics in all sectors of society. The information has already become fundamental piece for the business, including achieving competitive advantage for organizations. However, as almost everything is interconnected and shared, information may be vulnerable. It's prudent to take measures to ensure the security of information, whether in logical access to systems, or physical to places where they are stored. It's also cause of attention the plan of continuity and preservation of information against accidents and natural incidents. For quite some time this discipline is in evidence, contributing to the advancement of protection of the systems. Meanwhile, this is not a widespread concern among organizations. In the private sector, security departments and policies of information security are more present. However, in the public sphere, city halls and other agencies have not given the due importance to the security of Information Technology (IT), creating a gap between the recommendations and what is actually implemented to protect that which is a major asset for any company, public or private ones. The purpose of this work is to create a checklist (computer system for collection, storage and analysis of data) based on best practices and recommendations from information security. The intention is that this tool does not perform only an evaluation role, but specially arouse consciousness, about the importance of information security. Also, will be used as a roadmap for research, in order to ascertain momentary compliance by public agencies in the region of Vale do Rio dos Sinos about some security requirements: prevention and contour of accidents, besides physical and logical control to environment of data storage and management systems, respectively.

Keywords: IT Security. Security evaluation. Public agency. Risk management. ABNT NBR ISO/IEC 27002.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
CSS	*Cascading Style Sheet* (Folha de Estilo em Cascata)
ER	Entidade-relacionamento
HTML	*HyperText Markup Language* (Linguagem de Marcação de Hipertexto)
IBGE	Instituto Brasileiro de Geografia e Estatística
JS	*JavaScript*
LAN	*Local Area Network* (Rede de Área Local)
NBR	Norma Brasileira
PHP	*Hypertext Preprocessor*
PSI	Política de Segurança da Informação
TI	Tecnologia da Informação
UCP	Unidade Central de Processamento
UML	*Unified Modeling Language* (Linguagem Unificada de Modelagem)

SUMÁRIO

INTRODUÇÃO

Conforme Rehbein (2002, p. 14), ao longo do tempo a utilização de tecnologia e sistemas de informação, como ferramenta de suporte à execução dos trabalhos, deixou de figurar apenas nas grandes corporações. Empresas de menor porte, bem como o setor público, iniciaram o controle de suas atividades e informações com auxílio da Tecnologia da Informação (TI).

Atualmente, a informação constitui-se como um dos principais ativos nas organizações. Segundo a Associação Brasileira de Normas Técnicas (2005, p. x), a informação pode existir em várias formas: "ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos [...]". Outrossim, salienta-se que ela está cada vez mais acessível, seja por meio da Internet, das *Local Area Networks* (LAN's), ou mídias eletrônicas.

Sob a análise de Freitas (2009, p. 8), os inúmeros recursos e a flexibilidade que a tecnologia propicia são atrativos para as pessoas e as empresas. Ambos estão cada vez mais dependentes da própria tecnologia e da informação, pois se tornaram vitais. Tendo em vista esse cenário, é fácil perceber que um requisito importantíssimo é a proteção e segurança da informação. "A informação é um ativo não tangível da organização e assim como os ativos tangíveis e financeiros, a organização deve dedicar sua atenção à segurança deste ativo que [...] possuem" (FREITAS, 2009, p. 8).

De acordo com a Associação Brasileira de Normas Técnicas (2005, p. x), a "segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". Outra abordagem válida, de Sêmola (2003, p. 43 apud FREITAS, 2009, p. 10), é de que "podemos definir Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade".

Por volta de 2006, "o assunto Segurança da Informação tornou-se um dos temas mais importantes dentro das organizações, devido as ***fortes necessidades de proteção das informações e grande dependência de TI***" (FERREIRA; ARAÚJO, 2006, p. 17, grifo nosso). Entretanto, Beal (2008, p. 61 apud FREITAS, 2009, p. 17-18) afirma que a segurança da informação está seguidamente ligada a aspectos negativos, como aumento de custos e perda

de desempenho. Para inibir tais fatos, os gestores de TI devem conseguir mensurar e enfatizar o valor agregado da segurança em TI para a organização. Não é tarefa simples, "[...] mas através da análise da classificação da informação e da gestão de riscos será possível demonstrar o quanto se deixou de perder caso algum desastre ocorresse, ou alguma informação confidencial fosse revelada ou mesmo um sistema crítico ficasse fora do ar".

Sob a ótica do *Committee of Sponsoring Organizations of the Treadway Commission*[1] (2007, p. 3), as empresas existem para gerar valor e ao longo de sua vida enfrentam problemas e desafios. "Incertezas representam riscos e oportunidades, com potencial para destruir ou agregar valor". Ainda de acordo com essa instituição, são os processos de gerenciamento de riscos que auxiliam a gerenciar e tratar as incertezas e os riscos. Nota-se que uma estratégia que alinhe gerenciamento de riscos e vulnerabilidades, com a segurança da informação, pode ser o ponto de equilíbrio para a preservação do próprio negócio e sobrevivência da organização.

Tamanho deve ser o cuidado com a informação e os dados, que a responsabilidade por criar a cultura de preservação e segurança das informações geralmente atribui-se à direção suprema da organização. Para Ferreira e Araújo (2006, p. 23), "[...] é responsabilidade da Alta Administração assegurar que todos os usuários dos sistemas de informação saibam como proteger os ativos da organização (informações, hardware, software etc.) [...]". A gerência deve, portanto, incentivar e homologar a criação de uma política de segurança. Ainda segundo Ferreira e Araújo (2006, p. 11), a recomendação é de que um comitê seja criado para tratar desse assunto. Esse, por sua vez, deveria ser formado por profissionais de vários departamentos, incluindo informática, jurídico, engenharia, recursos humanos, dentre outros, reiterando que a responsabilidade é de toda a organização.

Percebe-se que a segurança da informação pode ser crucial para o adequado andamento dos negócios, seja na gestão pública ou privada. Módulo (2006, p. 8) salienta que a estruturação da área de segurança da informação está avançando nas empresas. Sobre a importância da informação no setor público, Rehbein (2002, p. 14) explica:

> O setor público, independentemente da esfera, sofre exigência da sociedade para melhorar sua produção de informações, sob argumento de ampliação da eficiência e transparência. Também conhecido por sua tradição burocrática e organizado segundo uma estrutura funcional estanque, o setor público encontra-se pressionado a

[1] O *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) é uma associação de cinco organizações do setor privado que busca fornecer auxílio à empresas quanto a estratégias de gestão de riscos, controle interno e prevenção de fraudes (COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, 2007).

> adotar modelos gerenciais de administração pautados pelo subsídio da informação para a eficácia da gestão. A informação é, portanto, pré-condição tanto para o funcionamento quanto para o atingimento dos objetivos de uma organização privada ou pública.

Módulo (2006, p. 9) apresenta resultados que mostram apenas 23% dos entrevistados do ramo Governo, com um departamento de segurança estruturado. Consoante com Diniz e Diniz (2009, p. 1), em 2008, a Secretaria de Fiscalização de Tecnologia da Informação do Tribunal de Contas da União realizou pesquisa que apontou dados preocupantes. "[...] constatou que 64% dos órgãos não possuíam uma Política de Segurança implantada, 80% não classifica suas informações e 75% não fazem análises de riscos". Verifica-se, com isso, que historicamente a preocupação não tem evoluído como deveria. De acordo com os mesmos autores, maior atenção deve ser desprendida por parte da Administração Pública, fundamentando sua afirmação ao dizer que a ausência de uma Política de Segurança da Informação delata a falta de cultura e conhecimento de segurança nos órgãos.

A transparência pública é um assunto em evidência. No entanto, há de se distinguir entre as diferenças do que deve ser realmente publicado, ao que é de caráter sigiloso e tem de ser protegido. A recente Lei da Transparência Pública (Lei Nº 12.527, de 18 de novembro de 2011), também conhecida como Lei de Acesso a Informação, pressupõe acesso à população referente aos investimentos e arrecadação dos entes públicos, por meio da Internet. Diniz e Diniz (2009, p. 21), comentam que, em geral, as informações armazenadas por órgãos públicos são relativas à sociedade. Seriam, portanto, públicas. Mas também "sensíveis". Interpretada pelos mesmos autores, "a CF 1988 em seu art. 5 considera o acesso à informação um direito fundamental, mas o limita perante o devido sigilo" (DINIZ; DINIZ, 2009, p. 21).

> Maior evidência se deu ao tratamento especial da informação nos órgãos públicos após os resultados de auditorias promovidas pelo Tribunal de Contas da União. O Acórdão 1063 (TCU, 2008) cita: A importância do correto tratamento para a confidencialidade, a integridade e a disponibilidade das informações de órgãos públicos é evidente, sem falar na autenticidade, na responsabilidade pelos dados e na garantia de não-repúdio. A própria prestação do serviço de uma instituição pública aos cidadãos depende da confiabilidade das informações por ela tratadas e ofertadas (DINIZ; DINIZ, 2009, p. 22-23).

Diante do que foi exposto acima, surge a questão problemática da presente pesquisa. Qual seja: a ***proposição de um instrumento para averiguar a segurança em órgãos públicos é viável?***

Propõe-se então, como objetivo geral para solucionar o questionamento hipotético levantado, o desenvolvimento de um *checklist* (sistema computacional para coleta, armazenamento e análise dos dados), baseado nas melhores práticas e recomendações de segurança da TI. Não obstante a função de conscientizar sobre a importância da segurança das

informações, este documento servirá como roteiro de pesquisa, averiguando a aderência de dois/três órgãos públicos da região do Vale do Rio dos Sinos, com relação a determinados requisitos de segurança. Sejam eles: prevenção e contorno de sinistros, controle de acesso lógico a sistemas de gestão e físico a ambientes de armazenamento de dados.

Como objetivos específicos, determinam-se os seguintes:

- Examinar e expor o embasamento teórico sobre a segurança de TI;
- Estabelecer parâmetros (métricas) para avaliar a condição de segurança, atrelados aos temas propostos;
- Estruturar o *checklist* para averiguar a segurança de TI em órgãos públicos;
- Analisar, através de *benchmarking*, a existência de alguma ferramenta que avalie a segurança de determinada empresa quanto aos processos de TI;
- Desenvolver uma ferramenta (sistema) para coleta e armazenamento das respostas do *checklist*;
- Verificar a viabilidade do *checklist* mediante levantamento e análise de informações em dois/três órgãos públicos da região do Vale do Rio dos Sinos.

1 FUNDAMENTAÇÃO TEÓRICA

O referencial teórico apresentado a seguir tem como objetivo principal embasar e justificar a importância da segurança da TI frente aos sistemas informatizados utilizados atualmente. Serão basilares para o entendimento desse tema, mas, sobretudo, servirão como ideais norteadores para a análise de segurança proposta por esta pesquisa.

Os conceitos apresentados serão, por vezes, direcionados a "organizações", "empresas" ou "companhias". Deve-se ter em mente que essa denominação também permite identificar órgãos públicos, foco desta pesquisa. "Embora seja um lugar-comum diferenciar-se as organizações governamentais das privadas e não-governamentais com base na aferição de lucros, deve-se salientar que a visão e o tratamento dos conceitos relacionados à informação não apresentam diferenças marcantes" (MARCIANO, 2006, p. 120).

1.1 A INFORMAÇÃO

"A informação é a fonte do conhecimento. O conhecimento não existirá se não houver uma origem de informação que possibilita a estruturação desse conhecimento" (SALES; ALMEIDA, 2007 apud FONTES, 2012, p. 3).

Marciano (2006, p. 44) prega que "anteriormente reconhecida por seu papel como redutora de incertezas, a informação é cada vez mais vista como um recurso transformador do indivíduo e da sociedade, cabendo-lhe papel essencial no contexto sócio-econômico vigente, não por acaso denominado de 'Era da Informação'".

1.1.1 Importância da informação para o negócio

A informação é um dos mais importantes, senão o principal bem de uma corporação. Fontes (2012, p. 1) caracteriza-a como "[...] um recurso essencial para toda a organização, independentemente do seu porte e do seu segmento de atuação no mercado". Destaca ainda que, além de ser fundamental para nossa sobrevivência enquanto seres humanos, ela é vital

para que os negócios aconteçam, as empresas produzam, e a renovação do conhecimento se perpetue.

Para Caruso e Steffen (1999, p. 22), todas as organizações humanas dependem fortemente da informação. E essa subordinação tem aumentado significativamente nas últimas décadas, principalmente com o advento da tecnologia e da informática.

> É inegável que todas as empresas, independentemente de seu segmento de mercado, de seu *core business*[1] e porte, em todas as fases de existência, sempre usufruíram da informação, objetivando melhor produtividade, redução de custos, ganho de *market share*[2], aumento de agilidade, competitividade e apoio à tomada de decisão (SÊMOLA, 2003 apud DINIZ; DINIZ, 2009, p. 6).

Silva e Tomaél (2007 apud FONTES, 2012, p. 1) elevam a análise ao afirmar que qualquer empresa, seja em qual esfera administrativa estiver, não consegue funcionar sem o elemento informação, pois sem ele o mercado competitivo acaba por reduzir suas chances perante a concorrência. Segundo os mesmos autores, "ter a informação correta e disponível no momento certo, se bem utilizada, pode ser uma vantagem competitiva da organização".

Sacilotti (2011, p. 21) fundamenta essas asserções colocando que uma TI eficiente pode propiciar grandes conquistas para a empresa. Sobretudo, na organização do trabalho e mais efetivamente sobre a gestão de produção. Diz ainda que a competição e a globalização fomentam avanços na área de TI, sendo "[...] indispensável que as pessoas que dirigem organizações tenham ferramentas que lhes permitam ter uma velocidade de resposta igual ou maior àquela que existe à sua volta" (MAÑAS, 2005 apud SACILOTTI, 2011, p. 21).

1.1.2 Importância da proteção das informações

Considerando o atual cenário de dependência completa frente à informação, a proteção desse ativo é crucial para os interesses das companhias. "Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado" (ABNT, 2005, p. x). Para mensurar essa afirmação, Brotby (2009 apud FONTES, 2012, p. 4) cita que "uma pesquisa realizada pela Universidade do Texas indicou que 93% das organizações que tiveram indisponibilidade de informação por mais de dez dias em função de desastre nos recursos de TI, chegaram à falência um ano depois".

---

[1] "[...] o ponto forte e estratégico da atuação de uma empresa" (MENDES, 2009 apud IMASTERS, 2009).
[2] "É a participação da empresa e dos concorrentes no mercado (fatia de mercado). Mostra o quanto cada empresa detém do mercado [...]" (KOTLER, 2007 apud BRUEL, 2009, p. 13).

Mas a fragilidade e violabilidade perante a informação também podem ser analisadas sob outra relevante perspectiva: a dos clientes. Brotby (2009 apud FONTES, 2012, p. 4) traz resultados de outra análise mercadológica efetuada junto a organizações que tiveram problemas com relação à segurança de suas informações. A presente pesquisa

> [...] identificou que 31 companhias que sofreram violações de informação em um período de doze meses tiveram uma perda média de US$ 4,8 milhões, além do que **19% dos clientes deixaram de se relacionar com a companhia e outros 40% dos clientes consideravam a possibilidade de deixar de serem clientes** (BROTBY, 2009 apud FONTES, 2012, p. 4, grifo nosso).

Com um valor tão expressivo para a empresa, "a segurança da informação deve, portanto, integrar a estratégia do negócio ou serviço, devendo se traduzir em lucro, ganho de competitividade ou confiabilidade no mercado" (FREITAS, 2009, p. 18). Fontes (2012, p. 4) segue a mesma linha de pensamento, colocando ainda que "as organizações precisam implantar um processo de segurança da informação, e este processo deve ser considerado um ativo da organização, como tantos outros". Ativo este, que Domeneghetti e Meir (2009 apud FONTES, 2012, p. 4-5) consideram como intangível de proteção de valor, assim como a Governança Corporativa e a Gestão de Riscos.

Apesar do que foi exposto, a realidade é paradoxal às recomendações. Módulo (2006, p. 6) apresenta resultados da sua 10ª, e mais recente, Pesquisa Nacional de Segurança da Informação, efetuada entre junho de 2005 e janeiro de 2006, junto a um universo de empresas brasileiras relacionadas entre as 1.000 (mil) maiores (59% delas com 500 ou mais funcionários). Aproximadamente 600 (seiscentos) profissionais de Segurança em TI responderam aos questionamentos. O maior percentual de entrevistados foi do ramo governo (21%), seguido por financeiro (15%), informática (14%), dentre outros. No contexto da segurança da informação, alguns resultados à época do estudo:

- 35% das empresas não possuem um planejamento formal de segurança. Somente no ramo comércio, 48% não possuem. Em empresas governamentais, 40% delas;
- 33% dos entrevistados dizem que sua empresa não sabe quantificar as perdas decorrentes dos incidentes. Atendo-se ao ramo governo, 56% disseram que não sabem em quanto ficou o prejuízo causado por ataques e invasões;
- 21% dos respondentes não podem nem mesmo identificar os responsáveis pelos eventos de segurança;
- 24% das organizações que conseguem descobrir as falhas, citam os funcionários como causadores;

- 55% apontam como principal obstáculo para implementação de segurança a falta de conscientização dos usuários e executivos, seguido pelo orçamento reduzido (28% dos casos);
- em contraponto, 31% afirmam que a consciência dos executivos e usuários é o principal motivador para a tomada de decisões que visem a segurança.

1.2 SEGURANÇA

Como demonstrado na seção anterior, a informação é substancial para o ser humano, sociedade e organizações. Sua proteção, assim sendo, torna-se imprescindível para a manutenção da vida particular e do negócio. "[...] segurança é uma questão de postura administrativa" (CARUSO; STEFFEN, 1999, p. 52).

1.2.1 Conceitos gerais

Para a ABNT (2005, p. x), as informações, as redes de computadores e os sistemas estão vulneráveis a diversos tipos de ameaças à segurança, cada vez mais incrementados e corriqueiros.

> A segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infra-estruturas críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como o governo eletrônico (*e-gov*) ou o comércio eletrônico (*e-business*), e evitar ou reduzir os riscos relevantes (ABNT, 2005, p. x).

Dias (2000, p. 41) explica que a segurança de TI não se atém apenas às informações, mas também a um conjunto de objetos tecnológicos que possibilitam à empresa exercer sua atividade. Segurança seria, em sua concepção, "[...] a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança". Porém, Fontes (2010 apud INFOSEC COUNCIL, 2010, p. 20) desperta para o fato de que a segurança não deve passar apenas pelos aspectos técnicos. Para ele, "as particularidades sociais referentes ao ambiente da organização e às pessoas também têm sua importância e devem ser consideradas". Ou seja, o foco da gerência de segurança não deve estar completamente dirigido aos quesitos tecnológicos, mas

também aos humanos, sendo que o cumprimento das regras de segurança só será efetivo com regras explícitas e rígidas.

Braga Filho (2004, p. 137) e Ferreira e Araújo (2006, p. 21) colocam que para uma política de segurança interna ser efetiva e, acima de tudo, positiva, o envolvimento e conscientização de todos os funcionários é primordial. "[...] a segurança frequentemente conflita com a facilidade de uso e, especialmente, de abuso" (BRAGA FILHO, 2004, p. 137). Marciano (2006, p. 114), em sua abordagem de enfoque social, amplia a própria definição da segurança da informação, integrando os recursos tecnológicos e os sujeitos que os utilizam, propondo que seja representada como

> [...] fenômeno social no qual os usuários (aí incluídos os gestores) dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio de regras, bem como sobre os papéis que devem desempenhar no exercício deste uso.

Com um olhar mais voltado ao negócio, Peltier (2004 apud FONTES, 2012, p. 8) enfatiza que

> [...] a Segurança da Informação direciona e suporta a organização para a proteção de seus recursos de informação contra divulgação indevida, seja ela intencional ou não intencional, modificação não autorizada, destruição não desejada, ou negação de serviço através da implantação de controles de segurança definidos em políticas e procedimentos.

Sêmola (2003 apud DINIZ; DINIZ, 2009, p. 8) apresenta a ideia de que "a segurança da informação tem como objetivo a preservação de três princípios básicos pelos quais se norteiam a implementação dessa prática". Todavia, esses princípios (ilustrados na Figura 1.1) devem ser vistos como os mais relevantes, mas não os únicos, uma vez que a ABNT (2005, p. 1) diz ainda que outros atributos podem ser envolvidos para conceituar a segurança da informação. Dentre eles, a autenticidade, a responsabilidade, o não repúdio e a confiabilidade.

Figura 1.1 – Princípios norteadores da segurança da informação
Fonte: Desenvolvida pelo autor, adaptada de Diniz e Diniz (2009, p. 9)

Estes preceitos podem ser mais claramente entendidos sob a análise de Dias (2000, p. 42-43):

- ***confidencialidade***: não disponibilização de informações às pessoas não autorizadas explicitamente pelo proprietário. “Esse objetivo envolve medidas tais como controle de acesso e criptografia”;
- ***integridade***: não permitir a deleção ou alteração de dados (no local ou durante sua transmissão) sem permissão do possuidor da informação. “O conceito de integridade está relacionado com o fato de assegurar que os dados não foram modificados por pessoas não autorizadas”;
- ***disponibilidade***: prevenção contra ataques ou panes que dificultem o acesso aos sistemas, ou seja, envolve a preservação dos serviços de informática como um todo, possibilitando acesso a quem autorizado, no momento em que for necessário. “[...] pode ser definida como a garantia de que os serviços prestados por um sistema são acessíveis [...]”.

A ABNT (2005, p. x-xii) preconiza que a segurança da informação é obtida através da implementação, monitoria e revisão de controles, que podem ser “[...] políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware”. Esses controles devem ser elaborados de acordo com a necessidade e realidade de cada organização em particular, passando por uma análise e avaliação sistemática de riscos aos quais a empresa pode estar submetida. Essa análise, por sua vez, pode ser promovida e facilitada com o auxílio de algumas indagações, apresentadas por Dias (2000, p. 44):

- O que se quer proteger?
- Contra que ou quem?
- Quais são as ameaças mais prováveis?
- Qual a importância de cada recurso?
- Qual o grau de proteção desejado?
- Quanto tempo, recursos financeiros e humanos se pretende gastar para atingir os objetivos de segurança desejados?
- Quais as expectativas dos usuários e clientes em relação à segurança de informações?
- Quais as consequências para a instituição se seus sistemas e informações forem corrompidos ou roubados?

1.2.2 Riscos

É inegável que com a popularização dos microcomputadores, as pessoas e companhias se tornaram dependentes da informática. Caruso e Steffen (1999, p. 35-36)

salientam que junto aos benefícios que a microcomputação traz consigo, vêm também os riscos. Pela facilidade de uso, baixo custo e características físicas, o tratamento frente à segurança deve ser diferenciado, se comparado a ambientes com servidores e alto poder de processamento.

Mas, apesar disso, "nem todos os riscos relacionados com o processamento de informações surgiram com o advento dos computadores; entretanto, estes contribuíram sobremaneira para o seu agravamento" (CARUSO; STEFFEN, 1999, p. 36). Isso se comprova pela vasta capacidade de armazenamento e processamento em uma caixa pouco maior que uma maleta (Unidade Central de Processamento - UCP), somadas ao advento da Internet que, segundo os autores, "[...] ampliou ainda mais os riscos decorrentes da concentração de informações ao interligar dezenas de milhares de *sites* ao redor do globo".

Para se ter um entendimento mínimo acerca do que representa um possível risco, Dias (2000, p. 54) coloca que não deve ser confundido com ameaça, ou a probabilidade de ela ocorrer, visto que essa confusão é seguidamente percebida. "Na verdade, risco é uma combinação de componentes, tais como ameaças, vulnerabilidades e impactos. A análise de riscos engloba tanto a análise de ameaças e vulnerabilidades quanto a análise de impactos [...]". COSO (2007, p. 16) complementa que "o risco é representado pela possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos" empresariais.

As definições conceituais de Dias (2000, p. 55) explicam de maneira mais concisa cada um dos termos:

- Recurso – componente de um sistema computacional, podendo ser recurso físico, software, hardware ou informação.
- Ameaça – evento ou atitude indesejável (roubo, incêndio, vírus, etc.) que potencialmente remove, desabilita, danifica ou destrói um recurso.
- Vulnerabilidade – fraqueza ou deficiência que pode ser explorada por uma ameaça. Pode ser associada à probabilidade da ameaça ocorrer.
- Ataque – ameaça concretizada.
- Impacto – consequência de uma vulnerabilidade do sistema ter sido explorada por uma ameaça. É o resultado da concretização de uma ameaça.
- Probabilidade – chance de uma ameaça atacar com sucesso o sistema computacional.
- Risco – medida da exposição a qual o sistema computacional está sujeito. Depende da probabilidade de uma ameaça atacar o sistema e do impacto resultante desse ataque. Nesse contexto, o risco envolve três componentes: ameaças, vulnerabilidades associadas e impactos.

