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

SISTEMA WEB PARA VERIFICAÇÃO DE BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO COM BASE NA NORMA ABNT NBR ISO/IEC 27002:2005

TRABALHO DE CONCLUSÃO DE CURSO

Matheus Righi Furlan

Santa Maria, RS, Brasil

2013

SISTEMA WEB PARA VERIFICAÇÃO DE BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO COM BASE NA NORMA ABNT NBR ISO/IEC 27002:2005

Matheus Righi Furlan

Trabalho de Conclusão de Curso (TCC) apresentado ao Curso Superior de Tecnologia em Redes de Computadores do Colégio Técnico Industrial de Santa Maria, da Universidade Federal de Santa Maria (UFSM,RS), como requisito parcial para obtenção de grau de
Tecnólogo em Redes de Computadores

Prof. Ms. Renato Preigschadt de Azevedo

Santa Maria, RS, Brasil

2013

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 o Trabalho de Conclusão de Curso

SISTEMA WEB PARA VERIFICAÇÃO DE BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO COM BASE NA NORMA ABNT NBR ISO/IEC 27002:2005

elaborado por
Matheus Righi Furlan

Como requisito parcial para a obtenção de grau de
Tecnólogo em Redes de Computadores

COMISSÃO EXAMINADORA:

Renato Preigschadt de Azevedo, Ms.
(Orientador)

Eugênio de Oliveira Simonetto, Dr. (UFSM)

Leandro Oliveira Freitas, Ms. (UFSM)

Santa Maria. 08 de janeiro de 2014

DEDICATÓRIA

Agradeço, em primeiro lugar, a Deus, por me proporcionar saúde, paz, tranquilidade, sustentação e condições para elaboração deste projeto tão importante em minha vida.

A minha família, Jucemar Lorenzoni Furlan (pai) e Ana Maria Righi Furlan (mãe), os quais me mostraram o caminho certo e agradeço a eles por terem proporcionado um lar em que podemos viver em harmonia, tranquilidade e também pelo incentivo e apoio para a conclusão da graduação, com todo o suporte financeiro e espiritual.

Aos meus parentes, cujos nomes não foram citados, mas que sempre me apoiaram em todos os momentos.

Ao professor Orientador Renato Azevedo, pelo auxilio na elaboração do projeto, tornando-o cada vez melhor, possibilitando assim sua conclusão.

A meus colegas de aula, pelo apoio e incentivo, pela amizade e convivência diária. Aos meus colegas do LAMI(Laboratório de Manutenção de Microcomputadores da UFSM), que me auxiliaram com diversas sugestões, em especial a Anderson Colvero, pelo aprendizado obtido ao longo deste trajeto.

Ao curso de Tecnologia em Redes de Computadores, também aos professores, que fizeram o possível para que seu conhecimento fosse repassado a nós alunos de forma a ser entendido e aplicado ao longo da jornada que está por vir.

RESUMO

Trabalho de Conclusão de Curso (TCC)
Colégio Técnico Industrial De Santa Maria
Curso Superior de Tecnologia em Redes de Computadores
Universidade Federal de Santa Maria

SISTEMA WEB PARA VERIFICAÇÃO DE BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO COM BASE NA NORMA ABNT NBR ISO/IEC 27002:2005

AUTOR: MATHEUS RIGHI FURLAN
ORIENTADOR: RENATO PREIGSCHADT DE AZEVEDO
Data e Local da Defesa: Santa Maria, 08 de janeiro de 2014.

Este trabalho apresenta o desenvolvimento de um questionário com base e referência na norma ABNT NBR ISO/IEC 27002:2005 Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação, cuja norma é internacional, sendo traduzida e adaptada para o português brasileiro pela Associação Brasileira de Normas Técnicas. O questionário esta embasado, nas seções de segurança da informação da norma ABNT NBR ISO/IEC 27002:2005, sendo: Política de Segurança da Informação, Organizando a Segurança da Informação, Gestão de Ativos, Segurança em Recursos Humanos, Segurança Física e do Ambiente e Gerenciamento das Operações e Comunicações. Foram feitas pesquisas relacionadas à segurança da informação, em especial a norma ABNT NBR ISO/IEC 27002:2005. Na elaboração do projeto, foram analisadas as seções de segurança da informação da norma, baseando-se nos controles de segurança de cada uma das seções citadas para a criação de um questionário referente às boas práticas para a manutenção da segurança da informação, e em seguida foi criada uma página Web com capacidade de aplicação do questionário. Como objetivo final, o trabalho propõe as organizações um *feedback* em relação ao seu nível de segurança da informação para que sejam mantidas boas práticas relativas à segurança da informação, e se necessário a busca de implementação de novos controles de segurança que estão dispostos na norma ABNT NBR ISO/IEC 27002:2005.

Palavras-chave: Segurança da Informação. NBR 27002. Questionário.

ABSTRACT

Completion Of Course Work
Colégio Técnico Industrial de Santa Maria
Universidade Federal de Santa Maria

WEB SYSTEM FOR VERIFICATION OF GOOD PRACTICE FOR INFORMATION SECURITY BASED ON STANDARD ABNT NBR ISO/IEC 27002:2005

AUTHOR: MATHEUS RIGHI FURLAN
SUPERVISOR: RENATO PREIGSCHADT DE AZEVEDO
Date and Place of Defense: Santa Maria, January 08, 2014.

This paper presents the development of a questionnaire based and referenced on standard ABNT NBR ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management , which is the international standard , being translated and adapted to Brazilian Portuguese by the Brazilian Association of Technical Standards . Based on the questionnaire in the safety sections of the standard ABNT NBR ISO/IEC 27002:2005 , Information Security Policy Information , Organizing Information Security , Asset Management , Human Security , Physical Security Resources and Environment and Operations Management and Communications . ABNT NBR ISO / IEC 27002:2005 queries related to information security were made, in particular . In preparing the project , sections of the standard security information were analyzed by relying on the security of each of the sections cited for the creation of a questionnaire on best practices for the maintenance of information security controls , and then created a Web page with ability to administer the questionnaire. As a final goal, the paper proposes organizations feedback regarding their level of information security . Where to search for the implementation of new security controls that are arranged in the standard ABNT NBR ISO/IEC 27002:2005 are kept good practices related to information security , and necessary.

Keywords: Information Security. NBR 27002. Questionnaire.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

Com o desenvolvimento de informações dentro de organizações, e pela quantidade de ativos, se torna cada vez mais difícil controlar como estas informações são tratadas e para onde elas vão ou de onde elas chegam. Segundo NBR 27002 (2005, p. X) "a informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas". Isto faz com que a informação, não importando o meio em que é estabelecida, seja importante e de grande valor a qualquer organização.

Cada vez mais empresas buscam formas de se adequar as mais diversas normas, sendo que essa adequação traz a elas uma maior segurança e domínio sobre os seus ativos. A segurança da informação é de grande valia para qualquer organização, podendo, melhorar a reputação através da agilidade com que os erros e problemas são corrigidos, ou seja, por meio da implementação de normas de segurança. Conforme NBR 27002 (2005, p. X) "a segurança da informação é obtida a partir da implementação de um conjunto de controles adequados incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware".

Uma das grandes preocupações das empresas é saber, como manter a segurança destas informações, e como adequar regras que possibilitem planejar, revisar e elaborar medidas de prevenção. É neste contexto que surge a norma ABNT NBR ISO/IEC 27002:2005 - Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Com o objetivo de servir como um guia para o estabelecimento de novos controles que auxiliem as organizações na garantia da segurança da informação, diminuindo os riscos e aumentando o retorno sobre investimentos. Segundo NBR 27002 (2005, p. X) "estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos".

