UNIVERSIDADE FEDERAL DE SANTA MARIA
COLÉGIO TÉCNICO INDUSTRIAL DE SANTA MARIA
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

UM SISTEMA WEB PARA ANÁLISE DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO SEGUNDO A NORMA ABNT NBR ISO IEC 27002

TRABALHO DE CONCLUSÃO DE CURSO

Lucimara Dalla Porta Menezes Friedrich

Santa Maria, RS, Brasil

2014

UM SISTEMA WEB PARA ANÁLISE DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO SEGUNDO A NORMA ABNT NBR ISO IEC 27002

Lucimara Dalla Porta Menezes Friedrich

Trabalho apresentado ao Curso de Graduação em Tecnologia em
Redes de Computadores, Área de concentração em Segurança da Informação, da
Universidade Federal de Santa Maria (UFSM, RS),
como requisito parcial para obtenção do grau de
Tecnólogo em Redes de Computadores.

Orientador: Prof. Me. Renato Preigschadt de Azevedo

Santa Maria, RS, Brasil
2014

Universidade Federal de Santa Maria
Colégio Técnico Industrial de Santa Maria
Curso Superior de Tecnologia em Redes de Computadores

A Comissão Examinadora, abaixo assinada,
aprova a Monografia

UM SISTEMA WEB PARA ANÁLISE DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO SEGUNDO A NORMA ABNT NBR ISO IEC 27002

elaborada por
Lucimara Dalla Porta Menezes Friedrich

como requisito parcial para a obtenção do grau de
Técnologo em Redes de Computadores

COMISSÃO EXAMINADORA

Renato Preigschadt de Azevedo, Me.
(Presidente/Orientador)

Murilo Cervi, **Dr.** (UFSM)

Simone Regina Ceolin, Dra. (UFSM)

Santa Maria, 08 de Janeiro de 2014

AGRADECIMENTOS

É difícil agradecer todas as pessoas que de algum modo, nos momentos serenos e ou apreensivos, fizeram ou fazem parte da minha vida, por isso primeiramente agradeço à todos.

Ao meu orientador Renato Preigschadt de Azevedo, pelo apoio e confiança depositada em mim.

Ao meu filho Arthur, uma criança maravilhosa, que é tudo para mim. Sempre inspirou-me a lutar pelos meus objetivos.

Ao meu esposo Giancarlo, agradeço a Deus por ter colocado você no meu caminho. Uma pessoa maravilhosa em todos os sentidos. Muito compreensivo, companheiro e principalmente sempre soube explicar ao nosso filho, meus momentos de ausência.

A minha mãe Elizabeth, ajudou-me a realizar esse grande desejo. Desde pequena, incentivou-me a estudar, e dizia que um dia valeria a pena todo o meu esforço.

A Lourdes e Mauro pessoas sensacionais, muito ajudaram-me indiretamente para eu completar essa jornada. Agradeço o carinho.

Agradeço a Deus, por ter colocado-me numa família de princípios e valores fundamentais, como união, ética, respeito e transparência.

RESUMO

Monografia
Curso Superior de Tecnologia de Redes de Computadores
Universidade Federal de Santa Maria

UM SISTEMA WEB PARA ANÁLISE DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO SEGUNDO A NORMA ABNT NBR ISO IEC 27002

AUTORA: LUCIMARA DALLA PORTA MENEZES FRIEDRICH
ORIENTADOR: RENATO PREIGSCHADT DE AZEVEDO
Data e Local da Defesa: Santa Maria, 08 de Janeiro de 2014

Este trabalho tem por objetivo desenvolver uma ferramenta *Web*, segundo a norma ABNT NBR ISO/IEC 27002:2005, para que as organizações verifiquem o seu grau de conformidade com a norma ou para auxiliar as corporações na adoção das práticas de gestão documentadas de acordo com a norma. A proposta da ferramenta Infoquiz, assim denominada é a elaboração de um *checklist* segundo especificações da norma (ABNT, 2005), o responsável pela gestão da área de segurança da informação de uma organização, responderá todas as questões desenvolvidas através de uma página *Web*, e terá como resultado a contabilização das suas respostas, em forma de percentual. O percentual corresponde a conformidade da gestão implementada com a norma (ABNT, 2005). A ferramenta Infoquiz representa um conjunto de benefícios para uma organização, tais como, demonstra um compromisso dos executivos da organização para com a segurança da informação. Aumenta a credibilidade e a segurança da informação e dos sistemas, em termos de confidencialidade, disponibilidade e integridade. Identifica e endereça de forma continuada a oportunidade para melhorias, sendo um processo em contínua melhoria, e principalmente dotar a organização de um sistema de controle da gestão, incrementando a eficácia da organização. Para garantir as funcionalidades da ferramenta, foram efetuados testes com uma empresa de Santa Maria – RS, e observou-se que a Infoquiz pode ser utilizada em ambientes que contém uma gestão implementada que servirá principalmente para monitoração e revisão. E também, ser um modelo adequado de estabelecimento, implementação ou operação de um Sistema de Gestão de Segurança da Informação.

Palavras-chave: Segurança da informação. Gestão de segurança da informação. Ferramenta Infoquiz.

ABSTRACT

Monography
Superior Course of Technology in Computer Networks
Federal University of Santa Maria

A SYSTEM FOR ANALYSIS OF WEB SECURITY MANAGEMENT INFORMATION ACCORDING TO STANDARD ABNT NBR ISO IEC 27002

AUTHORESS: LUCIMARA DALLA PORTA MENEZES FRIEDRICH
ADVISOR: RENATO PREIGSCHADT DE AZEVEDO
Defense Place and Date: Santa Maria, January 08th 2014

This work aims to develop a web tool, according to the standard ISO / IEC 27002:2005, allowing the organizations to check their degree of compliance with the standard, and to assist in the adoption of management practices documented in accordance with the standard. This work proposes a tool called Infoquiz that contains a checklist of the standard specification, allowing the user to answer questions developed through a Web page, and result in the percentage of conformity according to the standard. The Infoquiz increases the credibility and security of information and systems, in terms of confidentiality, availability and integrity. Identifies and addresses the continuing opportunity for improvement being a continuous improvement process, and mainly provide the organization with a system of management control, increasing the effectiveness of the organization. To ensure the functionality of the tool, tests were performed with a company in Santa Maria – RS, and it was observed that the Infoquiz can be used in environments containing a management implemented which will serve mainly for monitoring and review.

Keywords: Information security. Management of information security. Infoquiz tool.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BS	*British Standard*
DER	Diagrama Entidade-Relacionamento
ER	Entidade-Relacionamento
HTML	*HyperText Markup Language*
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
PIN	*Personal Identification Number*
TI	Tecnologia da Informação

APÊNDICES

SUMÁRIO

INTRODUÇÃO

Com o avanço constante das tecnologias, a importância da segurança da informação aumenta significativamente. Está cada vez mais difícil manter em segurança as informações referentes as empresas ou pessoas. Um descuido nessa área pode trazer prejuízos significativos, o desafio está em obter o equilíbrio (Pwc, 2013).

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Em meio a todas essas informações que circulam nas organizações se faz necessária a implementação de regras. Para tornar seguro um ambiente cooperativo, existem normas nacionais e internacionais que tratam da segurança (Nakamura e Geus). Essas normas visam nortear as atividades realizadas a fim de tornarem os sistemas de informações[1] mais seguros.

Em particular, destacamos a norma ABNT NBR ISO/IEC 27002 (Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da Informação), em sua seção introdutória, refere-se que a segurança da informação é obtida por implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Esses controles precisam ser analisados criticamente, estabelecidos, implementados, monitorados e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos (ABNT, 2005).

Segundo a Pesquisa Global de Segurança da Informação (PwC, 2013), houve uma queda no uso de ferramentas de segurança da informação, observou-se um relaxamento das políticas que estabelecem padrões nas organizações.

A Figura 1, mostra as estatísticas da Pesquisa Global de Segurança da Informação (PwC, 2013), onde afirma-se que 51% dos participantes da pesquisa confirmam que as políticas relativas a *backup* e recuperação e a continuidade dos negócios permanecem em vigor em suas empresas, que houve queda em relação ao ano passado. Observa-se também relaxamento em questões importantes, como gestão de usuários, segurança de aplicações, segurança física, e classificação o valor dos dados para o negócio.

---

1 Um sistema de informação usa “a tecnologia de computador para realizar algumas ou todas as tarefas pretendidas. Os componentes básico dos sistemas de informação são: hardware, software, banco de dados, rede, procedimentos e pessoas. Os sistemas coletam, processam, armazenam, analisam, e disseminam informações para um fim específico.” (Turban *et al*, 2003, p. 33)

A pesquisa diz que, “as empresas atuam em movimento pendular, os padrões de segurança são rígidos ao máximo ou relaxando-os de maneira excessiva. E que o grande desafio está em manter o equilíbrio”.

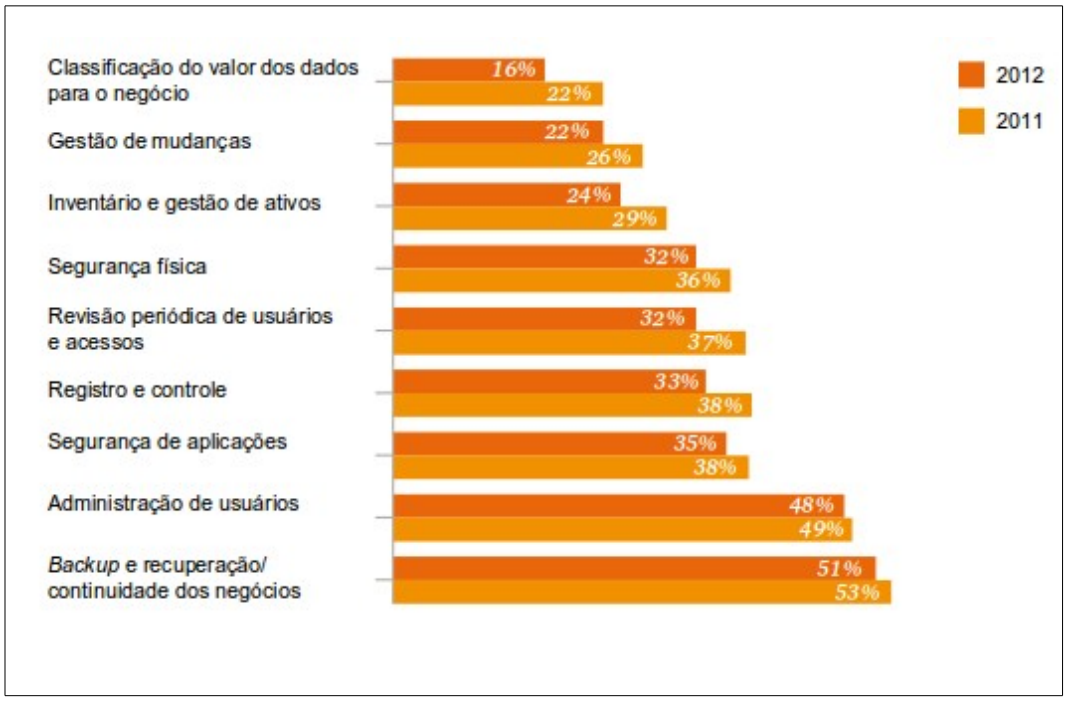


Figura 1 - Elementos que compõem a política de segurança no mundo

Fonte:http://www.pwc.com.br/pt_BR/br/estudos-pesquisas/asets/pesquisa-seguranca-informacao-13.pdf

Nakamura e Geus no ano de 2007 diz que, “o que mais preocupa as organizações são ataques que ocorrem internamente”.

Segurança da informação é um jogo de técnicas e estratégias avançadas que se transforma com rapidez. Como consequência, os modelos da década passada, não são mais adequados. Os líderes reconhecem que, para ter uma segurança eficaz é preciso se transformar e adotar uma nova maneira de pensar. Eles estão cientes de que a própria sobrevivência do negócio exige a compreensão das ameaças de segurança, o preparo para enfrentá-las e respostas rápidas. (PwC, 2013).

O presente trabalho apresenta um sistema *Web* para análise de gestão da segurança da informação segundo a norma (ABNT, 2005). A partir da compreensão das informações de seus negócios, a ferramenta é uma oportunidade de medir e avaliar a efetividade da gestão de segurança da informação, ou seja, procurar equilibrar a gestão. Servirá para fortalecer as práticas de segurança que as empresas devem implantar. A ferramenta busca ser uma

estratégia rápida para os gestores analisarem/avaliarem os seus riscos e tratarem eles de acordo com a norma.

O trabalho está organizado da seguinte maneira: no Capítulo 1 é abordado o tema do trabalho, com seus respectivos objetivos. No Capítulo 2 são abordados alguns conceitos importantes para o entendimento do trabalho. No Capítulo 3 demais conceitos e entendimento do surgimento da norma trabalhada. No Capítulo 4 é tratado o funcionamento da ferramenta desenvolvida e também a metodologia utilizada para a sua implementação. No Capítulo 5 traz os resultados da avaliação da gestão de segurança da informação, com estudo de caso. E no Capítulo 6 são apresentadas as considerações finais e sugestões para trabalhos futuros.

1 TEMA

Análise do nível de um Sistema de Gestão de Segurança da Informação em conformidade com a norma ABNT NBR ISO/IEC 27002:2005.

1.1 Delimitação do Tema

O objetivo de desenvolvimento da ferramenta Infoquiz a partir da norma (ABNT, 2005) é ser capaz de mostrar o nível em que encontra-se a gestão da segurança da informação, enfocando em um ambiente organizacional para análise.

1.2 Objetivos

1.2.1 Objetivo geral

Através de uma página *Web*, o usuário responderá um questionário desenvolvido, baseado na norma (ABNT, 2005). Suas respostas serão contabilizadas e a Infoquiz gerará um relatório, mostrando a concordância da gestão implementada com a norma.

1.2.2 Objetivos específicos

- Facilitar a aplicação da norma num ambiente organizacional.
- Tornar mais simples a verificação de conformidade, caso a norma já sera utilizada na organização, através do questionário desenvolvido.
- Aumentar a credibilidade e a segurança da informação dos sistemas.
- Identificar e endereçar a oportunidade para melhorias.
- Dotar a organização de um sistema de controle de gestão, incrementando a eficácia da organização.
- Servir de monitoração, revisão, um modelo adequado de estabelecimento de Sistema de Gestão de Segurança da Informação.

2 REFERENCIAL TEÓRICO

Para o desenvolvimento do referencial teórico deste trabalho, primeiramente foi pesquisado na literatura da área o conceito de segurança da informação. Em seguida, o porquê da segurança da informação ser necessária num ambiente organizacional e como implementar a segurança da informação baseado em uma norma. Procurou-se levantar o estudo da norma trabalhada, desde sua estrutura até o ponto de partida para a segurança da informação.

2.1 Conceito de Segurança da Informação

Segurança da informação é um tema atual em constante discussão nas mais diversas organizações, seja governo, educação, indústria, comércio ou serviços; visto que as organizações utilizam-se da Tecnologia da Informação (TI) para apoiar e gerar negócios, aliados aos benefícios da Internet. Desse modo, independentemente do segmento de mercado, todas as organizações sempre usufruirão da informação, objetivando melhor produtividade, redução de custos, ganho na participação de mercado, aumento de agilidade, competitividade e apoio à tomada de decisão. (SÊMOLA, 2003, p. 1).

Segurança da informação, conforme Beal (2005), é o processo de proteção da informação das ameaças à sua integridade, disponibilidade e confidencialidade. Sêmola (2003) define segurança da informação como "uma área do conhecimento dedicada à proteção de ativos[2] da informação contra acessos não autorizados, alterações indevidas ou sua indisponiblidade".

A norma ISO/IEC 27002:2005, em sua seção introdutória, define segurança da informação como "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." Assim, pode-se definir a segurança da informação como a área do conhecimento que visa a proteção da informação das ameaças à sua integridade, disponibilidade e confidencialidade, a fim de garantir a continuidade do negócio e minimizar os riscos.

2 Conforme Sêmola (2003), ativo é tudo aquilo que tem valor para a organização.

Beal (2005) e Sêmola (2003) asseveram que o objetivo da segurança da informação é preservar os ativos de informação quanto à sua confidencialidade, integridade e disponibilidade:

- a **confidencialidade** da informação é a garantia de que somente pessoas autorizadas terão acesso a ela, protegendo-a de acordo com o grau de sigilo do seu conteúdo;
- a **integridade** da informação tem como objetivo garantir a exatidão da informação, assegurando que pessoas não autorizadas possam modificá-la, adicioná-la ou removê-la, seja de forma intencional ou acidental;
- a **disponibilidade** garante que os autorizados a acessarem a informação possam fazê-lo sempre que necessário.

Conforme Beal (2005, p. XII) “os problemas de segurança da informação são complexos, e normalmente têm sua origem em preocupações organizacionais e de negócio, não de tecnologia.” A fim de garantir um nível de proteção adequado para seus ativos de informação, as organizações e seus principais gestores precisam ter uma visão clara das informações que estão tentando salvaguardar, de que ameaças e por que razão, antes de poder passar a seleção de soluções específicas de segurança. Grande parte dos dados importantes ao negócio da empresa está armazenada em computadores, por isso as organizações dependem da confiabilidade de seus sistemas baseados em TI; se a confiança nesses dados for destruída, o impacto pode ser comparável à própria destruição do sistema. Ainda conforme a autora, os administradores devem preocupar-se com a segurança dos componentes de TI e da informação neles armazenada por quatro razões principais:

- Dependência da tecnologia da informação;
- Vulnerabilidade da infraestrutura tecnológica – *hardware e software*;
- Alto valor da informação armazenada;
- Pouca atenção dada à segurança nos estágios iniciais do desenvolvimento e software.

Dessa forma, as organizações precisam adotar controles de segurança – medidas de proteção que abranjam uma grande diversidade de iniciativas – que sejam capazes de proteger adequadamente dados, informações e conhecimentos, escolhidos levando-se em conta os riscos reais a que estão sujeitos esses ativos. (BEAL, 2005).

3 NORMA PARA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Antes de iniciar o estudo da norma, da metodologia e da ferramenta, apresentadas nos capítulos 3, 4 e 5, respectivamente, cabe elucidar alguns conceitos sobre cada um desses elementos.

Norma é aquilo que se estabelece como medida para a realização de uma atividade. Uma norma tem como propósito definir regras e instrumentos de controle para assegurar a conformidade de um processo ou serviço (FAGUNDES).

Conforme definido pela Associação Brasileira de Normas Técnicas (ABNT), os objetivos da normalização são:

- Comunicação: proporcionar meios mais eficientes na troca de informação entre o fabricante e o cliente, melhorando a confiabilidade das relações comerciais e de serviços;
- Segurança: proteger a vida humana e a saúde;
- Proteção do consumidor: prover a sociedade de mecanismos eficazes para aferir qualidade dos produtos;
- Eliminação de barreiras técnicas e comerciais: evitar a existência de regulamentos conflitantes sobre produtos e serviços em diferentes países, facilitando assim o intercâmbio comercial.