A fim de proporcionar maior cautela perante os riscos e ameaças à segurança atualmente, há uma disciplina a ser adotada junto aos procedimentos de segurança em TI da organização: a gestão/gerenciamento de riscos. ABNT (2005, p. xi) explica que "os requisitos de segurança da informação são identificados por meio de uma análise/avaliação sistemática

dos riscos de segurança da informação". Quanto ao efetivo gerenciamento de riscos, ele "[...] ajuda a organização a concretizar seus objetivos e evitar armadilhas e acontecimentos indesejáveis ao longo do exercício de suas atividades" (COSO, 2007, p. 16).

Com uma avaliação dirigida à missão das empresas, que é a de gerar valor às partes interessadas, COSO (2007, p. 13) ainda narra que "o gerenciamento de riscos corporativos não apenas permite identificar, avaliar e administrar riscos diante de incertezas, como também integra o processo de criação e preservação de valor". Verifica-se então que é um processo contínuo, uma vez que riscos e ameaças podem surgir a qualquer momento.

Freitas (2009, p. 49) opina quanto ao êxito na gestão de riscos: "ter sucesso na Gestão de Riscos não significa necessariamente que não haverá riscos, mas que fomos capazes de quantificar o risco e decidir que riscos estamos dispostos a correr". Para chegar a um resultado satisfatório nesta equação, o autor sugere considerar o valor da informação perante os custos de manter a segurança da mesma. "[...] não existe como eliminar 100% dos riscos. Fazer gestão de riscos é descobrir qual nível de risco é aceitável para o seu negócio ou até mesmo para sua vida" (SALES, 2010 apud INFOSEC COUNCIL, 2010, p. 18).

Sales (2010 apud INFOSEC COUNCIL, 2010, p. 18) discorre sobre o Planejamento Estratégico de Segurança da Informação. Frisa que

> Mais do que arriscar para ter sucesso em um bom planejamento, é necessário ter apetite pelo risco, quantificar corretamente e escolher os tipos de riscos que uma organização está preparada para correr ou perseguir. É o risco aceitável que nos faz diferentes e competitivos na sociedade moderna. O risco deve ser retido de forma consciente e alinhado aos nossos objetivos. Devemos sempre, a cada passo, estar preparados para escolher qual o risco que desejamos aceitar para atingir nossos objetivos.

A Figura 1.2 apresenta 3 (três) perspectivas a serem consideradas na tarefa de levantamento e medição de riscos.

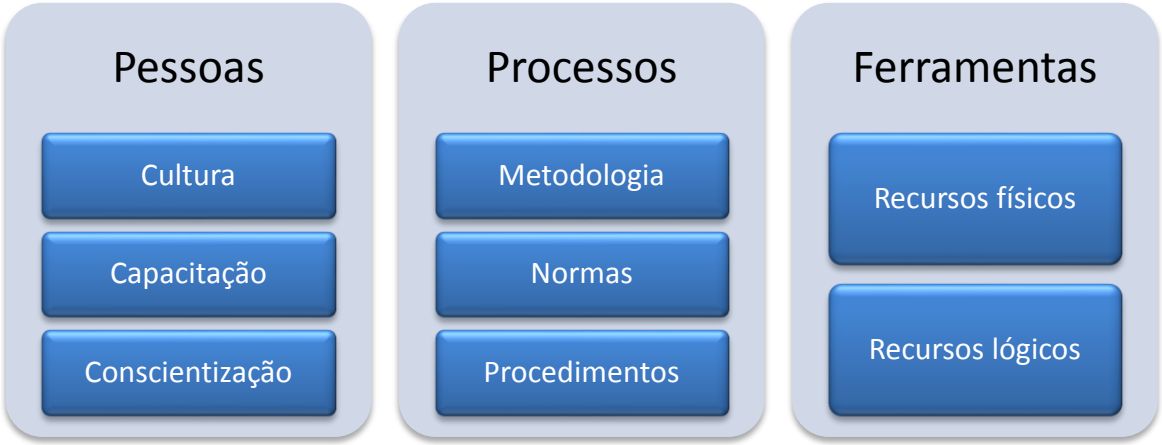


Figura 1.2 – Perspectivas para análise de riscos
Fonte: Desenvolvida pelo autor, adaptada de Freitas (2009, p. 49)

Peltier (2001 apud FONTES, 2012, p. 20) menciona que o gerenciamento de risco é fator relevante para o sucesso da implantação de segurança da informação. Já a ABNT (2005, p. 6) indica que "convém que a análise/avaliação de riscos de segurança da informação tenha um escopo claramente definido para ser eficaz e inclua os relacionamentos com as análises/avaliações de riscos em outras áreas, se necessário".

1.2.3 Política de segurança da informação

É de entendimento de Fontes (2012, p. 12-15), que uma política de segurança da informação (PSI) é requisito "chave" para o processo de zelo das informações nas instituições. É esse artefato que definirá a tendência e o caminho que a administração deseja para a segurança de seus ativos informacionais. "A política é o mais alto nível de declaração do que a organização acredita e quer que exista em todas as suas áreas. [...] é uma diretiva da direção executiva para criar um programa de segurança da informação, estabelecer seus objetivos e definir responsabilidades". Sua importância já está consolidada. Isso se comprova ao observar o RFC 2196, da *Internet Engineering Task Force* (1977 apud DINIZ; DINIZ, 2009, p. 19), que na década de 1970 já citava o objetivo da PSI como "[...] informar aos usuários, funcionários e gestores de seus requisitos obrigatórios para proteger a tecnologia e ativos de informação. A política deve especificar os mecanismos através do qual essas exigências podem ser cumpridas". Mais recentemente, a ABNT (2005, p. 8) descreve o propósito da política como sendo o de "prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes".

Conceitualmente, a política de segurança da informação é melhor entendida sob a perspectiva da ABNT (2005, p. 2), representando as "intenções e diretrizes globais formalmente expressas pela direção", e no modo de pensar de Chiavenatto (2010, p. 173 apud FONTES, 2012, p. 16) que declara que

> Uma política é um guia genérico para a ação. Ela delimita uma ação, mas não especifica o tempo. É uma definição de propósitos de uma empresa e estabelece linhas de orientação e limites para a ação dos indivíduos responsáveis pela implantação. As políticas são princípios que estabelecem regras para a ação e contribuem para o alcance bem-sucedido dos objetivos.

Ferreira e Araújo (2006, p. 9-11) comentam que essa é uma ferramenta crucial para a organização, pois envolve seus distintos setores e processos. Esse documento, que se

recomenda produzir e implantar preventivamente (antes de um infortúnio com a segurança), deve expressar os desejos e deliberações dos proprietários, sendo desenvolvida sob "[...] uma visão metódica, criteriosa e técnica [...]".

Caruso e Steffen (1999, p. 51), sob a ótica do processo, comparam a criação da política de segurança a qualquer outra atividade organizacional. Inicialmente deve-se definir o que se deseja, fitar objetivos a alcançar, a forma e recursos a serem despendidos, para então delinear etapas e prazos para execução. Entretanto, a singularidade está atrelada "[...] a forma de implantação, a rigidez dos controles, a abrangência do público que será atingido e a granularidade das regras [...]" (FONTES, 2012, p. 82).

Em termos de conteúdo a ser inserido e explicitado pela política de segurança da informação, os aspectos ***mínimos*** fornecidos por Caruso e Steffen (1999, p. 52-53) são:

- Objetivo da segurança – deve explicar de forma rápida e sucinta a finalidade da política de segurança.
- A quem se destina – deve definir claramente quais as estruturas organizacionais às quais a mesma se aplica.
- Propriedade dos recursos – deve definir de forma clara as regras que regerão os diversos aspectos relacionados com a propriedade de ativos de informações.
- Responsabilidades – deve definir de forma clara qual o tipo de responsabilidades envolvidas com o manuseio de ativos de informações, a quem as mesmas devem ser atribuídas e os mecanismos de transferência.
- Requisitos de acesso – deve indicar de forma clara quais os requisitos a serem atendidos para o acesso a ativos de informações.
- Responsabilização – deve indicar as medidas a serem tomadas nos casos de infringência às normas da mesma.
- Generalidades – nesta seção da política podem ser incluídos os aspectos que não cabem nas demais. Pode-se incluir aqui uma definição dos conceitos envolvidos, um glossário e uma indicação das normas acessórias.

Ferreira e Araújo (2006, p. 11) recomendam que as normas, políticas e demais processos que envolvam a almejada segurança das informações, devem ser desenvolvidas para uma implantação em fases e alinhadas com as estratégias e procedimentos já efetivos na organização. As 4 (quatro) fases do processo de desenvolvimento de uma PSI são apresentadas na Figura 1.3:

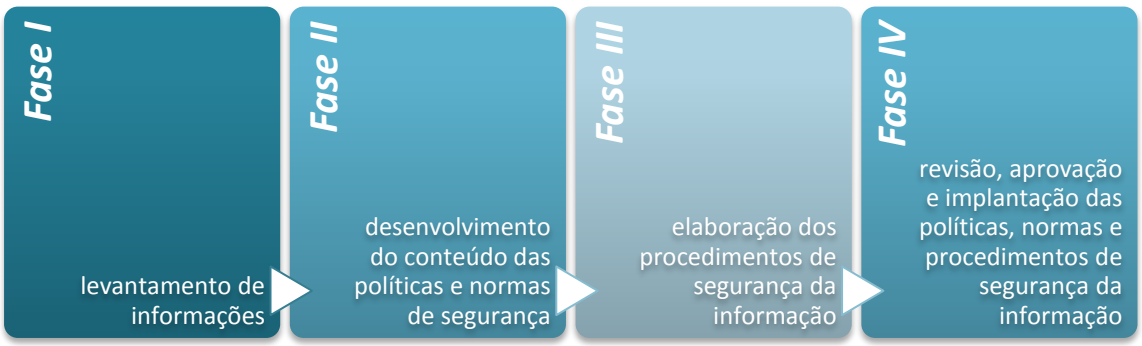


Figura 1.3 – Fases do processo de desenvolvimento de uma PSI
Fonte: Desenvolvida pelo autor, baseada em Ferreira e Araújo (2006, p. 12-14)

Quanto ao processo de implantação, Fontes (2012, p. 87) alerta para o fato de que a política só será efetiva e eficiente se houver apoio e patrocínio da direção. Deve ficar claro à todos, através de uma comunicação formal, que a cultura deve ser ajustada para o novo momento. “Todos precisam saber das novas regras. E, mais do que isto, todas as pessoas que são consideradas nestes regulamentos precisam ser treinadas nestas novas ou atualizadas regras”. É preciso, inclusive, planejar tempo para conscientização e educação dos funcionários e demais envolvidos. Ferreira e Araújo (2006, p. 21) também indicam que os documentos com políticas e normas devem ficar disponíveis para serem consultados em locais de fácil acesso (virtual ou físico), pois servirão de guia em determinadas situações.

1.2.4 Aspectos sociais e cultura organizacional

Fontes (2010 apud INFOSEC COUNCIL, 2010, p. 20) sustenta a tese de que o aspecto humano é tão importante quanto as dimensões financeira e técnica do processo de planejamento de segurança, sendo que os 3 (três) fatores conjugados permeiam o sucesso na execução do processo de segurança.

Como apresentado por Módulo (2006, p. 8), percebe-se um avanço na preocupação com a segurança de TI. Todavia, dada a sua importância, espera-se que a cada dia mais e mais empresas despertem para a necessidade desse processo. Sabe-se que esse novo padrão cultural, como qualquer outro, enfrenta resistência no âmbito dos usuários, principalmente. Mas, por mais ingrato que seja, o trabalho de conscientização deve ser realizado. “É preciso vender a cultura da segurança para o corpo da organização” (CARUSO; STEFFEN, 1999, p. 55).

Entende-se que o aspecto social possa demorar para ser consolidado. E o processo de segurança deve considerar isso. Não significa deixar de executar suas tarefas ou garantir a segurança de um recurso. Fontes (2010 apud INFOSEC COUNCIL, 2010, p. 22) esclarece que ao implantar um controle em uma área sensível, “[...] devemos considerar seu impacto sobre as pessoas e a cultura organizacional existente”. O autor ainda discute sobre o “clima organizacional”. Segundo ele, esse pode ser um facilitador para a criação da cultura de segurança. Se os funcionários estão satisfeitos e interessados pelo negócio, terão uma atitude profissional e estarão abertos a entender a importância desses novos comportamentos a que devem seguir.

Uma das maneiras de conseguir levantar o apoio e incentivar a participação desejada é através de treinamentos e palestras. Ferreira e Araújo (2006, p. 21) citam que a mobilização deve ser de todos os funcionários e também dos prestadores de serviços. Segundo eles, o elo mais fraco da corrente da segurança são os usuários que não participam dos programas de conscientização. Na opinião de Fontes (2010 apud INFOSEC COUNCIL, 2010, p. 23), os treinamentos contínuos estimulam e valorizam o empregado, que se sente mais estimulado a trabalhar e cooperar. "A realização de campanhas de segurança é recomendável, mas elas devem fazer parte de um conjunto de medidas praticadas por toda a vida da organização". O autor ainda coloca que certos elementos, como palestras, livros e teatro corporativo, auxiliam no processo. Além disso, o profissionalismo é citado como critério substancial e deve imperar na companhia. "Organizações pautadas pelo profissionalismo desenvolvem e implantam mais facilmente regulamentos deste tipo".

1.3 ELEMENTOS DE CONTROLE A AVALIAR EM SEGURANÇA DA TI

Nesta seção vão ser apresentados determinados requisitos de segurança estabelecidos de acordo com as melhores práticas de TI sobre o tema. O enfoque será direcionado aos controles de acesso físico e lógico, bem como aos conceitos e entendimentos acerca da prevenção de sinistros.

As seções descendentes, denominadas "Controles" (1.3.1.3 e 1.3.2.4), serão baseadas na Norma ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação, pois a mesma se constitui como referência técnica sobre os temas em questão. Nelas serão elencados os principais controles, recomendados pela Norma, para auxiliar no processo de garantia da segurança em TI na organização.

1.3.1 Prevenção de sinistros

Dias (2000, p. 56) conceitua as ameaças de segurança em ambientes computacionais: "ameaça é tudo aquilo que pode comprometer a segurança de um sistema, podendo ser acidental [...] ou deliberada [...]". Dentre essas ameaças, estão os vírus, ataques de hackers,

falhas de hardware, erro humano e desastres naturais. A segurança ambiental, relativa a ameaças físicas como fogo e inundação, será abordada em seção futura.

Todos os incidentes anteriormente mencionados se qualificam como um potencial desastre para a organização. “Desastre é um acontecimento que afeta de tal forma um serviço ou sistema, que a restauração do seu nível de desempenho original exige considerável esforço” (VERAS, 2009, p. 232).

1.3.1.1 Preservação dos dados e do negócio

Para Dias (2000, p. 116), devem ser identificados controles que possam minimizar possíveis acidentes com a informação. Para tanto, fixa alguns artefatos que podem auxiliar na prevenção de sinistros:

- Equipamentos de detecção e extinção de fogo;
- Manutenção preventiva de equipamentos;
- Políticas de backup, armazenamento e recuperação de sistemas computacionais e dados;
- Controles de acesso ao prédio e sistemas de alarme para detecção de intrusos;
- Proteção aos documentos não magnéticos (papéis, microfichas, microfilmes);
- Política de pessoal adequada (tanto na contratação como na demissão de funcionários);
- Campanha de conscientização dos funcionários quanto à segurança de recursos materiais e informações.

Caruso e Steffen (1999, p. 31) afirmam que a preservação e a recuperação das informações são conceitos e atividades fortemente ligados à segurança física e ao plano de continuidade da empresa. A respeito das informações, dizem que “se elas não forem preservadas, ou em caso de perda não houver como recuperar a operacionalidade das mesmas, a sobrevivência da organização tornar-se-á impossível”.

Nessa conjuntura, “[...] o procedimento de backup é um dos recursos mais efetivos para assegurar a continuidade das operações em caso de paralisação na ocorrência de um sinistro” (FERREIRA; ARAÚJO, 2006, p. 86). Os backups são cópias dos dados, criadas para recuperá-los caso sejam deletados, venham a ser corrompidos ou até mesmo ocorra um desastre. Veras (2009, p. 244) o julga como parte de um processo maior, ligado a disponibilidade e continuidade da infraestrutura de TI. Já Dias (2000, p. 116), recomenda que uma **política de backups** seja instituída, contento os procedimentos e a infraestrutura essencial à manutenção do acervo informacional da organização. “O grau de importância do sistema e de seus dados determina sua política de backup”. A autora, conjuntamente com

Ferreira e Araújo (2006, p. 89), lembram também de uma atividade muito esquecida, que deve ser integrante do processo de backup e segurança como um todo: os testes de restauração das cópias de segurança. “[...] só assim você terá certeza de que eles serão realmente úteis e cumprirão com seu objetivo de recuperar os sistemas e os dados da organização” (DIAS, 2000, p. 117).

1.3.1.2 Plano de continuidade

“A disponibilidade do ambiente de processamento de dados é fundamental em qualquer organização, independentemente de seu tamanho e valor de suas receitas” (FERREIRA; ARAÚJO, 2006, p. 85).

Brasil (2007, p. 33) expressa que o plano de contingências, ou continuidade, é um documento que normatiza estratégias e procedimentos a serem adotados quando a corporação enfrentar problemas que impeçam ou atrasem o andar normal das atividades. “Essas estratégias e procedimentos deverão minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade”. Diz ainda que suas ações são tanto preventivas, quando corretivas. Miora (2002 apud MARCIANO, 2006, p. 86) menciona que a aplicação do Plano de Continuidade objetiva proteger as operações da companhia, não apenas em caráter ferramental, mas também quanto a processos, conectividade e pessoal.

ABNT (2005, p. 103) recomenda que o processo de gestão da continuidade seja implantado a fim de

> [...] minimizar um impacto sobre a organização e recuperar perdas de ativos da informação (que pode ser resultante de, por exemplo, desastres naturais, acidentes, falhas de equipamentos e ações intencionais) a um nível aceitável através da combinação de ações de prevenção e recuperação. Convém que este processo identifique os processos críticos e integre a gestão da segurança da informação com as exigências da gestão da continuidade do negócio com outros requisitos de continuidade relativo a tais aspectos como operações, funcionários, materiais, transporte e instalações.

Dias (2000, p. 110) aprofunda o relacionamento do plano de continuidade junto aos demais documentos e processos de negócio. O plano de recuperação de desastres (como também pode ser chamado) “[...] deve fazer parte de uma estratégia ou política de continuidade de negócios mais abrangente na empresa, que busca assegurar a manutenção de seus negócios e objetivos, mesmo durante ou após a ocorrência de desastres”. Ressalta ainda

que o plano de continuidade não deve ser pensado apenas para atender situações emergenciais. Outras falhas, como indisponibilidade de serviços de terceiros, também podem afetar o negócio, confirmando sua importância para a organização. Brasil (2007, p. 35-36) complementa, sustentando que

> É imprescindível o comprometimento da alta administração com o Plano de Contingências. Na verdade, este Plano é de responsabilidade direta da alta gerência, é um problema corporativo, pois trata-se de estabelecimento de procedimentos que garantirão a sobrevivência da organização como um todo e não apenas da área de informática. Ainda, muitas das definições a serem especificadas são definições relativas ao negócio da organização e não à tecnologia da informação.

1.3.1.3 Controles

Nesta seção são apresentados os principais controles constantes na Norma ABNT NBR ISO/IEC 27002, alusivos à segurança da informação e que podem ser considerados fundamentais para a continuidade do negócio. O Quadro 1 apresentará tais controles, sendo que os mesmos não estão ordenados quanto ao aparecimento na Norma, tampouco por sua relevância.

Área	Controle
Documento da política de segurança da informação	Convém que um documento da política de segurança da informação seja aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.
Inventário dos ativos	Convém que todos os ativos sejam claramente identificados e um inventário de todos os ativos importantes seja estruturado e mantido.
Proprietário dos ativos	Convém que todas as informações e ativos associados com os recursos de processamento da informação tenham um proprietário[3] designado por uma parte definida da organização.
Uso aceitável dos ativos	Convém que sejam identificadas, documentadas e implementadas regras para que sejam permitidos o uso de informações e de ativos associados aos recursos de processamento da informação.
Documentação dos procedimentos de operação	Convém que os procedimentos de operação sejam documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem.
Controles contra códigos maliciosos	Convém que sejam implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.
Cópias de segurança das informações	Convém que as cópias de segurança das informações e dos softwares sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.

continua

[3] "[...] identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. O termo 'proprietário' não significa que a pessoa realmente tenha qualquer direito de propriedade ao ativo" (ABNT, 2005, p. 22).

conclusão

Área	Controle
Gerenciamento de mídias removíveis	Convém que existam procedimentos implementados para o gerenciamento de mídias removíveis.
Descarte de mídias	Convém que mídias sejam descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais.
Notificação de eventos de segurança da informação	Convém que os eventos de segurança da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível.
Notificando fragilidades de segurança da informação	Convém que os funcionários, fornecedores e terceiros de sistemas e serviços de informação sejam instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade em sistemas ou serviços.
Incluindo segurança da informação no processo de gestão da continuidade de negócio	Convém que um processo de gestão seja desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da organização.
Continuidade de negócios e análise/avaliação de riscos	Convém identificar os eventos que podem causar interrupções aos processos de negócio, junto a probabilidade e impacto de tais interrupções e as consequências para a segurança da informação.
Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação	Convém que os planos sejam desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.
Estrutura do plano de continuidade do negócio	Convém que uma estrutura básica dos planos de continuidade do negócio seja mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção.
Testes, manutenção e reavaliação dos planos de continuidade do negócio	Convém que os planos de continuidade do negócio sejam testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.
Prevenção de mau uso de recursos de processamento da informação	Convém que os usuários sejam dissuadidos de usar os recursos de processamento da informação para propósitos não autorizados.

Quadro 1 – Controles pertinentes à categoria "Prevenção de sinistros"
Fonte: Desenvolvido pelo autor, baseado em ABNT (2005)

1.3.2 Segurança física e lógica

"[...] segurança da informação é a garantia de que as informações da organização serão protegidas de três maneiras: serão acessadas apenas pelas pessoas que devem ter acesso a elas, estarão corretas e completas e estarão disponíveis sempre que seus usuários precisarem" (ALBUQUERQUE; SANTOS, 2011, p. 3). Portanto, para garanti-la se faz necessária a reunião de diversos métodos, preventivos ou reativos. As seguranças de nível físico e lógico podem ser consideradas a linha de frente na tentativa de impedir acessos não autorizados, auxiliando até mesmo na prevenção de sinistros.

Brasil (2007, p. 9) aborda os objetivos dos controles de acesso, físicos ou lógicos. Eles têm como finalidade a proteção dos equipamentos, aplicativos e arquivos, contra perda, divulgação ou modificação não autorizada. Já a ABNT (2005, p. 65) resume por "controlar acesso à informação". Moura e Gaspary (2008 apud ALBUQUERQUE JUNIOR; SANTOS, 2011, p. 3) vão além e revelam que "[...] a proteção da informação é conseguida através da aplicação de segurança física e lógica nas operações das empresas [...]".

No âmbito da segurança física, Dias (2000, p. 100) esclarece que existem 2 (duas) maneiras de abordar a segurança: 1) quanto ao acesso aos recursos informacionais; e 2) quanto a segurança ambiental. Enquanto a vigilância com ênfase humana discute os processos para segurança contra acesso físico não autorizado, o controle atinente ao ambiente prevê o monitoramento e manutenção da segurança contra danos motivados por causas naturais e que possam comprometer os serviços.

Ferreira e Araújo (2006, p. 60-61) avaliam que os recursos tecnológicos da organização devem ser disponibilizados aos funcionários apenas com o intuito de auxiliá-los em suas tarefas profissionais e intimamente ligadas ao negócio propriamente dito, provendo condições para que desempenhem as atribuições inerentes à sua função. Na PSI deve constar este regramento, além de especificar as responsabilidades dos colaboradores e medidas disciplinares para casos de descumprimento. Uma vez que os funcionários sejam responsáveis pelo cuidado e bom uso dos recursos, medidas administrativas podem ser tomadas para manter a ordem.