Em termos de escopo, o objetivo é proporcionar as organizações um questionário referente a algumas seções, sendo referenciado na norma ABNT NBR ISO/IEC 27002:2005, baseando o mesmo, nos controles de segurança da informação apresentados nas seções da norma. É importante lembrar também, que o questionário não serve como mecanismo de validação de segurança da informação, mas sim como um auxílio para a verificação dos pontos

fracos e fortes, possibilitando assim um maior foco auxiliador para as organizações na busca da norma para a implantação de novos controles de segurança.

Para que as organizações tenham o acesso a esse questionário, o intuito é disponibiliza-lo em uma página Web para que possa ser acessado através da efetuação prévia de um cadastro e assim, manter organizado as respostas das questões, onde ao final o usuário que respondeu ao questionário recebe um *feedback* de como está sua segurança da informação, verificando assim o nível de segurança da informação em relação as boas práticas para a manutenção da segurança da informação que são adotadas pela norma ABNT NBR ISO/IEC 27002:2005.

O trabalho compreende sete capítulos, onde no primeiro capítulo e feita uma introdução e contextualização sobre segurança da informação. No segundo capítulo são abordados os objetivos que o trabalho pretende atingir. O terceiro capítulo mostra alguns conceitos relativos a segurança da informação, possíveis ameaças às organizações. Também uma contextualização em relação ao SGSI(Sistema de Gestão da Segurança da Informação), abordando algo sobre o que é análise de riscos e posteriormente o que se deve proteger em uma organização.

No capítulo quatro são abordadas as seções de segurança da informação utilizadas para a elaboração do questionário, e uma exemplificação das questões propostas.

No quinto capitulo, a criação da página Web de aplicação do questionário. No sexto capitulo é abordado a criação do sistema de *feedback*. Por último, no sétimo capitulo, temos considerações finais e trabalhos futuros.

2. OBJETIVOS

2.1.Objetivo Geral

Desenvolver um *checklist* segundo os controles apresentados na norma ABNT NBR ISO/IEC 27002: 2005 - Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da Informação, e disponibilizá-lo através de uma página Web a organizações interessadas em verificar o nível de segurança da informação da sua organização.

2.2.Objetivos Específicos

-Realizar um estudo referente à segurança da informação na norma ABNT NBR ISO/IEC 27002:2005;

-Elaborar a partir dos controles apresentados nas seções da norma, o *checklist*;

-Desenvolver uma página Web com capacidade de aplicar o *checklist*;

-Gerar um *feedback* ao usuário, em relação as suas respostas no questionário.

3. DESENVOLVIMENTO

Com o crescente desenvolvimento das organizações, torna-se e cada vez mais importante a utilização de mecanismos que possibilitem o tratamento e segurança das informações, como complementam Geus e Nakamura (2007, p. 25), "a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar em grandes prejuízos e falta de novas oportunidades de negócios". A proteção das informações no mundo globalizado torna-se cada vez mais essencial, sendo necessário, criar mecanismos para que a segurança destas informações sejam estabelecidas. Desta forma, é de extrema importância, que esses meios de segurança, sejam elas, regras internas da organização, ou em normas que regulamentem qual a melhor maneira de tratar estas informações.

3.1. Histórico da Norma ISO/IEC 27002

Os passos iniciais para elaboração da norma foram dados pelo Governo do Reino Unido, com seu Centro Comercial de Segurança de Computadores (*Commercial Computer Security Centre*), encarregado de várias tarefas importantes na área da Segurança da Informação, dentre elas a elaboração de um critério para avaliação de produtos e segurança na área de TI (Tecnologia da Informação) e também a criação de regras para boas práticas da segurança da informação. Em meados de 1990 foi publicado um documento organizado em 10 seções com controles e objetivos chamado de PD0003. Este documento ficou sobre cuidados da BSI (*British Standards Institution*) que em 1995 tornou-se o documento formal BS7799.(27000.org, *History*, 2013, tradução nossa);

Em abril de 2001, em uma reunião de trabalho da ISO/IEC JTC1 SC27, e em outras reuniões que foram acontecendo em anos posteriores, foi decidido e publicado a nova versão chamada ISO/IEC 17799 em 2005. No final de 2007 para seguir a numeração da série, a ISO 17799 foi renomeada para ISO/IEC 27002.

A ABNT NBR ISO/IEC 27002:2005 é composta pelo mesmo conteúdo da ISO/IEC 27002:2005 traduzido para o Português Brasileiro. A primeira edição da ABNT NBR ISO/IEC 27002 tem conteúdo idêntico a ABNT NBR ISO/IEC 17799.

A ABNT NBR ISO/IEC 27002 tem como principal objetivo ajudar as organizações com sugestões de boas práticas que mantenham a integridade e segurança da informação. A norma

foi dividida em 11 seções que possuem no total 39 categorias, sendo elas; Política de Segurança da Informação, Organizando a Segurança da Informação, Gestão de Ativos, Segurança em Recursos Humanos, Segurança Física e do Ambiente, Gestão das Operações e Comunicação, Controle de Acesso, Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação, Gestão de Incidentes a Segurança da Informação, Gestão da Continuidade do Negócio, Conformidade. Sendo compostas por controles, e a aplicação destes, faz com que a segurança da informação seja melhorada.

3.2.O que é Informação?

Sabe-se que nos dias atuais o que mais trafega dentro das organizações, não são pessoas, mas sim, as informações, sendo que esta pode estar disposta de várias formas, ou seja, escrita em papel, armazenada em mídias ou eletronicamente (sistemas com computação na nuvem) e falada no dia a dia. Toda esta informação que é de posse da organização, possui grande valor, com isso a NBR 27002(2005, p. X) complementa, "a informação é um ativo que, como qualquer outro ativo importante é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida".

Esta informação que trafega nas organizações tem por objetivo o desenvolvimento e sustentabilidade, pois é através dela que a organização pode desenvolver conteúdo e consequentemente gerar lucros, como complementam Geus e Nakamura(2007, p. 50) "neste mundo globalizado, onde as informações atravessam fronteiras com velocidade espantosa, a proteção do conhecimento é de vital importância para a sobrevivência das organizações". Por este motivo é necessária à prevenção, ou seja, a segurança da informação que segundo NBR 27002(2005, p. X) "é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio".

3.3.Segurança da Informação

É a proteção de informações e recursos desenvolvidos por organizações. Nota-se que é importante e se faz necessária a proteção de qualquer tipo de ataque vindo da internet, mas isto é apenas uma pequena parte do que se precisa proteger, como complementam Geus e Nakamura(2007), os ataques internos são os que mais preocupam as organizações. Estas

possuem pessoas trabalhando, e como garantir que as pessoas não subtraiam dados da organização, ou tentem algo que possa ferir o patrimônio. Por esse motivo deve ser levado em consideração alguns requisitos que formam a segurança da informação (Peixoto, 2006):

- Confidencialidade: se refere à proteção dos dados contra acesso indevido de terceiros, o controle pode ser feito por meio de criptografia de dados, quando se referir a dados trafegados na internet, ou transporte seguro, quando se refere a documentos importantes.
- Disponibilidade: é disponibilizar a entidades ou órgãos relacionados à organização, recursos e documentos que os interessem.
- Integridade: garantir com que a informação não seja alterada, mesmo que de forma acidental ou intencional.

Dentre outros requisitos, temos:

- Autenticidade: é a verificação da identidade entre transmissor e receptor, gerando uma comunicação confiável, sem que alguém possa usar a identidade do receptor ou transmissor.
- Não Repúdio: através de métodos de criptografia, impedir que alguém, algum indivíduo ou entidade neguem a execução de uma ação particular relacionada a troca de dados. (PNDE- Portal Nacional do Documento Eletrônico)
- Conformidade: alguma ação que quando executada, deve estar nas leis e regulamentos internos e externos da organização.
- Controle de Acesso: proteger qualquer dado ou informação relacionado, à organização contra acesso indevido de terceiros, sendo ele lógico, através de computadores, ou físicos, como por exemplo, o acesso a salas com ativos importantes.