As ferramentas são instrumentos que facilitam a aplicação de determinada metodologia. Neste caso, foi elaborada uma página Web para a geração de relatórios, com objetivo de mostrar o nível de conformidade dos processos da corporação com a norma.

A norma apresentada neste capítulo trata especificamente desde seu surgimento, mas principalmente a sua estrutura ABNT NBR ISO/IEC 27002.

3.1 Evolução da norma ISO/IEC 27002:2005

Essa norma teve origem em 1989, a fim de implementar e normalizar a atuação das empresas na gestão da segurança da informação, o *Commercial Computer Security Center*, órgão ligado ao departamento de indústria e comércio do Reino Unido, publicou a primeira versão do Código para Gerenciamento de Segurança da Informação – PD0003. Seis anos depois, este código foi revisado e publicado como uma *British Standard*, denominado

BS7799, que apresentava as melhores práticas em controles de segurança para auxiliar as organizações comerciais e de governo na implantação e crescimento da segurança da informação. (OLIVA e OLIVEIRA, 2003).

Devido ao interesse internacional em uma norma de segurança da informação, a BS 7799-1:1999 foi submetida à *International Organization for Standardization* (ISO), organização internacional que aglomera os grêmios de padronização/normalização de 148 países.

Em dezembro de 2000, a BS 7799-1:1999 foi publicada como norma internacional ISO 17799:2000 (parte 1 BS)

Em 2001, a Associação Brasileira de Normas Técnicas – ABNT, publicou a versão brasileira da ISO 17799:2000 que ficou com a denominação de NBR/ISO 17799 – Código de Prática para a Gestão da Segurança da Informação.

Em setembro de 2005, a norma foi revisada e publicada como NBR ISO/IEC 17799:2005. As séries de normas ISO 27000 foram especificamente reservadas pela ISO para as questões de segurança da informação. Pode-se observar pela Figura 2 essa evolução.

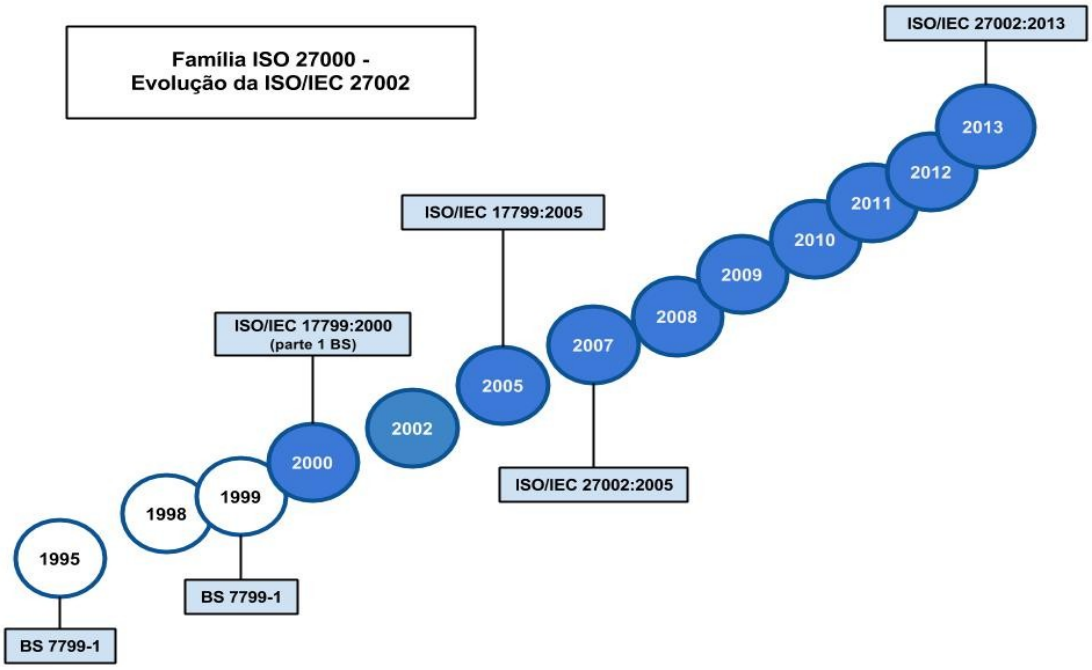


Figura 2 - Evolução da norma 27002

Em 2007, a nova edição da ISO/IEC 17799 foi incorporada ao novo esquema de numeração ISO/IEC 27002 (ABNT, 2005).

No dia 18 de novembro de 2013 foi lançada a nova versão ABNT NBR ISO/IEC 27002:2013 – Código de Prática para controles de Segurança da informação. A atualização da norma reflete a evolução de práticas de gestão e governança de segurança da informação nos últimos oito anos (RNP, 2013).

Salienta-se que, para uma organização obter a certificação, que significa que um organismo de certificação independente confirmou que a segurança da informação está sendo implementada da melhor maneira possível na organização, depende da ISO 27001, a ISO 27002:2005 é uma norma "auxiliar" que fornece mais detalhes sobre como implementar os controles de segurança especificados na ISO 27001 (ABNT, 2005).

3.1.1 A norma ABNT NBR ISO/IEC 27002

A norma, nos primeiros Capítulos, contêm o seu Objetivo, Termos e Definições, Estrutura da Norma e uma seção introdutória. Essa seção introdutória trata da Análise, Avaliação e Tratamento de Riscos a fim de orientar na identificação, quantificação e priorização do gerenciamento do risco, e os critérios definidos para aceitar o risco ou não (ABNT, 2005). Nas demais seções da norma, contêm 11 controles de segurança da informação, conforme a Tabela 1, e juntos totalizam 39 categorias principais de segurança.

Tabela 1 - Seções e suas respectivas quantidades de categorias

Capítulo	Título	Número sub-capítulos
5	Política de segurança da Informação	1
6	Organizando a Segurança da Informação	2
7	Gestão de Ativos	2
8	Segurança em Recursos Humanos	3
9	Segurança Física e do Ambiente	2
10	Gestão de Operações e Comunicações	10
11	Controle de Acesso	7
12	Aquisição, Desenvolvimento e Manutenção de SI	6
13	Gestão de Incidentes de Segurança Informação	2

14	Gestão da Continuidade do Negócio	1
15	Conformidade	3

Os títulos de cada seção, com suas respectivas recomendações são descritos abaixo:

1. Política de Segurança da Informação: recomendações para a formalização de uma política.

Contendo: diretrizes, princípios e regras que irão prover orientação e apoio para implantação e manutenção da segurança.

2. Organização da Segurança da Informação: recomendações para o estabelecimento de uma estrutura de gestão para planejar e controlar a implementação da segurança da informação na organização.

3. Gestão de Ativos: recomendações sobre a realização de inventário dos ativos informacionais e atribuição de responsabilidades pela manutenção dos controles necessários para protegê-los;

4. Segurança em Recursos Humanos: recomendações para reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações;

5. Segurança Física e do Ambiente: recomendações para a proteção dos recursos e instalações de processamento de informações críticas ou sensíveis ao negócio contra acesso não autorizado, dano ou interferência;

6. Gestão das Operações e Comunicações: recomendações para garantir a operação correta e segura dos recursos de processamento de informações e proteger a integridade de serviços e informações;

7. Controle de Acesso: recomendações para a monitoração e o controle do acesso a recursos computacionais, para protegê-los contra abusos internos e ataques externos;

8. **Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação**: recomendações para o uso de controles de segurança em todas as etapas do ciclo de vida forçam que, com todos os esforços de TI, tudo seja implementado e mantido com a segurança em mente, usando controles de segurança em todas as etapas do processo;

9. Gestão de Incidentes da Segurança da Informação: recomendações para notificação de fragilidades e eventos de segurança da informação, responsabilidades e procedimentos e coleta de evidências.

10. Gestão da Continuidade do Negócio: recomendações para preparar a organização para neutralizar as interrupções às atividades comerciais e proteger os processos críticos em caso de ocorrência de falha ou desastre;

11. Conformidade: recomendações para a preservação da conformidade com requisitos legais (tais como direitos autorais e direito à privacidade), com normas e diretrizes internas e com os requisitos técnicos de segurança.

3.1.2 Seções e controles da norma ABNT NBR ISO/IEC 27002:2005

A norma, em sua estrutura ABNT NBR ISO/IEC 27002 da versão 2005, encontra-se estruturada nas seguintes seções e seus respectivos controles. A Tabela 2, na sequência até a Tabela 12, de uma forma resumida, cita todas as seções, as categorias existentes e os controles principais que compõem essa estrutura.

Tabela 2 - Política de Segurança da Informação.

5. Política de Segurança da Informação
5.1 Política de Segurança da Informação
Objetivo: 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 relevantes.
1. documento aprovado pela direção, publicado e comunicado para todos os funcionários e terceiros; 2. deve ser analisada criticamente a intervalos planejados ou quando ocorrem mudanças significativas.

Tabela 3 - Organização da Segurança da Informação.

6. Organização da Segurança da Informação
6.1 Infraestrutura da Segurança da Informação
Objetivo: gerenciar a segurança de informação dentro da organização;
1. a direção deve apoiar ativamente a segurança da informação dentroa da organização; 2. as atividades de segurança devem ser coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes; 3. todas as responsabilidades pela segurança da informação estejam claramente definidas; 4. definir e implementar um processo de gestão de autorização para novos recursos e processamento da informação; 5. definir acordos de confidencialidade e de não divulgação; 6. quando e quais autoridades devem ser contatadas no caso de incidentes de segurança da informação; 7. contatos com grupos de interesse especiais ou outros fóruns especializados e associações profissionais; 8. análise crítica independente da segurança da informação (gerência de outra área ou empresa terceira)
6.2 Partes Externas
Objetivo: manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas.
1. avaliar os riscos de processos de negócios com terceiros implementando controles apropriados antes de se

conceder o acesso; 2. considerações sobre o acesso de clientes aos ativos da informação; 3. acordos com terceiros assegurando que não existe mal-entendido entre as partes e possibilidade de indenização.

Tabela 4 - Gestão de Ativos.

7. Gestão de Ativos
7.1 Responsabilidade pelos ativos Objetivo: alcançar e manter a proteção adequada dos ativos da organização. 1. todos os ativos devem ser identificados, inventariados e documentada sua importância; 2. todos ao tivos de informação devem possuir um proprietário; 3. definição de regras para uso da informação e dos recursos de processamento da informação (Internet, e-mail, dispositivos móveis);
7.2 Classificação da informação Objetivo: assegurar que a informação receba um nível adequado de proteção. 1. classificação da informação em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização; 2. definição de um conjunto de procedimentos para rotulação e tratamento da informação, tanto dos ativos da informação no formato físico quanto no eletrônico.

Tabela 5 - Segurança em Recursos Humanos.

8. Segurança em Recursos Humanos
8.1 Antes da contratação Objetivo: assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordos com seus papéis e reduzir o risco de roubos, fraudes ou mau uso de recursos. 1. papéis e responsabilidades; 2. seleção; 3. termos e condições de contratação;
8.2 Durante a contratação Objetivo: assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, de suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano. 1. responsabilidades da direção; 2. conscientização, educação e treinamento em segurança da informação; 3. processo disciplinar.
8.3 Encerramento ou mudança da contratação Objetivo: assegurar que os funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada. 1. encerramento de atividades; 2. devolução de ativos; 3. retirada de direitos de acesso.

Tabela 6 - Segurança Física e do Ambiente.

9. Segurança Física e do Ambiente
9.1 Áreas seguras
Objetivo: prevenir o acesso físico não-autorizado, danos e interferências com as instalações e informações da organização.
1. perímetro de segurança física; 2. controles de entrada física; 3. segurança em escritórios, salas e instalações; 4. proteção contra ameaças externas e do meio ambiente; 5. trabalhando em áreas seguras; 6. acesso do público, áreas de entrega e de carregamento.
9.2 Segurança de equipamentos
Objetivo: impedir perdas, danos, furto ou comprometimento de ativos e interrupções das atividades da organização.
1. instalação e proteção do equipamento; 2. utilidades (falha de energia elétrica); 3. segurança do cabeamento; 4. manutenção dos equipamentos; 5. segurança de equipamentos fora das dependências da organização; 6. reutilização e alienação segura de equipamentos; 7. remoção de propriedade.

Tabela 7 - Gerenciamento das Operações e Comunicações.

10. Gerenciamento das Operações e Comunicações
10.1 Procedimentos e responsabilidades operacionais
Objetivo: garantir a operação segura e correta dos recursos de processamento da informação;
1. documento formal com procedimentos operacionais para: backup, contatos de suporte, recuperação em caso de falha do sistema etc. 2. existência de ambiente separado para recursos de desenvolvimento, teste e produção em sistemas
10.2 Gerenciamento de serviços terceirizados
Objetivo: implementar e manter o nível apropriado de segurança da informação e entrega de serviços em consônancia com acordos de entrega de serviços terceirizados.
1. monitoramento dos serviços terceirizados quanto à entrega do serviço, relatórios e possíveis mudanças
10.3 Planejamento e aceitação dos sistemas
Objetivo: minimizar o risco de falhas nos sistemas.
1. implantação de novos sistemas, atualizações e novas versões somente após serem devidamente testados, considerando o impacto na segurança da organização como um todo
10.4 Proteção contra códigos maliciosos e códigos móveis
Objetivo: proteger a integridade do software e da informação.
1. antivírus 2. proibição de uso de softwares não autorizados
10.5 Cópias de segurança
Objetivo: manter a integridade e disponibilidade da informação e dos recursos de processamento da informação.
1. implantação de sistema de backup

10.6 Gerenciamento da segurança em redes

Objetivo: garantir a proteção das informações em redes e a proteção da infraestrutura de suporte.

1. firewalls
2. sistema de detecção de intrusos – IDS

10.7 Manuseio de mídias

Objetivo: prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos, e interrupções das atividades do negócio.

1. manter as mídias e documentação de sistemas seguras em um ambiente protegido
2. existência de cópia em outro local
3. descarte seguro da mídia removível: incineração ou trituração
4. identificação da classificação da mídia; confidencial, restrita etc

10.8 Troca de informações

Objetivo: manter a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades externas.

1. uso de criptografia na troca de informações, principalmente entre empresas e mensagens com anexos
2. conscientização das pessoas sobre o risco de troca de informações em locais não seguros: corredores, bares, cafés, banheiros, celulares em local público etc.
3. compartilhamento adequado e seguro das informações

10.9 Serviços de comércio eletrônico

Objetivo: garantir a segurança de serviços de comércio eletrônico e sua utilização segura.

1. uso de criptografia de chave pública
2. uso de assinaturas digitais

10.10 Monitoramento

Objetivo: detectar atividades não autorizadas de processamento da informação.

1. monitoramento, proteção e análise crítica dos registros (*logs*) de auditoria com atividades dos usuários, exceções e outros eventos de segurança da informação para assegurar que os usuários estão executando somente as atividades que foram explicitamente autorizadas, melhorar a compreensão das ameaças encontradas no sistema e a maneira pela qual isto pode acontecer
2. sincronização dos relógios de todos os sistemas de acordo com uma hora oficial

Tabela 8 - Controle de Acesso.

11. Controle de Acesso
11.1 Requisitos de negócio para controle de acesso
Objetivo: controlar acesso à informação
1. política de controle de acesso
11.2 Gerenciamento de acesso do usuário
Objetivo: assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação
1. registro de usuário 2. gerenciamento de privilégios 3. gerenciamento de senha do usuário 4. análise crítica dos direitos de acesso de usuário
11.3 Responsabilidade dos usuários
Objetivo: prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou furto da informação e dos recursos de processamento da informação.
1. uso de senhas

2. equipamento de usuário sem monitoração
3. política de mesa limpa e tela limpa

11.4 Controle de acesso à rede

Objetivo: prevenir acesso não autorizado aos serviços da rede.

1. política de uso dos serviços da rede
2. autenticação para conexão externa do usuário
3. identificação de equipamento em redes
4. proteção e configuração de portas de diagnóstico remotas
5. segregação de redes
6. controle de conexão de rede
7. controle de roteamento de redes

11.5 Controle de acesso ao sistema operacional

Objetivo: prevenir acesso não autorizado aos sistemas operacionais
1. procedimentos seguros de entrada no sistema (*log-on)*
2. identificação e autenticação de usuário
3. sistema de gerenciamento de senha
4. uso de utilitários de sistema
5. desconexão de terminal por inatividade
6. limitação de horário de conexão

11.6 Controle de acesso à aplicação e à informação

Objetivo: prevenir acesso não autorizado à informação contida nos sistemas de aplicação.

1. restrição de acesso à informação
2. isolamento de sistemas sensíveis

11.7 Computação móvel e trabalho remoto

Objetivo: garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.

1. computação e comunicação móvel
2. trabalho remoto

Tabela 9 - Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação.

12. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
12.1 Requisitos de segurança de sistemas de Informação
Objetivo: garantir que segurança é parte integrante de sistemas de informação.
1. análise e especificação dos requisitos de segurança
12.2 Processamento correto nas aplicações
Objetivo: prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.
1. validação dos dados de entrada 2. controle de processamento inerno 3. integridade de mensagens 4. validação de dados de saída
12.3 Controles criptográficos
Objetivo: proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos.
1. política para o uso de controles criptográficos 2. gerenciamento de chaves

12.4 Segurança dos arquivos do sistema

Objetivo: garantir a segurança de arquivos de sistema

1. controle de software operacional
2. proteção dos dados para teste de sistema
3. controle de acesso ao código-fonte de programa

12.5 Segurança em processos de desenvolvimento e de suporte

Objetivo: manter a segurança de sistemas aplicativos e da informação.

1. procedimentos para controle de mudanças
2. análise crítica técnica das aplicações após mudanças no sistema operacional
3. restrições sobre mudanças em pacotes de software
4. vazamento de informações
5. desenvolvimento terceirizado de software

12.6 Gestão de vulnerabilidades técnicas

Objetivo: reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.

1. controle de vulnerabilidades técnicas

Tabela 10 - Gestão de Incidentes de Segurança da Informação.

13. Gestão de Incidentes de Segurança da Informação
13.1 Notificação de fragilidades e eventos de segurança da informação
Objetivo: assegurar que um enfoque consistente e efetivo seja aplicado a gestão de incidentes da segurança da informação.
1. notificação de eventos e segurança da informação 2. notificando fragilidades de segurança da informação
13.2 Gestão de incidentes de segurança da informação e melhorias
Objetivo: assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes da segurança da informação.
1. responsabilidades e procedimentos 2. aprendendo com os incidentes de segurança da informação 3. coleta de evidências

Tabela 11 - Gestão da Continuidade do Negócio.

14. Gestão da Continuidade do Negócio
14.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação
Objetivo: não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil se for o caso.
1. incluindo segurança da informação no processo de gestão da continuidade e negócio 2. continuidade de negócios e análise/avaliação de riscos 3. desenvolvimento e implementação de planos de continuidade relativos à segurança da informação 4. estutura do plano de continuidade do negócio 5. testes, manutenção e reavaliação dos planos de continuidade do negócio

Tabela 12 - Conformidade.