1.3.2.1 Controle de acesso físico

"Os controles de acesso físico têm como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos" (DIAS, 2000, p. 100). A autora elenca os equipamentos (servidores, estações de trabalho, impressoras, cabeamento, etc.), a documentação (política e procedimentos de segurança, manuais, etc.), os suprimentos e as próprias pessoas, como recursos a serem protegidos. E faz ainda uma evidente constatação: os processos de segurança física são barreiras de proteção anteriores aos controles lógicos, "portanto, pode-se até dizer que, indiretamente, os controles de acesso físico também protegem os recursos lógicos, como programas e dados".

Dados de Módulo (2006, p. 7), em sua pesquisa sobre segurança, revelaram diagnósticos interessantes. Dentre as empresas entrevistadas, as dos setores de Governo e de Serviços reconheceram que sofrem falhas na segurança física. Ferreira e Araújo (2006, p. 97) sentenciam que "qualquer acesso às dependências da organização, desde as áreas de trabalho até àquelas consideradas críticas (onde ocorrem o processamento de informações críticas e confidenciais) deve ser controlado sempre fazendo necessária sua formalização". Dias (2000, p. 100-101) identifica que os crachás são os meios mais comuns de reconhecimento, facilitando inclusive o controle visual no ambiente da corporação, permitindo diferenciar funcionários de visitantes, por exemplo.

1.3.2.2 Controle de acesso lógico

Dias (2000, p. 84-85) conceitua o **acesso lógico** como o processo de determinado usuário acessar um recurso como memória, impressora, um simples arquivo, ou até mesmo um aplicativo. A autora ainda define os **controles de acesso lógico** como "[...] um conjunto de medidas e procedimentos, adotados pela organização ou intrínsecos aos softwares utilizados, cujo objetivo é proteger dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por usuários ou outros programas". Os recursos comumente protegidos por controles de acesso são os aplicativos, os arquivos de dados, o sistema operacional e utilitários, além de arquivos de *log*[4] e senhas.

Ferreira e Araújo (2006, p. 71) destacam que

> Os controles de acesso lógico devem assegurar que:
> - Apenas usuários autorizados tenham acesso aos recursos;
> - Os usuários tenham acesso apenas aos recursos realmente necessários para a execução de suas atividades;
> - O acesso aos recursos críticos seja constantemente monitorado e restrito;
> - Os usuários sejam impedidos de executar transações incompatíveis com a sua função.

Outra vez, Dias (2000, p. 84) informa que a peça-chave para um controle efetivo é a conscientização do usuário. O elemento humano é o ponto fraco, uma vez que o descuido quanto a proteção de informações confidenciais, compartilhamento de senhas, ou sua simplicidade, podem prejudicar a segurança. "Um usuário bem treinado é uma das melhores maneiras de garantir a segurança de informações".

---

[4] "Os arquivos de *log* são usados para registrar ações dos usuários [...]" (BRASIL, 2007, p. 10).

1.3.2.3 Segurança ambiental

Os controles de segurança ambiental devem estar definidos e presentes na política de segurança da informação. Eles têm como função proteger as informações e recursos de tecnologia da empresa perante os danos causados pelo meio ambiente ou utilidades (DIAS, 2000, p. 104). Os acidentes citados pela autora incluem desastres ocasionados por incêndios, enchentes, falha no abastecimento de energia, aquecimento por problemas de climatização, dentre outros.

Um dos piores incidentes em nível ambiental é o fogo. Não somente pelos danos aos equipamentos e instalações, mas pelo risco que oferece, sobretudo, ao ser humano. Caruso e Steffen (1999, p. 267) ratificam que "todas as pessoas dentro da organização devem receber treinamento sobre os riscos e a maneira como agir em caso de fogo". A título de prevenção, são dispostas algumas precauções importantes, tais como:

- deixar ligado apenas os equipamentos em funcionamento e necessários;
- não permitir qualquer meio que produza fumaça no ambiente, principalmente onde houverem instalações críticas (servidores, equipamentos de rede, etc.);
- ao término de expediente verificar se todas as chaves foram desligadas, luzes apagadas, equipamentos desligados e portas fechadas.

Percebe-se que o bom senso deve estar presente, mas não sobrepor análises e aferições técnicas quanto aos controles ambientais. Ferreira e Araújo (2006, p. 99-101) citam outros elementos que podem auxiliar a segurança do ambiente, como:

- rede elétrica estabilizada e bem dimensionada;
- utilização adequada de ar-condicionado, mensurada de acordo com a necessidade dos equipamentos;
- instalação de detectores de fumaça e alarmes;
- efetuar análise de risco quanto a localização do ambiente, considerando a possibilidade de um desastre natural no local;
- não instalar servidores em locais que contenham material combustível.

Quanto ao quesito energia, Dias (2000, p. 105) recomenda a instalação de para-raios como contramedida a descargas elétricas provocadas pelo clima. Sobre as falhas ou flutuações de energia, salienta que elas podem ocasionar problemas aos equipamentos, afetando até

mesmo a disponibilidade dos sistemas. Recomenda o uso de estabilizadores, *no-breaks* e/ou geradores. Perante a água, os equipamentos não devem ser instalados em ambientes suscetíveis a ela, seja por meio de inundação ou encanamento com defeito.

1.3.2.4 Controles

Nesta seção são apresentados os principais controles constantes na Norma ABNT NBR ISO/IEC 27002, congruentes à segurança da informação, mais especificamente quanto aos controles de acesso às informações da organização. Vale lembrar que os controles, apresentados no Quadro 2 também não estão ordenados quanto ao aparecimento na Norma, nem por sua importância efetiva para a proteção dos sistemas.

Área	Controle
Devolução de ativos	Convém que todos os funcionários, fornecedores e terceiros devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.
Retirada de direitos de acesso	Convém que os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação sejam retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades.
Perímetro de segurança física	Convém que sejam utilizados perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e instalações de processamento da informação.
Controles de entrada física	Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.
Segurança em escritórios, salas e instalações	Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações.
Proteção contra ameaças externas e do meio ambiente	Convém que sejam projetadas e aplicadas proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem.
Acesso do público, áreas de entrega e de carregamento	Convém que os pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.
Instalação e proteção do equipamento	Convém que os equipamentos sejam colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.
Utilidades	Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.

continua

Área	Controle
Manutenção dos equipamentos	Convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanentes.
Segurança de equipamentos fora das dependências da organização	Convém que sejam tomadas medidas de segurança para equipamentos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.
Reutilização e alienação segura de equipamentos	Convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos os sobregravados com segurança.
Remoção de propriedade	Convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia.
Registros (*log*) de administrador e operador	Convém que as atividades dos administradores e operadores do sistema sejam registradas.
Política de controle de acesso	Convém que a política de controle de acesso seja estabelecida, documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e segurança da informação.
Registro de usuário	Convém que exista um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informações e serviços.
Gerenciamento de privilégios	Convém que a concessão e o uso de privilégios sejam restritos e controlados.
Gerenciamento de senha do usuário	Convém que a concessão de senhas seja controlada através de um processo de gerenciamento formal.
Análise crítica dos direitos de acesso de usuário	Convém que o gestor conduza a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal.
Uso de senhas	Convém que os usuários sejam solicitados a seguir as boas práticas de segurança da informação na seleção e uso de senhas.
Equipamento de usuário sem monitoração	Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada.
Política de mesa limpa e tela limpa	Convém que seja adaptada uma política de mesa limpa de papéis e mídias de armazenamento removível e política de tela limpa para os recursos de processamento da informação.
Política de uso dos serviços de rede	Convém que usuários somente recebam acesso para os serviços que tenham sido especificamente autorizados a usar.
Controle de conexão de rede	Para redes compartilhadas, especialmente essas que se estendem pelos limites da organização, convém que a capacidade dos usuários para conectar-se à rede seja restrita, alinhada com a política de controle de acesso e os requisitos das aplicações do negócio.
Procedimentos seguros de entrada no sistema (*log-on*)	Convém que o acesso aos sistemas operacionais seja controlado por um procedimento seguro de entrada no sistema (*log-on*).
Identificação e autenticação de usuário	Convém que todos os usuários tenham um identificador único (ID de usuário) para uso pessoal e exclusivo, e convém que uma técnica adequada de autenticação seja escolhida para validar a identidade alegada por um usuário.
Sistema de gerenciamento de senha	Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade.
Limite de tempo de sessão	Convém que sessões inativas sejam encerradas após um período definido de inatividade.
Limitação de horário de conexão	Convém que restrições nos horários de conexão sejam utilizadas para proporcionar segurança adicional para aplicações de alto risco.

continua

conclusão

Área	Controle
Restrição de acesso à informação	Convém que o acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte seja restrito de acordo com o definido na política de controle de acesso.
Computação e comunicação móvel	Convém que uma política formal seja estabelecida e que medidas de segurança apropriadas sejam adotadas para a proteção contra os riscos do uso de recursos de computação e comunicação móvel.
Trabalho remoto	Convém que uma política, planos operacionais e procedimentos sejam desenvolvidos e implementados para atividades de trabalho remoto.

Quadro 2 – Controles pertinentes à categoria "Segurança física e lógica"
Fonte: Desenvolvido pelo autor, baseado em ABNT (2005)

1.4 O *CHECKLIST*

Nas seções anteriores foram expressos os mais importantes conceitos e as melhores práticas quanto a segurança em TI. Com esses conhecimentos pode-se compreender sua relevância, além de propiciar embasamento para a criação de uma ferramenta que possa validar a questão problemática proposta por esta pesquisa: o *checklist*.

O referido *checklist*, apresentado no Apêndice A desse trabalho, será utilizado em uma pesquisa com alguns órgãos públicos da região do Vale do Rio dos Sinos, como instrumento de coleta de dados. Os resultados serão analisados e será possível avaliar se a problemática é válida, ou não. Para ilustrar os tópicos a serem analisados pelo questionário, a Figura 1.4 apresenta o mapa mental da segurança em TI e seus desdobramentos.

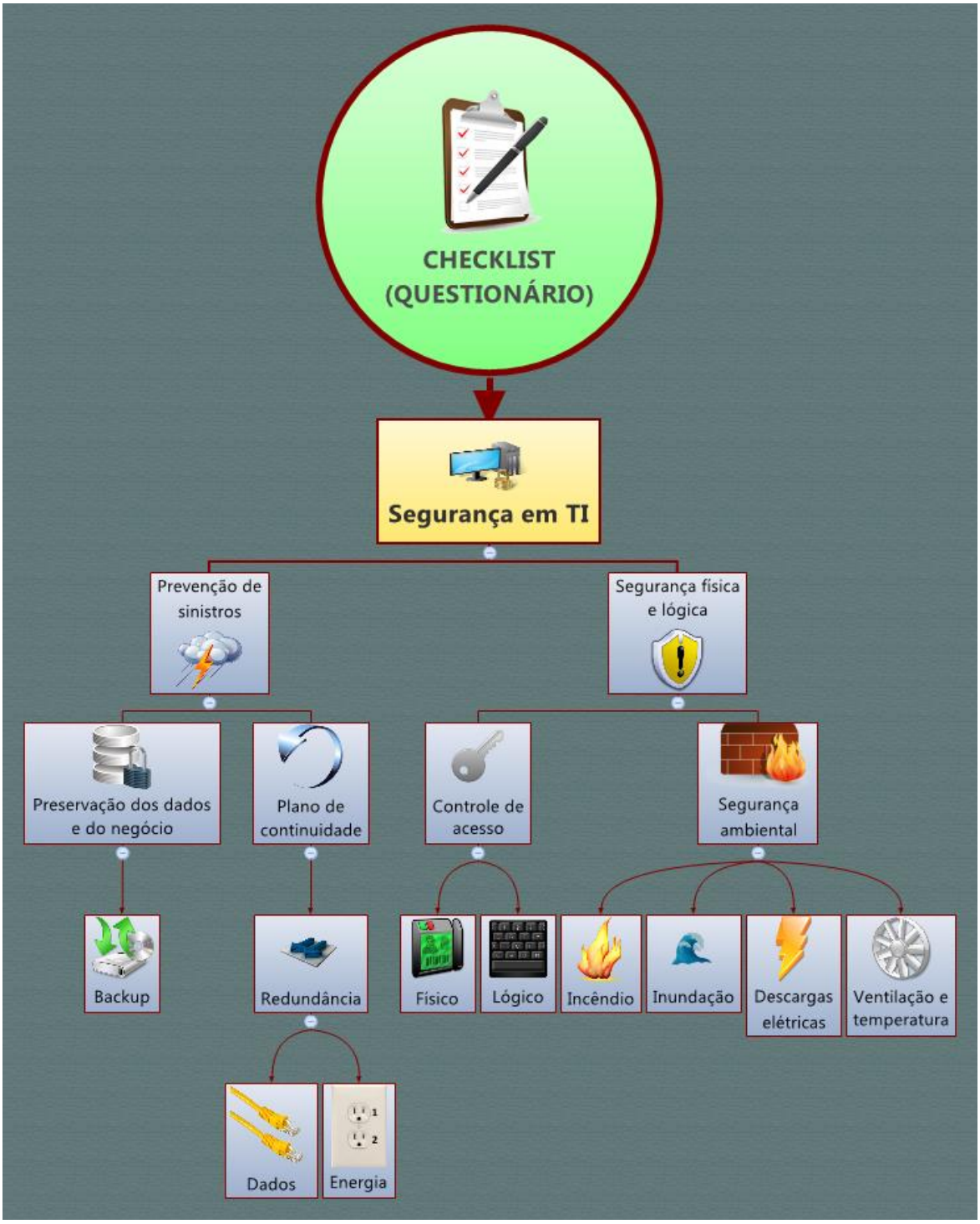


Figura 1.4 – Mapa mental da segurança em TI
Fonte: Desenvolvida pelo autor, imagens extraídas da internet

1.5 SÍNTESE DA FUNDAMENTAÇÃO TEÓRICA

Nesse primeiro capítulo foram apresentados os principais conceitos acerca da segurança em TI e algumas das melhores recomendações para assegurá-la.

A informação é alicerce para o ser humano e sua vida em sociedade. Irrefutável é, também, a sua participação no mundo globalizado dos negócios. Como fonte de diferencial competitivo, presume-se que seja tratada com o devido respaldo por parte da administração, no que tange a sua segurança. Pressupõe-se que as empresas que mantêm um planejamento de segurança correm menores riscos, ao passo que as demais podem até mesmo encerrar as atividades após um incidente com suas informações.

Constatações de pesquisas sobre o tema demonstram que os avanços na área de segurança da TI estão sendo feitos. Porém, talvez não se desenvolvam tão rapidamente quanto a formação de novos riscos e vulnerabilidades, uma vez que a agilidade das transformações no mercado supera a capacidade de planejamento. As estratégias e políticas de segurança da informação são, dessa forma, imprescindíveis para a atividade das organizações, sejam públicas ou privadas.

A Governança Corporativa, a Gestão de Riscos e a Segurança da TI perfazem um rol de atividades relevantes às empresas, desde as "micro" até as multinacionais. Os riscos são inerentes a prática empresarial. Uma gestão de riscos, suportada pela identificação, análise e avaliação dos mesmos, é o processo inicial de levantamento dos requisitos de segurança. Através destes requisitos é que se poderão estabelecer controles para a monitoria de segurança. Aliados a uma política de segurança efetiva, homologada e declarada pela direção, avaliada e melhorada continuamente, os controles são os recursos mínimos para a implantação de segurança de TI nas organizações.

A efetiva segurança física, tanto quanto a lógica, são desafios para as empresas que pretendem controlar seus dados, pois envolvem diversos fatores que podem introduzir risco para o negócio. Talvez o principal deles seja o fator humano. Intencional ou não, as falhas provocadas pelo elemento usuário estão entre as mais custosas. Certamente, inúmeros requisitos técnicos são necessários para a manutenção da segurança. Mas, não obstante, o olhar humano também é imperativo, perspectiva pela qual se devem prever controles e processos voltados à preservação dos dados, e uma cultura organizacional que a sustente. As bibliografias citam os treinamentos e a forte conscientização como métodos auxiliares eficazes para incremento de segurança. Entretanto, percebe-se que esse ainda é o principal foco de insegurança.

Nas últimas seções foram elencados e conceituados os controles de segurança da informação almejados nessa pesquisa. Os processos de garantia da continuidade e prevenção de sinistros permitem que a organização esteja preparada para contornar situações desastrosas,

caso seja impossível evitá-las. São medidas que propiciam maior segurança, principalmente quanto a permanência no mercado, posterior as eventualidades.

Os conceitos e realidades apresentadas nessa pesquisa são aplicáveis a empresas privadas, públicas, sem fins lucrativos, dentre outras. Sua natureza administrativa não exime a preocupação com segurança em TI. As organizações privadas podem ter como fonte de ameaças as especulações de mercado, segredos industriais, dentre outras. Já os órgãos públicos lidam com questões políticas e horizontes de transparência e prestação de serviços. Ou seja, vulnerabilidades e motivações para ataques sempre vão existir. Cabe a companhia mensurar os riscos aos quais está vulnerável, seu impacto provável, e prudentemente conjugar meios pelos quais pode se acautelar.

A continuação do presente trabalho será o desenvolvimento de uma pesquisa junto a alguns órgãos públicos da região do Vale do Rio dos Sinos, para averiguar sua preocupação quanto aos conceitos e controles apresentados nessa primeira parte. Os questionamentos a serem respondidos estão elencados no Apêndice A desse trabalho. O desenvolvimento de uma pequena aplicação para a resposta autônoma dos entrevistados também está prevista. Com esses elementos pretende-se solucionar a questão problemática introduzida pela pesquisa, auxiliar os órgãos públicos em sua gestão de segurança, além de colaborar com quem destina estudos sobre a temática da segurança em TI.

2 METODOLOGIA

De acordo com Fachin (2001, p. 27), a metodologia é fonte de orientação para o planejamento de uma pesquisa. De uma forma mais indistinta, seja qual for a área estudada ou o tipo da pesquisa, o método "[...] é a escolha de procedimentos sistemáticos para descrição e explicação do estudo". O autor explica ainda que, para cada problema examinado, devem ser definidos os métodos apropriados àquele estudo, ambicionando sempre "o saber".

Prodanov e Freitas (2009, p. 20) conceituam e esclarecem que "a Metodologia é a aplicação do método através de técnicas". O método sendo o modo ordenado e regrado de alcançar um propósito, enquanto a técnica define-se pela maneira de como se empregará o método. Dessa forma, "[...] o método estabelece, de modo geral, o que fazer e a técnica nos dá o como fazer [...]".

A ciência é um processo de observação e análise que anseia produzir conhecimento sistematizado e irrefutável. Mas para Köche (1997, p. 121), atingir esse objetivo deve passar pelo planejamento de todo o processo de investigação. Determinar o plano de ação a ser percorrido durante a averiguação. Contudo,

> Essa exigência de planejamento não significa [...] que se sigam normas rígidas. A flexibilidade deve ser a característica principal do planejamento da pesquisa, de tal forma que as estratégias previstas não bloqueiem a criatividade e a imaginação crítica do investigador. A investigação não deve estar em função das normas mas em função do seu objetivo que é buscar a explicação para o problema investigado.

Este capítulo visa conceituar e qualificar a pesquisa proposta pelo trabalho, de forma a elucidar o método empregado durante todo o estudo.

2.1 PESQUISA CIENTÍFICA

"Pesquisar, num sentido amplo, é procurar uma informação que não se sabe e que se precisa saber" (CARVALHO, 1997, p. 99). Mas esse é um entendimento genérico, de certa forma incorreto, pois, sob a análise de Prodanov e Freitas (2009, p. 51), "[...] tem sido quase sempre mal compreendida quanto à sua natureza e à finalidade [...]". Para os autores, muitas das pesquisas são apenas cópias e integralização de informações aleatórias. Já Demo (2000, p. 20 apud PRODANOV; FREITAS, 2009, p. 51), conjuga os diferentes entendimentos afirmando que "pesquisa é entendida tanto como procedimento de fabricação do

conhecimento, quanto como procedimento de aprendizagem (princípio científico e educativo), sendo parte integrante de todo processo reconstrutivo de conhecimento".

Cervo, Bervian e Silva (2007, p. 57) definem a pesquisa como uma prática dirigida a perquirir problemas teóricos ou práticos por intermédio da utilização de processos científicos. Ela, a pesquisa, advém "[...] de uma dúvida ou problema e, com o uso do método científico, busca uma resposta ou solução". Os escritores ainda citam que os três elementos (dúvida/problema, método científico e resposta/solução) são de extrema importância, pois a "[...] solução poderá ocorrer somente quando algum problema levantado tenha sido trabalhado com instrumentos científicos e procedimentos adequados".

Como apresentado anteriormente, o processo de planejamento é de suma importância para a pesquisa. E para Köche (1997, p. 122), essa fase preliminar leva em consideração tanto o problema investigado, quanto sua natureza e grau de conhecimento do observador. "Isso significa que podem existir vários tipos de pesquisa. Cada tipo possui, além do núcleo comum de procedimentos, suas peculiaridades próprias" (PRODANOV; FREITAS, 2009, p. 60).

A Figura 2.1 elucida resumidamente a qualificação da pesquisa e as abordagens que serão utilizadas neste trabalho, identificadas em preto e explicadas nas subseções seguintes:

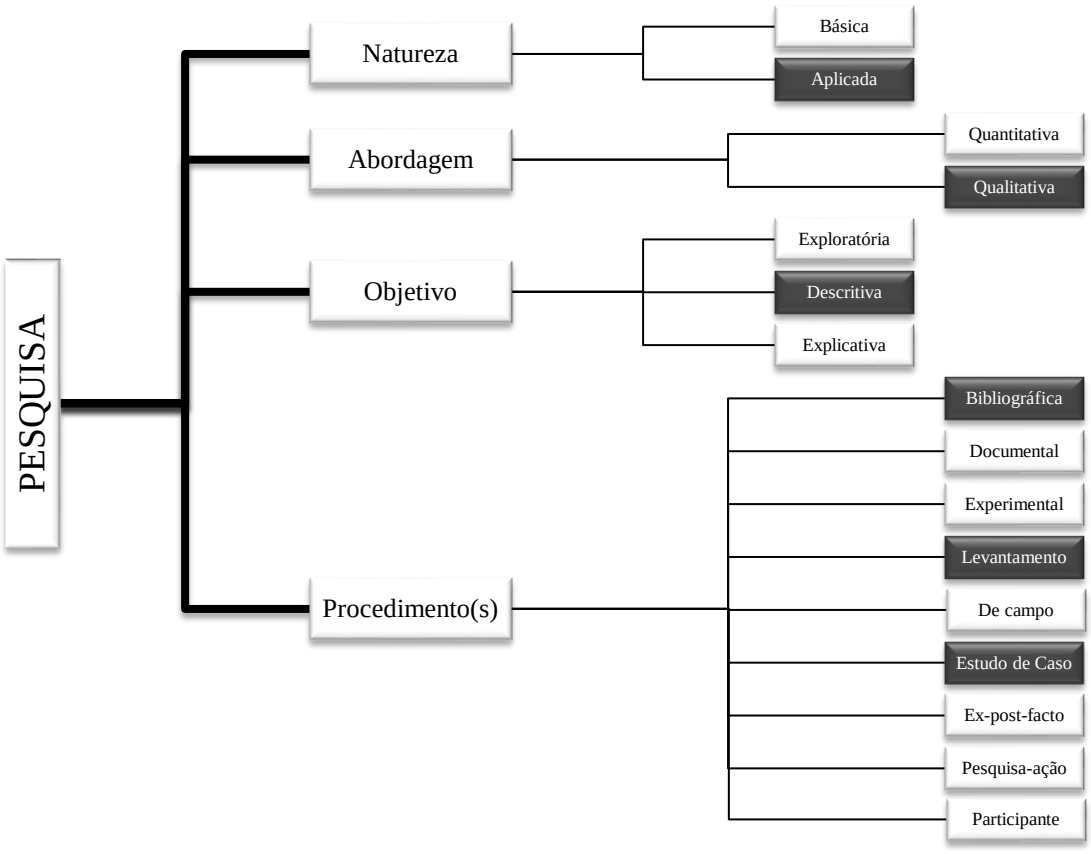


Figura 2.1 – Qualificação da pesquisa
Fonte: adaptada de BEZ (2011, p. 34)

2.1.1 Quanto a natureza

O presente trabalho, quanto a sua natureza de exploração, pode ser caracterizado como uma **pesquisa aplicada**. Uma vez que não se pretende criar novos conceitos ou redefinir padrões, mas sim utilizar concepções já definidas e melhores práticas da segurança em TI, a proposta é estabelecer um enfoque pontual quanto ao tema em questão, aplicado sob a ótica da área pública. Para Prodanov e Freitas (2009, p. 62), esse é um tipo de pesquisa com aplicação prática e que envolve verdades e relevância locais.