Contudo, para que a organização possa iniciar seus projetos relacionados à segurança da informação, é necessário, que estes itens citados acima possuam relevância. Dentre esses fatores que fazem parte da segurança da informação, deve-se observar com cautela e analisar, o que proteger, e é nesta faze que descobre-se o mais importante para a organização.

A segurança da informação nos remete a tratar de muitos pontos que podemos chamar de ameaças, sendo estas na maioria das vezes proporcionada por fatores humanos.

3.4. Tipos de Ameaças

Ameaças são um dos principais fatores de risco perante a segurança da informação, estas ameaças podem ocorrer por um vírus, sabotagem, desastres naturais que afetam o sistema ou através da engenharia social, sendo este um dos principais métodos, pois a pessoa em questão participa ativamente na elaboração de conteúdo da organização e possui acesso a parte interna da organização. Estas ameaças podem ocorrer devido à curiosidade das pessoas em querer ver algum equipamento ou serviço que está sendo executado, ou por um dos principais motivos que são o roubo de informações para tomar vantagem, explorar e arrecadar informações competitivas no mercado.

Segundo Pinheiro (2007) existem dois tipos de ameaças, a acidental aquela que não foi planejada e a intencional e como o nome já diz, foi pretendida. Dentre estes dois tipos de ameaças, temos as seguintes:

-Vulnerabilidade: pode ser alguma falha em um equipamento causado por código malicioso ou por intervenção de terceiros, produzindo falha e até danificando o equipamento, colocando em risco dados ou sistemas importantes.

-*Phishing*: utilização de comunicações fraudulentas, onde na maioria dos casos os usuários são desviados, para páginas Web falsas correndo o risco de roubo de informações.

-*Malware*: códigos maliciosos, que podem causar vulnerabilidade em equipamentos e possível perda de dados.

-Vírus: programas capazes de se alojar na máquina podendo subtrair informações sigilosas e causar dano aos equipamentos da organização.

-Negação de Serviço ou *Denial of Service*: é o método em que são enviadas inúmeras mensagens fazendo com que o equipamento atacado fique sobrecarregado esgotando sua capacidade de processamento.

-Engenharia Social: são práticas cometidas por um indivíduo com capacidade de persuadir pessoas, fazendo com que acreditem em seu caráter, após receberem esta confiança se torna mais fácil explorar as vulnerabilidades e assim acontece, a subtração de informações.

3.5.Sistema de Gestão de Segurança da Informação(SGSI).

O sistema de gestão da segurança da informação é estabelecido segundo alguns princípios, como, implementar, operar, monitorar e analisar criticamente este sistema.(NBR 27001). Este sistema é constituído, segundo princípios e metas que a organização pretende atingir. A norma ABNT NBR ISO/IEC 27001 adota o modelo conhecido como " Plan-do-Check-Act".

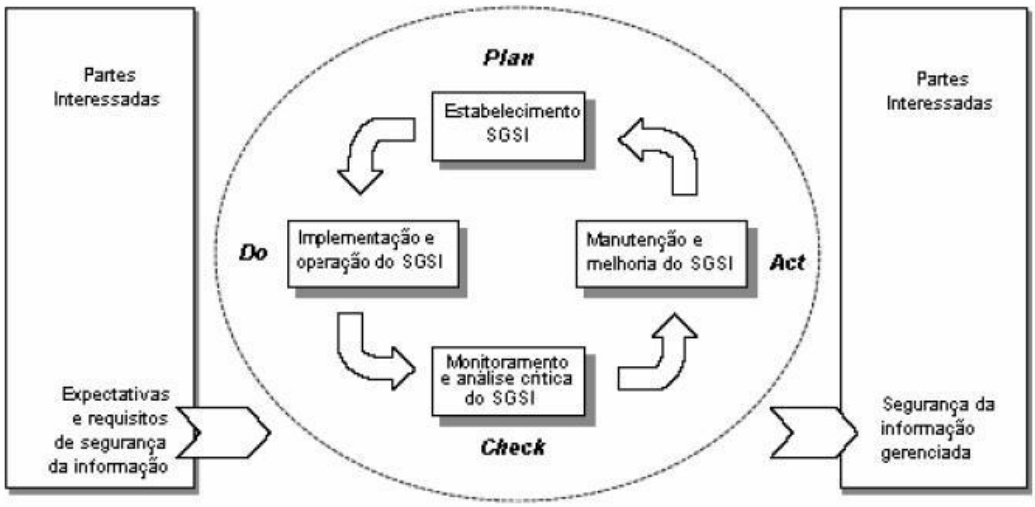


Figura 1 – Ciclo PDCA (*Plan- Do- Check- Act*), Planejar- Fazer-Checar-Agir
Fonte: Norma ABNT NBR ISO/IEC 27001:2006

Plan-planejar : estabelecer a política, objetivos, processo e procedimentos do SGSI relevantes para a gestão de risco e melhoria da segurança da informação. (NBR 27001, 2006, p. vi).

Do-fazer: "programar e operar a política, controles, processos e procedimentos do SGSI".(NBR 27001, 2006, p. vi).

Check-checar: "avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI".(NBR 27001, 2006, p. vi).

Act-agir: Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI para alcançar a melhoria continua do SGSI.(NBR 27001, 2006, p. vi).

- Estabelecer o SGSI:

Para que o estabelecimento do SGSI ocorra, são necessários analisar quais os principais objetivos da organização, qual seu tipo de negócio, e quais seus ativos e tecnologia. (NBR 27001). Deve-se também utilizar a análise de riscos e documentar quais possíveis ímpetos o sistema está exposto com base no tipo de organização, estimando critérios para o nível que cada risco está exposto e selecionar controles para que ocorra o devido tratamento a estas riscos. (NBR 27001).

- Pôr em prática o SGSI:

Segundo a NBR 27001(2006, p. 6) "é necessário formular o plano de tratamento de riscos que identifique a ação de gestão apropriada", e assim efetivar o plano de tratamento para alcançar os objetivos de controle identificados.

Utilizar medidas e controles para colocar em execução o treinamento e conscientização de funcionários. (NBR 27001).

- Realizar monitoramento do SGSI:

Detectar erros de resultados no processamento, identificar tentativas de violações ajudando a descobrir eventos de segurança da informação prevenindo os incidentes de segurança da informação. (NBR 27001).

- Continuar com o desenvolvimento do SGSI:

Implementar melhorias, comunicando-as a todas as partes envolvidas com o nível de detalhamento apropriado e assegurar que estes progressos atinjam o seu objetivo.(NBR 27001)

3.6.Analisar Riscos

A análise de riscos relacionada à segurança da informação refere-se a relatar possíveis riscos pertinentes aos ativos (equipamentos, pessoas, informações), sendo que esta análise retrata os pontos em que a organização deve priorizar para manter o controle, podendo prevenir possíveis riscos e soluciona-los antes que um desastre aconteça.

Para que uma organização possa desenvolver seus projetos de segurança da informação, é importante observar a legislação vigente segundo seus objetivos, e também identificar controles adequados que foram destacados na análise de risco. (Coelho e Araújo, 2013).

Com a identificação da análise de riscos, a organização obterá um melhor controle com relação às restrições do seu negócio, estabelecendo possíveis políticas para controle de riscos como, por exemplo;

Elaboração da política de Segurança: é um documento que consta considerações da direção perante a segurança da informação e requisitos do negócio.

Organizar a Segurança da Informação: diretrizes que programam controles para implementação da segurança da informação.

Inventário de Ativos: manutenção de uma lista de todos os ativos da organização.

Segurança de Recursos Humanos: manter informado a todos os envolvidos com a organização, os seus direitos e deveres.

Segurança Física e do Ambiente: assegurar que locais que necessitam de proteção adequada, tenham sua devida segurança.

Gerenciamento das operações e comunicação: proteção adequada e correta dos recursos de processamento de informação.