15. Conformidade
15.1 Conformidade com requisitos legais
Objetivo: evita violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.
1. identificação da legislação vigente 2. direitos de propriedade intelectual 3. proteção de registros organizacionais 4. proteção de dados e privacidade de informações pessoais 5. prevenção de mau uso de recursos de processamento da informação 6. regulamentação de controles de criptografia
15.2 Conformidade com normas e políticas de segurança da informação e conformidade técnica
Objetivo: garantir a conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.
1. conformidade com as políticas e normas de segurança da informação 2. verificação da conformidade técnica
15.3 Considerações quanto à auditoria de sistemas de informação
Objetivo: maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.
1. controles de auditoria de sistemas de informação 2. proteção de ferramentas de auditoria de sistemas de informação

3.1.3 Ponto de partida para a segurança da informação

Segundo (ABNT, 2005), um certo número de controles pode ser considerado um bom ponto de partida para a implementação da segurança da informação. ABNT (2005, p XII.) diz que “estes controles são baseados tanto em requisitos legais como nas melhores práticas de segurança da informação normalmentes usadas”.

Os controles considerados essenciais para uma organização, sob o ponto de vista legal, incluem, dependendo da legislação aplicável são eles:

> a) proteção de dados e privacidade de informações pessoais;
> b) proteção de registros organizacionais;
> c) direitos de propriedade intelectual; (ABNT, 2005, p. XII)

Os controles considerados práticas para a segurança da informação incluem:

> a) documento da política de segurança da informação;
> b) atribuição de responsabilidades para a segurança da informação;
> c) conscientização, educação e treinamento em segurança da informação;
> d) processamento correto nas aplicações;
> e) gestão de vulnerabilidades técnicas;
> f) gestão da continuidade do negócio;
> g) gestão de incidentes de segurança da informação e melhorias; (ABNT, 2005, p. XII)

Esses controles se aplicam para a maioria das organizações e na maioria dos ambientes. Embora o enfoque acima seja considerado um bom ponto de partida, ele não substitui a seleção de controles, baseado na análise/avaliação de riscos (ABNT, 2005).

4 FERRAMENTA INFOQUIZ

Conforme observado anteriormente, o foco deste trabalho é gerar uma ferramenta capaz de contabilizar respostas baseadas na norma (ABNT,2005) através de uma página *Web*.

O desenvolvimento deste trabalho foi realizado em diferentes etapas. Inicialmente, realizou-se uma pesquisa em documentos existentes que obtivesse a implementação de um *checklist*, segundo a referida norma. Essa pesquisa mostrou que não havia soluções implementadas.

Analisando a estrutura da norma 27002, verificou-se que ela é distribuída em várias seções, categorias e controles. Os controles, dispostos em cada categoria da norma, definem os principais pontos a serem aplicados no desenvolvimento do checklist. Foram trabalhadas algumas seções da referida norma, convém observar que, embora toda as seções da norma sejam importantes, a relevância de qualquer controle da seção deve ser determinada segundo os riscos específicos a que uma organização está exposta (ABNT, 2005). São eles: o Controle de Acessos, Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação, Gestão da Continuidade do Negócio, Gestão de Incidentes de Segurança da Informação e Conformidade.

A elaboração da ferramenta Infoquiz foi realizada com o *framework* Django, que é um ambiente apropriado para desenvolvimento de aplicações *Web* (SANTANA, 2010). Ele é escrito em linguagem de programação Python. Ao atingir a finalização do questionário ocorre a disponibilização de um relatório, o qual mostra, em percentual, o nível de segurança da organização com base na norma 27002.

4.1 Desenvolvimento do questionário

O questionário, foi realizado da seguinte forma: no primeiro momento, compreender a estrutura da norma para gerar as questões.

A estrutura da norma é dividida em seções, categorias e controles (ABNT, 2005). Na seção, mostra-se o objetivo e como convém implementá-la. (ABNT, 2005). Por exemplo, na seção controle de acesso, explica-se o seu objetivo (controlar acesso à informação) e como convém implementá-la (a partir de regras de controle de acesso).

Na categoria, explica-se o seu objetivo somente. (ABNT, 2005). No controle, define qual a regulação específica é utilizada para atender ao objetivo. As diretrizes para implementação contêm informações detalhadas para apoiar a implementação do controle além de atender o objetivo de controle (ABNT, 2005).

Na Figura 3 ilustra-se a estrutura da norma em Seção, Categoria e os Controles. Na Seção Política de Segurança da Informação, encontram-se os controles: Documento da Política de Segurança da Informação e a Análise Crítica da Política de Segurança da Informação. A partir deles que as perguntas foram elaboradas do questionário. Logo mais abaixo será explicado o desenvolvimento.

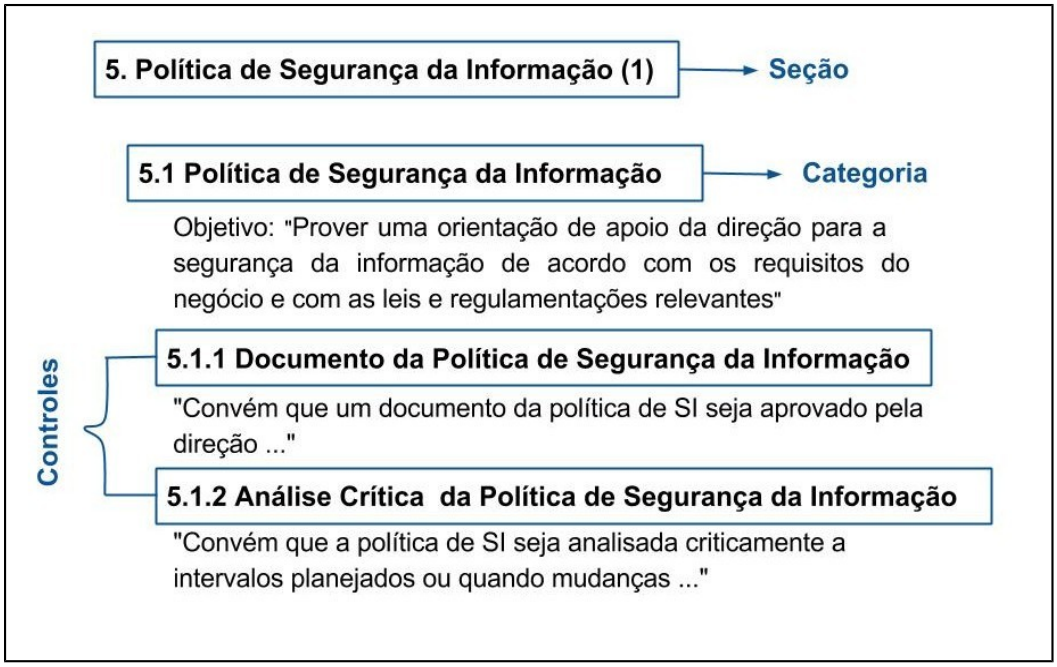


Figura 3 - Estrutura da norma seção/categoria/controle

4.1.1 Questionário

A partir da compreensão da estrutura da norma, conforme explicado na Figura 3, as perguntas foram realizadas. Os controles são os procedimentos práticos para alcançar um objetivo na gestão da segurança da informação (ABNT, 2005).

Na Figura 4 mostra-se, por exemplo, a Seção Controle de Acesso, a Categoria Requisitos de Negócio para controle de acesso e seus respectivo objetivo, nesses itens não foram mexidos para a elaboração das perguntas do questionário. O objetivo é trabalhar nos

controles como explicado anteriormente. No Controle Requisitos de negócio para controle de acesso foi realizada uma pergunta principal, as demais questões foram realizadas a partir dos controles seguintes, conforme a Figura 4. No APÊNDICE A do trabalho, traz todas as questões que foram elaboradas das respectivas seções.

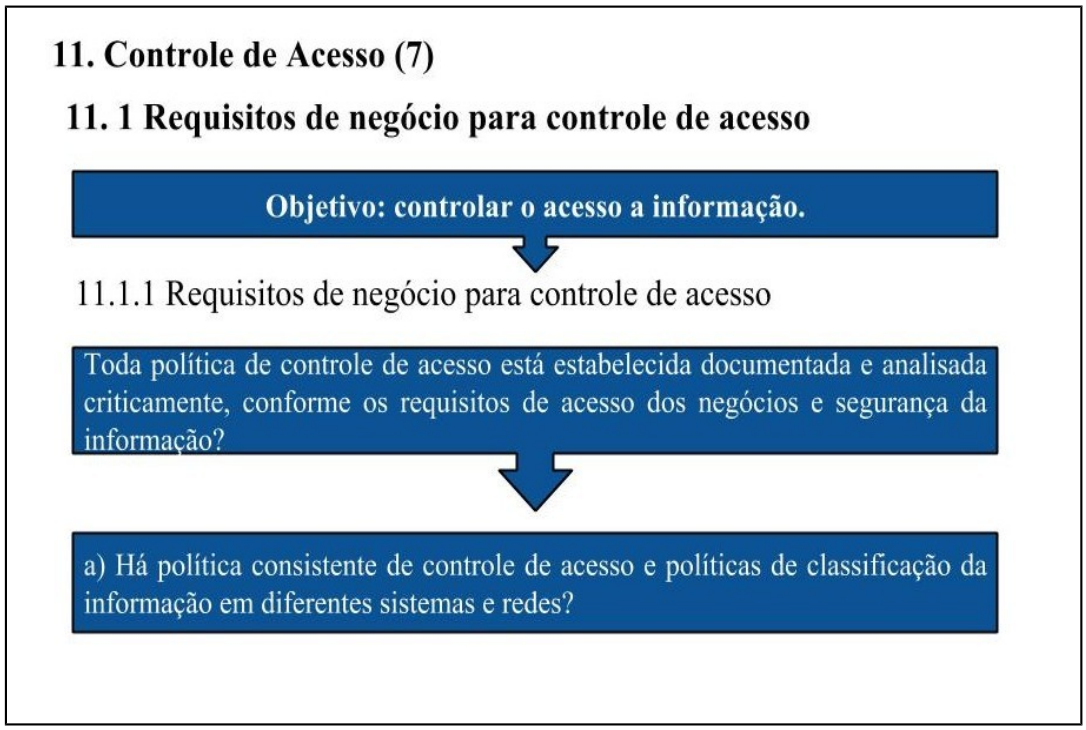


Figura 4 - Estrutura do questionário baseado nos controles

4.2 Desenvolvimento do diagrama do banco de dados da ferramenta Infoquiz

A ferramenta Infoquiz conta com um banco de dados para armazenar as questões elaboradas, tendo no APÊNDICE B uma imagem do banco utilizado. A primeira etapa do projeto de um banco de dados é a construção de um modelo conceitual, a chamada modelagem conceitual. O objetivo da modelagem conceitual é obter uma descrição abstrata, independentemente de implementação em computador dos dados que serão armazenados no banco de dados, segundo (HEUSER, 1998).

HEUSER cita que a técnica de modelagem dos dados mais difundida e utilizada é a abordagem entidade-relacionamento (ER). Usualmente, um modelo ER é representado graficamente através de um diagrama entidade-relacionamento (DER).

Uma entidade representa, no modelo conceitual, um conjunto de objetos da realidade modelada, (HEUSER, 1998).

Um relacionamento é representado por um losango, ligado por linhas aos retângulos representativos das entidades, que participam do relacionamento. Logo, um relacionamento é um conjunto de associações entre entidades (HEUSER, 1998).

Para fins de projeto de banco de dados, uma propriedade importante de um relacionamento é a de quantas ocorrências de uma entidade podem estar associadas a uma determinada ocorrência através do relacionamento. Segundo (HEUSER, 1998), esta propriedade chama-se de cardinalidade. Há duas a considerar, a cardinalidade máxima e mínima.

A cardinalidade que foi utilizada é a máxima. Na Figura 5 mostra-se os relacionamentos seguintes.

O primeiro relacionamento corresponde:

- 1 CATEGORIA (pai) para N CATEGORIAS (filhas). O 1 expressa que há (“1”) ocorrência de CATEGORIA (filha), que pode estar associada ao máximo uma (“1”) ocorrência de CATEGORIA (pai). O N expressa que (“1”) ocorrência de CATEGORIA pode estar associada a muitas (“n”) ocorrências de CATEGORIAS. Assim, nas demais entidades e seus relacionamentos.

O segundo relacionamento corresponde:

- 1 CATEGORIA (pai) para N QUESTÕES (questões).

Na entidade QUESTÕES, o primeiro relacionamento corresponde:

- 1 QUESTÃO (pai) para N QUESTÕES (filhas).

O segundo corresponde:

- 1 QUESTÃO (pai) para N RESPOSTAS (respostas).

A partir do diagrama construído, conforme a Figura 5, foi implementada a ferramenta Infoquiz.

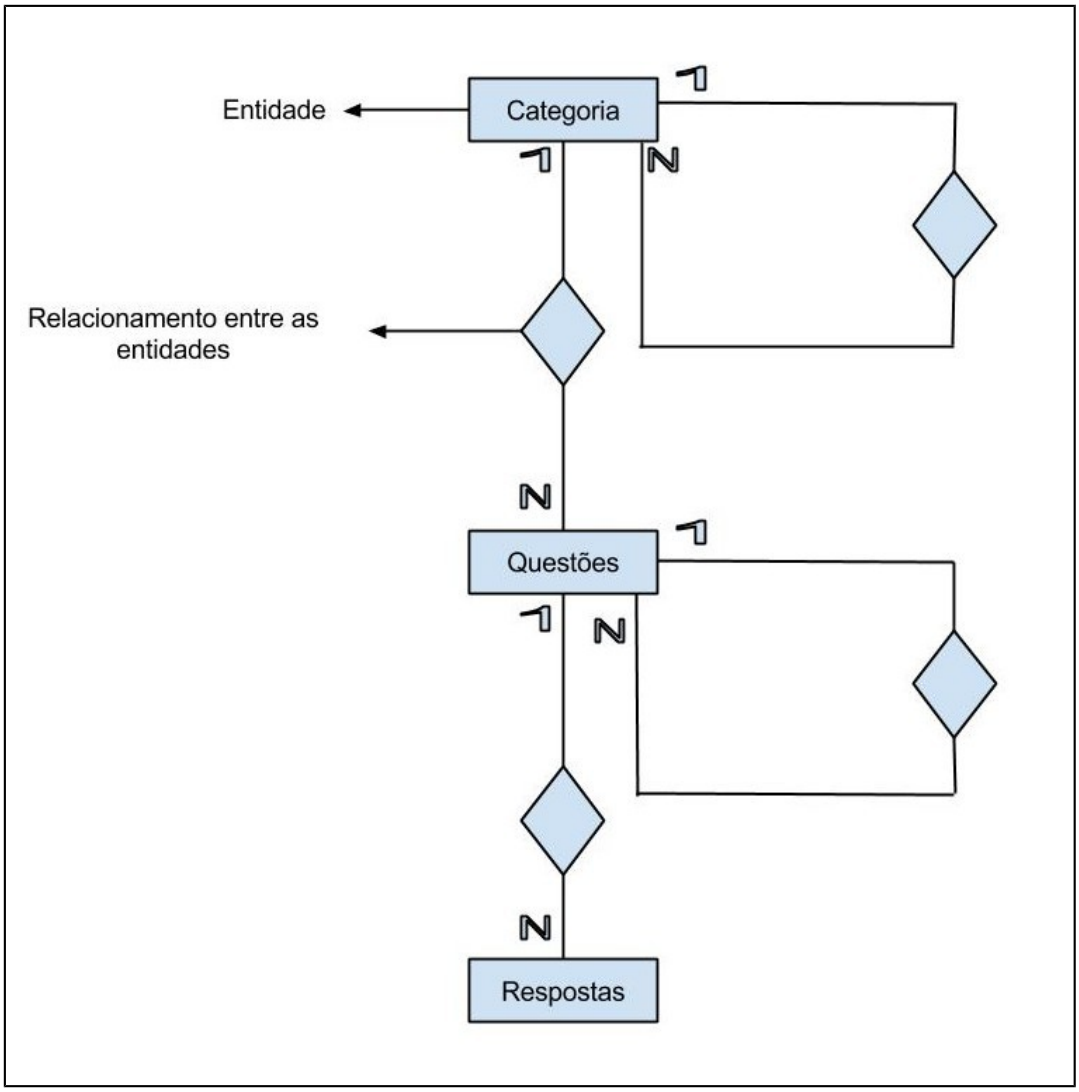


Figura 5 - Digrama entidade-relacionamento da ferramenta Infoquiz

4.3 Ambiente de desenvolvimento da ferramenta Infoquiz

Todo o projeto, desenvolveu-se no ambiente Django, que é um *framework* de desenvolvimento w*eb*, escrito em Python, criado pelo grupo editorial “The world Company” para a criação da versão *web* dos seus jornais. Posteriormente, em 2005, foi liberado sob a licença BSD (*Berkeley Software Distribution)*, tornando-se assim um *software* de código aberto, segundo (SANTANA, 2010).

A escolha desse ambiente de desenvolvimento w*eb* (Django) é baseado nas vantagens que são, por ele, disponibilizadas. Ainda, oferece um sistema de *templates* para a geração de páginas *HyperText Markup Language* (HTML). E também, contém um sistema de administração, cujo sistema fornece uma interface automática de administração, sendo um mecanismo extremamente poderoso para gerenciar os dados da aplicação. O APÊNDICE C

traz a imagem do sistema de administração do f*ramework* Django. Esse *framework* suporta, nativamente, vários bancos de dados. O escolhido para a aplicação, trata-se do SQLite3 e vem instalado juntamente com o Python. O APÊNDICE D, mostra as configurações iniciais feitas no Django para adicionar o banco escolhido e também ilustra as habilitações dos módulos feitas para obter as vantagens que o ambiente proporciona, bem como o módulo da administração do *site* (Django.contrib.admin).

O APÊNDICE E ilustra as categorias que foram adicionadas no banco de dados e no APÊNDICE F, as questões.

4.3.1 Funcionamento da ferramenta Infoquiz

É essencial que uma organização identifique os seus requisitos de segurança da informação. Existem três fontes principais de requisitos de segurança da informação, (ABNT, 2005).

> 1. Uma fonte é apartir da análise/avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócio da organização. Por meio da análise/avaliação de riscos, são identificadas as ameaças aos ativos e as vulnerabilidades destes, e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.
> 2. Uma outra fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural.
> 3. A terceira fonte é um conjunto particular de princípios, objetivos e os requisitos do negócio para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações. (ABNT, 2005, p. XI)

A partir desses requisitos analisados, o gestor responsável da área de segurança da informação, responderá o questionário.

A Figura 6 mostra a imagem da página inicial da ferramenta, o usuário selecionará a seção desejada para responder. No APÊNDICE G contém a programação da página inicial.