2.1.2 Quanto a abordagem

Essa pesquisa pode ser considerada, também, como **qualitativa**, referindo à sua abordagem. O resultado almejado, bem como sua análise, não se dará por averiguação estatística, mas sim por coerência e homologação da proposta perante a pesquisa a ser realizada com as organizações públicas. A ênfase será dirigida, portanto, às respostas do *checklist* como forma de validação da ferramenta desenvolvida para coleta das informações, e sua apreciação será efetuada caso a caso, apresentando os dados de forma, também, a averiguar o desempenho dos entes públicos quanto à segurança de TI.

2.1.3 Quanto ao objetivo

O objetivo desse trabalho visa estabelecer um conjunto de fatores (quesitos) a serem utilizados na análise da segurança em TI. O *checklist*, produto final contido desses pontos a serem observados, será validado mediante um levantamento executado junto a alguns entrevistados. No que concerne aos objetivos da investigação, pode-se afirmar que essa é uma **pesquisa descritiva**, pois buscará levantar fatos para posteriormente analisá-los, sem manipulação do pesquisador. Esse é um fator destacado por Prodanov e Freitas (2009, p. 63), que definem ainda o intuito dessa classe de estudo como o de apenas "[...] descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis".

2.1.4 Quanto ao(s) procedimento(s)

Os procedimentos previstos para o presente trabalho envolvem três atividades distintas, mas complementares no âmbito da execução absoluta do estudo. Quais sejam:

a) **pesquisa bibliográfica**: já executada no capítulo anterior, essa ação teve o objetivo de agregar conhecimento e enfatizar as peculiaridades da área em estudo. Conforme Prodanov e Freitas (2009, p. 68), "[...] todas as pesquisas necessitam de um referencial teórico". Portanto, é extremamente prudente uma análise inicial ampla sobre o assunto, já que essa será fato gerador do produto final do trabalho. Ainda, de acordo com Fachin (2001, p. 125), esse conhecimento conduz "[...] o leitor a determinado assunto e a produção, coleção, armazenamento, reprodução, utilização e comunicação das informações coletadas [...]" durante a execução da pesquisa;
b) **levantamento**: também conhecido como *survey*, é o modelo mais tradicional de pesquisa. Será aplicado para a coleta de informações que, ao final, sustentarão a análise sobre o tema, assim como servirão para validar, ou não, o emprego do *checklist* proposto. "Esse tipo de pesquisa ocorre quando envolve a interrogação direta das pessoas cujo comportamento desejamos conhecer [...]" (PRODANOV; FREITAS, 2009, p. 71);
c) **estudo de caso**: essa forma de pesquisa também pode ser considerada válida para o trabalho. Prodanov e Freitas (2009, p. 74) destacam que esse método "[...] envolve o estudo profundo e exaustivo de um ou poucos objetos de maneira que permita o seu amplo e detalhado conhecimento". Como é desejável conhecer e verificar os níveis de segurança em alguns órgãos públicos, o seu estudo, avulso e particular, justifica a adoção dessa técnica, que será empregada no quarto capítulo.

2.2 ALVO DA PESQUISA

Este projeto de pesquisa tem como propósito responder a problemática previamente difundida, cujo cerne concentra-se na averiguação de segurança da TI em órgãos públicos.

Esse tipo de instituição é, comprovadamente, fonte de desconfiança quanto a sua preocupação com a segurança de informações.

A viabilidade e a relevância do estudo justificam-se também, conforme apontado na fundamentação teórica, pelo notável despreparo das equipes de informática e usuários de forma geral, além da falta de investimentos para incremento da segurança. Desde pequenas prefeituras ou autarquias, até grandes órgãos da Administração Federal, o assunto segurança de TI não é levado a sério tanto quanto deveria. Pressupõe-se então que, a análise encabeçada por esse trabalho, possa servir para aumentar o senso de engajamento desses entes quanto à atenção aos quesitos de proteção da informação e sistemas.

2.2.1 Sujeitos da pesquisa

Como a área de estudo está direcionada a TI, designa-se a equipe de informática dos entes públicos como sujeitos para a resposta ao *checklist*. A preferência quanto a esse tipo de profissional se dá exclusivamente pelos conhecimentos técnicos necessários ao entendimento e resolutividade do questionário proposto.

3 O INSTRUMENTO DE COLETA DE DADOS

Como destacado anteriormente, o escopo deste trabalho prevê o desenvolvimento inicial de uma simples aplicação para coleta de dados. Informações essas, que sirvam de subsídio para a avaliação da problemática em questão.

Com o *checklist* proposto, busca-se angariar respostas que reflitam a segurança de TI implementada em alguns órgãos públicos da região do Vale do Rio dos Sinos. As perguntas do referido questionário foram elaboradas para que seja avaliado, em cada instituição pesquisada, o atendimento, ou não, aos critérios de segurança preventivos, tanto quanto corretivos, já apresentados na fundamentação teórica.

Para o desenvolvimento da ferramenta optou-se pela adoção de um método que permitisse ao respondente ampla autonomia no processo de solução das questões. Essa escolha possibilitou além da facilidade e serenidade no processo de resolução das perguntas (por parte do usuário), um número relativamente adequado de dados para o trabalho estabelecido. A forma de programação escolhida para o instrumento de pesquisa foi a de uma aplicação web.

Explicar-se-ão nas próximas seções os detalhes quanto ao banco de dados, as linguagens utilizadas e telas reais da página de internet concebida para este projeto.

3.1 MODELO ENTIDADE-RELACIONAMENTO

Teorey, Lightstone e Nadeau (2007, p. 3-9) explicam que as modelagens ER ou UML, são componentes da fase de projeto lógico do banco de dados. O modelo de dados conceitual, que mostra os dados e seus relacionamentos, é desenvolvido sob tais técnicas. Ainda segundo os autores,

> Na modelagem de dados conceitual, a ênfase dominante está na simplicidade e na legibilidade. O objetivo do projeto do esquema conceitual, em que as abordagens ER e UML são mais úteis, é capturar os requisitos de dados do mundo real de uma maneira simples e significativa, que seja inteligível pelo projetista de banco de dados e pelo usuário final.

O banco de dados utilizado para a aplicação é o MySQL. A Figura 3.1 apresenta o modelo ER da aplicação de coleta de dados desenvolvida nesse trabalho:

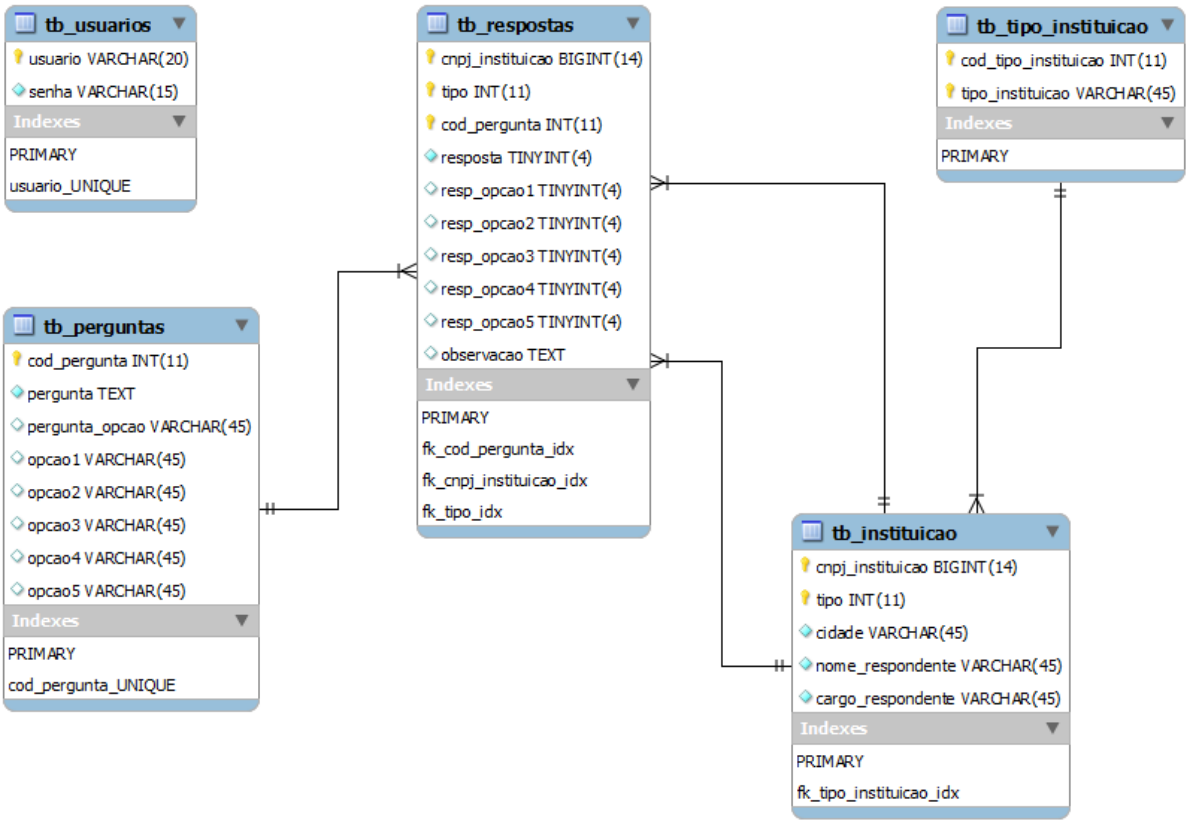


Figura 3.1 – Modelo ER da aplicação proposta
Fonte: Desenvolvida pelo autor, com auxílio da ferramenta MySQL Workbench

Complementarmente, a fim de ilustrar melhor a aplicação implementada e o seu banco de dados, o Apêndice B deste documento apresenta os seguintes diagramas: de casos de uso, de classes e de objetos (em determinado instante), além do dicionário de dados.

3.2 LINGUAGENS

Leite (2006, p. 49) diz que o intuito de se utilizar um sistema computacional é sempre extrair informação que solucione determinado problema do usuário. Como os computadores somente entendem a linguagem de máquina, o processo inicial de entendimento humano-computador se dá pelo desenvolvimento do código-fonte do programa por ele interpretado.

Seja para qual ambiente for, *desktop* ou web, e independente da linguagem, para Lopes e Garcia (2002, p. 5) um “programa de computador nada mais é do que um algoritmo escrito numa linguagem de computador [...]”, sendo que o mais importante é sua lógica, advinda do raciocínio para resolver o problema em questão.

Nas próximas subseções serão apresentadas, sucintamente, as linguagens utilizadas no desenvolvimento da aplicação de coleta de dados para essa pesquisa.

3.2.1 HTML/PHP

Silva (2008, p. 28-29) atrela a criação da HTML a invenção da web, na década de 1990. Web é o termo utilizado para designar a rede mundial de computadores, enquanto HTML (abreviação de *HyperText Markup Language*) é um código "[...] que se destina a escrever documentos que possam ser lidos por softwares genericamente chamados de agentes de usuário".

O conceito é expandido por Oliviero (2007, p. 41), ao explicar que

> O HTML [...] é uma linguagem de elaboração (marcação) de documentos com hipertexto, que funciona como se fossem sinais de trânsito para uma página da web, cuja função é enviar para o navegador instalado no cliente (Internet Explorer, Firefox etc.) comandos de formatação (marcas) que informam ao navegador de que maneira textos, imagens etc. devem ser exibidos na tela. Além dessas marcações, o HTML contém comandos que permitem fazer links de uma página para outra.

Paradoxal a HTML, PHP é uma linguagem dinâmica, totalmente voltada à internet, sendo "[...] uma das linguagens mais utilizadas na web" (NIEDERAUER, 2011, p. 23). Segundo o autor, sua principal vantagem está na possibilidade de transformar e melhorar os sites desenvolvidos estaticamente. Isso representa agilidade e eficácia para programação de páginas atualmente.

A PHP é uma linguagem gratuita, multiplataforma e baseada no servidor. Diferentemente do JavaScript por exemplo, em que o programa é carregado e executado no computador do usuário, os trechos de código em PHP são procedidos no servidor da página e o retorno enviado ao navegador do cliente. "[...] o navegador exibe a página já processada, sem consumir recursos de seu computador" (NIEDERAUER, 2011, p. 25).

3.2.2 CSS

W3C (apud SILVA, 2008, p. 49) define de forma simples e bastante precisa a CSS: "Folha de estilo em cascata é um mecanismo simples para adicionar estilos (por exemplo: fontes, cores, espaçamentos) aos documentos web".

No entendimento de Silva (2008, p. 50), sua finalidade é devolver à (X)HTML o seu propósito inicial, uma vez que essa última tenha sido criada tão somente para "[...] marcação e estruturação de conteúdos. Isto significa que, segundo seus idealizadores, não cabe à HTML fornecer informações ao agente do usuário sobre a apresentação dos elementos".

Oliviero (2007, p. 170) vislumbra que a CSS é uma revolução no design de páginas para web. Para o autor, "[...] com algumas linhas de código e um punhado de regras a serem seguidas, um site passa a ter maior consistência em seu layout, além de ser montado e carregado mais rapidamente pelo navegador". Existe também a possibilidade de separar o conteúdo HTML do layout, o que é visto como vantagem, pois simplifica a manutenção.

3.2.3 JS

JavaScript é uma linguagem interpretada, que permite criar páginas HTML dinâmicas. "[...] permite a execução de instruções de acordo com a intenção do programador" (YNEMINE, 2005, p. 1). Validação de formulários, criação de pequenas animações, controles de execução de eventos, etc. estão entre as possibilidades dessa linguagem.

Ramalho (2000, p. 5-6) explica que JavaScript é uma linguagem complementar a HTML, e "[...] que se 'aloja' dentro de um programa HTML. Você não pode criar um programa em JavaScript e executá-lo sem um browser". Quanto a sua tipificação, o autor afirma que é uma linguagem baseada em objetos, tratando todos os elementos de uma página como tal.

3.3 TELAS DA APLICAÇÃO

Nesta subseção apresentar-se-ão algumas telas da aplicação desenvolvida para a coleta de dados da pesquisa (Figuras 3.2 a 3.11).

A Figura 3.2 apresenta a tela inicial da página de pesquisa, extraída diretamente do *website* onde a ferramenta pode ser acessada:

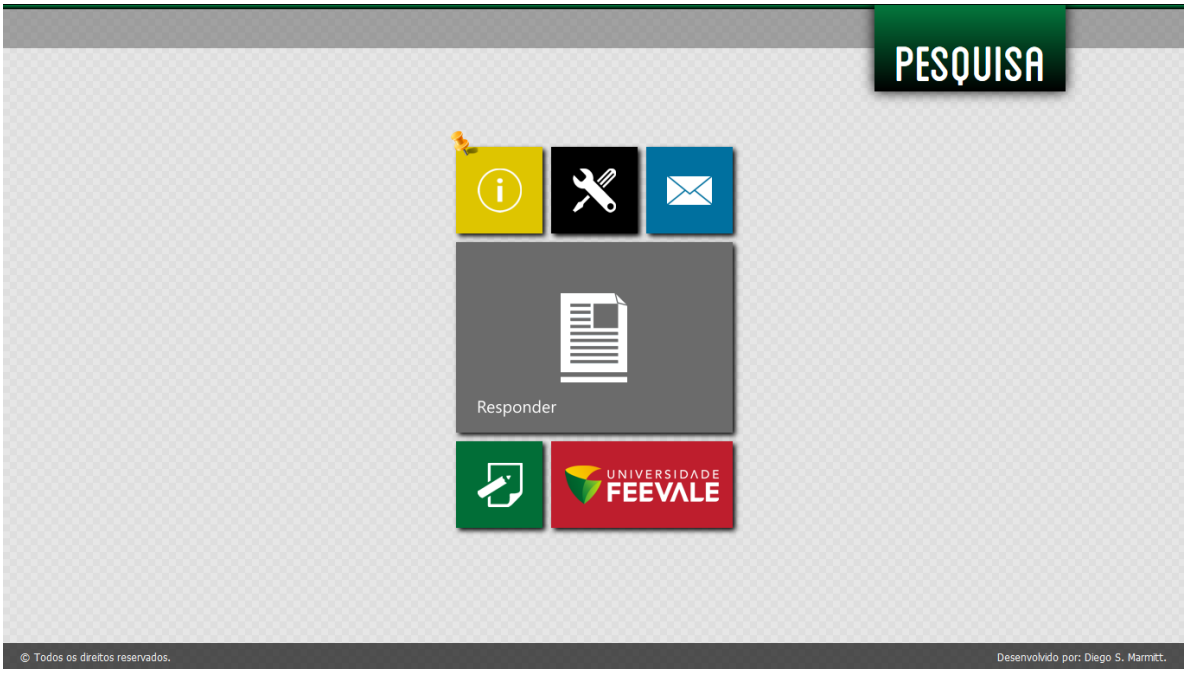


Figura 3.2 – Tela inicial da aplicação
Fonte: Aplicação desenvolvida pelo autor

Já na Figura 3.3 é apresentada a tela com informações gerais sobre o projeto:

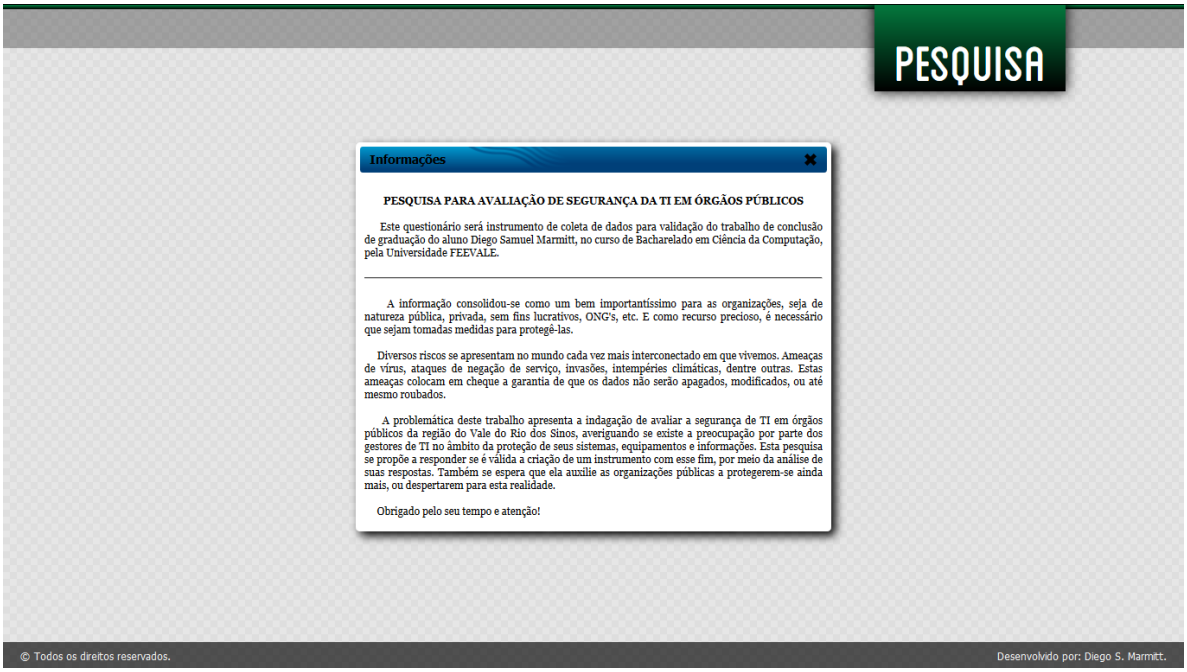


Figura 3.3 – Tela "Informações" da aplicação
Fonte: Aplicação desenvolvida pelo autor

Na Figura 3.4 é mostrada a tela com dados pessoais do aluno que propõe esse trabalho:

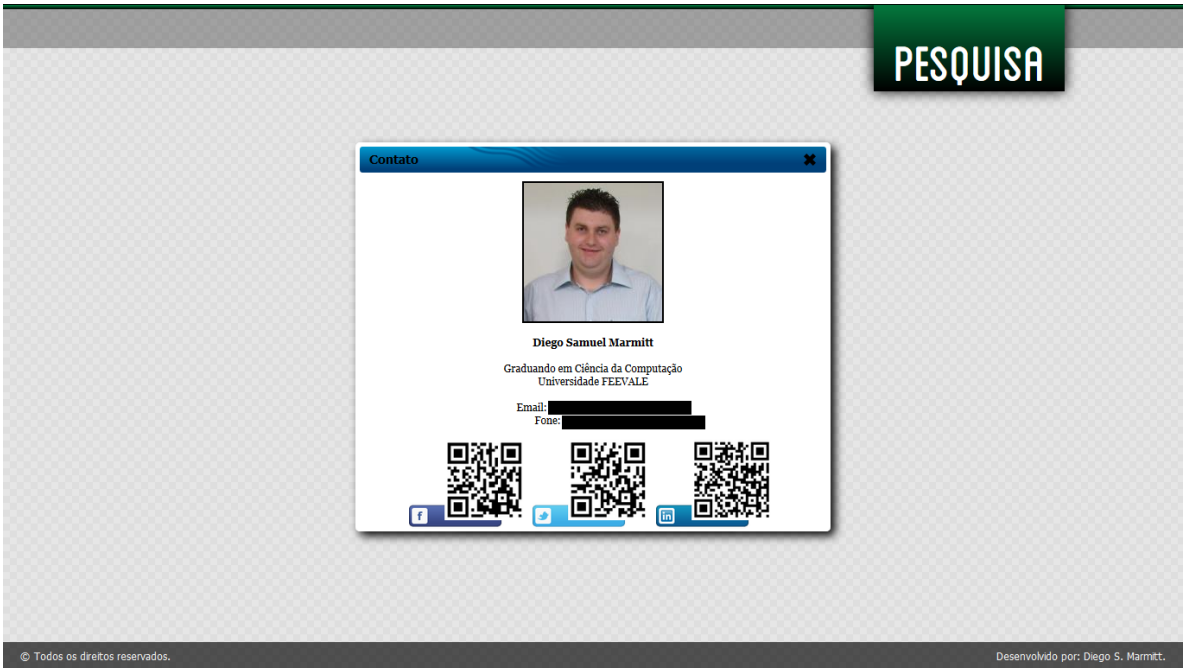


Figura 3.4 – Tela "Contato" da aplicação
Fonte: Aplicação desenvolvida pelo autor

Uma tela para o envio de sugestões por parte do respondente da pesquisa também foi criada e pode ser vista na Figura 3.5 abaixo:

Figura 3.5 – Tela "Envie sua sugestão" da aplicação
Fonte: Aplicação desenvolvida pelo autor

A Figura 3.6 apresenta a tela inicial da pesquisa, onde o entrevistado deve cadastrar os dados de sua instituição. Essa tela alerta para o usuário de que os dados ali informados, que identifiquem seu órgão público, não serão divulgados neste trabalho.

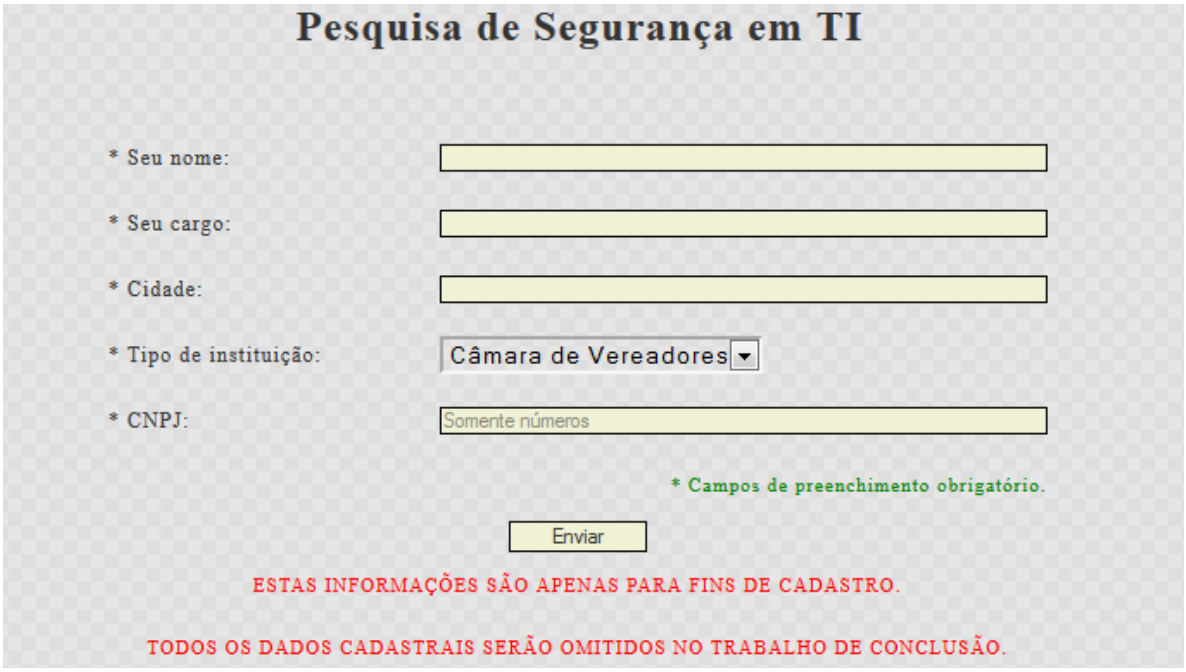


Figura 3.6 – Tela "Responder" da aplicação
Fonte: Aplicação desenvolvida pelo autor

A tela a seguir, na Figura 3.7, exemplifica a janela de resposta ao questionário propriamente dita. De forma bastante simples, são apresentados ao usuário a pergunta, opções de resposta, além de campo para observação.