Com a fase de análise e avaliação de riscos determinada, se faz necessária à implementação de controles, estes por sua vez, podem ser relacionados segundo critérios apresentados nas normas ABNT NBR ISO/IEC 27001:2006 e ABNT NBR ISO/IEC 27002:2005.

3.7.O que são controles de segurança

Conforme Coelho e Araújo (2013, p. 10) “controles são medidas ou um conjunto de medidas adotadas para tratar vulnerabilidades e reduzir o risco de incidentes de segurança da informação.”

Segundo a NBR 27002:

> A seleção de controles de segurança da informação depende das decisões da organização, baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado na organização, e convém que também está sujeito a todos as legislações e regulamentações nacionais e internacionais relevantes.(NBR 27002, 2005, p. xi)

Cada organização deve através de sua análise de risco, selecionar os controles a serem destacados e utilizados. A norma ABNT NBR ISO/IEC 27002:2005 considera que alguns

controles dela, podem ser como princípios básicos para a gestão da segurança da informação e que pode ser aplicado na maioria das organizações.

3.8.O que proteger em uma organização

Organizações estão sendo atacadas em todo o momento, segundo Symantec (2013), em 2012, 31% dos ataques foram direcionados a organizações com menos de 250 funcionários, isso nos mostra que todas as organizações devem se preocupar com questões de segurança. Esta estatística refere-se a ataques ocorridos pela internet, porém não são somente estes tipos de incidentes que ocorrem dentro das organizações, sabe-se que ocorrem imprevistos, vindos de pessoas que operam equipamentos vitais a organização. Outro tipo de ataque é a subtração de informações em mídias removíveis ou até mesmo em e-mails que podem ser enviados com informações importantes.

As organizações em geral possuem documentos importantes para seu desenvolvimento, estes são de grande valia, porém não são somente documentos que a organização disponibiliza para acesso dos funcionários. Em uma organização constam equipamentos, como mesas, cadeiras computadores, aparelhamentos de rede, dependendo em alguns casos, eletrodomésticos, entre outros, todos estes fazem parte da organização e devem ser protegidos adequadamente.

A norma ABNT NBR ISO/IEC 27002:2005 estabelece diretrizes para estabelecimento e manutenção da segurança da informação e de equipamentos, e formas para a implementação de desenvolvimento de sistemas para a proteção adequada dos dados e aparelhamentos.

4. ESTABELECIMENTO DA SEGURANÇA DA INFORMAÇÃO

Estabelecer a segurança da informação não é uma decisão somente da camada superior da organização, pois segundo a NBR 27002(2005, p. X) "a gestão de segurança da informação requer pelo menos a participação de todos os funcionários da organização. Pode ser também que seja necessária também a participação de acionistas, fornecedores, terceiras partes, clientes e outras partes externas".

A norma ABNT NBR ISO/IEC 27002:2005 trata de questões relativas à segurança da informação, que é estabelecida por um conjunto de regras e diretrizes, baseados na análise e avaliação de riscos gerados a partir de especificação do negócio e objetivos da organização; com isso a NBR 27002 (2005, p. X) complementa, "a segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados".

Com o estabelecimento destas regras tratadas perante os requisitos da organização, a gestão da informação nos remete a utilização das seções apresentadas na norma ABNT NBR ISO/IEC 27002:2005, utilizando a partir destas seções os controles e diretrizes apresentados para a elaboração de um *checklist*, para a verificação do nível de segurança da informação nas organizações. Contudo, o auxilio as organizações com a verificação de boas práticas de segurança da informação, que são adotadas pela norma. Possibilitando assim, que as organizações, foquem na adição de controles de segurança da informação e no estabelecimento de possíveis novas regras aumentando o tratamento de ameaças e diminuindo o risco de se criar vulnerabilidades.

Segundo a DiálogoTI/*Next Generation Center*(2013):

> Estabelecer procedimentos em transações corporativas, operar por meio de regras de acesso e restrições, criar hierarquias de responsabilidades, métodos de reação a eventuais falhas ou vulnerabilidades é, acima de tudo, manter um padrão no que se refere à segurança da companhia.(INTEL/DiálogoTI, p.6)

Todos os controles apresentados na norma, se aplicados de forma correta e conforme os requisitos do negócio irão trazer mais segurança da informação às organizações. Determinar qual o tipo de requisitos que a organização deve obedecer é de grande importância para que a proteção das informações seja alcançada, conforme a norma ABNT NBR ISO/IEC 27002 as suas sessões apresentadas são princípios básicos de segurança da informação.

A seguir serão apresentadas as seções da norma ABNT NBR ISO/IEC 27002:2005, sendo abordados alguns aspectos relativos à norma, com uma breve descrição ao que se refere cada item de segurança apresentado nela, e posteriormente uma exemplificação de algumas questões elaboradas a partir dos controles de segurança da informação. Como contexto inicial surge à política de segurança da informação, que apresenta os requisitos em relação à segurança da informação da organização, um dos pontos importantes para um bom início da manutenção da seguridade da informação.

4.1.Documento da Política de Segurança da Informação

A Política de Segurança da Informação, segundo Coelho e Araújo (2013, p. 71) "é um conjunto de regras gerais que direcionam a segurança da informação e são suportadas por normas e procedimentos".

Este item está disposto na norma ABNT NBR ISO/IEC 27002 como Política de Segurança da Informação, e o objetivo dele é propor a orientação e apoio da direção com a proteção da informação de acordo com as determinações do negócio e leis vigentes. Na elaboração do documento da Política de Segurança da Informação é necessário que a direção esteja a par das mudanças relativas à manutenção da segurança da informação mostrando seu interesse por melhorias. Como um exemplo de pergunta adicionado ao questionário relativo à política de segurança, podemos citar duas questões:

Pergunta 1: Na organização, existe um documento relacionado a política de segurança da informação?

Pergunta 2: Este documento tem apoio da direção?

Estas questões estão relacionadas aos controles do item, verificando se a organização possui ou não este requisito de segurança, tudo dependendo das condições do negócio. Para acessar ao resto do questionário, visite o apêndice A.

No documento, os limites para a elaboração da política devem ir além da segurança relacionada à informática, ela deve estar associada com todo o negócio envolvido, proporcionando maior abrangência e proteção de diversas áreas. Para que as boas práticas de segurança da informação sejam seguidas, se faz necessário o envolvimento de usuários, funcionários e terceiros com a segurança, e que estes tenham consciência de suas obrigações e deveres para a manutenção da segurança. Segundo a ABNT NBR ISO/IEC 27002:2005 o

documento também deve estar em conformidade com as legislações vigentes, e que seja analisada regularmente.

4.2.Organizar a Segurança da Informação

É a definição de estratégias para o gerenciamento de segurança da informação, onde são denominadas regulamentações para controlar e gerenciar a segurança da informação na organização. (NBR 27002, 2006, p. 10). A direção deve ter a consciência de que o apoio a segurança da informação, traz a todos os outros envolvidos, uma maior segurança e confiabilidade, e a equipe diretiva, deve usar isto a seu favor mostrando que todos devem buscá-la para correção de qualquer problema relativo à segurança da informação. E, como exemplificação a respectiva pergunta abaixo:

Pergunta 1: A direção evidência um claro comprometimento, reconhecendo responsabilidades perante a segurança da informação?

A norma NBR 27002 (2005, p. 11) nos diz a segurança da informação deve ser discutida por todos os representantes de diferentes partes da organização, sejam funcionários, administradores, desenvolvedores, auditores e o pessoal de segurança especializada que podem orientar no esclarecimento de dúvidas e sugestões. Através de um mecanismo de troca de ideias, duvidas e sugestões que são impostas pelos diferentes representantes, pode-se elaborar um sistema, onde essa troca de ideias auxilie consideravelmente na melhoria da segurança da informação.

Para exemplificação com uma pergunta do questionário:

Pergunta 2 : Existem atividades relacionadas à segurança da informação, como por exemplo, um sistema de troca de ideias e dúvidas?