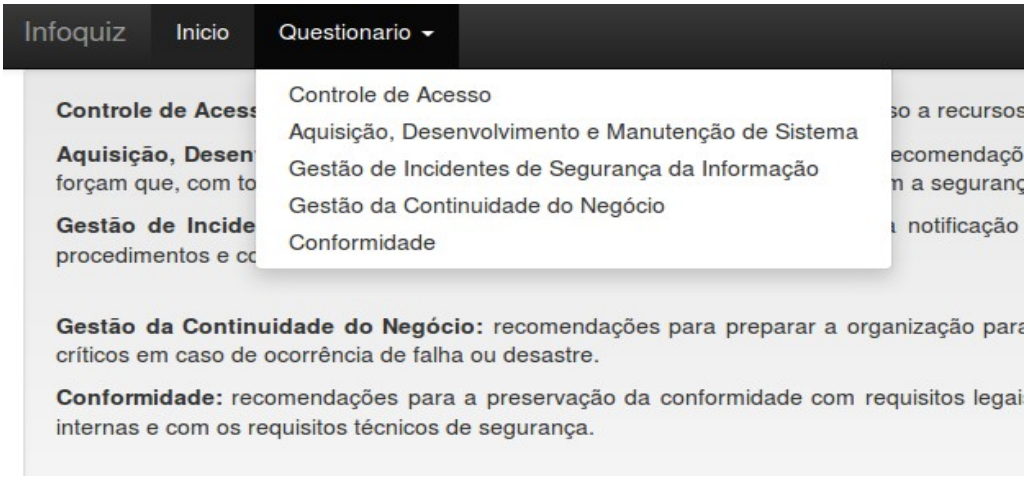


Figura 6 - Página Inicial da Infoquiz

A Figura 7 mostra a página da Infoquiz, conforme a seção que o usuário selecionou, nesse exemplo, trata da seção controle de acesso. Pode-se observar que algumas categorias são listadas, tais como, Requisitos de negócio para controle de acesso, Gerenciamento de acesso do usuário e assim sucessivamente.

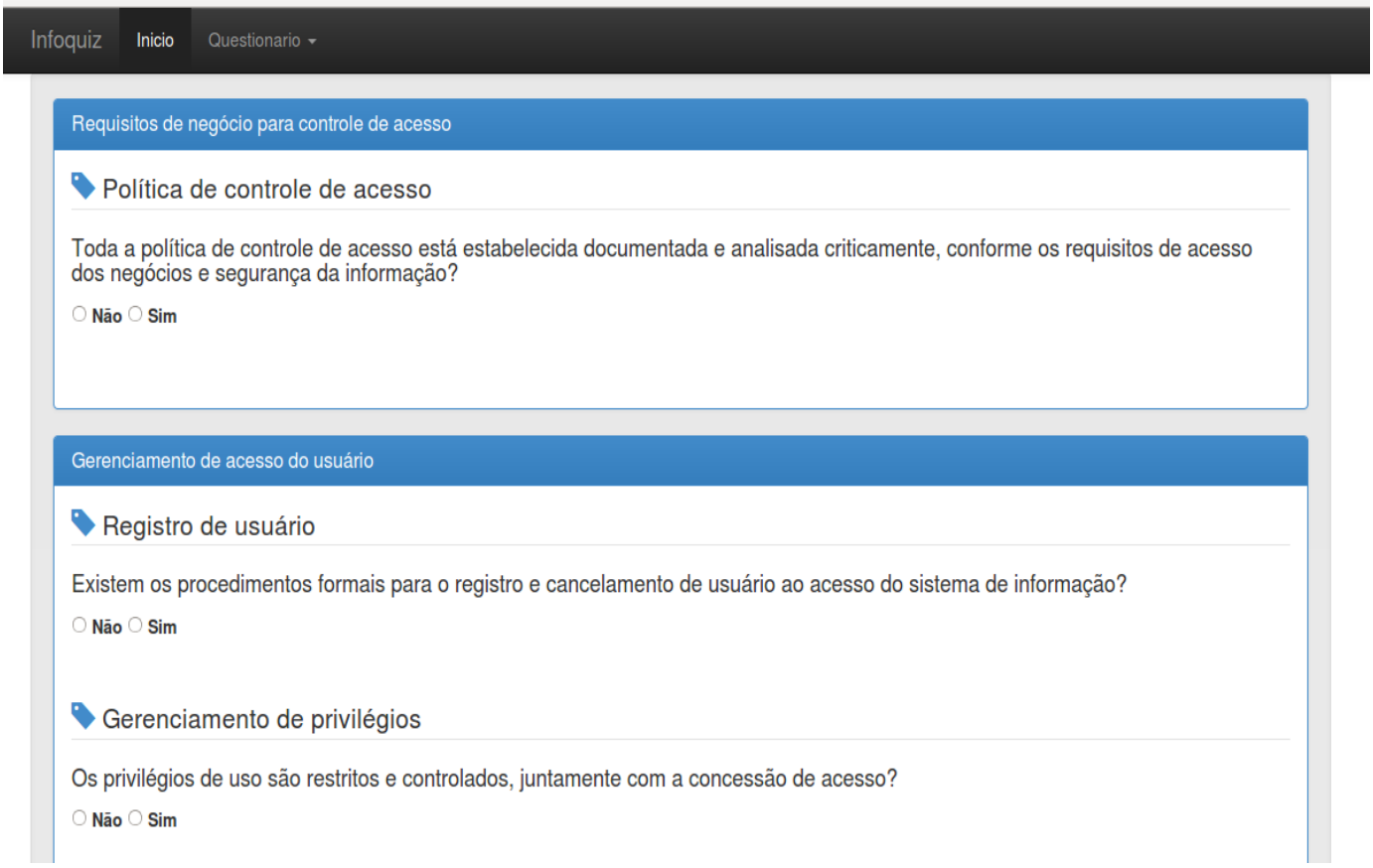


Figura 7 - Página da Infoquiz para responder o questionário

O gestor responderá de acordo com o controle existente no sistema de gestão da empresa. Existe uma pergunta principal, que é referente ao controle existir ou não, apresenta-se duas opções: (NÃO ou SIM). Diante do (NÃO), o gestor passará para a próxima categoria e a resposta não é salva. Quando a resposta for (SIM), as demais questões em controles detalhados serão mostrados para serem respondidas, Figura 8.

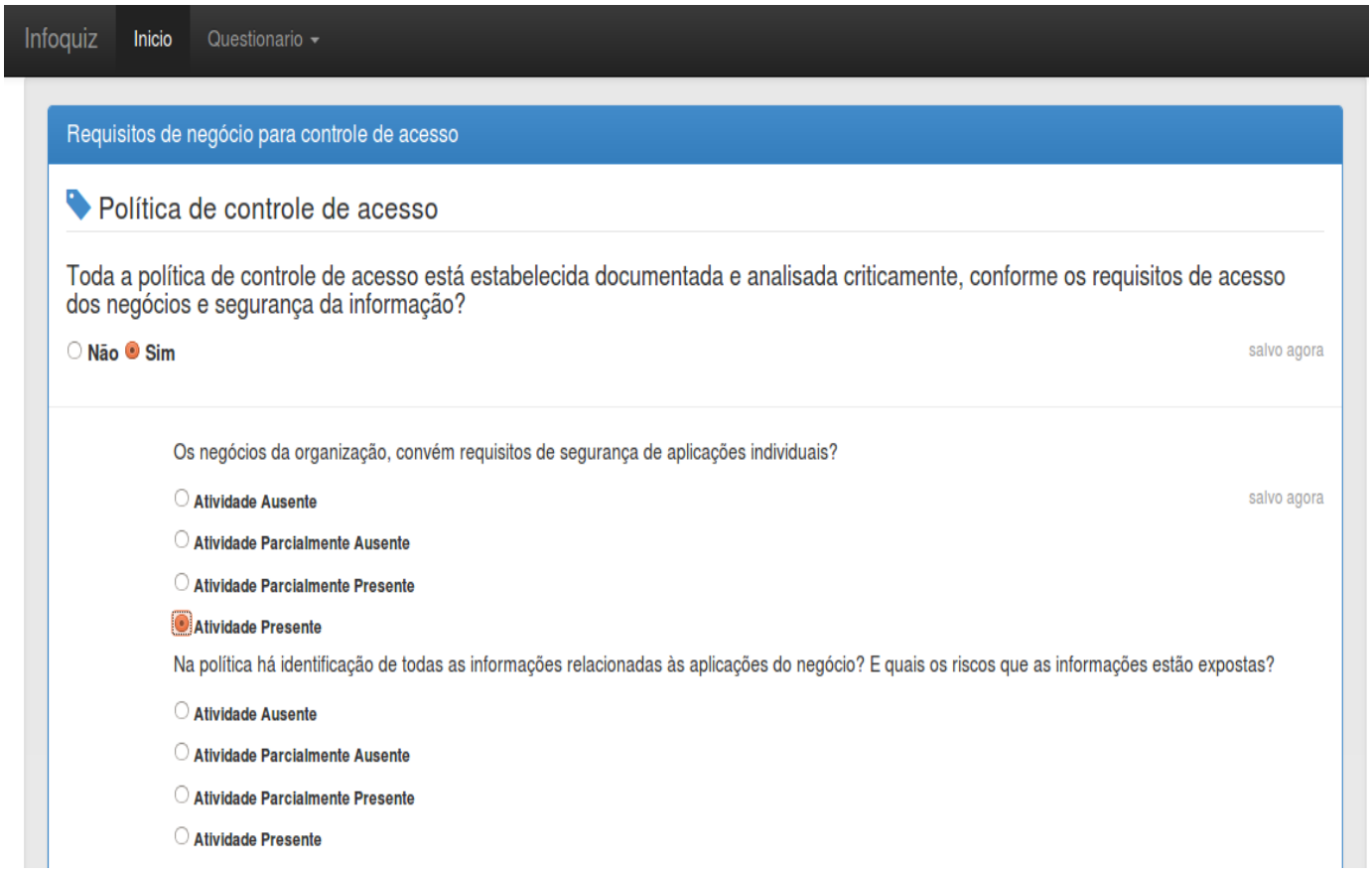


Figura 8 - Questão principal selecionada para respondê-la

Neste momento, o gestor analisará o controle, conforme a Figura 9 e responderá a altenativa correspondente com sua atividade. Caso a atividade não encontra-se empregada na empresa marcará (ATIVIDADE AUSENTE). Se a atividade, encontra-se de forma parcial ausente, ou seja, algumas atividades não são realizadas e outras sim, selecionará a (ATIVIDADE PARCIALMENTE AUSENTE), e algumas atividades são realizadas, responderá (ATIVIDADE PARCIALMENTE PRESENTE).

Diante das atividades que estão na sua totalidade empregada na empresa marcará (ATIVIDADE PRESENTE) e as respostas são salvas no banco de dados.

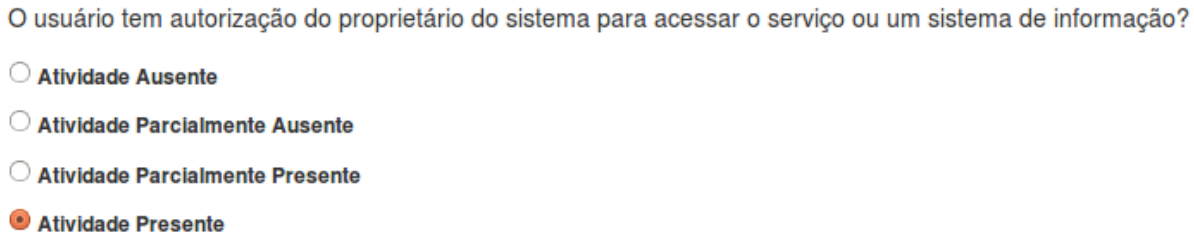


Figura 9 - Questão do controle mais específico

Após o gestor responder todas as questões de acordo com o sistema da gestão de segurança da informação, clicará em (ENVIAR), conforme a Figura 10.

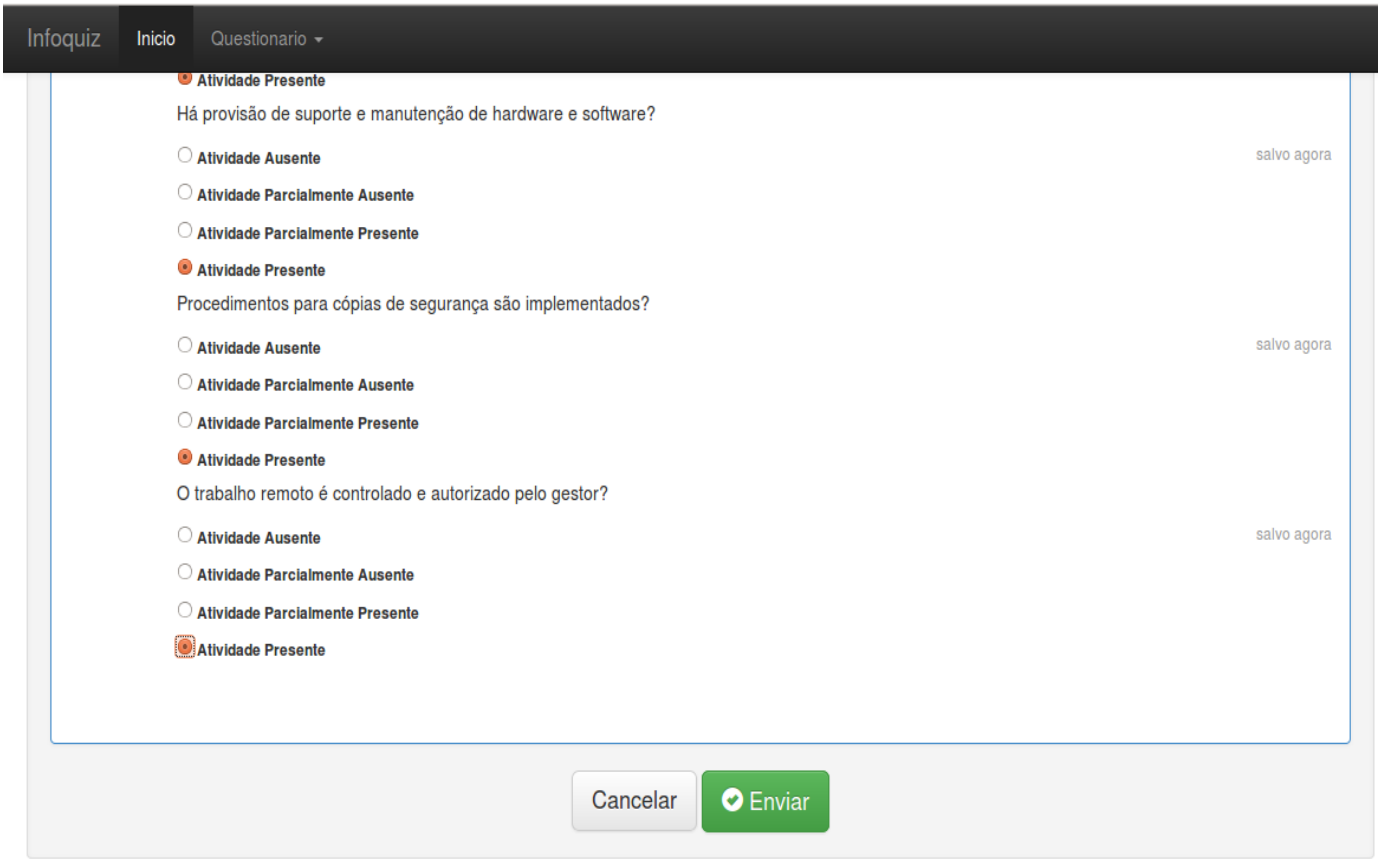


Figura 10 - Enviar as respostas para a contabilização

Após as respostas serem contabilizadas, o resultado final será mostrado conforme a Figura 11. Neste exemplo, todas as questões estavam selecionadas como (ATIVIDADE PRESENTE), por isso da resposta 100%.

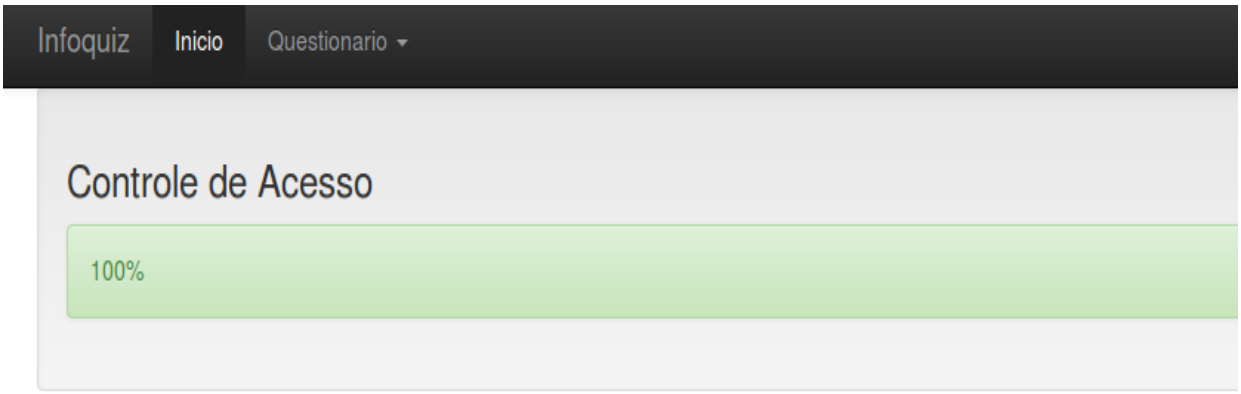


Figura 11 - Enviar as respostas para a contabilização

4.3.2 Cálculo da ferramenta Infoquiz

O cálculo da ferramenta é de extrema importância, pois ele mostra o resultado final das questões respondidas na Infoquiz. Para efetuar o cálculo, salienta-se que, ele é realizado a partir da questão principal no momento que o usuário da ferramenta selecionar o (SIM). E adentrar nas questões (filhas), que equivalem aos controles mais específicos. As alternativas, de cada questão (filha) corresponde, conforme a Figura 12, a valores definidos entre (zero e três).

```
RESPOSTA_CHOICES = (
        (0, u'Atividade Ausente'),
        (1, u'Atividade Parcialmente Ausente'),
        (2, u'Atividade Parcialmente Presente'),
        (3, u'Atividade Presente'),
    )
```

Figura 12 - Valores dados a cada resposta

Para efetuar o cálculo (percentual) da ferramenta Infoquiz, partindo do pressuposto que o número de questões é variável, bem como o valor resultante da cada resposta, temos:

Por exemplo: 08 (questões respondidas) – cada uma pode variar de (zero a três) pontos.