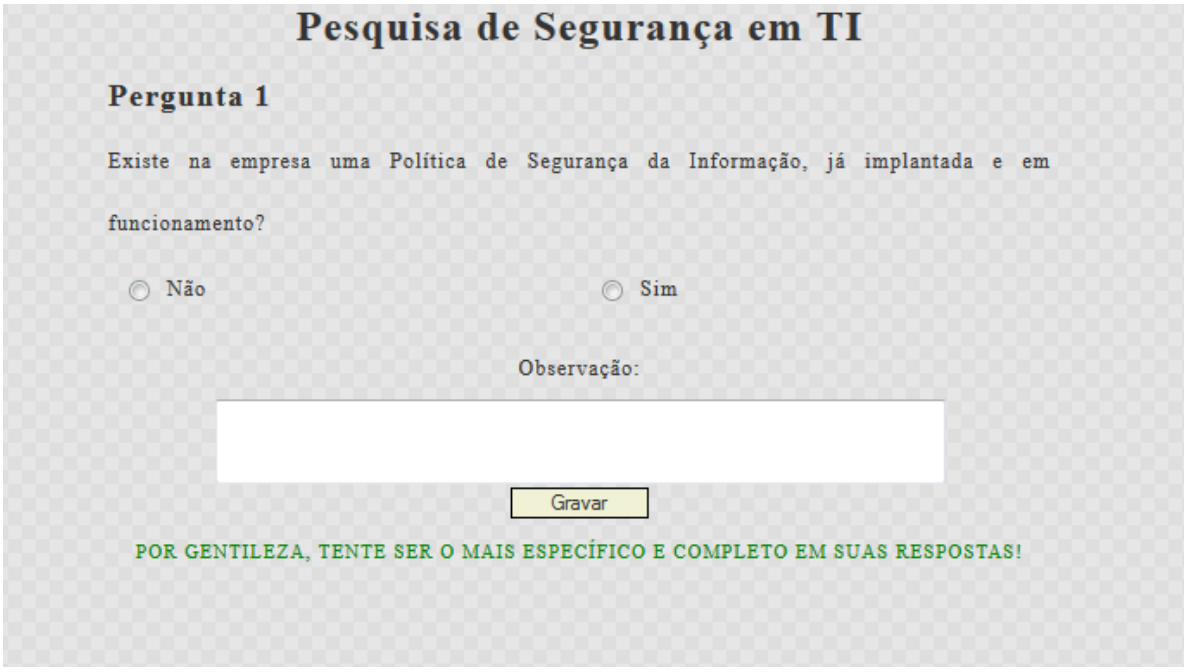


Figura 3.7 – Tela com pergunta na aplicação
Fonte: Aplicação desenvolvida pelo autor

A Figura 3.8 exibe a página de acesso ao menu restrito da aplicação, onde podem ser visualizados os relatórios com as respostas da pesquisa.

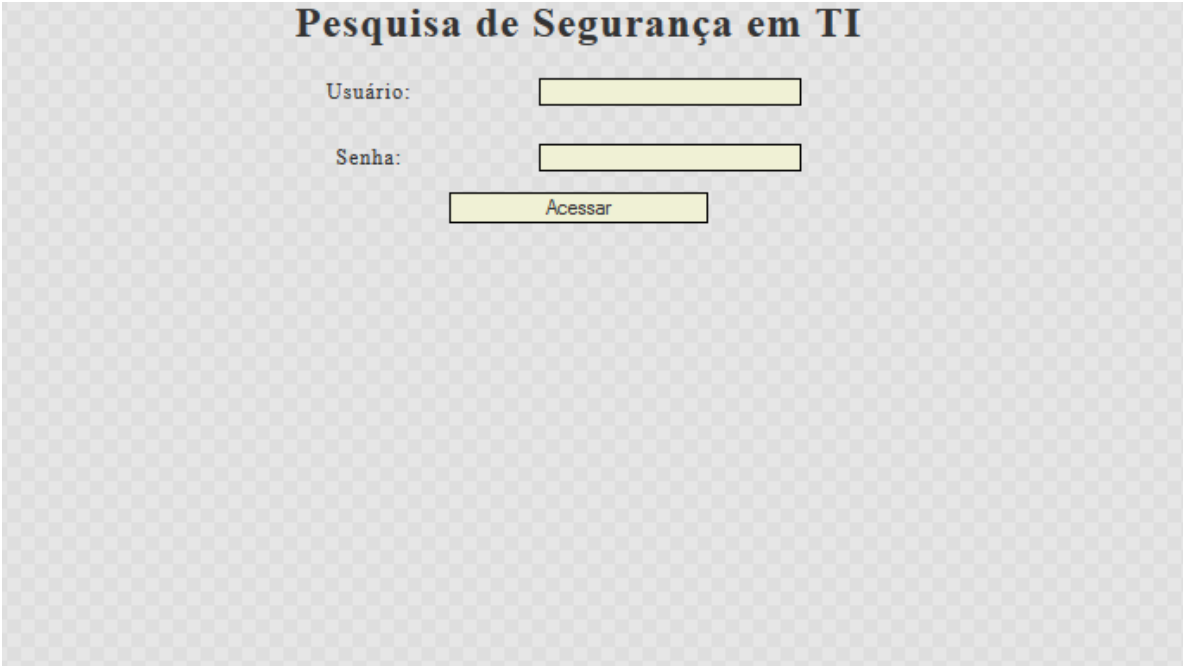


Figura 3.8 – Tela de acesso aos relatórios na aplicação
Fonte: Aplicação desenvolvida pelo autor

Após o *login* na tela de acesso limitado, é exposta a janela com a listagem dos respondentes do *checklist*. A Figura 3.9 mostra essa página, na qual pode ser escolhida uma instituição e solicitados dois tipos distintos de relatórios. Os campos sobrescritos em preto foram inseridos para preservar a identidade das instituições que responderam a pesquisa.

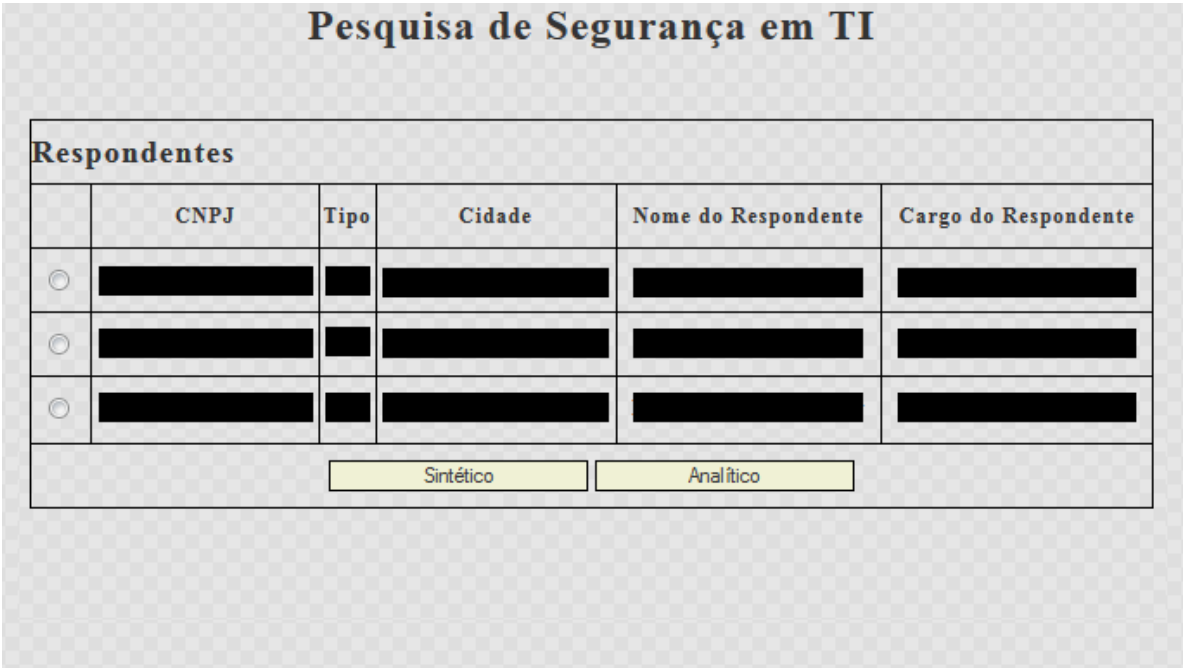
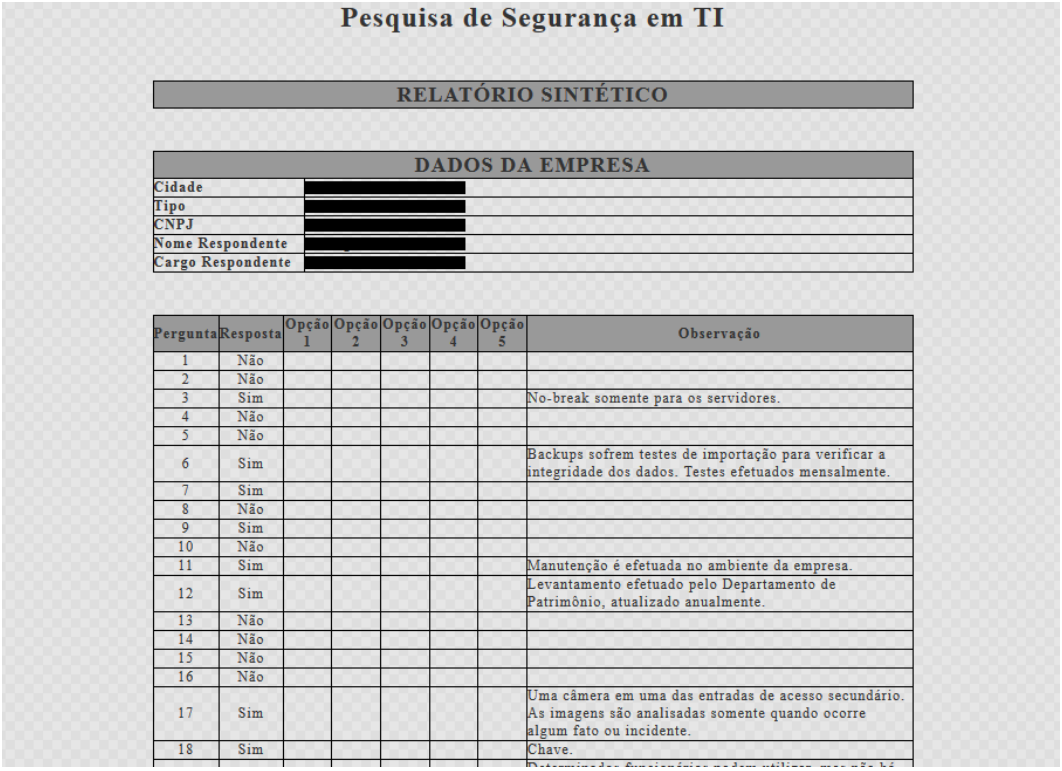


Figura 3.9 – Tela de visualização dos respondentes
Fonte: Aplicação desenvolvida pelo autor

As Figuras 3.10 e 3.11 apresentam os relatórios disponíveis na aplicação: sintético e analítico, respectivamente. Estes relatórios apresentam as respostas fornecidas pelos entrevistados.



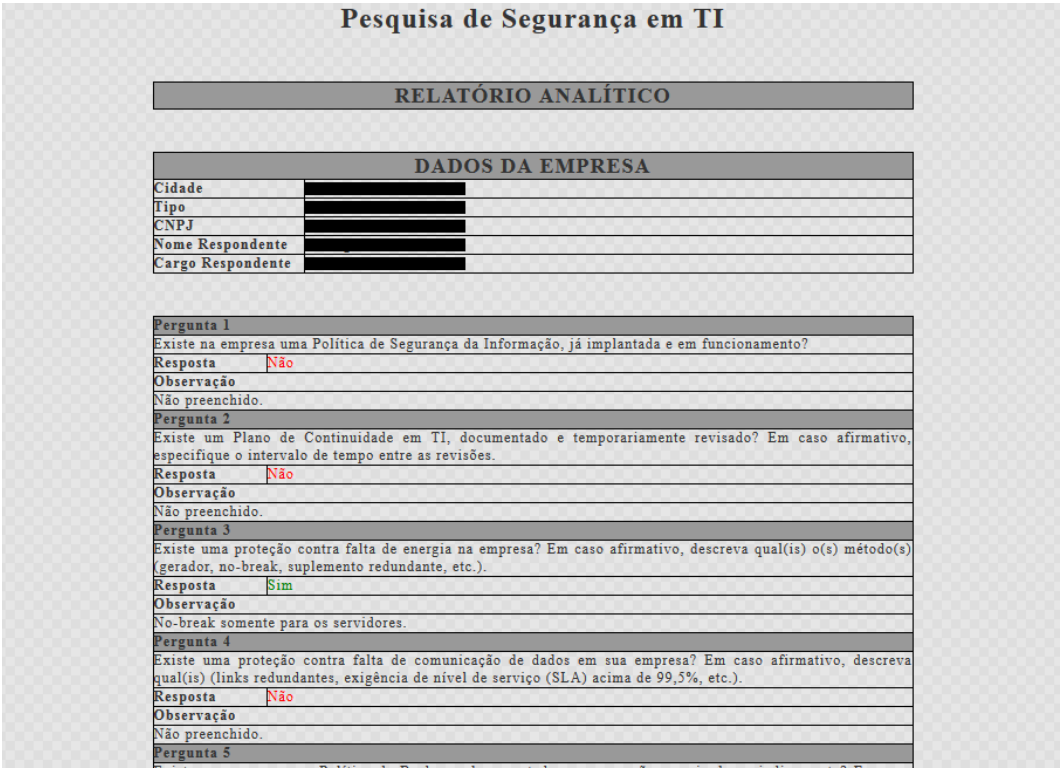
Pesquisa de Segurança em TI

RELATÓRIO SINTÉTICO

DADOS DA EMPRESA	
Cidade	[redacted]
Tipo	[redacted]
CNPJ	[redacted]
Nome Respondente	[redacted]
Cargo Respondente	[redacted]

Pergunta	Resposta	Opção 1	Opção 2	Opção 3	Opção 4	Opção 5	Observação
1	Não						
2	Não						
3	Sim						No-break somente para os servidores.
4	Não						
5	Não						
6	Sim						Backups sofrem testes de importação para verificar a integridade dos dados. Testes efetuados mensalmente.
7	Sim						
8	Não						
9	Sim						
10	Não						
11	Sim						Manutenção é efetuada no ambiente da empresa.
12	Sim						Levantamento efetuado pelo Departamento de Patrimônio, atualizado anualmente.
13	Não						
14	Não						
15	Não						
16	Não						
17	Sim						Uma câmera em uma das entradas de acesso secundário. As imagens são analisadas somente quando ocorre algum fato ou incidente.
18	Sim						Chave.

Figura 3.10 – Tela de visualização do relatório sintético
Fonte: Aplicação desenvolvida pelo autor



Pesquisa de Segurança em TI

RELATÓRIO ANALÍTICO

DADOS DA EMPRESA	
Cidade	[redacted]
Tipo	[redacted]
CNPJ	[redacted]
Nome Respondente	[redacted]
Cargo Respondente	[redacted]

Pergunta 1	
Existe na empresa uma Política de Segurança da Informação, já implantada e em funcionamento?	
Resposta	Não
Observação	
Não preenchido.	
Pergunta 2	
Existe um Plano de Continuidade em TI, documentado e temporariamente revisado? Em caso afirmativo, especifique o intervalo de tempo entre as revisões.	
Resposta	Não
Observação	
Não preenchido.	
Pergunta 3	
Existe uma proteção contra falta de energia na empresa? Em caso afirmativo, descreva qual(is) o(s) método(s) (gerador, no-break, suplemento redundante, etc.).	
Resposta	Sim
Observação	
No-break somente para os servidores.	
Pergunta 4	
Existe uma proteção contra falta de comunicação de dados em sua empresa? Em caso afirmativo, descreva qual(is) (links redundantes, exigência de nível de serviço (SLA) acima de 99,5%, etc.).	
Resposta	Não
Observação	
Não preenchido.	
Pergunta 5	

Figura 3.11 – Tela de visualização do relatório analítico
Fonte: Aplicação desenvolvida pelo autor

4 ANÁLISE DOS DADOS COLETADOS

O *checklist* proposto por esta pesquisa foi aplicado e respondido por três órgãos públicos da Região do Vale do Rio dos Sinos. Os questionários replicados, com as informações recebidas completas, estão no Apêndice C desse trabalho.

A forma de estudo das respostas fornecidas pelos entrevistados se dará sob a análise de cada caso em particular, conforme adiantado no segundo capítulo. Todavia, para facilitar o entendimento e agrupar as perguntas em áreas de estudo, o questionário foi dividido em quatro categorias, conforme visto na Figura 4.1:

Figura 4.1 – Categorias de perguntas
Fonte: Desenvolvida pelo autor

O Quadro 3 identifica as perguntas de acordo com sua categoria:

Categorias	Perguntas (Apêndice A)
Prevenção e contorno de sinistros	1; 2; 5; 6; 12; 13; 14; e 15.
Segurança física	3; 4; 7; 8; 9; 10; 11; 16; 17; 18; e 19.
Segurança lógica	20; 21; 22; 23; 24; 25; 26; 27; 28; 29; 30; 31; 32; 33; 34; e 35.
Outras	36; 37; e 38.

Quadro 3 – Categorização das perguntas
Fonte: Desenvolvido pelo autor

As subseções a seguir apresentarão uma análise dos principais tópicos respondidos pelas instituições públicas pesquisadas. As perguntas foram respondidas por três instituições

do tipo Prefeitura. As cidades serão mantidas em sigilo para preservação da imagem pública. Entretanto, destaca-se, como pode ser visto no Quadro 4, que são municípios de pequeno porte:

Instituição	Número de habitantes
1	Entre 40.000 e 45.000
2	Entre 25.000 e 30.000
3	Entre 20.000 e 25.000

Quadro 4 – Característica demográfica dos municípios participantes da pesquisa
Fonte: Desenvolvido pelo autor, baseado em IBGE (2010)

4.1 INSTITUIÇÃO 1

O primeiro ente público a ser analisado é a Prefeitura de um município com aproximadamente 42.000 habitantes (IBGE, 2010). As respostas na íntegra podem ser vistas no questionário integralizado e apresentado no Apêndice C, as quais apontam para as seguintes conclusões:

a) **prevenção e contorno de sinistros**: a segurança implantada por esta instituição, quanto ao quesito de prevenção e contorno de sinistros é extremamente básica, praticamente inexistente. Não há políticas estabelecidas para segurança da informação, não existe plano de continuidade, tampouco análise de riscos. Os eventos que possam comprometer a segurança da informação não são reportados nem mesmo para a equipe de TI, uma vez que não há um departamento para gestão de segurança. Dos quesitos interrogados, apenas os testes de backups e inventário são realizados;
b) **segurança física**: nesta classificação a empresa já se apresenta mais engajada quanto a instauração de meios para segurança. Ainda que de uma forma bastante simples, existe vídeo-monitoramento em uma das entradas, controle de acesso à sala do datacenter e no-break para os servidores. Entretanto, é bastante contraditório que se tenham tomadas elétricas estabilizadas para a ligação dos microcomputadores, mas não haja aterramento adequado. A manutenção dos equipamentos é realizada por pessoal contratado, dentro do ambiente da empresa, o que é bastante sensato. Ponto de destaque negativo nessa categoria é a afirmação de que não existe proteção para incêndios, sobretudo no ambiente de alocação dos servidores;

c) **segurança lógica**: percebe-se o mesmo nível de cuidado e proteção do grupo anterior. Por exemplo, há a preocupação de que as senhas dos usuários sejam de boa qualidade, mas não se exige que as mesmas sejam trocadas com frequência. Também não existe um processo formal de cancelamento dos dados de *login* dos funcionários que deixam a atividade na prefeitura. As senhas de acesso aos servidores não são diferentes entre si e não há política de acesso aos sistemas. Contudo, o órgão garante que as permissões de acesso aos sistemas são analisadas criticamente, grava *logs* de sites e sistemas aplicativos, possui *firewall* e listas de bloqueio de tráfego e impede acesso externo aos seus servidores para usuários administrativos. A empresa utiliza antivírus gratuito em estações de trabalho, mas não em servidores. Afirma ainda realizar a destruição de mídias antes do descarte, o que é de suma importância;

d) **outras**: o respondente alega que a administração e chefia do órgão não entende a importância da segurança de TI, sendo que as políticas de implantação são atribuição exclusiva do pessoal de informática. Há o entendimento de que a segurança implantada é demasiadamente básica e insuficiente. O entrevistado atribuiu nota 4 (de 0 a 10) para a segurança implementada, diz estar ciente da situação e considera que existem fatores internos que impedem o desenvolvimento e avanço da segurança interna. Todas as opções foram assinaladas como verdadeiras: falta de conscientização da administração, dos usuários, de investimentos e profissionais qualificados para o aprimoramento.

Com esses resultados da pesquisa pode-se verificar o escasso e amador nível de segurança implantado na Prefeitura. A falta de controles, políticas claramente definidas e divulgadas, acaba por dificultar todo o processo de segurança de TI. Os mecanismos existentes são extremamente elementares e não propiciam tranquilidade para o órgão público. Mas o que mais chama a atenção é a falta de conscientização de todos os envolvidos (administração e funcionários), inclusive podendo influenciar nos investimentos da área. Conclui-se, para essa instituição, de que medidas em caráter imediato devem ser tomadas para incremento e desenvolvimento da compreensão de que a segurança de TI é importante e fundamental.

4.2 INSTITUIÇÃO 2

Outro órgão público inquirido é a Prefeitura de um município com uma população aproximada de 27.000 habitantes (IBGE, 2010). Os dados apresentados nessa pesquisa apontam para a seguinte análise:

a) **prevenção e contorno de sinistros**: essa segunda instituição possui uma política de segurança já implantada e um plano de continuidade em implementação. Segundo o respondente, a mesma dispõe também de uma política de backups, revisada mensalmente, apesar de não exercer testes com os arquivos de cópia de segurança para validar os dados reproduzidos. O inventário dos equipamentos é realizado, mas pelo setor de patrimônio. Consonante com a primeira organização, esta também não mantém um departamento de gestão segurança, não realiza o reporte de eventos de segurança, nem realiza análise e avaliação de riscos;
b) **segurança física**: o ente demonstra preocupação quanto a continuidade dos serviços de TI, com link redundante de dados e fonte de energia para momentos de falha na utilidade. Disponibiliza tomadas estabilizadas, aterradas e suprimentos para extinção de incêndios. Os microcomputadores são alocados em áreas de acesso dificultado a qualquer pessoa, mas não possui vídeo-monitoramento. O datacenter é trancado apenas com chave e o órgão não possui sala-cofre para armazenagem de ativos importantes. A manutenção dos equipamentos é feita por pessoal contratado e a empresa não permite o uso das ferramentas tecnológicas fora do ambiente da empresa;
c) **segurança lógica**: quanto aos servidores, percebe-se uma preocupação maior, pois as senhas são todas diferentes, os acessos de usuários com perfil de administrador foram bloqueados e é utilizada solução antivírus paga, assim como nos microcomputadores. As pastas compartilhadas na rede estão com controle de criação/edição/exclusão. Quanto aos acessos dos funcionários, apenas é solicitado que escolham senhas fortes, mas não é solicitado que efetuem a troca em intervalos de tempo. É indicado que, ao deixar o equipamento, o usuário bloqueie sua sessão de trabalho, induzindo à reentrada de senha no retorno a atividade. A concessão de privilégios de acesso não é controlada e revisada periodicamente, possivelmente pelo fato de também não possuir uma política de acesso aos sistemas, estruturada e documentada. No entanto, o processo de

registro e cancelamento de usuários está formalmente instituído. A concessão de direitos de acesso remoto não está normatizada, não há limite de horário para conexão aos recursos de rede, não existe impedimento de uso de mídias por parte dos usuários, nem inutilização de discos no momento do descarte. A organização ainda possui *firewall* para controle de tráfego, mas não efetua registros de *log*, tanto de sites, quanto nos sistemas aplicativos;

d) **outras**: segundo o respondente, a administração do município entende e apoia a segurança de TI. Na opinião do entrevistado, a segurança implementada na Prefeitura é suficiente, apesar de não apontar uma nota que a qualifique e nem vislumbrar obstáculos internos que frustrem a melhoria no processo de segurança de TI.