As organizações processam um grande número de dados ou informação em diferentes locais, e designar responsabilidades pelo tratamento destas informações, as quais, são importantes para a manutenção de um sistema confiável. Assim como tratar todas as informações com terceiros através de termos que comprometam as responsabilidades, com acordos de segurança para tratamento de informações sensíveis ao negócio da organização, reduzindo o risco de perda e adulteração de informações.

4.3.Gerenciamento dos Ativos

Os ativos de uma organização são todos os bens que a organização possui. Segundo Módulo (2013) os ativos são “todos os itens da organização onde informações são criadas, processadas, armazenadas, transmitidas ou descartadas”. Entre outros, os funcionários que fazem parte do desenvolvimento dos processos e segundo a norma NBR 27002(2005, p. 21), temos também os “intangíveis, tais como reputação e a imagem da organização”. Para a organização se faz necessário que todos estes ativos estejam identificados, para possíveis esclarecimentos em caso de desastres, sendo estes itens analisados com perguntas do questionário, como por exemplo:

Pergunta 1: Existe um inventário de todos os ativos?

Pergunta 2: Os ativos estão claramente identificados?

Dentre a verificação dos ativos, outro ponto analisado pela norma ABNT NBR ISO/IEC 27002 é que sejam definidas regras para o uso e processamento dos ativos, especialmente por pessoas não vinculadas a organização e que estão associados aos recursos de processamento.

> A gestão patrimonial de ativos é um trabalho que identifica e cataloga os bens físicos de uma organização para averiguar se determinado ativo existe na empresa, se está em sua devida localização e se está sendo utilizado pelas pessoas corretas, dentro de um prazo de vida útil adequado. (SOUSA, Revista Infra Magazine).

Em uma organização nem todos os ativos possuem um mesmo critério para sua utilização, ou seja, existem ativos que devem possuir um maior grau de cuidado e proteção, por serem informações sensíveis e de grande importância para a organização, a NBR 27002 (2005, p. 36) destaca “que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização”, sendo que esta citação pode ser representa pela pergunta do questionário:

Pergunta 3: A informação é classificada conforme criticidade e vulnerabilidade?

Não importando qual o tipo de ativo que a organização possui, todos devem ser tratados de forma segura, pois todos são importantes para o desenvolvimento da organização.

4.4.Proteção dos Recursos Humanos

A maioria ou senão todas as organizações possuem funcionários, fornecedores e terceiros e todos tem responsabilidades perante o uso de recursos da organização e estes segundo a ABNT NBR ISO/IEC 2007:2005 devem ser acordados para que os riscos de furto e roubo ou mau uso possam ser controlados em casos de não cumprimento do contrato. Abordado no questionário, com o exemplo a seguir:

Pergunta 1: Em contratos, estão definidos as responsabilidades pela segurança da informação conforme a política de segurança da informação?

Todo o planejamento relacionado com recursos humanos deve ser estrategicamente elaborado. O recrutamento de funcionários fixos ou temporários, tanto quanto a escolha de fornecedores, precisa ser cauteloso. Para exemplificação, através do questionário, temos:

Pergunta 2: São efetuadas verificações dos históricos dos candidatos, fornecedores e terceiros?

Estes processos de seleção visam a melhor escolha para a funcionalidade ou cargo pretendido, estes processos podem ser usados para testar habilidades, tipo de conduta que a pessoa pode apresentar em seu ambiente de trabalho e o trabalho sobre pressão entre outros.

Em relação a segurança da informação, os contratados devem ser informados de suas responsabilidades perante a segurança da informação, e caso alguma destas reponsabilidades for infringida, serão tomadas as devidas punições perante a lei (NBR 27002, 2005, 29). E que devem ser informados da delimitação de seus deveres e acessos às informações relacionados a seus futuros cargos.

Segundo a NBR 27002(2005, p. 30) no encerramento de atividades, convém que seja efetuada a devolução dos ativos que estão de posse do funcionário, e os direitos de acesso aos sistemas sejam removidos, priorizando assim a integridade do sistema e proteção das informações. É importante que contratos sejam regularmente revisados para que não ocorram surpresas relacionadas à segurança de acesso aos dados, pois a curiosidade atrai as pessoas a locais onde o acesso pode ser limitado, e que os funcionários também sejam fiscalizados, procurando possíveis brechas que possam afetar os sistemas de desenvolvimento de atividades importantes à continuidade do negócio.

4.5.Segurança Física e do Ambiente(Intempéries)

Conforme a GRIS (2013), “por mais que os casos de roubo de informações mais conhecidos sejam feitos através de redes, o comprometimento físico de informações, por diversos motivos, também gera diversos transtornos”, por este motivo utilizar a segurança física para a prevenção de acesso e intervenções naturais a equipamentos e informação e um bom meio de se minimizar o risco de perda de dados.

Organizações estão expostas a qualquer tipo de intervenção natural, prevenir a organização contra possíveis catástrofes é essencial, pois imagine que o sistema de backup esteja instalado num local muito próximo a organização, não seria viável. Caso ocorresse algum problema físico na organização, estes dados poderiam estar comprometidos. Pois segundo a NBR 27002(2005, p. 34) convém que “os equipamentos para contingencia e mídia de backup fiquem a uma distância segura, para que não sejam danificados por um desastre que afete o local principal”.

A proteção física deve levar em consideração o controle de acesso a locais onde o processamento de informações sensíveis é realizado e este controle deve ser feito de forma eletrônica por meio de mecanismos de controle de acesso, como por exemplo cartões de permissão de acesso, ou por pessoas designadas como porteiros. Os locais onde há o processamento de informação devem estar em conformidade com as leis vigentes de segurança física, e que estes locais sejam protegidos de forma adequada. Para maior exemplificação, temos as seguintes perguntas do questionário:

Pergunta 1: Existem controles de acesso físico, como portões de entrada ou recepcionistas para proteger salas de processamento de informações?

Pergunta 2: Locais de acesso restrito, são monitorados adequadamente?

Os sistemas de produção e armazenamento na maioria das vezes possui uma grande demanda de energia elétrica, e se torna cada vez mais indispensável à construção de uma boa rede de energia, a utilização de bons equipamentos de distribuição de energia e essencial para o bom desempenho dos sistemas de processamento. Em termos de segurança de cabeamento, a norma NBR 27002(2005, p. 37) sugere que as linhas de dados e energia sejam separadas para que o risco de interferência seja minimizado, e que o cabeamento seja protegido contra acesso não autorizado e assim, para prevenir a perda de informações.

4.6.Gerenciamento das Operações e Comunicações

Esta ação administrativa da norma diz respeito à utilização de mecanismos apropriados para que o gerenciamento das operações e comunicações seja estabelecido de forma a prover maior segurança dos recursos e sistemas. Através da documentação dos processos, dividindo as funções de processamento de informações para diversas pessoas, monitorando os serviços executados por terceiros. Utilizar políticas de proteção contra códigos auto executáveis e estabelecer políticas para a troca de informações de forma segura entre os diversos setores da organização e também, com terceiros.

No estabelecimento da documentação do processo a norma NBR 27002(2005, p.40) declara que é interessante que os processos de documentação sejam mantidos atualizados e disponíveis a todos os usuários que necessitem ter o acesso, e a mesma trate de itens como sistemas associados, processamento de informações, procedimentos de backup, manutenção de equipamentos, tratamento de mídias, entre outros, sendo analisados por alguns dos exemplos de perguntas do questionário:

Pergunta 1: Os procedimentos de operações são documentados e mantidos em constante atualização?

Pergunta 2: Estes procedimentos são disponibilizados a todos as pessoas que necessitarem deles?