Q1= 02 pts, Q2= 03 pts, Q3= 0 pts, Q4= 0 pts, Q5= 01 pts, Q6= 0 pts, Q7= 01 pts e Q8= 01 pts: Somatório= 08 pts

Logo, tem-se (Somatório*100)/valor máximo da pontuação (número de questões respondidas*3)

Então temos: (08*100)/24 = **33,33%**

Exemplo 02: (24*100)/24 = **100%**

Assim, a Figura 13 ilustra uma pequena parte dos processos, principalmente o cálculo. No APÊNDICE H mostra todos os procedimentos realizados para a verificação de todas questões, inclusive a busca no banco de dados. O APÊNDICE I contém a programação das tabelas (categoria e questão) de suma importância para administrar a adição das categorias e questões no banco de dados e, no APÊNDICE J as ilustrações de ambas.

```
#loop para percorrer as questoes da categoria e buscar suas respostas
for x in q:

    try:
        #vericar se existe resposta
        res = Resposta.objects.get(Q(questao=x) & Q(skey=request.session.session_key))
        re = res.resposta
        #add resposta na lista
        r_list.append(float(re))
    except:
        #se nao existir colocar zero na lista
        re = 0
        r_list.append(re)
#somar a resposta do usuario
soma = sum(r_list)
#pegar qual a pontuacao maxima do usuario
pontuacao_maxima = nquestoes*3
#fazer a regra de 3 para obter  o %
percent = int(round((soma*100)/pontuacao_maxima))
```

Figura 13 - Cálculo da ferramenta Infoquiz

5 AVALIAÇÃO DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO COM A FERRAMENTA INFOQUIZ: ESTUDO DE CASO

Para garantir as funcionalidades apresentadas da ferramenta Infoquiz, foi experimentada numa Rede de Supermercados de Santa Maria - RS. A empresa, contém (matriz e filiais), porém cada loja tem acesso somente ao seu sistema, eles não são integrados. Na empresa testada, segundo a executiva (responsável pela administração da empresa), contam com 300 colaboradores, destes somente 60 usuários são ativos no que se refere a utilização do sistema. O *software* que a empresa trabalha chama-se Superus. É um *software* terceirizado pela empresa Sicom, a qual presta serviços de atualização e manutenção do sistema. O Superus contêm vários módulos, cada um com sua função. Ele comporta vários setores, como o financeiro, recursos humanos, estoque e etc.

As questões foram direcionadas a dois colaboradores da empresa, sendo um deles o supervisor, que possui completo acesso ao sistema Superus e, outro que desempenha atividades na área de TI.

5.1 Análise do sistema com a ferramenta Infoquiz e resultados

O acesso do sistema da empresa (Superus) não tem alta rotatividade, geralmente são pessoas de confiança com anos de empresa que possuem o acesso, conforme mencionado pela executiva.

Segundo a norma (ABNT, 2005), precisa-se analisar cada requisito conforme os negócios da empresa. De acordo com a ferramenta criada, a primeira seção testada foi o controle de acesso.

Na seção controle de acesso, o objetivo é analisar o controle do acesso à informação. A primeira pergunta realizada trata-se da utilização da política de controle de acesso. Se existe uma política documentada com base nos requisitos de acesso dos negócios da Rede de Supermercados. As demais questões foram respondidas em relação ao gerenciamento de acesso do usuário ao sistema, suas responsabilidades, controle de acesso à rede da empresa, e também, se há controle de acesso ao sistema operacional, quando é utilizada computação móvel e recursos de trabalhos remoto. Nesta seção de controle de acesso a empresa obteve 71% em conformidade. Nem todos os controles e diretrizes, segundo (ABNT, 2005), podem

ser aplicados. Consta, na mesma norma, ABNT (2005, p XIII.) que “deve-se observar que as medições de segurança da informação estão fora do escopo desta Norma”, logo a ferramenta Infoquiz não analisa parâmetros para calcular o quantitativo de segurança da informação, num determinado local. E sim, como citado anteriormente, analisar a conformidade da gestão de segurança da informação da empresa, com a norma trabalhada.

Na seção Aquisição, Desenvolvimento e Manutenção de Sistema, algumas categorias foram respondidas tais como requisitos de segurança de sistemas de informação, que tem por objetivo garantir que segurança é parte integrante de sistemas de informação. As demais categorias respondidas foram processamento correto das aplicações, controles criptográficos, segurança dos arquivos do sistema, segurança em processos de desenvolvimento/suporte e gestão de vulnerabilidades técnicas. O negócio da empresa em certas categorias não se adequaram, por isso obteve 30% em conformidade.

Na seção Gestão de Incidentes de Segurança da Informação, tem por objetivo notificar eventos de segurança da informação. As perguntas realizadas referem-se aos eventos de incidentes, quando ocorre um evento referente a segurança da informação, se eles são divulgados por canais apropriados da direção e o mais breve possível. Como que são feitas as coletas de evidências até os responsáveis serem responsabilizados e entre outras perguntas realizadas Obteve-se 39% em conformidade neste quesito.

Na seção Gestão da Continuidade do Negócio, trata sobre os aspectos da gestão da continuidade do negócio relativos à segurança da informação. Questões foram indagadas, referente aos riscos da organização se estão expostos, se há uma visão de entendimento quanto aos pequenos ou mais sérios problemas, se eles são vistos como riscos para a organização. Eventos por exemplo, como falha de equipamento, erros humanos, furto ou roubo, incêndio, desastres naturais e atos terroristas. Foi perguntado se ocorre avaliações de riscos para determinar a probabilidade e impacto de tais interrupções. Também foi perguntado se existe procedimentos que permitem a recuperação e restauração das operações do negócio. E quanto ao melhor compreendimento do plano de continuidade dos negócios, se ocorre atividades de treinamento, conscientização e educação, para os processos continuarem efetivos. As respostas foram contabilizadas e obteve-se 72 % em conformidade com a norma.

Na seção Conformidade com os requisitos legais, questões foram perguntadas sobre os seguintes itens: a proteção de qualquer material que possa ser considerado como propriedade intelectual é divulgada uma política de conformidade com os direitos onde definem o uso legal de produtos de *software* e de informação. Da mesma forma, se são mantidas provas e evidências da propriedade de licenças manuais. Referente a

implementação de controles para assegurar que o número máximo de usuários permitidos não excede o número de licenças adquiridas foi perguntado. Os gestores analisam criticamente a intervalos regulares, a conformidade do processamento da informação com as políticas, normas e quaisquer outros requisitos de segurança? Para usar testes de invasão ou avaliações de vulnerabilidades do sistema, são tomadas precauções, uma vez que tais atividades podem comprometer a segurança do sistema? E demais questões que foram indagadas, obteve-se 64 % em conformidade.

A ferramenta Infoquiz, diante do seu propósito, contabilizou as respostas e gerou os relatórios de cada categoria. Pode-se observar em alguns critérios que, a avaliação de gestão de segurança da informação da Rede de Supermercados de Santa Maria – RS, poderia efetuar alguns ajustes quanto a conformidade com a norma. Salienta-se que, a executiva da empresa ficou grata por questões que foram perguntadas restando um alerta de extrema relevância no estudo. A pergunta realizada focou-se nas trocas de senhas dos usuários do sistema. O controle de acesso ao sistema é individual. Cada usuário possui seu (login e senha). Essa troca de senha pessoal somente existe no primeiro acesso ao sistema. Eles não tem por regra trocarem periodicamente as senhas. Logo, esse controle da senha pode se ajustar sendo relevante para o sistema de gestão da empresa. A Tabela 3 sumariza os relatórios finais da ferramenta Infoquiz.

Tabela 13 - Avaliação da gestão de segurança da informação em conformidade com a norma

Seções	100%
Controle de acesso	**71%**
Aquisição, Desenvolvimento e Manutenção de Sistema	**30%**
Gestão de Incidentes de Segurança da Informação	**39%**
Gestão da Continuidade do Negócio	**72%**
Conformidade	**64%**

6 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Este trabalho apresentou um sistema *Web* denominado como ferramenta Infoquiz, cuja principal função é analisar a gestão de segurança da informação de uma organização em conformidade com a norma (ABNT, 2005). A ferramenta Infoquiz possui mecanismos que servirá para medir a efetividade da gestão. É uma estratégia rápida para os gestores avaliarem os seus riscos e tratarem eles de acordo com a norma.

Como visto, de acordo com as estatísticas da pesquisa global de segurança da informação (PwC, 2013), afirma-se que as políticas de gestão de usuários, segurança da aplicações, entre outros, permanecem em vigor em suas empresas, mas houve queda em relação ao ano passado. A pesquisa diz que, “as empresas atuam em movimento pendular, os padrões de segurança são rígidos ao máximo ou relaxando-os de maneira excessiva. E que o grande desafio está em manter o equilíbrio”, isso é o que se busca com a ferramenta Infoquiz, além de colaborar com o equilíbrio dos padrões adotados de segurança. Percebe-se que a empresa estudada, num descuido, não troca a senha do controle de acesso ao sistema periodicamente. Pode parecer um mero detalhe, mas isso faz grande diferença. Os efeitos pelo vazamento da senha do sistema, por aquelas pessoas que são mal intencionadas, podem ser enormes para empresa, tanto prejuízo financeiro como comprometer o sistema de informação. Esses riscos precisam ser avaliados e mantidos sob controle, para isso, é fundamental estar em acordo com a norma que norteia a política de segurança da informação da empresa. A Infoquiz mostra-se efetiva para manter uma gestão sob constante monitoração e revisão.

No referencial bibliográfico pesquisado não identificou-se propostas que utilizassem uma abordagem em página *Web* como apresentado neste trabalho.

Adicionalmente, pretende-se, como trabalho futuro, completar as seções que faltaram para serem trabalhadas. Pretende-se também, testar a ferramenta em outros ambientes organizacionais para poder efetuar uma comparação de cada gestão adotada nas empresas. E realizar a atualização do questionário implementado com a nova norma ABNT NBR ISO/IEC 27002:2013 – Código de Prática para controles de Segurança da informação. Essa norma, foi atualizada no período em desenvolvimento do presente trabalho, observou-se algumas modificações, porém sua essência continua a mesma. Segundo (ABNT, 2013), ela fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização, tendo o mesmo objetivo que a norma 27002:2005.

REFERÊNCIAS

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2005. 120 p.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=306582> Acesso em: 27 de dez.2013

BEAL, A. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações** – São Paulo: Atlas, 2005.

CARUSO, A. A.C.; STEFFEN, F. D. **Segurança em Informática e de Informações** – São Paulo: Editora SENAC São Paulo, 1999.

COELHO, F. E. S.; ARAÚJO, L. G. S. de. **Gestão da Segurança da Informação: NBR 27001 e 27002**. Rio de Janeiro: Escola Superior de Redes, 2013.

FAGUNDES, L. L.; de.. In: **Aula 02 27k - Normas para Gestão da Segurança da Informação** : São Leopoldo: UNISINOS Notas de aula. Disponível em: <professor.unisinos.br/llemes/Aula02/Aula02.pdf> Acesso em: 05 de dez.2013

HEUSER, C. A.; **Projeto de Banco de Dados**. RS: UFRGS, 1998. Disponível em :

<http://www.passeidireto.com/arquivo/1925740/projeto-de-banco-de-dados-carlos-alberto-heuser>. Acesso em: 26 de out.2013

NAKAMURA, E. T.; GEUS, P. L. de. **Segurança de Redes em Ambientes Cooperativos**. 7th.ed São Paulo, Brasil: Novatec Editora, 2007.

OLIVA, R. P.; OLIVEIRA, M. **Elaboração, Implantação e Manutenção de Política de Segurança por Empresas no Rio Grande do Sul em relação às recomendações da NBR/ISO17799** - ENANPAD, 2003.

PwC. **Pesquisa Global de Segurança da Informação 2013**. Disponível em: <http://www.pwc.com.br/pt_BR/br/estudos-pesquisas/assets/pesquisa-seguranca-inforrmacao-13.pdf >. Acesso em: 08 dez. 2013

RNP. REDE NACIONAL DE PESQUISAS. **Atualizadas as normas 27001 e 27002 - Técnicas de Segurança.** Disponível em: <http://esr.rnp.br/noticias/atualizadas-as-normas-27001-e-27002-tecnicas-de-seguranca> Acesso em: 06 de dez.2013

SANTANA, O.; GALESI, T. **Python e Django: Desenvolvimento ágil de aplicações web –** São Paulo: Novatec, 2010

SÊMOLA, M. **Gestão da Segurança da informação: uma visão executiva** – Rio de Janeiro: Campus, 2003.

TURBAN, E.; RAINER JR, R. K.; POTTER, R. E. **Administração de Tecnologia da Informação: Teoria e Prática.** Rio de Janeiro: Campus, 2003.

APÊNDICE A – QUESTÕES ELABORADAS

11. Controle de Acesso (Seção)

11.1. Requisitos do negócio para controle de acesso (Categoria)
Objetivo: Controlar o acesso à informação.

11.1.1 Política de controle de acesso (Controle)

Toda a política de controle de acesso está estabelecida documentada e analisada criticamente, conforme os requisitos de acesso dos negócios e segurança da informação? (Sim ou não)

Observação: Se sim, responde-se as demais questões.

a) Os negócios da organização, convém requisitos de segurança de aplicações individuais?

b) Na política há identificação de todas as informações relacionadas às aplicações do negócio? E quais os riscos que as informações estão expostas?

c) Existe autorização da informação ser disseminada, os níveis de segurança a classificação das informações?

d) Há política consistente de controle de acesso e políticas de classificação da informação em diferentes sistemas e redes?

e) A proteção de acesso para dados ou serviços estão seguindo a legislação pertinente?

f) Os trabalhos comuns na organização possui um perfil de acesso de usuário-padrão?

g) Existe administração de direitos de acesso em um ambiente distribuído e conectado à rede que reconhece todos os tipos de conexões disponíveis?

h) As funções de controle de acesso, por exemplo pedido de acesso, autorização de acesso, administração de acesso, são isoladas umas das outras?

11.2. Gerenciamento de acesso do usuário
Objetivo: assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.

11.2.1 Registro de usuário

Existem os procedimentos formais para o registro e cancelamento de usuário ao acesso do sistema de informação? (sim ou não)

a) No procedimento para registro, são utilizados um identificador de usuário (ID de usuário) único ou para grupo? Se grupo é realmente necessário para o negócio? E está documentado e aprovado?

b) O usuário tem autorização do proprietário do sistema para acessar o serviço ou um sistema de informação?

c) O nível do acesso do usuário concedido é compatível com o propósito do negócio? E de acordo com a política de segurança da organização? Ou seja, não compromete nenhuma função.

d) Disponibilizam ao usuário uma declaração por escrito dos seus direitos de acesso?

e) Solicitam a assinatura do usuário, referente ao que estão cientes nas condições de acesso?

f) Asseguram ao provedores de serviço, que somente após o término dos procedimentos de autorização, que serão dados os acessos?

g) Utilizam registros formais de todas as pessoas registradas para usarem o serviços?

h) Quando os funcionários mudam de cargos, funções ou deixam a organização, removem imediatamente ou bloqueiam seus identificadores (ID) quanto ao seus direitos de acesso?

i) Periodicamente verificam as contas de usuário, caso estejam redundantes removem ou bloqueiam seus identificadores (ID)?

j) Asseguram para não atribuir para outros usuários os identificadores (ID) redundantes?

11.2.2 Gerenciamento de privilégios

Os privilégios de uso são restritos e controlados, juntamente com a concessão de acesso? (Sim ou não)

a) São identificados os privilégios para acesso a cada produto do sistema? Por exemplo, o sistema operacional, sistema de banco de dados e cada aplicação.

b) Os privilégios serão concedidos aos usuários, conforme a necessidade de uso? Por exemplo, requisitos mínimos para a sua função.

c) Há registros mantidos de todos os privilégios concedidos? Processo de autorização em andamento, convém que os privilégios não sejam fornecidos.

d) Para evitar que privilégios sejam estimulados, são incentivados a usarem rotinas de sistemas, programas de forma a não ter necessidade dos privilégios?

e) Os privilégios atribuídos aos identificadores de usuários (ID de usuário) são diferentes daqueles usados normalmente para os negócios?

11.2.3 Gerenciamento de senha do usuário

As senhas que são concedidas, são controladas através de um processo de gerenciamento formal? (Sim ou não)

a) São fornecidas senhas inicialmente seguras e temporárias, que obriga o usuário alterá-las posteriormente, para manter suas próprias senhas?

b) Fazem procedimentos de identificação do usuário, antes de fornecer senhas temporárias, substituições ou novas?

c) As senhas padrões são alteradas, após um procedimento de instalação de sistemas ou software?

11.2.4 Análise crítica dos direitos de acesso de usuário

O gestor da organização verifica a intervalos regulares a análise crítica dos direitos de acesso dos usuários ? (Sim ou não)

a) Os direitos de acesso dos usuários são revisados num período por exemplo, a cada seis meses, promoção, rebaixamento ou encerramento do contrato?

b) Caso ocorra mudança de função, encerramento de contrato os direitos são analisados e adaptados para a nova função ou cancelamento do direito de acesso?

c) Quando há autorização para direitos de acesso privilegiado especial, analisam em intervalos mais freqüentes?

11.3. Responsabilidade dos usuários

Objetivo: Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou furto da informação e dos recursos de processamento da informação.

11.3.1. Uso de senhas

Aos usuários são solicitados a seguir as boas práticas de segurança da informação nos usos da senha? (Sim ou não)

a) Aos usuários é pedido para manter a confidencialidade das senhas?

b) São informados para evitar o uso das senhas anotadas em papéis, arquivos ou dispositivos móveis?

c) Caso haja um possível comprometimento do sistema ou da própria senha, são alteradas para evitar riscos?

d) São selecionados senhas de qualidades? Por exemplo, ter tamanho mínimo, possuem facilidade para a lembrança, não usar palavras vulneráveis que possam ser encontradas facilmente em um dicionário. Ou, ter como base algo ou alguém, (telefone, datas de aniversário ou nomes).

e) As senhas são modificadas regularmente, as privilegiadas são trocadas com certos intervalos de tempo?

f) No momento de primeiro acesso ao sistema, as senhas temporárias são trocadas?

11.3.2 Equipamento de usuário sem monitoração

Os equipamentos que não possuem monitoração, os usuários são cientes da segurança da informação e procedimentos para protegê-los desacompanhados? (Sim ou não)

a) Utilizam um procedimento de proteção de tela com senha?

b) Proteger os computadores, procurando desconectar o login de usuário dos computadores de grande porte, como servidores e computadores pessoais, quando a sessão for terminada?

11.3.3 Política de mesa limpa e tela limpa

É adotada a política de mesa limpa e tela limpa? (Sim ou não)

a) As informações do negócio salvas em papéis ou em mídias de armazenamento eletrônicas, são guardadas em locais seguros quando não em uso?

b) Os computadores são protegidos com o procedimento de travamento de tela e teclado, tudo controlado por senha, ou mecanismo de autenticação quando sem monitoração ou não usados ?

c) São evitados o uso de máquinas fotográficas digitais, ou outro tipo de tecnologia de reprodução?

d) São consideradas impressoras com função de código PIN?

11.4. Controle de acesso à rede
Objetivo: prevenir acesso não autorizado aos serviços da rede.

11.4.1. Política de uso dos serviços da rede
Os usuários recebem seus acessos para os serviços confome sua autorização de usar? (Sim ou não)

a) Existe um procedimento de autorização para determinar quem tem permissão para acessar em quais redes e também serviços de rede?

b) Há proteção de acesso a conexões ?

11.4.2. Autenticação para conexão externa do usuário

O acesso de usuários remotos são controlados através de métodos apropriados de autenticações? (Sim ou não)

a) Para alcançar essa autenticação segura dos usuários remotos numa conexão externa, é usada alguma técnica baseada em criptografia?

b) Alguma linha privada dedicada é usada para garantir a origem das conexões?

c) Há algum controle adicional para controlar o acesso a redes sem fios?