A Prefeitura analisada nesta subseção apresenta-se levemente mais estruturada em seus mecanismos de segurança, se comparada com a Instituição 1. Percebe-se que o desenvolvimento de políticas que regrem as atividades é uma preocupação, já estando com algumas em utilização ou em desenvolvimento. A segurança física está mais apta e implantada. Já a segurança lógica apresenta diversos requisitos com respostas negativas, o que elege essa categoria como a de maior problema no ente público em questão. A administração entende que a segurança é importante e isso tende a facilitar novas implementações. Apesar de não serem apontados problemas e de o entrevistado considerar a segurança da TI satisfatória, verifica-se que ainda pode ser aprimorada.

4.3 INSTITUIÇÃO 3

Esta última instituição pesquisada é de uma cidade com pouco menos de 22.000 moradores (IBGE, 2010). O órgão também é do tipo Prefeitura, de onde se podem firmar tais julgamentos:

a) **prevenção e contorno de sinistros**: essa organização possui políticas de segurança da informação e de backups já implantada. A última, revisada mensalmente. Contudo, não é documentado o plano de continuidade, assim como não foi instituído um departamento de segurança específico. Os backups são revisados semanalmente. Os riscos são avaliados somente contra invasão,

trimestralmente, e a comunicação de eventos relativos a segurança é formal. O inventário é atribuição do setor de patrimônio, que o gerencia;

b) **segurança física**: a Prefeitura possui link redundante para continuidade de serviço, assim como no-break, e estuda a viabilidade de um gerador de energia. As tomadas elétricas possuem aterramento e não são estabilizadas. Não existe sala-cofre para guarda de dados e documentos. O datacenter é protegido apenas com chave e não há vídeo-monitoramento. Outro ponto falho é a falta de extintores. A utilização de equipamentos fora do local de trabalho não é permitida. Ainda quanto aos recursos informacionais, não são disponibilizados em áreas de fácil acesso e são revisados e consertados internamente, por pessoal próprio;

c) **segurança lógica**: uma política de acessos aos sistemas ainda não foi implantada, apesar da concessão de privilégios ser analisada pela equipe de TI em conjunto com o superior da secretaria ao qual o funcionário está alocado. Quanto as senhas, nos servidores todas são diferentes e estão de acordo com requisitos mínimos. Porém, o acesso aos usuários com poderes administrativos não é bloqueado. Para os usuários é solicitado que utilizem senhas fortes, alternando letras e números, e que bloqueiem sua sessão ao deixarem o PC. Todavia, não é realizada troca de senha regularmente. Não há também um procedimento formal para liberação e bloqueio de acesso quando da admissão ou exoneração do funcionário na Prefeitura. No quesito rede, as pastas compartilhadas possuem restrições de criação/edição/exclusão, mas não há horários limítrofes para concessão de acesso. O uso de mídias removíveis pelos funcionários não possui restrição. Ao pessoal de suporte não há normas ou procedimentos para regrar o acesso remoto. A instituição utiliza *firewall* para controle de acesso e só registra *log* de acesso aos sites. Antivírus pago é utilizado tanto em microcomputadores quanto nos servidores. Fato positivo é a destruição de mídias e discos antes do descarte;

d) **outras**: o respondente apresentou ponderações bastante pertinentes nas respostas desta categoria. Relata que a administração entende e valoriza os processos de segurança e, quando há necessidade de investimento, um estudo é apresentado, contemplando a previsão de gastos e os benefícios que poderá introduzir. Segundo o entrevistado, a segurança aplicada no momento é suficiente, mas indica que existe uma preocupação persistente na busca por melhorias. Cita ainda

> que o único obstáculo para a implementação plena da segurança no órgão público é a falta de conscientização dos usuários.

Essa entidade pública aparenta ser a mais preparada e munida de recursos para a plena implantação de segurança em TI. Quando se fala em segurança, todos os recursos são importantes, mas, apesar de não contar com diversos requisitos, conta com outros bastante importantes em todas as categorias. Essa realidade projeta uma perspectiva de implantação em curto prazo, se assim desejado, de mais ferramentas que completem o aparato necessário. O consentimento da gerência é fundamental e está presente na Prefeitura. Já a preocupação quanto ao descuido por parte dos usuários é previsível, mas também passível de solução com treinamentos e esforço coletivo no desenvolvimento da mentalidade e bom senso na utilização dos equipamentos e sistemas.

CONCLUSÃO

O presente estudo apresentou um modelo de *checklist* para averiguação de segurança da TI em órgãos públicos. O questionário foi aplicado em alguns entes governamentais da Região do Vale do Rio dos Sinos, no Rio Grande do Sul. Entretanto, como essa é uma área de estudo bastante ampla e não restrita a entes públicos, verificou-se que a pesquisa pode ser aplicada em distintos gêneros de empresas.

Não obstante, também foi desenvolvida uma ferramenta para coleta, armazenagem e extração de relatórios, a qual possibilitou que os entrevistados pudessem responder autonomamente as indagações quanto a proteção de seus dados, equipamentos e sistemas. O desenvolvimento se deu na modalidade de uma aplicação web, hospedada e utilizada diretamente através do site registrado para esse propósito.

Quanto aos objetivos propostos para esse trabalho, conclui-se que todos foram atingidos. Foi apresentado um embasamento teórico acerca das áreas escolhidas, abordando tópicos relevantes e normatizados por uma entidade referência no Brasil (objetivo 1). Fez-se uma reunião dos principais controles recomendados para uma segurança de TI efetiva (objetivo 2). Estabeleceu-se também o *checklist* para a pesquisa (objetivo 3) e o instrumento de coleta de dados (*website*) previsto (objetivo 5). Essas atividades iniciais possibilitaram a análise da segurança em certos órgãos públicos, mediante o conhecimento da realidade ímpar de cada um, além de sustentar a viabilidade do instrumento sugerido (objetivo 6) e auxiliar na resolução da problemática indicada inicialmente. O objetivo 4 propunha a verificação da existência de uma ferramenta capaz de avaliar a segurança de TI aplicada nas organizações. Tal pesquisa não encontrou um sistema de levantamento de dados como o proposto neste trabalho.

Com a aplicação do questionário averiguou-se que a proteção imposta pelos entes públicos respondentes é relativamente fraca. Há uma preocupação mínima e simplória quanto às implementações de mecanismos que efetivamente os protejam de ataques, roubo de informações, desastres – naturais ou de ordem interna, dentre outros.

Uma revisão e análise profunda são recomendadas às instituições pesquisadas, fomentando o incremento e desenvolvimento de novos artifícios e formas de controle que assegurem uma segurança mais eficiente e robusta. Com os dados averiguados pode-se

perceber que a preocupação, por menores que sejam essas entidades, é muito distante da recomendada e necessária para o momento tecnológico pelo qual se está passando.

Quanto à questão problemática do trabalho, acredita-se que tenha sido solucionada. O desenvolvimento de uma ferramenta para averiguar a segurança de TI em órgãos públicos é viável, não somente por seu caráter avaliativo e facilitador de pesquisa, mas sobretudo como conscientizador de que a segurança deva ser interpretada de forma mais profissional e efetiva.

A limitação do trabalho se deu pela aplicação do questionário em apenas alguns entes públicos da região domicílio do aluno, de onde foram extraídas as respostas que balizaram a averiguação da proteção dos recursos de TI.

Por fim, esse trabalho pode contribuir para quem dispensa tempo ao estudo de normatização, indicadores e requisitos de segurança da TI, principalmente à Norma ABNT NBR ISO/IEC 27002, mas não exclusivamente. Sugere-se ainda, para trabalhos futuros:

- a melhoria e ampliação do *checklist*;
- o aperfeiçoamento da ferramenta de coleta de dados, possibilitando ainda a avaliação automatizada da segurança de TI sob critérios de pontuação;
- a aplicação do questionário em um número maior de órgãos públicos, e até mesmo empresas privadas, com o intuito de que seja utilizado para mensuração dos níveis de segurança e entendimento quanto ao assunto.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBUQUERQUE JUNIOR, Antonio Eduardo de; SANTOS, Ernani Marques dos. Controles e práticas de segurança da informação em um instituto de pesquisa federal. In: SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA, 8., 2011, Resende. **Anais eletrônicos...** Resende: AEDB, 2011. Disponível em: <http://www.aedb.br/seget/artigos11/3414310.pdf>. Acesso em: 13 nov. 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: tecnologia de informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005. 120 p. Disponível em: <http://www.abntcolecao.com.br>. Acesso em: 10 ago. 2012.

BEZ, Marta Rosecler. **O uso de tecnologia para apoiar a implantação de métodos ativos nos currículos de medicina**. 2011. 117 p. Proposta de Tese (Doutorado em Informática na Educação) – Programa de Pós-graduação em Informática na Educação, Centro Interdisciplinar de Novas Tecnologias na Educação, Universidade Federal do Rio Grande do Sul, UFRGS, Porto Alegre, 2011.

BRASIL. Lei Nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**, Poder Legislativo, Brasília, DF, 18 nov. 2011. Disponível em: <http://www.in.gov.br/visualiza/index.jsp?data=18/11/2011&jornal=1000&pagina=1&totalArquivos=12>. Acesso em: 03 set. 2012.

_____. Tribunal de Contas da União. **Boas práticas em segurança da informação**. 2. ed. Brasília, DF: Tribunal de Contas da União, 2007. 70 p. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2059162.PDF>. Acesso em: 02 set. 2012.

BRUEL, Mônica. **A relação entre notoriedade espontânea, intenção de comportamento e compra efetiva com a lealdade à marca**. 2009, 58 p. Monografia (Bacharelado em Administração) – Programa de Graduação em Administração, Escola de Administração, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2009. Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/19170/000734775.pdf?sequence=1>. Acesso em: 24 nov. 2012.

CARUSO, Carlos Alberto Antônio; STEFFEN, Flávio Deny. **Segurança em informática e de informações**. 2. ed. São Paulo: SENAC, 1999. 367 p.

CARVALHO, Maria Cecília Maringoni de. **Construindo o saber - metodologia científica**: fundamentos e técnicas. 6. ed. Campinas: Papirus, 1997. 175 p.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino; SILVA, Roberto da. **Metodologia científica**. 6. ed. São Paulo: Pearson Prentice Hall, 2007. 162 p.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **Gerenciamento de riscos corporativos**: estrutura integrada. [S.l.], 2007. 135 p.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books do Brasil, 2000. 218 p.

DINIZ, Flávio Luiz Ribeiro; DINIZ, Priscila Escórcio de França. **Avaliação preliminar da gestão de segurança da informação em duas organizações públicas**. 2009. 89 p. Monografia (Curso de Computação – Licenciatura), Universidade de Brasília, Brasília, DF, 2009. Disponível em: <http://monografias.cic.unb.br/dspace/bitstream/123456789/235/1/projeto_final_flavio_priscila.pdf>. Acesso em: 05 set. 2012.

FACHIN, Odília. **Fundamentos de metodologia**. 3. ed. São Paulo: Saraiva, 2001. 200 p.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Marcio Tadeu de. **Política de segurança da informação**: guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006. 177 p.

BRAGA FILHO, João Rocha. **Os dados da sua empresa estão seguros? Duvido!** Rio de janeiro: Brasport, 2004. 154 p.

FONTES, Edison Luiz Gonçalves. **Políticas e normas para a segurança da informação**: como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012. 269 p.

FREITAS, Eduardo Antônio Mello. **Gestão de riscos aplicada a sistemas de informação**: segurança estratégica da informação. 2009. 71 p. Monografia, Curso de Pós-graduação "Lato Sensu" em Gestão Estratégica e Qualidade, Universidade Cândido Mendes, Brasília, DF, 2009. Disponível em: <http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/3564/gestao_riscos_freitas.pdf?sequence=4>. Acesso em: 05 set. 2012.

IMASTERS. **Core Business - excelência em tudo ou focar no negócio principal?** Rio de Janeiro, 2009. Disponível em: <http://imasters.com.br/artigo/14501/gerencia-de-ti/core-business-excelencia-em-tudo-ou-focar-no-negocio-principal>. Acesso em: 13 nov. 2012.

INFOSEC COUNCIL. **Planejamento estratégico da segurança da informação.** São Paulo, 2010. 50 p. Disponível em: <http://www.infoseccouncil.org.br/publicacoes/201001_whitePaper_PlanejamentoPT.pdf>. Acesso em: 27 ago. 2012.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **XII censo demográfico**. Rio de Janeiro, 2010. 19 p. Disponível em: <http://www.ibge.gov.br/home/estatistica/populacao/censo2010/tabelas_pdf/total_populacao_rio_grande_do_sul.pdf>. Acesso em: 01 jun. 2013.

KÖCHE, José Carlos. **Fundamentos de metodologia científica**: teoria da ciência e iniciação à pesquisa. 20. ed. Petrópolis, RJ: Vozes, 1997. 182 p.

LEITE, Mário. **Técnicas de programação**: uma abordagem moderna. Rio de Janeiro: Brasport, 2006. 405 p.

LOPES, Anita; GARCIA, Guto. **Introdução à programação**. Rio de Janeiro: Elsevier, 2002. 469 p.

MARCIANO, João Luiz Pereira. **Segurança da informação – uma abordagem social**. 2006. 211 p. Tese (Doutorado em Ciência da Informação) – Programa de Pós-graduação em Ciência da Informação, Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília, DF, 2006. Disponível em: <http://www.enancib.ppgci.ufba.br/premio/UnB_Marciano.pdf>. Acesso em: 06 nov. 2012.

MÓDULO. **10ª pesquisa nacional de segurança da informação**. Rio de Janeiro, 2006. 18 p. Disponível em: <http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf>. Acesso em: 04 set. 2012.

NIEDERAUER, Juliano. **Desenvolvendo websites com PHP**. 2. ed. São Paulo: Novatec, 2011. 301 p.

OLIVIERO, Carlos Antonio José. **Faça um site HTML 4.0**: conceitos e aplicações. 1. ed. São Paulo: Érica, 2007. 270 p.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. Novo Hamburgo: Feevale, 2009. 288 p.

RAMALHO, José Antônio. **Javascript**: prático e rápido. 2. ed. São Paulo: Berkeley, 2000. 265 p.

REHBEIN, Airton Roberto. **Avaliação de sistemas de informação**: estudo do sistema de administração tributária da Prefeitura Municipal de Canoas/RS. 2002. 159 p. Dissertação (Mestrado Profissional em Controladoria) – Programa de Pós-graduação em Economia, Faculdade de Ciências Econômicas, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2002. Disponível em: <http://hdl.handle.net/10183/4200>. Acesso em: 04 set. 2012.

SACILOTTI, Adaní Cusin. **A importância da tecnologia da informação nas micro e pequenas empresas**: um estudo exploratório na região de Jundiaí. 2011. 116 p. Dissertação (Mestrado em Administração) – Programa de Mestrado em Administração, Faculdade Campo Limpo Paulista, Campo Limpo Paulista, 2011. Disponível em: <http://www.faccamp.br/madm/Documentos/producao_discente/2011/04abril/AdaniCusinSacilotti/a_importAncia_da_tecnologia_da_informaCAo_nas_micro_e_pequenas_empresas-um_estudo_exploratOrio_na_regiAo_de_jundiaI.pdf>. Acesso em: 07 nov. 2012.

SILVA, Maurício Samy. **Construindo sites com CSS e (X)HTML**: sites controlados por folhas de estilo em cascata. São Paulo: Novatec, 2008. 446 p.

TEOREY, Toby; LIGHTSTONE, Sam; NADEAU, Tom. **Projeto e modelagem de bancos de dados.** Rio de Janeiro: Elsevier, 2007. 276 p.

VERAS, Manoel. **Datacenter**: componente central de infraestrutura de TI. Rio de Janeiro: Brasport, 2009. 347 p.

YNEMINE, Silvana Tauhata. **Conhecendo o Javascript**. 2. ed. Florianópolis: VisualBooks, 2005. 228 p.

APÊNDICE A – *CHECKLIST*

Checklist de Avaliação de Segurança da TI em Órgãos Públicos

Este questionário será instrumento de coleta de dados para validação do trabalho de conclusão de graduação do aluno Diego Samuel Marmitt, no curso de Bacharelado em Ciência da Computação, pela Universidade FEEVALE.

A informação consolidou-se como um bem importantíssimo para as organizações, seja de natureza pública, privada, sem fins lucrativos, ONG's, etc. E como recurso precioso, é necessário que sejam tomadas medidas para protegê-las.

Diversos riscos se apresentam no mundo cada vez mais interconectado em que vivemos. Ameaças de vírus, ataques de negação de serviço, invasões, intempéries climáticas, dentre outras. Estas ameaças colocam em cheque a garantia de que os dados não serão apagados, modificados, ou até mesmo roubados.

A problemática deste trabalho apresenta a indagação de avaliar a segurança de TI em órgãos públicos da região do Vale do Rio dos Sinos, averiguando se existe a preocupação por parte dos gestores de TI no âmbito da proteção de seus sistemas, equipamentos e informações. Esta pesquisa se propõe a responder se é válida a criação de um instrumento com esse fim, por meio da análise de suas respostas. Também se espera que ela auxilie as organizações públicas a protegerem-se ainda mais, ou despertarem para esta realidade.

Obrigado pelo seu tempo e atenção!

DADOS DE IDENTIFICAÇÃO (Estes dados serão mantidos em sigilo)	
Nome completo: _____	
Cargo: _____	
Órgão: □ Prefeitura □ Câmara de Vereadores CNPJ: _____	
Cidade:_____	
QUESTÕES (Somente as caixas de seleção são obrigatórias, mas, por favor, responda todas as perguntas, apresentando os detalhes de sua infraestrutura de segurança e TI como um todo)	
Questão 1	Existe na empresa uma Política de Segurança da Informação, já implantada e em funcionamento?
Resposta →	□ Sim □ Não Observação:_____
Questão 2	Existe um Plano de Continuidade em TI, documentado e temporariamente revisado? Em caso afirmativo, especifique o intervalo de tempo entre as revisões.
Resposta →	□ Sim □ Não Observação:_____
Questão 3	Existe uma proteção contra falta de energia na empresa? Em caso afirmativo, descreva qual(is) o(s) método(s) (gerador, *no-break*, suplemento redundante, etc.).
Resposta →	□ Sim □ Não Observação:_____
Questão 4	Existe uma proteção contra falta de comunicação de dados em sua empresa? Em caso afirmativo, descreva qual(is) (links redundantes, exigência de nível de serviço (SLA) acima de 99,5%, etc.).
Resposta →	□ Sim □ Não Observação:_____
Questão 5	Existe na empresa uma Política de Backups, documentada, em execução e revisada periodicamente? Em caso afirmativo, informe a periodicidade das revisões.
Resposta →	□ Sim □ Não Observação:_____
Questão 6	Os backups de sua empresa são testados aleatoriamente para verificar sua integridade e eficiência dos *scripts* que os geram? Em caso afirmativo especifique a periodicidade dos testes e dê detalhes de como são realizados.
Resposta →	□ Sim □ Não Observação:_____

Questão 7	Sua empresa possui "sala cofre" para armazenamento de ativos importantes, inclusive mídias de backup?
Resposta →	□ Sim □ Não Observação:_____
Questão 8	Existem equipamentos de extinção de incêndios em sua empresa, inclusive na sala onde os servidores estão alocados? Em caso afirmativo, informe a categoria do extintor presente na sala de servidores.
Resposta →	□ Sim □ Não Observação:_____
Questão 9	As tomadas elétricas onde são ligados os microcomputadores de sua empresa são estabilizadas? Comente de que forma (estabilizador central, avulsos, etc.).
Resposta →	□ Sim □ Não Observação:_____
Questão 10	As tomadas de sua empresa possuem aterramento, conforme recomendações dispostas na norma ABNT NBR 5410:2004?
Resposta →	□ Sim □ Não Observação:_____
Questão 11	A manutenção dos equipamentos de sua empresa é efetuada por pessoal contratado e altamente técnico? Em caso negativo, como terceirização, explique se o processo é realizado dentro da empresa ou no ambiente do contratado.
Resposta →	□ Sim □ Não Observação:_____
Questão 12	Existe na empresa um inventário atualizado dos ativos de informação (computadores, servidores, impressoras)? Em caso afirmativo, especifique o intervalo de tempo entre as atualizações.
Resposta →	□ Sim □ Não Observação:_____
Questão 13	Existe um processo rotineiro de análise e avaliação de potenciais riscos que envolvem os recursos informacionais? Em caso afirmativo, dê detalhes quanto a periodicidade desses estudos e quais as áreas averiguadas.
Resposta →	□ Sim □ Não Observação:_____
Questão 14	Existe na empresa um Departamento específico para gestão de segurança e requisitos de proteção da informação? Em caso afirmativo, especifique a quem está subordinado.
Resposta →	□ Sim □ Não Observação:_____

Questão 15	Existe uma declaração de que, qualquer evento quanto à segurança e integridade dos equipamentos e informações, devam ser comunicados ao Departamento de Segurança ou TI? Em caso afirmativo, comunique como esse reporte é feito (formalmente, informalmente, por formulário, memorando, etc.).
Resposta →	□ Sim □ Não Observação:_____
Questão 16	Os microcomputadores de sua empresa estão instalados em salas ou locais onde o acesso de pessoas estranhas à empresa possa ser dificultado, impossibilitado ou até mesmo monitorado?
Resposta →	□ Sim □ Não Observação:_____
Questão 17	Em sua empresa existe vídeo-monitoramento? Em caso afirmativo, explique como as imagens são monitoradas/vistas (tempo real, somente quando ocorre um incidente, etc.).
Resposta →	□ Sim □ Não Observação:_____
Questão 18	A sala de servidores ou datacenter de sua empresa é protegida por algum meio de controle de acesso físico? Em caso afirmativo, descreva qual(is) (chave, biometria, fechadura inteligente, *smartcard*, retina, etc.).
Resposta →	□ Sim □ Não Observação:_____
Questão 19	Sua empresa permite o uso de microcomputadores, notebooks ou tablets, por funcionários, fora do ambiente da empresa? Em caso afirmativo, descreva se existe um documento que homologa esta decisão.
Resposta →	□ Sim □ Não Observação:_____
Questão 20	As senhas de acesso aos servidores são todas diferentes, possuem letras e números, e contém pelo menos 10 (dez) caracteres?
Resposta →	□ Sim □ Não Observação:_____
Questão 21	O acesso remoto aos servidores de sua empresa (SSH, etc.) foi bloqueado para o usuário *root*/administrador? Em caso afirmativo, explique se os usuários liberados para esse tipo de acesso possuem senhas fortes, ao mesmo estilo das senhas de usuário administrador?
Resposta →	□ Sim □ Não Observação:_____
Questão 22	Existe na empresa uma Política de Acesso aos sistemas, claramente definida e documentada, atualizada temporariamente? Em caso afirmativo, informe o período com que é revisada.
Resposta →	□ Sim □ Não Observação:_____

Questão 23	É recomendado aos usuários de sistemas de sua empresa que escolham senhas com um nível mínimo de segurança, exigindo que contenha letras e números, e com 6 (seis) caracteres pelo menos? Explique quais são as recomendações utilizadas.
Resposta →	□ Sim □ Não Observação:_____
Questão 24	Sua empresa exige que os funcionários troquem suas senhas de acesso aos sistemas regularmente? Em caso afirmativo, especifique qual(is) a(s) senha(s) e o período de tempo entre as trocas?
Resposta →	□ Sim □ Não Qual(is) sistema(s): □ Sistema operacional (*logon*) □ Aplicativos □ E-mail Observação:_____
Questão 25	A concessão de privilégios de acesso aos sistemas é controlada, analisada criticamente e seguidamente revisada? Em caso afirmativo, dê detalhes de como são autorizadas as concessões e o prazo de revisão.
Resposta →	□ Sim □ Não Observação:_____
Questão 26	É recomendado aos usuários que, ao saírem de suas estações de trabalho, bloqueiem a sessão de seu microcomputador, ou existe um bloqueio de sessão inativa que exija senha na retomada de acesso?
Resposta →	□ Sim □ Não Observação:_____
Questão 27	Existe um procedimento formal de registro e cancelamento de usuários para permitir e revogar acesso dos funcionários que entram ou deixam a empresa? Em caso afirmativo, explique como é feito o procedimento.
Resposta →	□ Sim □ Não Observação:_____
Questão 28	As pastas e arquivos compartilhados na rede de sua empresa estão sob controle de acesso como privilégios de criação/edição/exclusão?
Resposta →	□ Sim □ Não Observação:_____
Questão 29	Sua empresa utiliza limite de horário para conexão aos recursos de rede e sistemas aplicativos?
Resposta →	□ Sim □ Não Observação:_____
Questão 30	Existe uma política, norma ou procedimentos claramente definidos quando da concessão do direito de acesso remoto a usuários e pessoal de suporte? Explique o processo utilizado em sua empresa.
Resposta →	□ Sim □ Não Observação:_____