Outro ponto analisado é a segregação de funções, que pode ser utilizada para que somente pessoas destinadas à utilização de determinados ativos possuam este acesso, diminuído os riscos de acesso indevido. Assim Gondim (2009, p. 13) complementa, “a segregação de funções contribui para a contenção de efeitos e redução de impactos no caso de algo de errado vir a acontecer”. A divisão dos sistemas de desenvolvimento, também, é um fator importante, assim como os de testes e produção. Proteger os sistemas contra acesso indevido, diminuindo os riscos de furto de informações sigilosas, que em forma de exemplificação do questionário, pode ser a seguinte:

Pergunta 3: Existe pessoal especializado para cada área?

Pergunta 4: Existe algum tipo de controle para impedir que pessoas não utilizem recursos sem autorização?

Em termos de políticas para o gerenciamento de serviço terceirizado a NBR 27002 (2005, p. 43), diz que convém que todos os processos ou serviços executados sejam verificados antes e após a entrega, e que os mesmos, sejam documentados, monitorados e analisados para

possíveis recursos de auditoria. Na obtenção ou criação de novos sistemas, é necessário que um planejamento seja executado, estabelecendo-se regras para que a disponibilidade do sistema seja garantida.

Outro tratamento abordado na norma é o de códigos móveis, que segundo Consult Corp (2012) são códigos que podem oferecer riscos quando implementados por pessoas mal-intencionadas. Sendo distribuídos pela rede, podem ser executados nos sistemas que foram hospedados, estes códigos podem ser, JavaScript, *applets*, *flash* e vírus, etc. Segundo a NBR27002 (2005, p. 46) convém que todos os usuários sejam informados dos possíveis riscos a organização caso algum destes códigos venha a ser executado internamente, e que exista uma política para a utilização destes códigos.

Contudo a importância da segurança dos sistemas de redes ao ponto de que o sistema não está restrito somente a parte interna da organização, ou seja, as organizações na maioria das vezes contratam provedores de internet para disponibilizar o acesso as *World Wide Web*. Por esse motivo a organização deve ter certeza de que sua comunicação não esteja sendo alvo de espionagem, e que o sistema também está seguro contra ataques ocorridos internamente, analisado pelo questionário através da seguinte pergunta:

Pergunta 5: Em acordos de serviço de redes, são incluídos características de segurança, níveis de serviço e requisitos para o gerenciamento destes serviços?

A manutenção ou descarte de mídias e equipamentos devem ser efetuados seguindo as políticas de segurança da organização, pois estes equipamentos descartados podem possuir informações sensíveis, e que o manuseio do mesmo e mídias sejam efetuados somente por pessoas autorizadas para prevenção de furtos.

Quando existe a troca de informações entre os diversos sistemas da organização, sejam escritos, falados ou transportados em mídias, devem existir políticas documentadas para esta troca de informações, para que a organização possa definir a quem atribuir possíveis responsabilidades, como abordado em uma pergunta do questionário, que é a seguinte:

Pergunta 6: Existem políticas documentadas para a troca de informações por qualquer meio de comunicação?

Sendo que esta troca de informações também pode ser feita através da internet, como por exemplo, no comercio eletrônico, que cada vez mais se desenvolve devido à grande comodidade oferecida por ele. Por isso as organizações devem se preocupar em garantir a integridade dos dados trafegados pela rede utilizando mecanismos de criptografia de dados, a utilização de recursos que identifiquem a autenticidade entre o emissor e o receptor .Com isso

a diminuição dos riscos de fraude tanto da organização quanto do usuário que está adquirindo o serviço ou produto da organização.

5. SISTEMA DE APLICAÇÃO WEB

Páginas Web tornam mais simples a interação entre um usuário e um serviço oferecido, esta ligação faz com que o acesso seja facilitado, pois o sistema está disposto em uma plataforma que pode ser acessada no local de trabalho ou na comodidade do lar. O presente sistema Web foi desenvolvido utilizando linguagens de programação: HTML (*HiperText Markup Language*), PHP(*HyperText Preprocessor*), CSS(*Cascading Style Sheets*), JavaScript e AJAX (*Asynchronous JavaScript and XML*), e foram destinados a situações especificas, onde a seguir irá constar a exemplificação de cada um deles e suas funções no projeto.

5.1.Sistema de Banco de Dados

Banco de Dados é um nome dado a uma coleção de informações ou dados referentes a um sistema, sendo organizados através de um modelo de banco de dados, que conforme Heuser (2010) "é uma descrição dos tipos de informações que estão armazenadas em um banco de dados". Todas estas informações, podem ser chamadas também de registros, onde estes podem ser gravados de diferentes maneiras, como por exemplo, em um supermercado onde consta os registros mantidos no banco de dados como: nome de produtos, preço, data de compra, valor do produto, também em relação a clientes e fornecedores pode ser guardados, os registros de nome, cidade, telefone, ..., sendo estes mantidos de forma organizada e de rápido acesso.

Para todo o banco de dados, existe um SGBD ou Sistema de Gerenciamento de Banco de Dados que tem por finalidade administrar e gerenciar base de dados, ou seja, manipular e organizar estes dados de forma correta. Dentre os modelos mais conhecidos temos: Microsoft SQL Server, MySQL, Oracle, DB2 entre outros.

Para o início da elaboração do banco de dados, devem-se estabelecer os requisitos do projeto, ou seja, que tipo de dados o sistema vai armazenar e quais são estes dados, através de uma modelagem do banco, bem como dos respectivos registros de dados. Dentre os processos de modelagem, temos:

Modelo Conceitual: que segundo Heuser (2010) "é uma descrição do banco de dados de forma independente de implementação em um SGBD", ou seja, esta modelagem nos apresenta somente quais são as informações que podem aparecer no banco de dados. Segundo Heuser (2010) "a técnica de modelagem conceitual mais difundida é a abordagem entidade-

relacionamento (DER)", que é representado por um diagrama como o exemplo do projeto, a seguir:

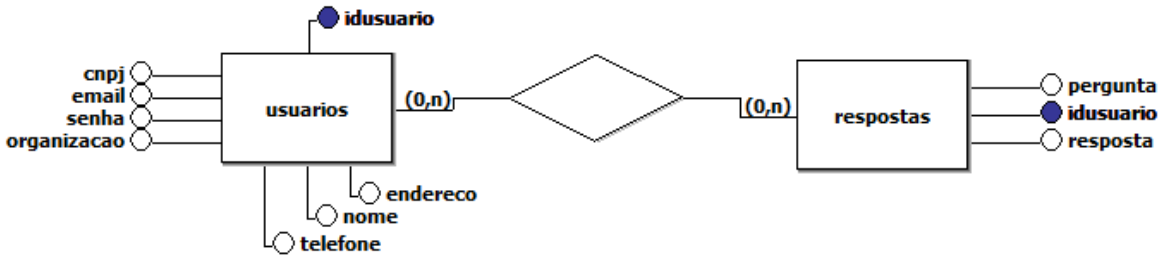


Figura 2 – Modelo conceitual do projeto

Fonte: Imagem própria do autor de autoria com BrModelo(2013)

Nesta modelagem conceitual (figura 2) são definidas as entidades que neste exemplo são: usuário e respostas, e os seus respectivos atributos onde os que possuem o círculo preenchido são chamados de atributos identificadores ou chaves primárias.

Para a criação das tabelas levou-se em consideração os requisitos do projeto, sendo necessário um cadastro de usuários, armazenando, o nome da organização, telefone, endereço e CNPJ por questões de manutenção de registros. Com finalidade de acesso ao sistema de respostas seria necessário solicitar um usuário/e-mail e uma senha, que além da função de acesso ao sistema, estabelecer um vínculo entre usuário e as suas repostas do questionário, identificadas pelo *idusuario* que foi definido no banco de dados.

Para o armazenamento das respostas foi criada uma tabela com as respostas do usuário, com atributos como o valor da resposta e o valor da pergunta, e o *idusuario* para relacionar as tabelas. A partir da modelagem conceitual estabelecida, é posteriormente iniciada a elaboração do banco de dados através da seleção de um sistema de gerenciamento de banco de dados.