11.4.3. Identificação de equipamento em redes

Existem identificações dos equipamentos? (Sim ou não)

a) O equipamento identificado pode ser usado para conectar-se a alguma rede, por exemplo?

b) Os identificadores fazem a proteção física do equipamento?

11.4.4. Proteção e configuração de portas de diagnóstico remotas

São controlados os acessos físicos e lógicos das portas de configurações e de diagnósticos?(Sim ou não)

a) Para o acesso às portas de diagnóstico e configuração é usado uma tecla de bloqueio?

b) Para controlar o acesso físico às portas são usados procedimentos de suporte? Por exemplo, combinação de acesso requerido entre o gestor dos serviços e pelo pessoal de suporte do hardware/software.

11.4.5. Segregação de redes

Os serviços de informação, usuários e sistemas de informação são divididos em grupos? (Sim ou não)

a) As grandes redes são divididas em diferentes domínios de redes lógicas para controlar a segurança da informação? Por exemplo, domínios externos de uma rede e internos de uma organização.

b) Os domínios externos e internos são definidos com base em uma análise/avaliação de riscos e os requisitos diferentes dentro de cada um dos domínios?

c) Para a implementação na rede, é utilizado um procedimento como um gateway instalado entre as duas redes? Esse mecanismo controla o acesso e o fluxo de informações entre os dois domínios.

d) Há outro método para segregar domínios lógicos? Como restringir acesso de rede usando redes privadas virtuais para grupos de usuário dentro da organização?

e) Nas redes sem fios de internas e privadas tem controles de autenticação forte ou métodos criptográficos?

11.4.6. Controle de conexão de rede

As redes compartilhadas nos limites da organização, possuem restrições quanto ao controle de capacidade de acesso dos usuários da rede? (Sim ou não)

a) As restrições de conexão de usuários são através dos gateways que filtram tráfico por meio de tabelas ou regras predefinidas? Por exemplo, mensagens, transferência de arquivo, acesso interativo acesso a aplicação.

b) As redes compartilhadas possuem também, direitos de acesso entre redes num certo período do dia ou datas?

11.4.7. Controle de roteamento de redes

O controle de roteamento na rede controla as conexões do computador e fluxos de informação para não violarem a política de controle de acesso das aplicações do negócio? (Sim ou não)

a) Há algum controle interno ou externo usado, por exemplo um gateway de segurança para validar endereços de origem e destino se o proxy e/ou a tecnologia de tradução de endereço forem empregados?

11.5. Controle de acesso ao sistema operacional

Objetivo: São usados procedimentos para prevenir acesso não autorizado aos sistemas operacionais.

11.5.1. Procedimentos seguros de entrada no sistema (log-on)

São utilizados procedimentos seguros na entrada do sistema operacional? (Sim ou não)

a) No acesso ao sistema operacional é mostrado um aviso geral para informar que o computador somente será acessado por usuários autorizados?

b) São exibidas mensagens de ajuda durante o procedimento de entrada (*log-on)* que poderiam auxiliar um usuário não autorizado?

c) É limitado o número de tentativas de acesso ao sistema (*log-on*), caso a tentativa tenha falhado, por questões tempo de espera antes de permitir novas tentativas?

d) A senha que está sendo mostrada é ocultado os caracteres por símbolos?

e) As senhas são trasmitidas em texto claro pela rede?

11.5.2. Identificação e autenticação de usuário

Todos os usuários possuem um identificador único (ID de usuário) para uso pessoal e exclusivo? (Sim ou não)

a) Esse tipo de controle são aplicados para cada tipo de usuário (pessoal do suporte, técnico, operadores, administradores de rede, programadores do sistema e admnistradores de banco de dados)?

b) Os identificadores são utilizados para rastrear atividades ao indivíduo responsável?

c) O gestor aprova a documentação, referente ao identificador de usuário (ID de usuário) compartilhado por um grupo para um trabalho específico, onde exista benefício ao negócio?

d) Para se obter autenticação forte e verificação de identidade é requerida, são utilizados alguns métodos como autenticação de senhas como meios criptográficos, cartões inteligentes, ou outro método?

11.5.3. Sistema de gerenciamento de senha

São usados gerenciamento de senhas para assegurar senhas de qualidade? (Sim ou não)

a) Para poder identificar as responsabilidades de cada usuário, são usados os identificadores de usuários (ID de usuário) e senha individual criados?

b) Os usuários podem modificar suas próprias senhas, sempre incluindo um procedimento de confirmação para evitar erros?

c) Sempre escolhem senhas de qualidade?

d) A troca de senha é obrigatória?

e) Os usuários são obrigados a trocarem a senha temporária no primeiro acesso?

f) São mantidos os registros das senhas anteriores utilizadas e bloqueadas a reutilização?

g) As senhas são armazenadas e transmitidas de forma protegida, (criptografada)?

11.5.4. Uso de utilitários de sistema
Para controle dos sistemas e aplicações são usados programas utilitários? (Sim ou não)

a) Há limitação do uso dos utilitários de sistema a um número mínimo de usuários confiáveis e autorizados?

b) Quando são desnecessários para o sistema, há remoção ou desabilitação de todos os softwares utilitários?

c) Para usar os utilitários de sistema são feitos os procedimentos de identificação, autenticação e autorização?

11.5.5. Limite de tempo de sessão
Quando alguma sessão está inativa após um período de tempo, são encerradas? (Sim ou não)

a) Para a desconexão da sessão, analisam os riscos de segurança da área, a classificação da informação, as aplicações que estão sendo utilizadas?

11.5.6. Limitação de horário de conexão
Para proporcionar uma segurança adicional, são levados em conta os horários de conexão, principalmente para aplicações de alto risco? (Sim ou não)

a) Para áreas públicas ou externas fora dos limites do gerenciamento de segurança da organização, são utilizados janelas de tempo predeterminadas para as sessões?

b) São considerados reautenticações em intervalos de tempo?

11.6. Controle de acesso à aplicação e à informação
Objetivo: prevenir acesso não autorizado à informação contida nos sistemas de aplicação.

11.6.1. Restrição de acesso à informação
Para o acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte são definidos essas restrições na política de controle de acesso? (Sim ou não)

a) Os requisitos de restrições de acessos, trata de controlar os menus de acesso às funções do sistema?

b) Outro ponto de controle de acesso dos usuários às informações, por exemplo somente leitura ou execução de um sistema de aplicação?

11.6.2. Isolamento de sistemas sensíveis
Um ambiente computacional que trata de um sistema de aplicação sensível é isolado? (Sim ou não)

a) Há cuidados quando se executa uma aplicação sensível em um ambiente?

b) Identificam os sistemas de aplicação com os quais compartilhará recursos?

c) A sensibilidade de um sistema de aplicação é analisado e executado em um computador dedicado? Ou compartilha recursos somente com sistemas de aplicação confiáveis?

11.7. Computação móvel e trabalho remoto
Objetivo: garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.

11.7.1. Computação e comunicação móvel
Para a segurança da informação dos negócios a política de computação móvel inclui requisitos de proteção física, controles de acesso, técnicas de criptográficas, cartões inteligentes e telefones celulares? (Sim ou não)

a) Cópias de segurança das informações críticas de negócio são feitas regularmente?

b) Os recursos de computação móvel estão protegidos fisicamente contra furto?

11.7.2. Trabalho remoto
Existe um política com planos operacionais, e procedimentos sejam desenvolvidos e implementados para atividades de trabalho remoto? Por exemplo, proteção ao local do trabalho remoto, o acesso remoto não autorizado aos sistemas internos da organização. (Sim ou não)

a) Para a segurança física no local do trabalho remoto é utilizado um procedimento de segurança?

b) No acesso remoto aos sistemas da organização interno, os requisitos de segurança são implementados?

c) Nesse ambiente externo a sua organização, equipamentos de propriedade particular que não esteja sob controle da organização é permitido?

d) São implementadas regras, quanto ao acesso de familiares e visitantes ao equipamento e à informação?

e) Quando as atividades de trabalhos remotos cessarem, são cessados os direitos de acesso e devolução do equipamento?

f) Há provisão de suporte e manutenção de hardware e software?

g) Procedimentos para cópias de segurança são implementados?

h) O trabalho remoto é controlado e autorizado pelo gestor?

12. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

12.1. Requisitos de segurança de sistemas de informação
Objetivo: garantir que segurança é parte integrante de sistemas de informação.

12.1.1. Análise e especificação dos requisitos de segurança
Um sistema de informação novo, ou melhorias num sistema existente são especificados requisitos de controle de segurança? (Sim ou não)

a) Na compra de produtos, um processo formal de aquisição de testes são seguidos?

b) Nas situações em que funcionalidades de segurança de um produto proposto que não satisfaçam requisitos especificados, o risco foi introduzido, essa situação é considerada antes da compra do produto?

c) Caso as funcionalidades adicionais incorporadas acarretem riscos à segurança, são desativadas ou a estrutura de controles proposta seja analisada criticamente para determinar se há vantagem na utilização das funcionalidades em questão?

12.2. Processamento correto nas aplicações
Objetivo: Prevenir as ocorrências de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.

12.2.1. Validação dos dados de entrada
Para garantir que os dados de entrada são corretos, eles passam por um processo de validação? (Sim ou não)

a) No primeiro momento são feitas checagens na entrada de transações de negócios em dados permanentes, por exemplo, nomes, endereços, limites de crédito e número de referência de clientes?

b) Outros métodos de checagem de entrada de dados, parâmetros em tabelas por exemplo, preços de venda, tarifas de impostos, esses tipos de diretrizes são implementadas?

12.2.2. Controle do processamento interno
Fazem checagem de validação para detectar corrupção de informações? (Sim ou não)

a) A implementação das aplicações garantem que os riscos de falhas de processamento que levem à perda de integridade sejam minimizados?

b) São utilizados procedimentos para evitar que programas rodem na ordem errada, e rodados no tempo certo?

c) Programas apropriados são utilizados para a recuperação de falhas?

d) Há verificações de integridade, autenticidade ou qualquer outra característica de segurança de dados?

e) As atividades envolvidas no processamento é guardada em registros?

12.2.3. Integridade de mensagens
Para garantir autenticidade em mensagens e proteção da integridade, são utilizados requisitos apropriados? (Sim ou não)

a) A integridade de uma mensagem requerida é analisada/avaliada quanto aos seus riscos?
b) Para implementação de autenticação de mensagens alguma técnica de criptografia é utilizada?

12.2.4. Validação de dados de saída
Para as informações armazenadas, os dados de saída das aplicações saber se estão corretas são verificados sua exatidão com algum procedimento? (Sim ou não)

a) Algum controle de contagem é usado para garantir o processamento de todos os dados?

b) O fornecimento de informação é suficiente para que um leitor ou um sistema de processamento possa determinar a exatidão, e classificação das informações?

c) Há procedimentos para responder os testes de validação dos dados de saída?

d) São criados registros de atividades do processo de validação dos dados de saída?

12.3. Controles criptográficos
Objetivo: Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos. Usando gerenciamento de chaves para apoiar as técnicas criptográficas.

12.3.1. Política para o uso de controles criptográficos
Existe alguma política para o uso de controle criptográfico, para a proteção da informação? (Sim ou não)

a) São requeridos a identificação do nível de proteção conforme a análise/avaliação de risco da informação?

b) Para informações sensíveis transportadas em celulares, mídias removíveis, dispositivos ou linhas de comunicação é analisado o uso de criptografia?

c) O gerenciamento de chaves lida com métodos para a proteção das chaves criptográficas? E também a recuperação de informações cifradas, no caso de chaves perdidas, comprometidas ou danificadas?

12.3.2. Gerenciamento de chaves
O processo de gerenciamento de chaves apoiam as técnicas criptográficas pela organização? (Sim ou não)

a) O gerenciamento de chaves usa métodos de segurança para gerar chaves para diferentes sistemas criptográficos e diferentes aplicações?

b) São gerados e obtidos certificados de chaves públicas?

c) A distribuição das chaves é verificado e os usuários devidos, incluindo como utilizar?

d) As chaves são armazenadas, guardadas quando informações são armazenadas em cópias de segurança?

e) Quando um usuário deixa organização, as chaves são desativadas, ou guardadas?

f) É tratado a recuperação das chaves perdidas ou corrompidas?

g) O gerenciamento das chaves são mantidas em registros e auditoria das atividades?

12.4. Segurança dos arquivos do sistema
Objetivo: garantir a segurança de arquivos de sistema.

12.4.1. Controle de software operacional
A instalação de software em sistemas operacionais são controlados através de procedimentos? (Sim ou não)

a) Para minimizar o risco de corrupções aos sistemas operacionais, a atualização do sofware operacional, de aplicativos e de bibliotecas de programas são executadas somente por administradores treinados ou autorização gerencial?

b) Os sistemas operacionais e aplicativos, após implementados são rigorosamente testados, testes que incluam uso e segurança?

c) Um sistema de controle de configuração é utilizado?

d) Todas as atualizações dos programas operacionais são mantidos em registros?

e) As versões antigas de software são guardadas ou arquivadas, junto com todas as informações, procedimentos e detalhes de configurações de software de suporte?

12.4.2. Proteção dos dados para teste de sistema
Quando são necessários testes do sistema, os dados são protegidos e controlados? (Sim ou não)

a) Os aplicativos de sistema em ambiente de teste, tem por procedimentos controles de acessos?

b) Sempre é pedido autorização, quando for utilizado uma cópia da informação operacional para uso de um aplicativo em teste?

c) A informação operacional é apagada do aplicativo em teste, após completar os testes?

d) A cópia e o uso de informação operacional são registrados para a auditoria?

12.4.3. Controle de acesso ao código-fonte de programa
O acesso ao código-fonte de programa é restrito? (Sim ou não)

a) As bibliotecas de programa-fonte são guardados num mesmo ambiente dos sistemas operacionais?

b) As bibliotecas de programa-fonte tem restritividade ao pessoal de suporte?

c) Listagem dos programas são mantidas em ambiente seguro?

d) O controle de acesso ao código-fonte de programa são mantidos em registro de auditoria?

12.5. Segurança em processos de desenvolvimento e de suporte
Objetivo: manter a segurança de sistemas aplicativos e da informação.

12.5.1. Procedimentos para controle de mudanças
Quando há mudanças no sistemas da informação, essas são controladas por procedimentos formais? (Sim ou não)

a) Os procedimentos de controle de mudanças para a manutenção de um registro são autorizados?

b) São identificados os softwares, banco de dados e hardware que precisam de emendas?

c) Antes da implementação há garantia da aceitação das mudanças por usuário autorizados?

d) A documentação do sistema atualizado trata de garantias e a documentação antiga é arquivada ou descartada?

e) As mudanças que são implementadas, convém em horários apropriados?

f) As atualizações automáticas são usadas em aplicações críticas?

g) Tem manutenção das atualizações de software?

12.5.2. Análise crítica técnica das aplicações após mudanças no sistema operacional
Quando os sistemas operacionais são mudados há garantia de que nenhum problema ocorrerá nas operações da organização ou na segurança? (Sim ou não)

a) As mudanças são analisadas criticamente e testadas?

b) O plano anual de suporte da garantia aos testes do sistema devido às mudanças no sistema operacional?

c) Existe tempo hábil para as mudanças pretendidas em relação a comunicação, ou seja para os teste e análises antes da implementação das mudanças?

d) As mudanças que necessárias são executadas pensando no plano de continuidade de negócios?

12.5.3. Restrições sobre mudanças em pacotes de software
As mudanças em pacotes de software são controladas e limitadas com restrições? (Sim ou não)

a) Quando é necessário modificação em pacotes de softwares o risco que ocorrem em controles e nos processos de integridade são avaliados?

b) Os pacotes de atualizações requerem autorização dos fornecedores?

c) Se mudanças forem necessárias, o software original mantido e as mudanças são aplicadas numa cópia claramente identificada?

12.5.4. Vazamento de informações
O controle para evitar vazamento de informações, são implementadas? (Sim ou não)

a) Limitar o risco de vazamento de informações requer alguns cuidados, a varredura do envio de mídia para evitar presença de informação oculta é analisada?

b) A dedução de informações é um dos métodos usados, para reduzir essa possibilidade é feito algum mascaramento e a modulação do comportamento dos sistemas?

c) Produtos avaliados e certificados como sistemas de softwares reconhecidos com alta integridade são usados?

d) Conforme a legislação ou regulamento, atividades monitoradas do pessoal são testadas?

e) Há monitoração dos recursos de sistemas de computação?

12.5.5. Desenvolvimento terceirizado de software
Para o desenvolvimento de software terceirizado a organização supervisiona e monitora-os? (Sim ou não)

a) É analisado o certificado de qualidade e garantia do serviço realizado?

b) É passível de garantia no caso de falha da terceira parte?

c) A organização têm direitos de acesso para auditorias de qualidade?

d) O desenvolvimento do software é protegido com funcionalidades de segurança do código?

e) O software pronto, é averiguado com testes antes da instalação na organização para detectar algum código malicioso?

12.6. Gestão de vulnerabilidades técnicas
Objetivo: reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.

12.6.1. Controle de vulnerabilidades técnicas
As vulnerabilidades técnicas dos sistemas de informação são identificadas e tomadas medidas apropriadas para tratarem esses riscos? (Sim ou não)

a) A organização define funções e responsabilidades associadas na gestão de vulnerabilidades técnicas?

b) A organização monitora as vulnerabilidades, a análise/avaliação de riscos de vulnerabilidades, acompanhamentos dos ativos?

c) No momento da detecção de alguma vulnerabilidade, é definido um prazo para a reação através das notificações ?

d) Para algumas ações tomadas pela organização, a partir dos riscos avaliados nos sistemas vulneráveis, tratam-se de *patches*?

e) Como a urgência é exigida para tratar da vulnerabilidade técnica, depende dos controles relacionados com a gestão de mudanças?

f) Os patches usados para tratar da vulnerabilidade técnica, são avaliados os riscos e testados antes de serem instalados?

g) Quando um patch não é disponível para alguma vulnerabilidade técnica, outros controles são acessíveis a situação? Por exemplo, um firewall nas fronteiras da rede.

h) A monitoração e avaliação regularmente do processo de gestão de vulnerabilidades técnicas, são mantidos em registros de auditoria dos processos realizados?

13. Gestão de Incidentes de Segurança da Informação

13.1. Notificação de fragilidades e eventos de segurança da informação
Objetivo: Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

13.1.1. Notificação de eventos de segurança da informação
Para relatar algum evento referente a segurança da informação, são divulgados por canais apropriados da direção, e o mais breve possível? (Sim ou não)

a) Quando surge um evento de segurança da informação, funcionários, fornecedores e terceiros sabem de suas responsabilidades de notificar o mais rápido possível?

b) Funcionários, fornecedores e terceiros estão cientes dos procedimentos definidos para notificar o evento de segurança da informação, como saber o ponto de contato designado para este fim?

c) Para ajudar as pessoas a lembrar de suas ações sobre a notificação do evento é usado algum tipo de formulário?

d) No evento ocorrido às pessoas sabem do comportamento correto e identificam detalhes importantes imediatamente, por exemplo, mau funcionamento, mensagens na tela, comportamento estranho?

e) As pessoas tem consciência de não tomar ações próprias, e sim informar o evento ocorrido ao ponto e contato?

f) Os procedimentos incluem referência para um processo disciplinar formal, para as pessoas que cometem violações de segurança da informação?