Questão 31	Sua empresa utiliza proteção antiviral em servidores e/ou microcomputadores? Em caso afirmativo, explique se é gratuita ou paga.
Resposta →	□ Sim □ Não Em qual(is) equipamento(s): □ Em servidores □ Em microcomputadores Observação:_____
Questão 32	Existe na empresa uma política quanto ao uso de mídias removíveis (pendrives, CD's/DVD's, etc.) por parte dos funcionários? Em caso afirmativo, o que ela estabelece?
Resposta →	□ Sim □ Não Observação:_____
Questão 33	A empresa utiliza recursos como *firewall* ou listas de bloqueio de tráfego? Em caso afirmativo, explique como é montada a lista de bloqueios (automática por software, manual, etc.).
Resposta →	□ Sim □ Não Observação:_____
Questão 34	Existem *logs* de acesso a sites e de transações nos aplicativos de gestão de sua empresa?
Resposta →	□ Sim □ Não Em qual(is) ambientes(s): □ De *sites* □ De sistemas aplicativos Observação:_____
Questão 35	Existe a preocupação de inutilizar quaisquer mídias e discos rígidos no momento do descarte? Em caso afirmativo, explique como é feita a inutilização e o descarte.
Resposta →	□ Sim □ Não Observação:_____
Questão 36	A administração de sua empresa entende a importância e apoia os processos de segurança? Comente e apresente detalhes em sua resposta.
Resposta →	□ Sim □ Não Observação:_____
Questão 37	No seu entendimento, a segurança mantida pela empresa é suficiente? Dê uma nota (de 0 a 10) que, em sua opinião, qualifique a segurança sobre os recursos de TI e informações de sua empresa. Comente sua resposta.
Resposta →	□ Sim □ Não Nota: _____ Observação:_____
Questão 38	Em sua opinião, você considera que existem obstáculos internos para a implementação de segurança em sua empresa? Comente sua resposta.
Resposta →	□ Sim □ Não Qual(is): □ Falta de conscientização da administração □ Falta de conscientização dos usuários □ Falta de investimento □ Falta de profissionais capacitados □ Outro(s): _____ Observação:_____

APÊNDICE B – DICIONÁRIO DE DADOS E DIAGRAMAS DA MODELAGEM PROPOSTA

Dicionário de dados:

TABELA: tb_tipo_instituicao				**FUNÇÃO:** cadastro dos tipos de instituições respondentes		
DESCRIÇÃO	**CAMPO FÍSICO**	**TIPO**	**PK**	**FK (TABELA / CAMPO)**	**RESTRIÇÕES**	**OBSERVAÇÃO**
Código do tipo	cod_tipo_instituicao	INT(11)	PK		Not Null	Auto incremento
Tipo da instituição	tipo_instituicao	VARCHAR(45)	PK		Not Null	

TABELA: tb_instituicao				**FUNÇÃO:** cadastro das instituições respondentes		
DESCRIÇÃO	**CAMPO FÍSICO**	**TIPO**	**PK**	**FK (TABELA / CAMPO)**	**RESTRIÇÕES**	**OBSERVAÇÃO**
CNPJ da instituição	cnpj_instituicao	BIGINT(14)	PK		Not Null	
Tipo da instituição	tipo	INT(11)	PK	FK (tb_tipo_instituicao / cod_tipo_instituicao)	Not Null	
Cidade do respondente	cidade	VARCHAR(45)			Not Null	
Nome do respondente	nome_respondente	VARCHAR(45)			Not Null	
Cargo do respondente	cargo_respondente	VARCHAR(45)			Not Null	

TABELA: tb_perguntas				**FUNÇÃO:** cadastro das perguntas do checklist		
DESCRIÇÃO	**CAMPO FÍSICO**	**TIPO**	**PK**	**FK (TABELA / CAMPO)**	**RESTRIÇÕES**	**OBSERVAÇÃO**
Código da pergunta	cod_pergunta	INT(11)	PK		Not Null	Auto incremento
Pergunta	pergunta	TEXT			Not Null	
Sub-pergunta	pergunta_opcao	VARCHAR(45)				
Opção 1	opcao1	VARCHAR(45)				
Opção 2	opcao2	VARCHAR(45)				
Opção 3	opcao3	VARCHAR(45)				
Opção 4	opcao4	VARCHAR(45)				
Opção 5	opcao5	VARCHAR(45)				

TABELA: tb_respostas				**FUNÇÃO:** armazenar as respostas colhidas na pesquisa		
DESCRIÇÃO	**CAMPO FÍSICO**	**TIPO**	**PK**	**FK (TABELA / CAMPO)**	**RESTRIÇÕES**	**OBSERVAÇÃO**
CNPJ da instituição	cnpj_instituicao	BIGINT(14)	PK	FK (tb_instituicao / cnpj_instituicao)	Not Null	
Tipo da instituição	tipo	INT(11)	PK	FK (tb_instituicao / tipo)	Not Null	
Código da pergunta	cod_pergunta	INT(11)	PK	FK (tb_perguntas / cod_pergunta)	Not Null	
Resposta	resposta	TINYINT(4)			Not Null	
Resposta da Opção 1	resp_opcao1	TINYINT(4)				
Resposta da Opção 2	resp_opcao2	TINYINT(4)				
Resposta da Opção 3	resp_opcao3	TINYINT(4)				
Resposta da Opção 4	resp_opcao4	TINYINT(4)				
Resposta da Opção 5	resp_opcao5	TINYINT(4)				
Observação	observacao	TEXT				

TABELA: tb_usuarios				**FUNÇÃO:** cadastro dos usuários administradores do sistema		
DESCRIÇÃO	**CAMPO FÍSICO**	**TIPO**	**PK**	**FK (TABELA / CAMPO)**	**RESTRIÇÕES**	**OBSERVAÇÃO**
Nome de usuário	usuario	VARCHAR(20)	PK		Not Null	
Senha do usuário	senha	VARCHAR(15)			Not Null	

Diagrama de casos de uso:

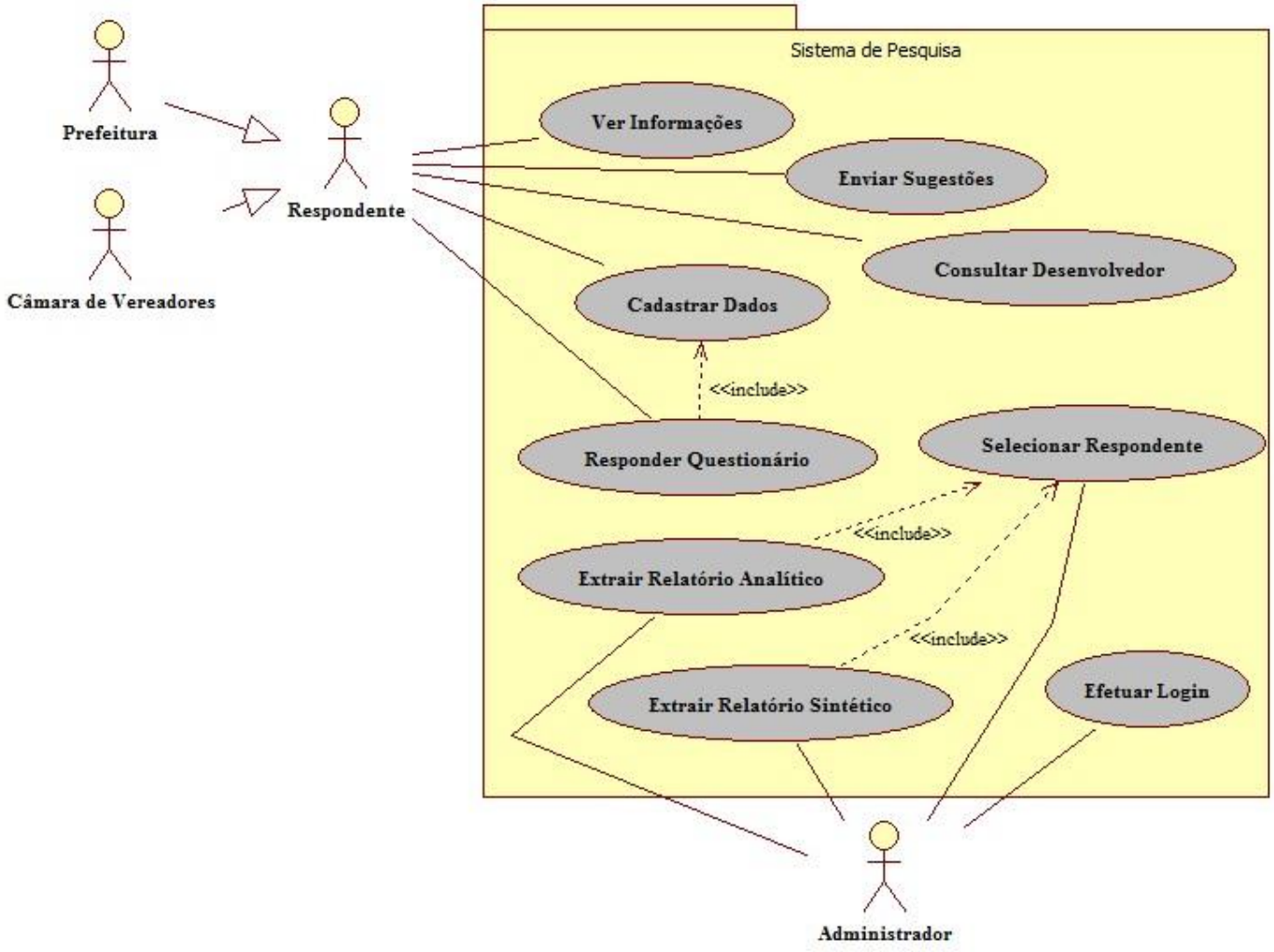


Diagrama de classes:

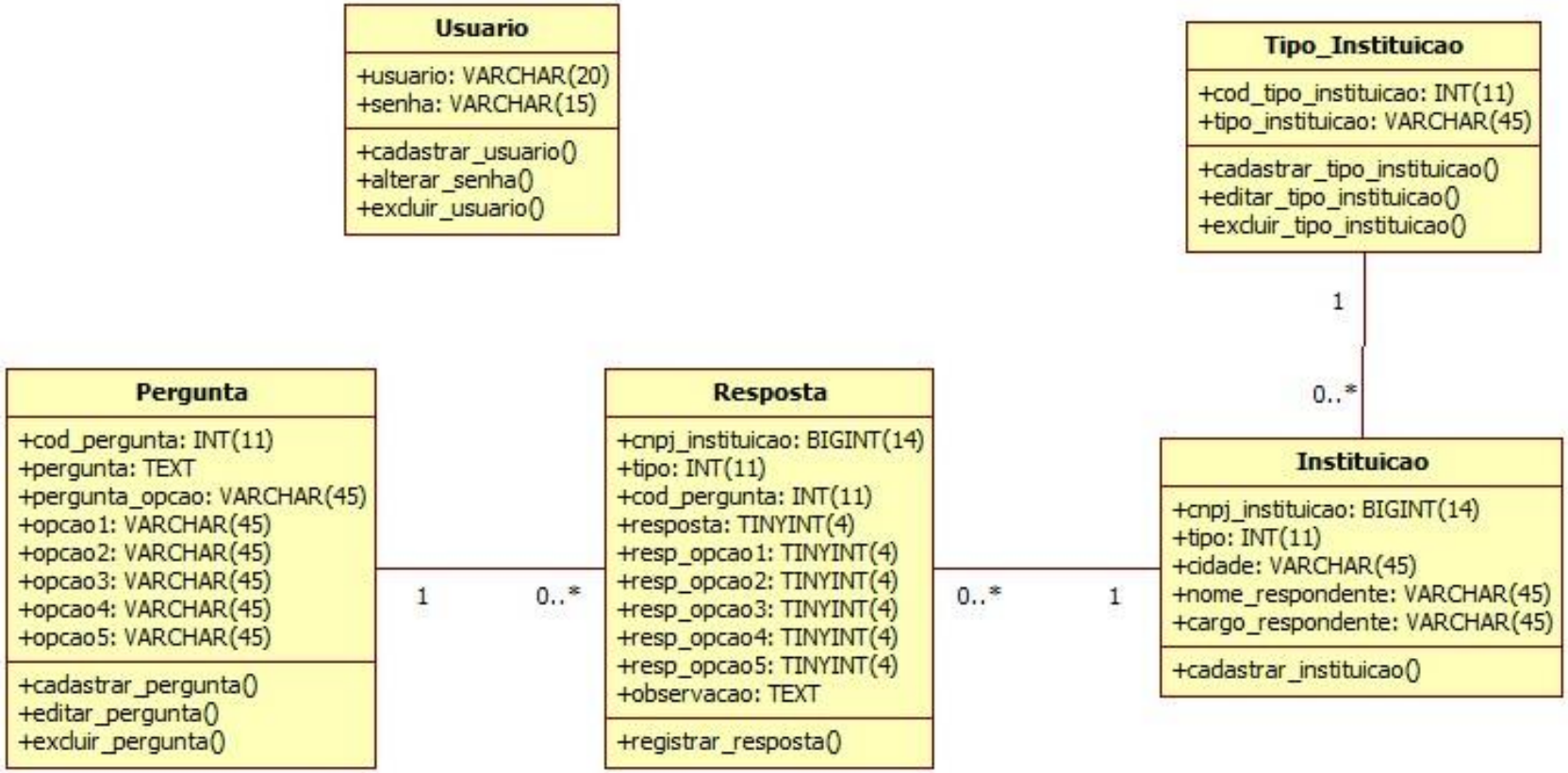
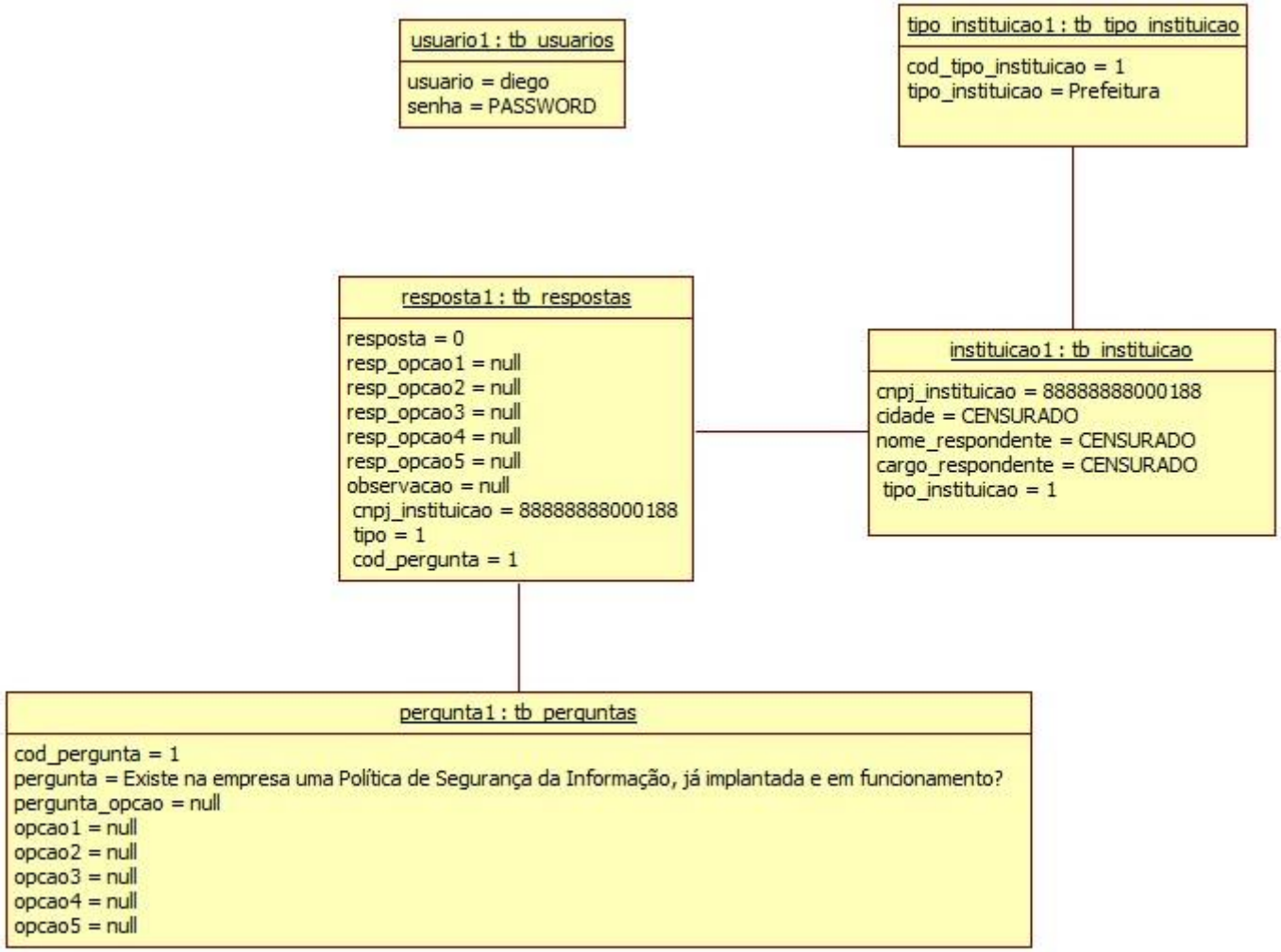


Diagrama de objetos (exemplo com uma pergunta e uma resposta):



APÊNDICE C – RESPOSTAS DA PESQUISA

Respondente 1:

Pesquisa de Segurança em TI

RELATÓRIO ANALÍTICO

DADOS DA EMPRESA

Cidade	##########
Tipo	Prefeitura
CNPJ	##.###.###/####-##
Nome Respondente	##########
Cargo Respondente	##########

Pergunta 1

Existe na empresa uma Política de Segurança da Informação, já implantada e em funcionamento?

Resposta Não

Observação

Não preenchido.

Pergunta 2

Existe um Plano de Continuidade em TI, documentado e temporariamente revisado? Em caso afirmativo, especifique o intervalo de tempo entre as revisões.

Resposta Não

Observação

Não preenchido.

Pergunta 3

Existe uma proteção contra falta de energia na empresa? Em caso afirmativo, descreva qual(is) o(s) método(s) (gerador, no-break, suplemento redundante, etc.).

Resposta Sim

Observação

No-break somente para os servidores.

Pergunta 4

Existe uma proteção contra falta de comunicação de dados em sua empresa? Em caso afirmativo, descreva qual(is) (links redundantes, exigência de nível de serviço (SLA) acima de 99,5%, etc.).

Resposta Não

Observação

Não preenchido.

Pergunta 5

Existe na empresa uma Política de Backups, documentada, em execução e revisada periodicamente? Em caso afirmativo, informe a periodicidade das revisões.

Resposta Não

Observação

Não preenchido.

Pergunta 6

Os backups de sua empresa são testados aleatoriamente para verificar sua integridade e eficiência dos scripts que os geram? Em caso afirmativo especifique a periodicidade dos testes e dê detalhes de como são realizados.

Resposta Sim

Observação

Backups sofrem testes de importação para verificar a integridade dos dados. Testes efetuados mensalmente.

Pergunta 7

Sua empresa possui “sala cofre” para armazenamento de ativos importantes, inclusive mídias de backup?

Resposta Sim

Observação

Não preenchido.

Pergunta 8

Existem equipamentos de extinção de incêndios em sua empresa, inclusive na sala onde os servidores estão alocados? Em caso afirmativo, informe a categoria do extintor presente na sala de servidores.

Resposta Não

Observação

Não preenchido.

Pergunta 9

As tomadas elétricas onde são ligados os microcomputadores de sua empresa são estabilizadas? Comente de que forma (estabilizador central, avulsos, etc.).

Resposta Sim

Observação

Não preenchido.

Pergunta 10

As tomadas de sua empresa possuem aterramento, conforme recomendações dispostas na norma ABNT NBR 5410:2004?

Resposta Não

Observação

Não preenchido.

Pergunta 11

A manutenção dos equipamentos de sua empresa é efetuada por pessoal contratado e altamente técnico? Em caso negativo, como terceirização, explique se o processo é realizado dentro da empresa ou no ambiente do contratado.

Resposta Sim

Observação

Manutenção é efetuada no ambiente da empresa.

Pergunta 12

Existe na empresa um inventário atualizado dos ativos de informação (computadores, servidores, impressoras)? Em caso afirmativo, especifique o intervalo de tempo entre as atualizações.

Resposta Sim

Observação

Levantamento efetuado pelo Departamento de Patrimônio, atualizado anualmente.

Pergunta 13

Existe um processo rotineiro de análise e avaliação de potenciais riscos que envolvem os recursos informacionais? Em caso afirmativo, dê detalhes quanto a periodicidade desses estudos e quais as áreas averiguadas.

Resposta Não

Observação

Não preenchido.

Pergunta 14

Existe na empresa um Departamento específico para gestão de segurança e requisitos de proteção da informação? Em caso afirmativo, especifique a quem está subordinado.

Resposta Não

Observação

Não preenchido.

Pergunta 15

Existe uma declaração de que, qualquer evento quanto à segurança e integridade dos equipamentos e informações, devam ser comunicados ao Departamento de Segurança ou TI? Em caso afirmativo, comunique como esse reporte é feito (formalmente, informalmente, por formulário, memorando, etc.).

Resposta Não

Observação

Não preenchido.

Pergunta 16

Os microcomputadores de sua empresa estão instalados em salas ou locais onde o acesso de pessoas estranhas à empresa possa ser dificultado, impossibilitado ou até mesmo monitorado?

Resposta Não

Observação

Não preenchido.

Pergunta 17

Em sua empresa existe vídeo-monitoramento? Em caso afirmativo, explique como as imagens são monitoradas/vistas (tempo real, somente quando ocorre um incidente, etc.).

Resposta Sim

Observação

Uma câmera em uma das entradas de acesso secundário. As imagens são analisadas somente quando ocorre algum fato ou incidente.

Pergunta 18

A sala de servidores ou datacenter de sua empresa é protegida por algum meio de controle de acesso físico? Em caso afirmativo, descreva qual(is) (chave, biometria, fechadura inteligente, smartcard, retina, etc.).

Resposta Sim

Observação

Chave.

Pergunta 19

Sua empresa permite o uso de microcomputadores, notebooks ou tablets, por funcionários, fora do ambiente da empresa? Em caso afirmativo, descreva se existe um documento que homologa esta decisão.

Resposta Sim

Observação

Determinados funcionários podem utilizar, mas não há um documento que homologue esta decisão.

Pergunta 20

As senhas de acesso aos servidores são todas diferentes, possuem letras e números, e contém pelo menos 10 (dez) caracteres?

Resposta Não

Observação

Possuem mais de 10 caracteres, mas não são todas diferentes.

Pergunta 21

O acesso remoto aos servidores de sua empresa (SSH, etc.) foi bloqueado para o usuário root/administrador? Em caso afirmativo, explique se os usuários liberados para esse tipo de acesso possuem senhas fortes, ao mesmo estilo das senhas de usuário administrador?

Resposta Sim

Observação

Usuários administradores foram bloqueados para acesso externo às dependências da empresa.

Pergunta 22

Existe na empresa uma Política de Acesso aos sistemas, claramente definida e documentada, atualizada temporariamente? Em caso afirmativo, informe o período com que é revisada.

Resposta Não

Observação

Não preenchido.

Pergunta 23

É recomendado aos usuários de sistemas de sua empresa que escolham senhas com um nível mínimo de segurança, exigindo que contenha letras e números, e com 6 (seis) caracteres pelo menos? Explique quais são as recomendações utilizadas.

Resposta Sim

Observação

É recomendado. Porém, alguns sistemas de gestão possuem exigências próprias, não atendendo estas recomendações (exemplo: menos de 6 caracteres).

Pergunta 24

Sua empresa exige que os funcionários troquem suas senhas de acesso aos sistemas regularmente? Em caso afirmativo, especifique qual(is) a(s) senha(s) e o período de tempo entre as trocas?