Dentre os sistemas de gerenciamento de bancos, temos o MySQL, sendo um SGBD de código aberto, gratuito e utilizado pela maioria dos sistemas, com, linguagem SQL(S*tructured Query Language* – Linguagem de consulta estruturada). Para melhor visão e montagem do banco de dados utilizou-se uma ferramenta chamada MySQL Workbenck, onde se pode gerenciar todo o sistema de banco de dados, efetuar testes, criar tabelas, consultas, alteração de dados, entre outros. Sendo este sistema conectado ao servidor MySQL presente na ferramenta XAMPP.

O XAMPP é uma ferramenta que disponibiliza um sistema de servidor Web, e um sistema de servidor de MySQL entre outros serviços, sendo que esta ferramenta gratuita é de fácil configuração, utilizada para criação e testes do banco de dados.

5.2.Linguagem HTML e sua aplicação

O HTML (*HiperText Markup Language*) trata-se de um agrupamento de etiquetas ou *tags* onde define-se de que forma o texto e elementos serão apresentados em uma página web (Criarweb.com, 2004). Ela é a que forma a estrutura básica para a criação de uma página Web, uma linguagem de fácil aprendizado por possuir uma simples estrutura. A linguagem possibilita que informações sejam apresentadas na tela do computador para serem processadas e visualizadas, essa visualização é gerada através de marcadores ou *tags* que são os comandos utilizados para apresentar as informações.

Dentre a estrutura básica de uma página HTML temos as seguintes *tags*/marcadores:

```
<html>Marca o inicio de uma pagina HTML
<head>Mostra o cabeçalho da página Web;
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> Codificação de caracteres;
<title>Minha Página</title>Título que aparece na aba do navegador;
</head>Fechamento da tag "head"
<body>Corpo do documento HTML;
======  Conteúdo mostrado no Navegador  ======
</body>Fechamento da tag "body";
</html>Fim do documento HTML;
```

Figura 3 – Estrutura básica de uma página HTML
Fonte: Própria do autor

Com estas *tags* formando uma estrutura de uma página, esta já pode ser exibida em um navegador. Porém o projeto não utilizou somente estas *tags*, uma das principais contribuições do HTML foi a *tag form* que possibilita a criação de formulários, os quais, juntamente com os campos *input* são usados para preenchimento de informações por parte do usuário, fazendo

com que através de atributos destas *tags* informações sejam enviadas a uma página de processamento de informações, sendo está uma página PHP.

Para exemplificação do projeto, temos o seguinte:

```
<form name="signup" method="post" action="efet_cadastro.php">
        Nome:<input  class="textbox" type="text" name="nome" />
</form>
```

Figura 4 – Exemplificação da *tag form*

Fonte: Própria do autor

A *tag form* (figura 4) possui alguns atributos, dentre eles podemos destacar os utilizados no projeto, que são uns dos principais para a elaboração de um sistema de cadastro em HTML, estes atributos auxiliam no envio e chamada de ações que serão executadas para a criação do cadastro no sistema.

Atributo *name* : é utilizado para dar ao formulário um nome, fazendo com que ele possa ser utilizado em outras partes da página.

Atributo *method* : neste atributo temos dois valores a serem escolhidos, o *get* e o *post*. No *get* os dados são enviados juntamente com URL(*Uniform Resource Locator*) e este é o melhor método utilizado em casos de consulta a informações no servidor Web, no *post* os dados são enviados no corpo da mensagem deixando a URL separada, podendo assim enviar qualquer informação quando é necessário uma alteração no servidor. Dentre estes métodos o mais apropriado para envio de um formulário é o método *post*.

Atributo *action* : este atributo refere-se ao local ou URL que receberá as informações referentes ao formulário no momento do envio, e onde as informações serão tratadas.

A *tag input* (figura 4) tem por função de receber informações que serão digitadas pelo usuário no ato do preenchimento de campos necessários. Refere-se também ao local de entrada dos dados que serão processados pelo *form* , possuindo alguns atributos, dentre eles:

Atributo *class*: utilizado juntamente com CSS(*Cascading Style Sheets*) para definição de estilos para o campo de texto, somente para questões de estética neste caso.

Atributo *type*: define-se o tipo de elemento a ser usado, neste caso será utilizado o valor *text*, que referencia um campo de texto. O *type* possui também como valor o campo *password*

que transforma o que foi digitado em “pontos” muito utilizado em campos onde é necessário, a solicitação de senhas. Outro valor que o *type* pode assumir é o valor de *submit* que transforma-se, em um botão de enviar os dados do formulário para a página referenciada no atributo *action*.

Atributo *name*: tem a função de referenciar um nome para o elemento, no caso do exemplo (figura 4), ele refere-se ao campo “Nome”.

As *tags form* e *input* foram utilizadas, tanto para o sistema de cadastro quanto *login*, cada página referenciando o seu mecanismo para tratamento de dados, onde cada mecanismo para tratamento destes dados e elaborado em programação PHP.

5.3.Cadastramento de Usuários

Foi desenvolvido um mecanismo de cadastramento de usuários, onde informações são enviadas através de um formulário HTML, para uma página chamada *efet_cadastro.php*. Esta página é composta por uma conexão com o banco de dados, a qual, é feita uma verificação se os campos obrigatórios estão preenchidos no formulário, verificação se o usuário/e-mail já existem no sistema, evitando duplicidade e por fim se erros não ocorrerem, o cadastro é efetuado.

Inicialmente é necessário, uma conexão com o banco de dados, esta conexão é efetuada através do seguinte *script*:

```
<?php
        $connect = mysql_connect("localhost","root","") or die(mysql_error());
        mysql_select_db("tcc") or die(mysql_error());
?>
```

Figura 5 – Criação da conexão entre banco de dados e código PHP

Fonte: Própria do autor

A variável $*conecct* (figura 5) é necessária para a criação da conexão com o banco de dados sendo efetuada através da função *mysql_connect*, onde o parâmetro *localhost* significa o endereço em que estará hospedado o banco de dados, por seguinte temos os parâmetros de usuário e senha do banco de dados. No caso da elaboração do projeto, como a página foi

elaborada na máquina local, foram usados o usuário “root” e senha “nulo” que são valores padrões do MySQL, e a função *die(mysql_error())* é utilizada para retorno de um erro, caso a conexão entre banco de dados e a página não for efetuada com sucesso.

O *mysql_select_db* (figura 5) tem a função de selecionar o nome do banco de dados que será usado para a consulta e inserção de informações. Com estas informações a conexão com o banco, está efetuada e os dados podem ser inseridos ou consultados.

Os dados são enviados pelo formulário, e precisam ser usados em uma consulta ou inserção, ou seja, é necessário que eles sejam recuperados para serem usados. Esta recuperação é feita através do método *post*, onde os dados que são enviados através do formulário para a página referenciada no atributo *action* (figura 5), devem ser armazenados em uma variável no código PHP e assim ser tratados.

Uma das primeiras operações efetuada antes do cadastro é a de verificar se o banco possui o usuário/e-mail válido, ou seja, se este usuário/e-mail já foi cadastrado ou não, para a verificação de existência de um usuário, é preciso uma consulta ao banco de dados e verificar seu retorno:

```
$resp = mysql_query("select count(*) as total from usuarios where email =
'$email'");

$total = mysql_result($resp, 0, "total");
```

Figura 6 – Verificação da existência de usuários cadastrados no banco de dados.
Fonte: Própria do autor.

A variável $*resp*(figura 6) receberá o valor da consulta do *mysql_query*, que possui a instrução de verificar no banco de dados a quantidade de usuários com o e-mail digitado pela pessoa que está efetuando o cadastro no sistema, após, guardado o valor desta consulta, a variável $*resp* por sua vez será usada pela variável *$total* com a função *mysql_result* que possui por parâmetros $*resp*, valor de onde os dados serão retirados, no caso será um valor inteiro, o valor 0(zero) será o índice ou linha que será retirada a resposta e o “total” refere-se ao campo da consulta realizada pelo *mysql_query*.