13.1.2. Notificando fragilidades de segurança da informação
Quando existe uma determinada fragilidade no sistema, os funcionários, fornecedores e terceiros são instruídos a registrar e notificar qualquer observação fora do comum? (Sim ou Nao)

a) As pessoas quando observam alguma situação possível de notificação, encaminham a direção ou ao provedor de serviços o mais rápido possível?

b) Esse mecanismo de notificação de uma determinada fragilidade, é fácil, acessível e disponível as pessoas?

c) Os usuários são informados que não podem averiguar fragilidade suspeita, somente o responsável?

13.2. Gestão de incidentes de segurança da informação e melhorias
Objetivo: assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.

13.2.1. Responsabilidades e procedimentos
Para controlar a gestão referente a incidentes de segurança da organização, de uma forma rápida, efetiva e ordenada são aplicados procedimentos para a tal? (Sim ou não)

a) São utilizados procedimentos de gestão para manusear diferentes tipos de incidentes de segurança da informação, por exemplo, violações de confidencialidade e integridade?

b) Quando há falhas de sistemas de informações e perda de serviços, existem procedimetos?

c) O uso impróprio do sistema de informação, é averiguado esse incidente?

d) Um ataque de negação de serviço, utiliza-se um procedimento?

e) Para seguir procedimentos de incidentes de segurança da informação, são importantes analisar e identificar a causa do incidente, isso é feito?

f) Há um planejamento e implementação de ação corretiva, para não ocorrer novos ou repetição de incidentes?

g) A autoridade apropriada , recebe a notificação de ação como plano?

h) Quanto a auditoria, evidências coletadas e protegidas são apropriadas para analisar problemas internos?

i) O uso de auditoria para um caso de violação de contrato ou normas reguladoras ou em caso de delitos civis ou criminais, relacionados ao uso impróprio de computadores?

j) A recuperação dos sistemas com violações de segurança e correções de falhas são cuidadosamentes formalmente controladas?

k) Os funcionários explicitamente identificados e autorizados estão liberados para acessar o sistema e dados em produção?

l) As ações de emergência são documentadas, e relatadas para a direção e analisadas de maneira ordenada?

m) O controle da integridade do sistema do negócio é de uma forma rápida?

13.2.2. Aprendendo com os incidentes de segurança da informação
Os tipos, a quantidade, e os custos dos incidentes de segurança da informação são monitorados? (Sim ou não)

a) A análise de incidentes de segurança da informação de uma forma é para identificar incidentes recorrentes e de alto impacto para o negócio?

b) Na análise de incidentes podemos saber da necessidade de melhorias ou controles adicionais para limitar a frequencia, danos e custos de ocorrências futuras, e é levado em conta para o processo de política de segurança da informação?

13.2.3. Coleta de evidências

Após algum incidente de segurança da informação é acompanhado todas as ações e as evidências são coletadas, armazenadas em conformidade com as normas? (Sim ou não)

a) Os procedimentos internos são elaborados para atividades de coleta e apresentação de evidências com o propósito de ação disciplinar movida em uma organização?

b) Para se ter admissibilidade das evidências, os sistemas de informação da organização estão de acordo com qualquer norma ou código de prática?

c) O valor de uma evidência depende de algum requisito aplicável, convém qualidade e controles usados para proteger evidências de forma correta e aplicável. Condições são estabelecidas para a tal? Por exemplo, para documentos em papel, o original é mantido de forma segura, com registro da pessoa que o encontrou quem testemunhou a descoberta e qualquer investigação assegure que não foi adulterado?

d) Diante de uma informação em mídia eletrônica, são guardadas cópias e registros de todas as ações tomadas durante o processo, são mantidas de forma segura e intocável?

e) O processo de cópia de todo material de evidência é supervisionado por pessoas confiáveis e as informações sobre local, ferramentas e programas envolvidos no processo são registradas?

14. Gestão da Continuidade do Negócio

14.1. Aspectos da gestão da continuidade do negócio, relativos à segurança da informação

Objetivo: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil se for o caso.

14.1.1. Incluindo segurança da informação no processo de gestão da continuidade de negócio

Para a organização ter continuidade nos negócios, necessita-se de um processo de gestão. Na organização é utilizado algum processo de gestão com requisitos de segurança da informação?

a) Para definir um processo de gestão de continuidade dos negócios, são entendidos os riscos que a organização está exposta? Incluindo a identificação e priorização dos processos críticos do negócio?

b) Os ativos envolvidos em processos críticos do negócio, são identificados?

c) Há uma visão e entendimento do impacto de incidentes de segurança da informação?

d) Os pequenos e os mais sérios problemas são vistos como riscos para o processo de continuidade dos negócios?

e) Há identificação e consideração da implementação de controles preventivos?

f) No processamento das informações e bens da organização, há proteção e garantia da segurança de pessoal?

g) Na gestão de continuidade do negócio os documentos e detalhamento dos planos contemplam requisitos de segurança da informação alinhados a estratégia da continuidade do negócio?

h) O processo de gestão de continuidade do negócio tem responsabilidades atribuidas a um nível adequado dentro da organização?

i) Testes são realizados e atualizações referente aos planos e processos implantados?

14.1.2. Continuidade de negócios e análise/avaliação de riscos

Os eventos que podem gerar interrupções aos processos de negócio, são identificados juntos com a probabilidade de impacto e consequencias para a segurança da informação? (Sim ou não)

a) Esses eventos por exemplo, falha de equipamento, erros humanos, furto ou roubo, incêndio, desastres naturais e atos terroristas são feitos análise/avaliação de riscos para determinar a probabilidade e impacto de tais interrupções?

b) A análise/avaliação identifica, quantifica, e prioriza os critérios baseados no riscos e os objetivos pertinentes a organização?

14.1.3. Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação

Planos são desenvolvidos e implementados para a manutenção ou recuperação das operações após a ocorrência de interrupções ou falhas dos processos críticos do negócio? (Sim ou não)

a) Os procedimentos de continuidade do negócio são identificados e as responsabilidades têm concordância com o pessoal responsável?

b) São feitos procedimentos que permitem a recuperação e restauração das operações do negócio?

c) Há implementação de procedimentos para disponibilizar a informação nos prazos necessários, principalmente dependências externas ao negócio e contratos existentes?

d) Para gerenciamento de uma crise é feito a educação adequada de pessoas nos procedimentos e processos definidos?

e) Os testes e atualizações dos planos são regulares?

14.1.4. Estrutura do plano de continuidade do negócio

O plano de estrutura de continuidade do negócio assegura planos consistentes, contemplando os requisitos de segurança da informação, identificando prioridades para testes e a manutenção? (Sim ou não)

a) Os planos contêm procedimentos de emergência caso ocorra um incidente que coloca em risco as operações dos negócios?

b) Os planos contêm condições claras para o ativamento dos processos, como avaliar a situação do risco, quem deve ser acionado, antes de entrar em vigor?

c) No processo de recuperação o plano descreve as ações necessárias para as transferências essenciais ao negócio, a reativação os processos do negócio no prazo necessário?

d) Um programa de manutenção é especificado para testar e como proceder o plano de mautenção?

e) Para um melhor compreendimento do plano de continuidade dos negócios são feitas atividades de treinamento, conscientização e educação, para os processos continuarem efetivos?

f) As responsabilidades individuais é descrita no plano, e também os responsáveis por cada item de execução do plano? Os suplentes são citados quando é necessário?

g) Quando é necessário um procedimento de urgência os ativos e recursos críticos estão aptos para desempenhar a recuperação e reativação?

14.1.5. Testes, manutenção e reavaliação dos planos de continuidade do negócio

Os planos de continuidade do negócio são testados e atualizados regularmente? (Sim ou não)

a) Os membros da equipe de recuperação dos planos e outras pessoas relevantes que estejam conscientes de suas responsabilidades para a continuidade do negócio conhecem suas atividades quando um plano for acionado?

b) É feito um planejamento e a programação do testes dos planos de continuidade de negócios? Onde indiquem como e quando cada elemento do plano será testado.

c) Várias técnicas são utilizadas para assegurar a confiança de que os planos irão operar consistentemente? Por exemplo, simulações, testes de recuperações, testes dos recursos e serviços e instalações de fornecedores?

d) São atualizados os planos de continuidade do negócio quando há aquisição de novos equipamentos, atualizações de sistemas e mudanças de pessoal, endereços ou números telefônicos, estratégia de negócios, legislação, fornecedores e prestadores de serviços, processos e risco?

15. Conformidade

15.1. Conformidade com requisitos legais
Objetivo: evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

15.1.1. Identificação da legislação vigente

Todos os requisitos estatutários, regulamentares e contratuais pertinentes são definidos documentados e mantidos atualizados para cada sistema de informação da organização? (Sim ou não)

a) Os controles específicos e as responsabilidades individuais para atender a estes requisitos sejam definidos e documentados de forma similar?

15.1.2. Direitos de propriedade intelectual
Procedimentos apropriados são implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, como o uso de produtos de software e de informação? (Sim ou não)

a) Para proteger qualquer material que possa ser considerado como propriedade intelectual, é divulgado uma política de conformidade com os direitos onde definem o uso legal de produtos de software e de informação?

b) Na aquisição de software as fontes são conhecidas e de reputação, para assegurar o direito autoral?

c) É feito algum processo para conscientização das políticas quanto a proteção dos direitos de propriedade intelectual e ações disciplinares contra pessoas que violarem essas políticas?

d) É mantido provas e evidências da propriedade de licenças, manuais etc?

e) Há implementação de controles para assegurar que o número máximo de usuários permitidos não excede o número de licenças adquiridas?

f) Quanto a conduzir verificações para que somente produtos de software autorizados e licenciados sejam instalados são utilizados?

g) É estabelecido uma política para a disposição ou transferência de software para outros?

15.1.3. Proteção de registros organizacionais

Os registros são protegidos contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, contratuais e do negócio? (Sim ou não)

a) Para a proteção dos registros, são emitidas diretrizes gerais para retenção, armazenamento, tratamento e disposição de registros e informações?

b) Identificam os registros essenciais e o período que cada um deve ser mantido?

15.1.4. Proteção de dados e privacidade de informações pessoais
Conforme as legislações e regulamentações são asseguradas a privacidade e a proteção dos dados? (Sim ou não)

a) A conformidade com esta política necessita de uma estrutura de gestão e de controles. Para ser melhor alcançado, um gestor de proteção de dados fornece orientações gerais para gerentes, usuários, e provedores de serviço?

15.1.5. Prevenção de mau uso de recursos de processamento da informação
Os usuários são informados que usar os recursos de processamentos da informação para propósitos não autorizados é impróprio? (Sim ou não)

a) Se alguma atividade não autorizada for identificada por processo de monitoração ou outros meios, esta atividade é levada ao conhecimento do gestor responsável para que sejam aplicadas as ações disciplinares e/ou legais pertinentes?

b) Todos os usuários são conscientes do escopo preciso de suas permissões de acesso e da monitoração realizada para detectar o uso não autorizado?

c) Para informar que um recurso de processamento da informação que está sendo usado é de propriedade da organização e que não são permitidos acessos não autorizados, alguma mensagem de advertência é apresentada?

15.1.6. Regulamentação de controles de criptografia
Os controles de criptografia são usados em conformidade com todas as leis, acordos e regulamentações pertinentes? (Sim ou não)

a) Os itens estão em conformidade com a lei, como restrições à importação e/ou exportação de *hardware* e *software* de computador para a execução de funções criptográficas?

b) Há restrições no uso de criptografia?

15.2. Conformidade com normas e políticas de segurança da informação e conformidade técnica
Objetivo: garantir a conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.

15.2.1. Conformidade com as políticas e normas de segurança da informação
Os gestores garantem que todos os procedimentos de segurança da informação dentro da sua área de responsabilidade estão sendo executados corretamente para atender à conformidade com as normas e políticas de segurança da informação? (Sim ou não)

a) Os gestores analisam criticamente a intervalos regulares, a conformidade do processamento da informação com as políticas, normas e quaisquer outros requisitos de segurança?

b) Se há caso de não-conformidade, os gestores determinam e implementam ações corretivas apropriadas?

c) Os resultados das análises críticas e das ações corretivas pelos gestores são registrados e esses registros mantidos de forma segura?

15.2.2. Verificação da conformidade técnica
Os sistemas de informação são periodicamente verificados em sua conformidade com as normas de segurança da informação implementadas? (Sim ou não)

a) A verificação da conformidade técnica, é feita por técnicos especialistas e de ferramentas automatizadas que geram relatórios?

b) Para usar testes de invasão ou avaliações de vulnerabilidades do sistema, são tomadas precauções, uma vez que tais atividades podem comprometer a segurança do sistema?

c) A verificação da conformidade técnica são executadas por pessoas autorizadas e competentes?

15.3. Considerações quanto à auditoria de sistemas de informação
Objetivo: maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.

15.3.1. Controles de auditoria de sistemas de informação
As atividades de auditoria são feitas envolvendo verificações nos sistemas operacionais, onde essas são planejadas para minimizarem os riscos de interrupções dos processos do negócio? (Sim ou não)

a) Os requisitos de auditoria é apropriados com o nível de administração?

b) A verificação está limitada ao acesso para somente leitura de *software* e dados?

c) Todos os procedimentos, requisitos e responsabilidades são documentados?

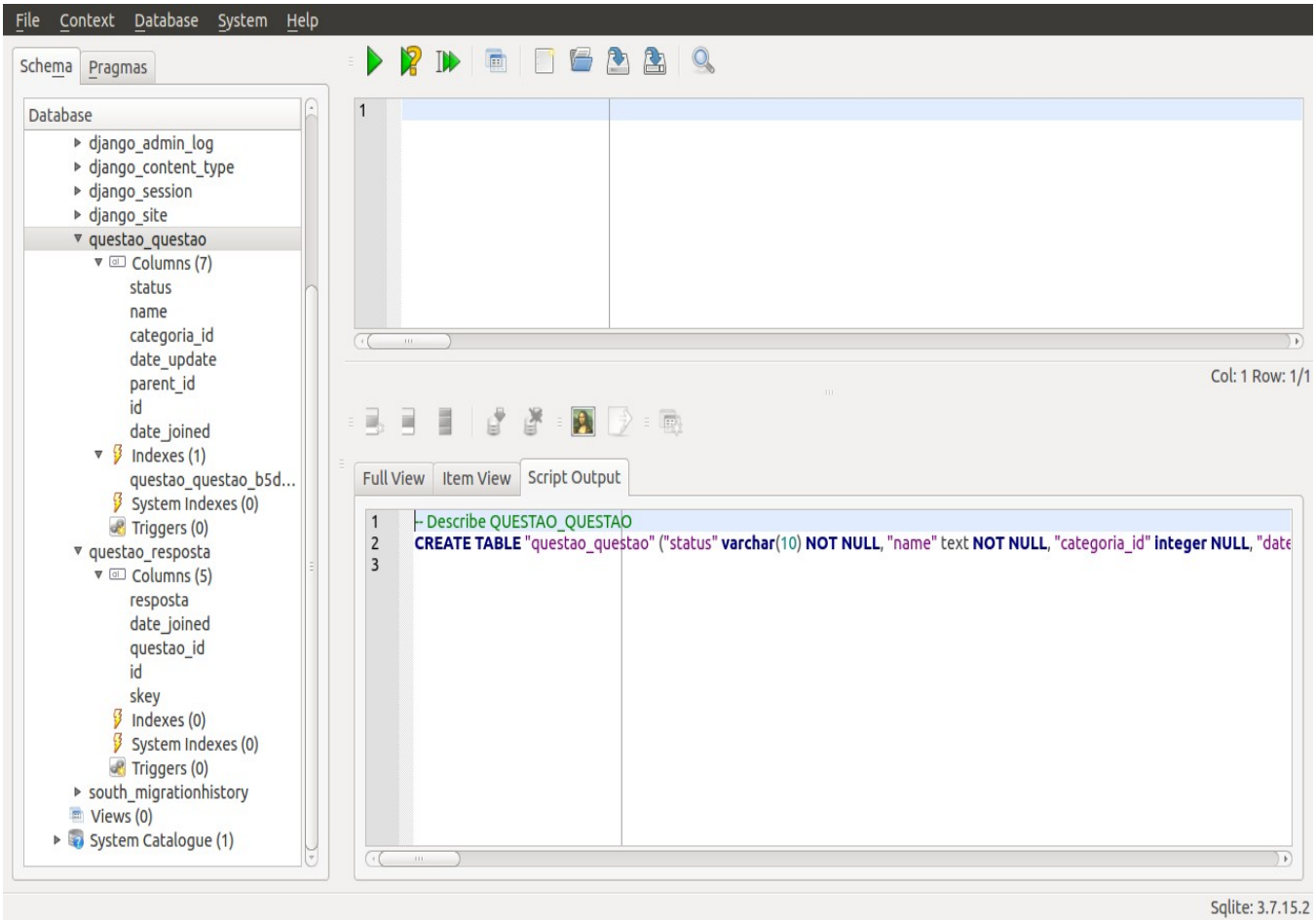
d) As pessoas que executam a auditoria de preferência são independentes das atividades auditadas?

15.3.2. Proteção de ferramentas de auditoria de sistemas de informação
O acesso as ferramentas de auditoria de sistema de informação são protegidas, para a prevenção de qualquer possibilidade de uso impróprio ou comprometimento? (Sim ou não)

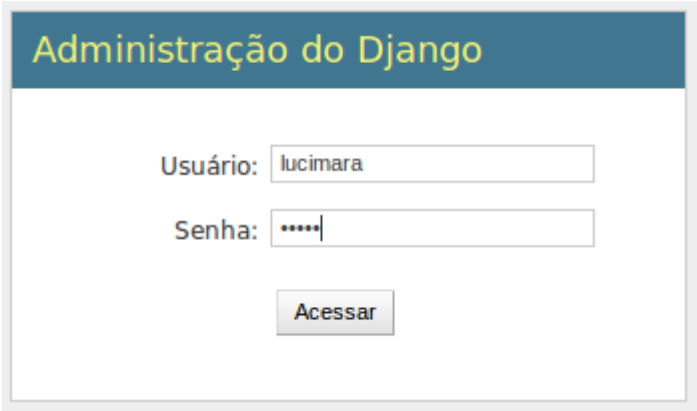
a) As ferramentas como software ou arquivos de dados, são separados de sistemas em desenvolvimento?

b) Quando terceiros estão envolvidos em uma auditoria, são feitos controles para avaliar riscos das senhas. Elas são trocadas imediatamente, após o trabalho ter sido concluído?