Resposta Não

Qual(is) sistema(s):

Opção 1	Sistema operacional (logon)	Não
Opção 2	Aplicativos	Não
Opção 3	E-mail	Não

Observação

Não preenchido.

Pergunta 25

A concessão de privilégios de acesso aos sistemas é controlada, analisada criticamente e seguidamente revisada? Em caso afirmativo, dê detalhes de como são autorizadas as concessões e o prazo de revisão.

Resposta Sim

Observação

Permissões de acesso aos sistemas são definidas pelo Departamento de Informática conjuntamente com o Departamento ao qual o funcionário está vinculado.

Pergunta 26

É recomendado aos usuários que, ao saírem de suas estações de trabalho, bloqueiem a sessão de seu microcomputador, ou existe um bloqueio de sessão inativa que exija senha na retomada de acesso?

Resposta Não

Observação

Não preenchido.

Pergunta 27

Existe um procedimento formal de registro e cancelamento de usuários para permitir e revogar acesso dos funcionários que entram ou deixam a empresa? Em caso afirmativo, explique como é feito o procedimento.

Resposta Não

Observação

Não preenchido.

Pergunta 28

As pastas e arquivos compartilhados na rede de sua empresa estão sob controle de acesso como privilégios de criação/edição/exclusão?

Resposta Não

Observação

Não preenchido.

Pergunta 29

Sua empresa utiliza limite de horário para conexão aos recursos de rede e sistemas aplicativos?

Resposta Não

Observação

Não preenchido.

Pergunta 30

Existe uma política, norma ou procedimentos claramente definidos quando da concessão do direito de acesso remoto a usuários e pessoal de suporte? Explique o processo utilizado em sua empresa.

Resposta Não

Observação

As empresas terceiras possuem acesso com usuários próprios.

Pergunta 31

Sua empresa utiliza proteção antiviral em servidores e/ou microcomputadores? Em caso afirmativo, explique se é gratuita ou paga.

Resposta Sim

Em qual(is) equipamento(s):

Opção 1	Em servidores	Não
Opção 2	Em microcomputadores	Sim

Observação

Antivírus gratuito.

Pergunta 32

Existe na empresa uma política quanto ao uso de mídias removíveis (pendrives, CD's/DVD's, etc.) por parte dos funcionários? Em caso afirmativo, o que ela estabelece?

Resposta Não

Observação

Uso é permitido, sem restrições.

Pergunta 33

A empresa utiliza recursos como firewall ou listas de bloqueio de tráfego? Em caso afirmativo, explique como é montada a lista de bloqueios (automática por software, manual, etc.).

Resposta Sim

Observação

Existe um firewall configurado, com lista de bloqueios por palavras. As palavras são introduzidas na lista manualmente. Há ainda uma lista de IP's com acesso irrestrito. Os demais passam pela filtragem da lista.

Pergunta 34

Existem logs de acesso a sites e de transações nos aplicativos de gestão de sua empresa?

Resposta Sim

Em qual(is) ambiente(s):

Opção 1	De sites	Sim
Opção 2	De sistemas aplicativos	Sim

Observação

Não preenchido.

Pergunta 35

Existe a preocupação de inutilizar quaisquer mídias e discos rígidos no momento do descarte? Em caso afirmativo, explique como é feita a inutilização e o descarte.

Resposta Sim

Observação

Os discos são removidos das máquinas antes do descarte das mesmas. Os HD's são armazenados para futura destruição.

Pergunta 36

A administração de sua empresa entende a importância e apoia os processos de segurança? Comente e apresente detalhes em sua resposta.

Resposta Não

Observação

Não existe essa preocupação por parte da administração. As diretrizes de segurança, ainda que básicas, são designadas totalmente ao pessoal de TI.

Pergunta 37

No seu entendimento, a segurança mantida pela empresa é suficiente? Dê uma nota (de 0 a 10) que, em sua opinião, qualifique a segurança sobre os recursos de TI e informações de sua empresa. Comente sua resposta.

Resposta Não

Observação

Nota: 4. Com as perguntas deste questionário pode-se notar que a segurança é demasiadamente básica. Novos instrumentos devem ser implantados para melhoria.

Pergunta 38

Em sua opinião, você considera que existem obstáculos internos para a implementação de segurança em sua empresa? Comente sua resposta.

Resposta Sim

Qual(is):

Opção 1	Falta de conscientização da administração	Sim
Opção 2	Falta de conscientização dos usuários	Sim
Opção 3	Falta de investimento	Sim
Opção 4	Falta de profissionais capacitados	Sim
Opção 5	Outro(s):	Não

Observação

Não preenchido.

Respondente 2:

Pesquisa de Segurança em TI

RELATÓRIO ANALÍTICO

DADOS DA EMPRESA

Cidade	##########
Tipo	Prefeitura
CNPJ	##.###.###/####-##
Nome Respondente	##########
Cargo Respondente	##########

Pergunta 1

Existe na empresa uma Política de Segurança da Informação, já implantada e em funcionamento?

Resposta Sim

Observação

Não preenchido.

Pergunta 2

Existe um Plano de Continuidade em TI, documentado e temporariamente revisado? Em caso afirmativo, especifique o intervalo de tempo entre as revisões.

Resposta Não

Observação

Em implementacao.

Pergunta 3

Existe uma proteção contra falta de energia na empresa? Em caso afirmativo, descreva qual(is) o(s) método(s) (gerador, no-break, suplemento redundante, etc.).

Resposta Sim

Observação

Nobreak.

Pergunta 4

Existe uma proteção contra falta de comunicação de dados em sua empresa? Em caso afirmativo, descreva qual(is) (links redundantes, exigência de nível de serviço (SLA) acima de 99,5%, etc.).

Resposta Sim

Observação

Link redundante.

Pergunta 5

Existe na empresa uma Política de Backups, documentada, em execução e revisada periodicamente? Em caso afirmativo, informe a periodicidade das revisões.

Resposta Sim

Observação

Revisada mensal.

Pergunta 6

Os backups de sua empresa são testados aleatoriamente para verificar sua integridade e eficiência dos scripts que os geram? Em caso afirmativo especifique a periodicidade dos testes e dê detalhes de como são realizados.

Resposta Não

Observação

Não preenchido.

Pergunta 7

Sua empresa possui “sala cofre” para armazenamento de ativos importantes, inclusive mídias de backup?

Resposta Não

Observação

Não preenchido.

Pergunta 8

Existem equipamentos de extinção de incêndios em sua empresa, inclusive na sala onde os servidores estão alocados? Em caso afirmativo, informe a categoria do extintor presente na sala de servidores.

Resposta Sim

Observação

Não preenchido.

Pergunta 9

As tomadas elétricas onde são ligados os microcomputadores de sua empresa são estabilizadas? Comente de que forma (estabilizador central, avulsos, etc.).

Resposta Sim

Observação

Estabilizador central.

Pergunta 10

As tomadas de sua empresa possuem aterramento, conforme recomendações dispostas na norma ABNT NBR 5410:2004?

Resposta Sim

Observação

Não preenchido.

Pergunta 11

A manutenção dos equipamentos de sua empresa é efetuada por pessoal contratado e altamente técnico? Em caso negativo, como terceirização, explique se o processo é realizado dentro da empresa ou no ambiente do contratado.

Resposta Sim

Observação

Não preenchido.

Pergunta 12

Existe na empresa um inventário atualizado dos ativos de informação (computadores, servidores, impressoras)? Em caso afirmativo, especifique o intervalo de tempo entre as atualizações.

Resposta Sim

Observação

Efetuado pelo setor de patrimonio.

Pergunta 13

Existe um processo rotineiro de análise e avaliação de potenciais riscos que envolvem os recursos informacionais? Em caso afirmativo, dê detalhes quanto a periodicidade desses estudos e quais as áreas averiguadas.

Resposta Não

Observação

Não preenchido.

Pergunta 14

Existe na empresa um Departamento específico para gestão de segurança e requisitos de proteção da informação? Em caso afirmativo, especifique a quem está subordinado.

Resposta Não

Observação

Não preenchido.

Pergunta 15

Existe uma declaração de que, qualquer evento quanto à segurança e integridade dos equipamentos e informações, devam ser comunicados ao Departamento de Segurança ou TI? Em caso afirmativo, comunique como esse reporte é feito (formalmente, informalmente, por formulário, memorando, etc.).

Resposta Não

Observação

Não preenchido.

Pergunta 16

Os microcomputadores de sua empresa estão instalados em salas ou locais onde o acesso de pessoas estranhas à empresa possa ser dificultado, impossibilitado ou até mesmo monitorado?

Resposta Sim

Observação

Não preenchido.

Pergunta 17

Em sua empresa existe vídeo-monitoramento? Em caso afirmativo, explique como as imagens são monitoradas/vistas (tempo real, somente quando ocorre um incidente, etc.).

Resposta Não

Observação

Não preenchido.

Pergunta 18

A sala de servidores ou datacenter de sua empresa é protegida por algum meio de controle de acesso físico? Em caso afirmativo, descreva qual(is) (chave, biometria, fechadura inteligente, smartcard, retina, etc.).

Resposta Sim

Observação

chave

Pergunta 19

Sua empresa permite o uso de microcomputadores, notebooks ou tablets, por funcionários, fora do ambiente da empresa? Em caso afirmativo, descreva se existe um documento que homologa esta decisão.

Resposta Não

Observação

Não preenchido.

Pergunta 20

As senhas de acesso aos servidores são todas diferentes, possuem letras e números, e contém pelo menos 10 (dez) caracteres?

Resposta Sim

Observação

Não preenchido.

Pergunta 21

O acesso remoto aos servidores de sua empresa (SSH, etc.) foi bloqueado para o usuário root/administrador? Em caso afirmativo, explique se os usuários liberados para esse tipo de acesso possuem senhas fortes, ao mesmo estilo das senhas de usuário administrador?

Resposta Sim

Observação

Não preenchido.

Pergunta 22

Existe na empresa uma Política de Acesso aos sistemas, claramente definida e documentada, atualizada temporariamente? Em caso afirmativo, informe o período com que é revisada.

Resposta Não

Observação

Não preenchido.

Pergunta 23

É recomendado aos usuários de sistemas de sua empresa que escolham senhas com um nível mínimo de segurança, exigindo que contenha letras e números, e com 6 (seis) caracteres pelo menos? Explique quais são as recomendações utilizadas.

Resposta Sim

Observação

Não preenchido.

Pergunta 24

Sua empresa exige que os funcionários troquem suas senhas de acesso aos sistemas regularmente? Em caso afirmativo, especifique qual(is) a(s) senha(s) e o período de tempo entre as trocas?

Resposta Não

Qual(is) sistema(s):

Opção 1	Sistema operacional (logon)	Não
Opção 2	Aplicativos	Não
Opção 3	E-mail	Não

Observação

Não preenchido.

Pergunta 25

A concessão de privilégios de acesso aos sistemas é controlada, analisada criticamente e seguidamente revisada? Em caso afirmativo, dê detalhes de como são autorizadas as concessões e o prazo de revisão.

Resposta Não

Observação

Não preenchido.

Pergunta 26

É recomendado aos usuários que, ao saírem de suas estações de trabalho, bloqueiem a sessão de seu microcomputador, ou existe um bloqueio de sessão inativa que exija senha na retomada de acesso?

Resposta Sim

Observação

Não preenchido.

Pergunta 27

Existe um procedimento formal de registro e cancelamento de usuários para permitir e revogar acesso dos funcionários que entram ou deixam a empresa? Em caso afirmativo, explique como é feito o procedimento.

Resposta Sim

Observação

Não preenchido.

Pergunta 28

As pastas e arquivos compartilhados na rede de sua empresa estão sob controle de acesso como privilégios de criação/edição/exclusão?

Resposta Sim

Observação

Não preenchido.

Pergunta 29

Sua empresa utiliza limite de horário para conexão aos recursos de rede e sistemas aplicativos?

Resposta Não

Observação

Não preenchido.

Pergunta 30

Existe uma política, norma ou procedimentos claramente definidos quando da concessão do direito de acesso remoto a usuários e pessoal de suporte? Explique o processo utilizado em sua empresa.

Resposta Não

Observação

Não preenchido.

Pergunta 31

Sua empresa utiliza proteção antiviral em servidores e/ou microcomputadores? Em caso afirmativo, explique se é gratuita ou paga.

Resposta Sim

Em qual(is) equipamento(s):

Opção 1 Em servidores Sim

Opção 2 Em microcomputadores Sim

Observação

paga

Pergunta 32

Existe na empresa uma política quanto ao uso de mídias removíveis (pendrives, CD's/DVD's, etc.) por parte dos funcionários? Em caso afirmativo, o que ela estabelece?

Resposta Não

Observação

Não preenchido.

Pergunta 33

A empresa utiliza recursos como firewall ou listas de bloqueio de tráfego? Em caso afirmativo, explique como é montada a lista de bloqueios (automática por software, manual, etc.).

Resposta Sim

Observação

Não preenchido.

Pergunta 34

Existem logs de acesso a sites e de transações nos aplicativos de gestão de sua empresa?

Resposta Não

Em qual(is) ambiente(s):

Opção 1 De sites Não

Opção 2 De sistemas aplicativos Não

Observação

Não preenchido.

Pergunta 35

Existe a preocupação de inutilizar quaisquer mídias e discos rígidos no momento do descarte? Em caso afirmativo, explique como é feita a inutilização e o descarte.

Resposta Não

Observação

Não preenchido.

Pergunta 36

A administração de sua empresa entende a importância e apoia os processos de segurança? Comente e apresente detalhes em sua resposta.

Resposta Sim

Observação

Não preenchido.

Pergunta 37

No seu entendimento, a segurança mantida pela empresa é suficiente? Dê uma nota (de 0 a 10) que, em sua opinião, qualifique a segurança sobre os recursos de TI e informações de sua empresa. Comente sua resposta.

Resposta Sim

Observação

Não preenchido.

Pergunta 38

Em sua opinião, você considera que existem obstáculos internos para a implementação de segurança em sua empresa? Comente sua resposta.

Resposta Não

Qual(is):

Opção 1	Falta de conscientização da administração	Não
Opção 2	Falta de conscientização dos usuários	Não
Opção 3	Falta de investimento	Não
Opção 4	Falta de profissionais capacitados	Não
Opção 5	Outro(s):	Não

Observação

Não preenchido.

Respondente 3:

Pesquisa de Segurança em TI

RELATÓRIO ANALÍTICO

DADOS DA EMPRESA

Cidade	##########
Tipo	Prefeitura
CNPJ	##.###.###/####-##
Nome Respondente	##########
Cargo Respondente	##########

Pergunta 1

Existe na empresa uma Política de Segurança da Informação, já implantada e em funcionamento?

Resposta Sim

Observação

Não preenchido.

Pergunta 2

Existe um Plano de Continuidade em TI, documentado e temporariamente revisado? Em caso afirmativo, especifique o intervalo de tempo entre as revisões.

Resposta Não

Observação

Não preenchido.

Pergunta 3

Existe uma proteção contra falta de energia na empresa? Em caso afirmativo, descreva qual(is) o(s) método(s) (gerador, no-break, suplemento redundante, etc.).

Resposta Sim

Observação

No-break, em fase de estudos um gerador de energia.

Pergunta 4

Existe uma proteção contra falta de comunicação de dados em sua empresa? Em caso afirmativo, descreva qual(is) (links redundantes, exigência de nível de serviço (SLA) acima de 99,5%, etc.).

Resposta Sim

Observação

Link redundante.

Pergunta 5

Existe na empresa uma Política de Backups, documentada, em execução e revisada periodicamente? Em caso afirmativo, informe a periodicidade das revisões.

Resposta Sim

Observação

Revisionada mensalmente.

Pergunta 6

Os backups de sua empresa são testados aleatoriamente para verificar sua integridade e eficiência dos scripts que os geram? Em caso afirmativo especifique a periodicidade dos testes e dê detalhes de como são realizados.

Resposta Sim

Observação

São revisados semanalmente, ou quando necessário.

Pergunta 7

Sua empresa possui “sala cofre” para armazenamento de ativos importantes, inclusive mídias de backup?

Resposta Não

Observação

Não preenchido.

Pergunta 8

Existem equipamentos de extinção de incêndios em sua empresa, inclusive na sala onde os servidores estão alocados? Em caso afirmativo, informe a categoria do extintor presente na sala de servidores.

Resposta Não

Observação

Não preenchido.

Pergunta 9

As tomadas elétricas onde são ligados os microcomputadores de sua empresa são estabilizadas? Comente de que forma (estabilizador central, avulsos, etc.).

Resposta Não

Observação

Não preenchido.

Pergunta 10

As tomadas de sua empresa possuem aterramento, conforme recomendações dispostas na norma ABNT NBR 5410:2004?

Resposta Sim

Observação

Não preenchido.

Pergunta 11

A manutenção dos equipamentos de sua empresa é efetuada por pessoal contratado e altamente técnico? Em caso negativo, como terceirização, explique se o processo é realizado dentro da empresa ou no ambiente do contratado.

Resposta Sim

Observação

Não preenchido.

Pergunta 12

Existe na empresa um inventário atualizado dos ativos de informação (computadores, servidores, impressoras)? Em caso afirmativo, especifique o intervalo de tempo entre as atualizações.

Resposta Sim

Observação

Setor de patrimônio é quem gerencia.

Pergunta 13

Existe um processo rotineiro de análise e avaliação de potenciais riscos que envolvem os recursos informacionais? Em caso afirmativo, dê detalhes quanto a periodicidade desses estudos e quais as áreas averiguadas.

Resposta Sim

Observação

Trimestralmente. Análise contra invasores.

Pergunta 14

Existe na empresa um Departamento específico para gestão de segurança e requisitos de proteção da informação? Em caso afirmativo, especifique a quem está subordinado.

Resposta Não

Observação

Não preenchido.

Pergunta 15

Existe uma declaração de que, qualquer evento quanto à segurança e integridade dos equipamentos e informações, devam ser comunicados ao Departamento de Segurança ou TI? Em caso afirmativo, comunique como esse reporte é feito (formalmente, informalmente, por formulário, memorando, etc.).

Resposta Sim

Observação

Formalmente.

Pergunta 16

Os microcomputadores de sua empresa estão instalados em salas ou locais onde o acesso de pessoas estranhas à empresa possa ser dificultado, impossibilitado ou até mesmo monitorado?

Resposta Sim

Observação

Não preenchido.

Pergunta 17

Em sua empresa existe vídeo-monitoramento? Em caso afirmativo, explique como as imagens são monitoradas/vistas (tempo real, somente quando ocorre um incidente, etc.).

Resposta Não

Observação

Não preenchido.

Pergunta 18

A sala de servidores ou datacenter de sua empresa é protegida por algum meio de controle de acesso físico? Em caso afirmativo, descreva qual(is) (chave, biometria, fechadura inteligente, smartcard, retina, etc.).

Resposta Sim

Observação

Chave.

Pergunta 19

Sua empresa permite o uso de microcomputadores, notebooks ou tablets, por funcionários, fora do ambiente da empresa? Em caso afirmativo, descreva se existe um documento que homologa esta decisão.

Resposta Não

Observação

Não preenchido.

Pergunta 20

As senhas de acesso aos servidores são todas diferentes, possuem letras e números, e contém pelo menos 10 (dez) caracteres?

Resposta Sim

Observação

Não preenchido.

Pergunta 21

O acesso remoto aos servidores de sua empresa (SSH, etc.) foi bloqueado para o usuário root/administrador? Em caso afirmativo, explique se os usuários liberados para esse tipo de acesso possuem senhas fortes, ao mesmo estilo das senhas de usuário administrador?

Resposta Não

Observação

Somente o administrador possui essas senhas.

Pergunta 22

Existe na empresa uma Política de Acesso aos sistemas, claramente definida e documentada, atualizada temporariamente? Em caso afirmativo, informe o período com que é revisada.

Resposta Não

Observação

Não preenchido.

Pergunta 23

É recomendado aos usuários de sistemas de sua empresa que escolham senhas com um nível mínimo de segurança, exigindo que contenha letras e números, e com 6 (seis) caracteres pelo menos? Explique quais são as recomendações utilizadas.

Resposta Sim

Observação

No mínimo 6 caracteres e alternando letras e números pelo menos.

Pergunta 24

Sua empresa exige que os funcionários troquem suas senhas de acesso aos sistemas regularmente? Em caso afirmativo, especifique qual(is) a(s) senha(s) e o período de tempo entre as trocas?

Resposta Não

Qual(is) sistema(s):

Opção 1	Sistema operacional (logon)	Não
Opção 2	Aplicativos	Não
Opção 3	E-mail	Não

Observação

Não preenchido.

Pergunta 25

A concessão de privilégios de acesso aos sistemas é controlada, analisada criticamente e seguidamente revisada? Em caso afirmativo, dê detalhes de como são autorizadas as concessões e o prazo de revisão.

Resposta Sim

Observação

São analisadas pelo Dpto de TI juntamante com Secretária da pasta do funcionário. Só são revisadas quando usuário troca de setor/cargo.

Pergunta 26

É recomendado aos usuários que, ao saírem de suas estações de trabalho, bloqueiem a sessão de seu microcomputador, ou existe um bloqueio de sessão inativa que exija senha na retomada de acesso?

Resposta Sim

Observação

Não preenchido.

Pergunta 27

Existe um procedimento formal de registro e cancelamento de usuários para permitir e revogar acesso dos funcionários que entram ou deixam a empresa? Em caso afirmativo, explique como é feito o procedimento.

Resposta Não

Observação

Não preenchido.

Pergunta 28

As pastas e arquivos compartilhados na rede de sua empresa estão sob controle de acesso como privilégios de criação/edição/exclusão?

Resposta Sim

Observação

Não preenchido.

Pergunta 29

Sua empresa utiliza limite de horário para conexão aos recursos de rede e sistemas aplicativos?

Resposta Não

Observação

Não preenchido.

Pergunta 30

Existe uma política, norma ou procedimentos claramente definidos quando da concessão do direito de acesso remoto a usuários e pessoal de suporte? Explique o processo utilizado em sua empresa.

Resposta Não

Observação

Não preenchido.

Pergunta 31

Sua empresa utiliza proteção antiviral em servidores e/ou microcomputadores? Em caso afirmativo, explique se é gratuita ou paga.

Resposta Sim

Em qual(is) equipamento(s):

Opção 1	Em servidores	Sim
Opção 2	Em microcomputadores	Sim

Observação

Solução paga.

Pergunta 32

Existe na empresa uma política quanto ao uso de mídias removíveis (pendrives, CD's/DVD's, etc.) por parte dos funcionários? Em caso afirmativo, o que ela estabelece?

Resposta Não

Observação

Não preenchido.

Pergunta 33

A empresa utiliza recursos como firewall ou listas de bloqueio de tráfego? Em caso afirmativo, explique como é montada a lista de bloqueios (automática por software, manual, etc.).

Resposta Sim

Observação

Manual.

Pergunta 34

Existem logs de acesso a sites e de transações nos aplicativos de gestão de sua empresa?

Resposta Sim

Em qual(is) ambiente(s):

Opção 1	De sites	Sim
Opção 2	De sistemas aplicativos	Não

Observação

Não preenchido.

Pergunta 35

Existe a preocupação de inutilizar quaisquer mídias e discos rígidos no momento do descarte? Em caso afirmativo, explique como é feita a inutilização e o descarte.

Resposta Sim

Observação

Desmontagem e avarias nas mídias.

Pergunta 36

A administração de sua empresa entende a importância e apoia os processos de segurança? Comente e apresente detalhes em sua resposta.

Resposta Sim

Observação

Sempre que alguma alteração e ou investimento nessa área, é necessário a apresentação de um estudo, formal ou informalmente. Contemplando os benefícios e gastos do mesmo.

Pergunta 37

No seu entendimento, a segurança mantida pela empresa é suficiente? Dê uma nota (de 0 a 10) que, em sua opinião, qualifique a segurança sobre os recursos de TI e informações de sua empresa. Comente sua resposta.

Resposta Sim

Observação

A área de TI, possui mudanças e atualizações quase que diárias. Com essa quadro a segurança pode nunca estar em 100%, mas o trabalho e pesquisa é quase que diário em busca de uma segurança eficiente.

Pergunta 38

Em sua opinião, você considera que existem obstáculos internos para a implementação de segurança em sua empresa? Comente sua resposta.

Resposta Sim

Qual(is):

Opção 1	Falta de conscientização da administração	Não
Opção 2	Falta de conscientização dos usuários	Sim
Opção 3	Falta de investimento	Não
Opção 4	Falta de profissionais capacitados	Não
Opção 5	Outro(s):	Não

Observação

Não preenchido.