APÊNDICE B – BANCO DE DADOS DO PROJETO



APÊNDICE C – ADMINISTRAÇÃO DO *SITE* DA APLICAÇÃO

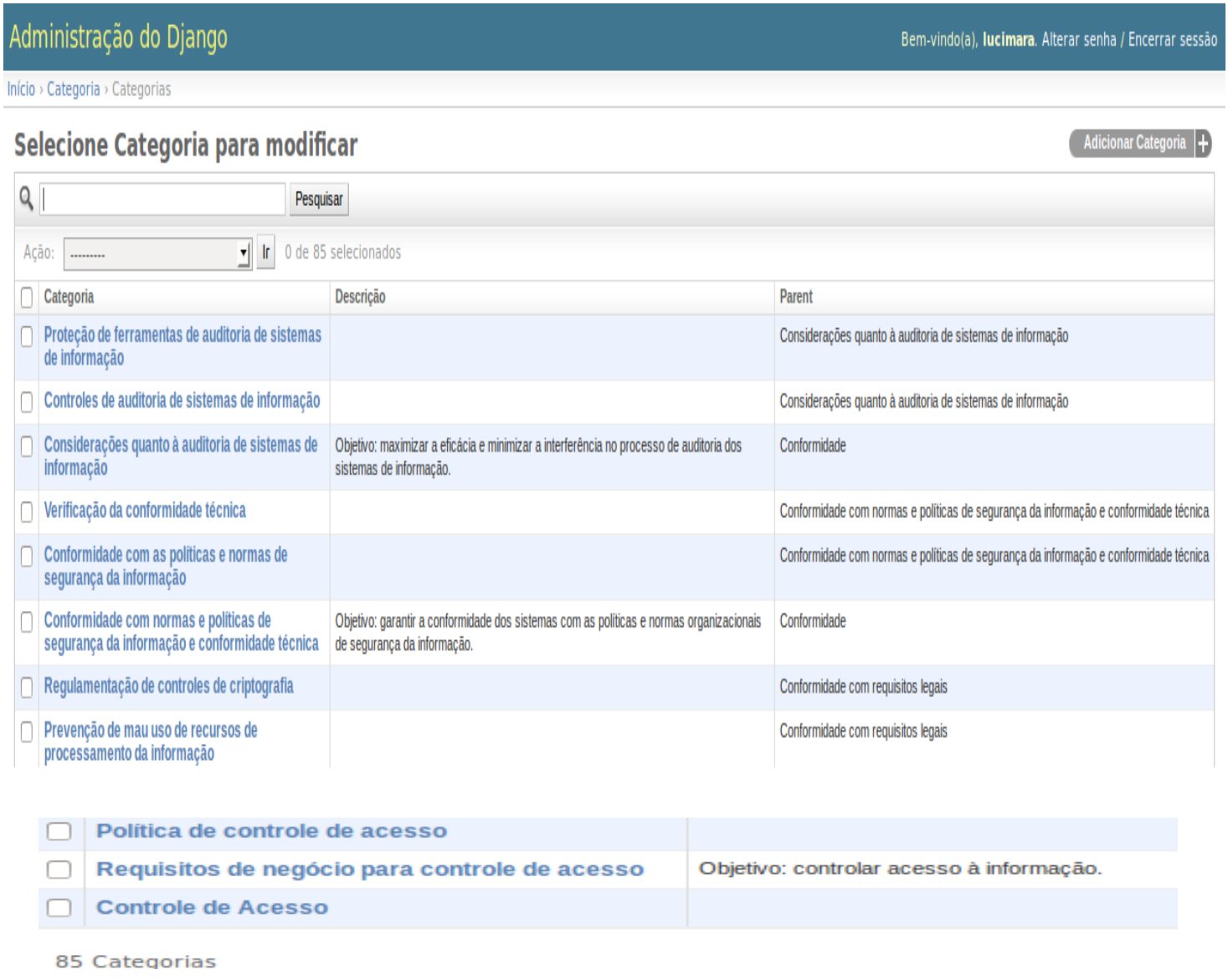


APÊNDICE D – CONFIGURAÇÕES INICIAIS DO PROJETO

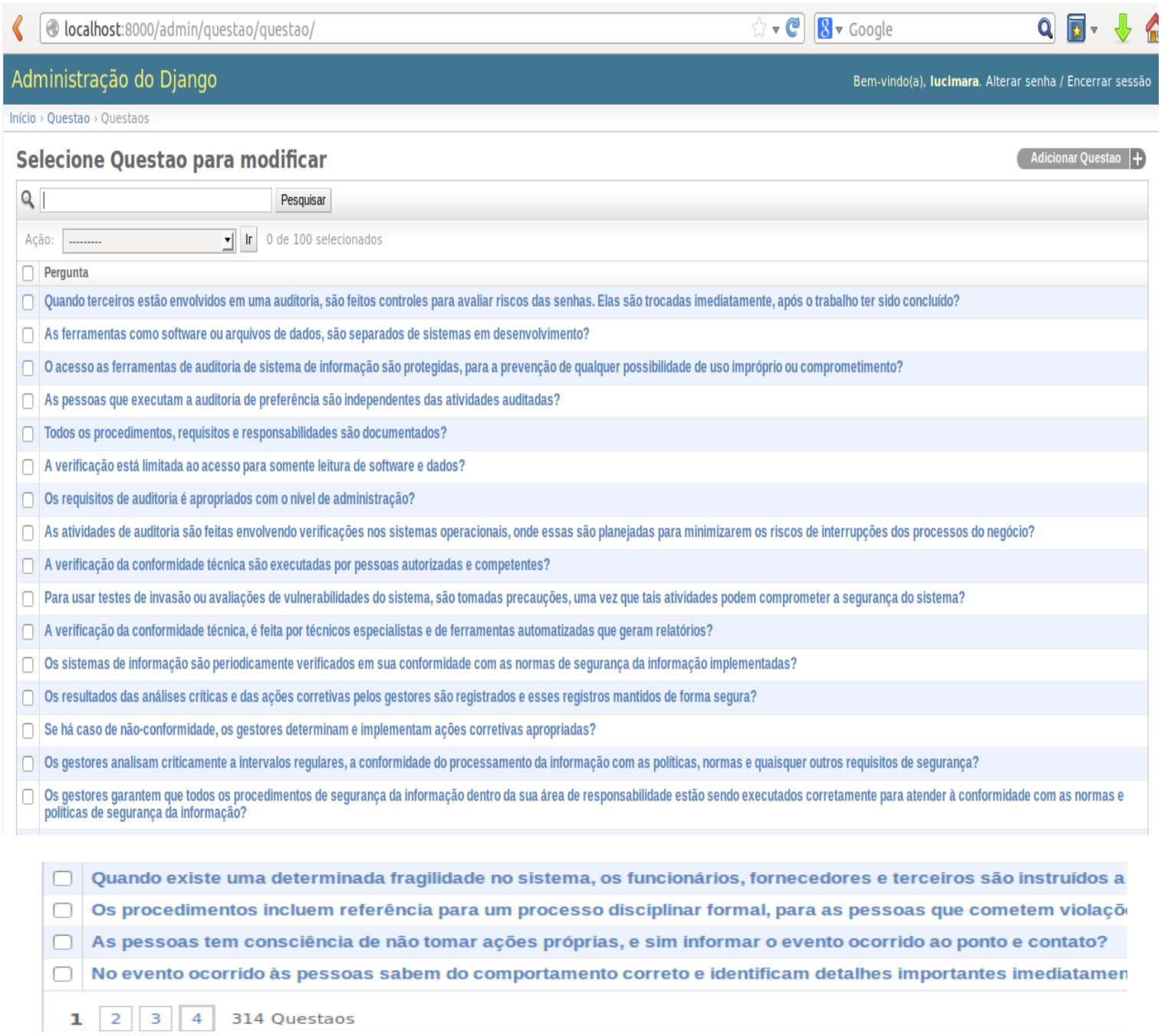
```
DATABASES = {
    'default': {
        'ENGINE': 'django.db.backends.sqlite3', # Add 'postgresql_psycopg2', 'mysql', 'sqlite3'
        'NAME': 'banco.bd',                      # Or path to database file if using sqlite3.
        # The following settings are not used with sqlite3:
        'USER': '',
        'PASSWORD': '',
        'HOST': '',                      # Empty for localhost through domain sockets or '127.0.
        'PORT': '',                      # Set to empty string for default.
    }
}
```

```
# Python dotted path to the WSGI application used by Django's
WSGI_APPLICATION = 'src.wsgi.application'

TEMPLATE_DIRS = (
    PROJECT_DIR.child('templates'),
    # Put strings here, like "/home/html/django_templates" or
    # Always use forward slashes, even on Windows.
    # Don't forget to use absolute paths, not relative paths.
)

INSTALLED_APPS = (
    'django.contrib.auth',
    'django.contrib.contenttypes',
    'django.contrib.sessions',
    'django.contrib.sites',
    'django.contrib.messages',
    'django.contrib.staticfiles',
    'django.contrib.humanize',
    # Uncomment the next line to enable the admin:
    'django.contrib.admin',
    'south',
    'src.categoria',
    'src.questao',
    # Uncomment the next line to enable admin documentation:
    # 'django.contrib.admindocs',
)
```

APÊNDICE E – LISTAGEM DAS CATEGORIAS



APÊNDICE F – LISTAGEM DAS QUESTÕES



APÊNDICE G – DESENVOLVIMENTO DA PÁGINA INICIAL USANDO HTML

```
{% load i18n %}
{% load categoria_extras %}
<!DOCTYPE html>
<!--[if lt IE 7]>      <html class="no-js lt-ie9 lt-ie8 lt-ie7"> <![endif]-->
<!--[if IE 7]>         <html class="no-js lt-ie9 lt-ie8"> <![endif]-->
<!--[if IE 8]>         <html class="no-js lt-ie9"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js"> <!--<![endif]-->
    <head>
        <meta charset="utf-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
        <title></title>
        <meta name="description" content="">
        <meta name="viewport" content="width=device-width">

        <link rel="stylesheet" href="{{MEDIA_URL}}css/bootstrap.min.css">
        <style>
            body {
                padding-top: 50px;
                padding-bottom: 20px;
            }
        </style>
        <link rel="stylesheet" href="{{MEDIA_URL}}css/bootstrap-theme.min.css">
        <link rel="stylesheet" href="{{MEDIA_URL}}css/main.css">

        <script src="{{MEDIA_URL}}js/vendor/modernizr-2.6.2-respond-1.1.0.min.js"></script>
    </head>
    <body>
        <!--[if lt IE 7]>
            <p class="chromeframe">You are using an <strong>outdated</strong> browser. Please <a href="http://browsehappy
            .com/">upgrade your browser</a> or <a href="http://www.google.com/chromeframe/?redirect=true">activate
            Google Chrome Frame</a> to improve your experience.</p>
        <![endif]-->
    <div class="navbar navbar-inverse navbar-fixed-top">
      <div class="container">
        <div class="navbar-header">
          <button type="button" class="navbar-toggle" data-toggle="collapse" data-target=".navbar-collapse">
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
          </button>
          <a class="navbar-brand" href="#">Infoquiz</a>
        </div>
```

```
          <div class="navbar-collapse collapse">
            <ul class="nav navbar-nav">
              <li class="active"><a href="/">Inicio</a></li>


              <li class="dropdown">
                <a href="#" class="dropdown-toggle" data-toggle="dropdown">Questionario <b class="caret"></b></a>
                <ul class="dropdown-menu">
                  {%show_categories%}
                </ul>
              </li>
            </ul>

          </div><!--/.navbar-collapse -->
        </div>
      </div>

      <div class="container">
        <div class="well">
          {% block well %}

          {% endblock well %}
        </div>

        <footer>
          <p>&copy; Company 2013</p>
        </footer>
      </div> <!-- /container -->        <script src="//ajax.googleapis.com/ajax/libs/jquery/1.10.1/jquery.min.js"></script>
          <script>window.jQuery || document.write('<script src="{{MEDIA_URL}}js/vendor/jquery-1.10.1.min.js"><\/script>')</
            script>

          <script src="{{MEDIA_URL}}js/vendor/bootstrap.min.js"></script>

          <script src="{{MEDIA_URL}}js/main.js"></script>

          {% block scripts %}

          {% endblock scripts %}
      </body>
    </html>
```

APÊNDICE H – FUNÇÕES PYTHON RECEBENDO REQUISIÇÕES WEB E RETORNA UMA RESPOSTA WEB.

```
def home(request):

    data = {

    }

    return render_to_response('questao/home.html', data, context_instance=RequestContext(request))


def questionario(request,id):
    category=Category.objects.filter(id=id)
    #print request.session.session_key
    category_children=Category.objects.filter(parent_id=id)

    for x in category_children:
        x.children  = Category.objects.filter(parent_id=x.id)
        for w in x.children:
            w.questao = Questao.objects.filter(Q(categoria_id=w.id) & Q(parent_id=None))
            #listando questoes pai
            for q in w.questao:
                #add form pai a questao pai
                #verifica se existe resposta no banco de dados
                try:
                    r = Resposta.objects.get(Q(questao=q) & Q(skey=request.session.session_key))
                    q.form = RespostaPaiForm(instance=r)
                    q.resposta = r

                except:
                    q.form = RespostaPaiForm(initial={"questao":q})

                #add questoes filho a variavel
                q.questao_filho = Questao.objects.filter(Q(parent_id=q.id))
                for qw in q.questao_filho:
                    try:
                        rw = Resposta.objects.get(Q(questao=qw) & Q(skey=request.session.session_key))
                        qw.form = RespostaFilhoForm(instance=rw)
                        qw.resposta = rw
                    except:
                        qw.form = RespostaFilhoForm(initial={"questao":qw})
```

```
    data = {
        "category":category_children,
        'cat_id':id,
    }

    return render_to_response('questao/perguntas.html', data, context_instance=RequestContext(request))

from django.contrib.humanize.templatetags.humanize import naturaltime
from django.utils.html import escape

def senderpost(request):
    if request.POST: #verifica se existe POST
        saved = False
        try:
            r = Resposta.objects.get(Q(questao_id=request.POST['questao']) & Q(skey=request.session.session_key))
            form = RespostaPaiForm(request.POST, instance=r)
            saved = True

        except:
            saved = True
            form = RespostaPaiForm(request.POST) #chama o form dos forms.py e add os dados do POST
            r = None
        #print request.session.session_key
        if form.is_valid() and saved:
            form_s = form.save(commit=False)
            form_s.skey = request.session.session_key
            form_s.save()
            msg = " salvo %s"%naturaltime(form_s.date_joined)
            response = HttpResponse(escape(msg))


            return response



    return HttpResponse('salvo')
```

```
def senderpost2(request):
    if request.POST: #verifica se existe POST
        try:
            r = Resposta.objects.get(Q(questao_id=request.POST['questao']) & Q(skey=request.session.session_key))
            form = RespostaFilhoForm(request.POST, instance=r)
        except:
            form = RespostaFilhoForm(request.POST) #chama o form dos forms.py e add os dados do POST
            r = None
        if form.is_valid():
            form_s = form.save(commit=False)
            form_s.skey = request.session.session_key
            form_s.save()

            r_list = []
            r = Resposta.objects.get(Q(questao_id=form_s.questao_id) & Q(skey=request.session.session_key))
            if r:
                for x in Questao.objects.filter(Q(parent_id=r.questao.parent_id)):
                    try:
                        res = Resposta.objects.get(Q(questao=x) & Q(skey=request.session.session_key))
                        r_list.append(int(res.resposta))
                    except:
                        r_list.append(0)
                media = sum(r_list) / float(len(r_list))

                Resposta.objects.filter(Q(questao__id=r.questao.parent_id)).update(resposta=media)

            msg = " salvo %s"%naturaltime(form_s.date_joined)
            response = HttpResponse(escape(msg))
            return response


    return HttpResponse('ok')
```

```
def report(request,id_cat):
    #Busca de categorias para as questoes
    category_children=[v.id for v in Category.objects.filter(parent_id=id_cat)]
    category_children2=[v.id for v in Category.objects.filter(parent_id__in=category_children)]
    q = Questao.objects.filter(Q(categoria_id__in=category_children2) & Q(parent_id=None))
    #contar o numero de questoes maximo da categoria x
    nquestoes = q.count()
    #criar uma lista
    r_list = []

    soma = 0

    #loop para percorrer as questoes da categoria e buscar suas respostas
    for x in q:

        try:
            #verificar se existe resposta
            res = Resposta.objects.get(Q(questao=x) & Q(skey=request.session.session_key))
            re = res.resposta
            #add resposta na lista
            r_list.append(float(re))
        except:
            #se nao existir colocar zero na lista
            re = 0
            r_list.append(re)
    #somar a resposta do usuario
    soma = sum(r_list)
    #pegar qual a pontuacao maxima do usuario
    pontuacao_maxima = nquestoes*3
    #fazer a regra de 3 para obter  o %
    percent = int(round((soma*100)/pontuacao_maxima))

    data = {
        "category":Category.objects.get(id=id_cat),
        'media':percent,

    }
    return render_to_response('questao/relatorio.html', data, context_instance=RequestContext(request))
```

APÊNDICE I – PROGRAMAÇÃO PARA ADICIONAR A TABELA CATEGORIA E QUESTÃO NO BANCO DE DADOS

```
from django.db import models

class Category(models.Model):

    class Meta:
        verbose_name = 'Categoria'


    STATUS_CHOICES = (
      (u'Ativo', u'Ativo'),
      (u'Inativo', u'Inativo'),
    )

    name = models.CharField(verbose_name=u"Categoria", max_length=255, blank=False, null=False)
    description = models.TextField(verbose_name=u"Descrição", blank=True)
    status = models.CharField(verbose_name=u"Status",max_length=10,blank=False, null=False,choices=STATUS_CHOICES,default=
    parent =  models.ForeignKey('self', null=True,blank=True,default=None, related_name='category__self')
    date_joined = models.DateTimeField(auto_now_add=True)
    date_update = models.DateTimeField(auto_now=True)


    def __unicode__(self):
        return self.name
```

```
class Questao(models.Model):

    class Meta:
        verbose_name = 'Questao'


    STATUS_CHOICES = (
      (u'Ativo', u'Ativo'),
      (u'Inativo', u'Inativo'),
    )

    name = models.TextField(verbose_name=u"Pergunta", blank=False, null=False)
    status = models.CharField(verbose_name=u"Status",max_length=10,blank=False, null=False,choices=STATUS_CHOICES,default=
    parent =  models.ForeignKey('self', null=True,blank=True,default=None, related_name='category__self')
    categoria =  models.ForeignKey(Category, null=True,blank=True,default=None, related_name='category__categoria')
    date_joined = models.DateTimeField(auto_now_add=True)
    date_update = models.DateTimeField(auto_now=True)


    def __unicode__(self):
        return self.name

RESPOSTA_CHOICES = (
      (0, u'Atividade Ausente'),
      (1, u'Atividade Parcialmente Ausente'),
      (2, u'Atividade Parcialmente Presente'),
      (3, u'Atividade Presente'),
    )
class Resposta(models.Model):

    class Meta:
        verbose_name = 'Resposta'


    resposta = models.CharField(verbose_name=u"Pergunta", blank=False, null=False,max_length=30)
    skey = models.CharField(blank=True, null=True,max_length=255) #sessão do usuario
    questao =  models.ForeignKey(Questao, null=False,blank=False, related_name='questao__resposta')
    date_joined = models.DateTimeField(auto_now=True) #atualizacao

    def __unicode__(self):
        return self.resposta
```

APÊNDICE J – TABELAS PARA ADICIONAR CATEGORIAS/QUESTÕES