Com a consulta efetuada o sistema verifica se o retorno da consulta feita ao banco de dados retorna 0(zero), caso o retorno seja nulo, significa que o sistema não possui usuários com aquele nome especifico, caso o valor retorne diferente de 0(zero) o sistema apresenta uma

mensagem que o usuário/e-mail já está cadastrado. Porém o sistema de cadastro utiliza o preenchimento de campos obrigatórios; ou seja não nulos, sendo estes: organização, nome, CNPJ, e-mail e senha, verificados através do exemplo de *script* a seguir:

```
if( !isset($_POST['organizacao']) || ($_POST['organizacao']==="")){
        echo "<script>cadastrofailed()</script>";
}
```

Figura 7 – Exemplo de verificação de campos obrigatórios

Fonte: Própria do autor.

Caso o sistema detecte campos nulos, uma função JavaScript mostra uma mensagem na tela ao usuário dizendo que o preenchimento dos campos obrigatórios é necessário, caso os campos sejam preenchidos de forma correta, o sistema cadastra o usuário, fazendo uma inserção dos dados do usuário no banco de dados e em seguida mostra uma mensagem de sucesso de cadastro, redirecionando o usuário para a página de *login* do sistema. Imagem do sistema de cadastro no Apêndice C.

5.4.Sistema de *Login*

Com o cadastramento efetuado com sucesso, o usuário é redirecionado para a página de *login*, é necessário somente utilizar o usuário/e-mail e a senha utilizados no momento do cadastro para que o acesso ao *checklist* seja liberado. O sistema se *login* funciona através da captura de dados que são digitados pelo usuário em um formulário. Este formulário por sua vez solicita através do atributo *action* a página para autenticação, ou seja, o sistema que irá verificar se o usuário/e-mail foi digitado de forma correta.

Primeiramente o sistema verifica se os campos de usuário/e-mail não estão nulos através do seguinte exemplo:

```
if( !isset($_POST['email']) || ($_POST['email']=="")
OR  !isset($_POST['senha']) || ($_POST['senha']=="")){

        echo "<center> Nome de Usuário ou Senha inválidos.Redirecionando
para a página de Login</center>";}
```

Figura 8 – Verificação de campos nulos

Fonte: Própria do autor

O comando *isset* (figura 8) é usado para verificar se a variável foi definida, ou seja, se ela foi declarada no campo de preenchimento, no caso do código acima foi usado uma !(exclamação) para verificar se ela não foi definida, caso não tenha sido definida, ou os campos não tenham sido preenchidos, o usuário recebe uma mensagem que os campos usuários/e-mail ou senha estão inválidos, redirecionado assim para a página de *login* novamente, até que os campos sejam preenchidos de forma correta.

Caso os campos possuam alguma informação o sistema então utiliza uma função de busca dos dados no banco de dados, verificando se o usuário/e-mail ou senha estão associados, utilizando a função *myslq_query* (figura 9) para a busca dos dados no banco, guardando na variável $*sql* (figura 9), utilizando posteriormente a função *mysql_num_rows* que obtém o número de linhas que foram efetuadas na consulta do *mysql_query* para verificação da existência de usuários.

```
$sql = mysql_query("SELECT * FROM usuarios WHERE email = '$email' and
senha = '$senha'") or die(mysql_error());

$row = mysql_num_rows($sql);
```

Figura 9 – Validação de usuário/senha no banco de dados

Fonte: Própria do autor.

Outra função usada na sequência dos comandos da mesma consulta, foi o *mysql_fetch_array*(figura 10), que possui a função de guardar índices numéricos da consulta e também guardar índice de dados associativos. Neste caso foi utilizado para associar o usuário/e-

mail e senha ao *idusuario* que será usado posteriormente para a realização do salvamento das respostas do questionário.

```
$resid = mysql_fetch_array($sql);
```

Figura 10 – Função de associação, útil ao estabelecer a seção, com identificador de usuário.
Fonte: Própria do autor

Após a realização da consulta e o salvamento nas variáveis necessárias, foi verificado através da variável $*row* (figura 9) se o número de linhas da consulta foi maior que 0(zero), ou seja, se os valores do *mysql_rows* (figura 9) for maior que 0(zero) é iniciada a seção do usuário através do *session_start*() (figura 11), atribuindo para a variável $*_SESSION* o nome do usuário/e-mail, senha e o valor do *idusuario* associado através do *mysql_fetch_array* (figura 10) com a variável $*resid*, liberando assim o acesso ao sistema do questionário, conforme a imagem a seguir:

```
if($row > 0){
        session_start();
        $_SESSION['email']=$_POST['email'];
        $_SESSION['senha']=$_POST['senha'];
        $_SESSION['idusuario']=$resid['idusuario'];
        echo "<center>Login efetuado com sucesso! Aguarde um
momento.</center>";
}
```

Figura 11 – Inicialização de seção de usuário
Fonte: Própria do autor

Caso o retorno do *mysql*_num_*rows*(figura 9) for menor que 0(zero) o sistema alerta o usuário com uma mensagem que o usuário/e-mail ou senha estão incorretos e redireciona novamente a página de *login*. No apêndice D consta uma imagem da página de *login*.

Para aplicação do *checklist*, ou seja, para que se possa obter dados referentes às respostas dos usuários, utilizou-se uma *tag* chamada *select* que possibilita ao usuário no momento de

responder aos questionários escolher uma opção que satisfaça sua posição referente à pergunta efetuada, por exemplo:

Pergunta: Na organização, existe um documento relacionado à política de segurança da informação? A *tag select* proporciona ao usuário quatro opções de respostas onde o usuário seleciona uma delas, como por exemplo na figura abaixo:

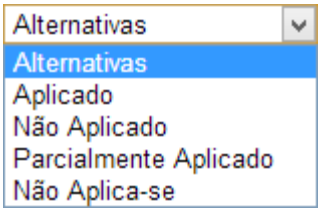


Figura 12 – Menu de seleção de respostas

Fonte: Própria do autor.

Esta *tag select* é implementada, somente em HTML, porém neste projeto ela foi atribuída em uma função PHP, que é chamada após cada questão a ser respondida. No Capítulo 6, é abordado o significado de cada alternativa de resposta.

A *tag select* é utilizada para criar menus de seleção, onde está *tag* possui a seguinte estrutura:

```
<select name="valores">
                <option value="-1">Alternativas</option>
                <option value="3">Aplicado</option>
                <option value="1">Não Aplicado</option>
                <option value="2">Parcialmente Aplicado</option>
                <option value="0">Não Aplica-se</option>
 </select>
```

Figura 13 – Estrutura de uma *tag select*

Fonte: Própria do autor

Esta *tag* possui também seus atributos que podem ser *name* (figura 13), que é o nome do elemento enviado no momento da submissão do campo *option* (figura 13) o qual foi selecionado, no atributo *value* (figura 13), pode-se definir um valor para cada resposta, caso não seja atribuído, será assumido o valor que está dentro do *option*. Para que a adição desta *tag*

não deixasse o código HTML muito grande, foi utilizado o mecanismo de função, onde esta pode ser utilizada em qualquer local da página otimizando o sistema.

Inicialmente é criada uma função com o nome de *criaselect* (figura 14), que recebe por parâmetro a variável *$nome* (figura 14). Como dito a *tag select* é uma *tag* da linguagem HTML, por consequência não teria a possibilidade de exibi-la dentro de um script PHP sem a utilização da função *echo*, dentre esta técnica da função *echo*, outra função muito importante foi utilizada, chamada de *onChange*, que é um evento de JavaScript, utilizado para atualizar outros elementos da página Web, trabalhando juntamente com a técnica AJAX, utilizada na captura das respostas selecionadas na *tag select*, como mostra a imagem a seguir:

```
<?php
        function criaselect( $nome){
        echo "<select name=\"" . $nome . "\" onChange=\"atualizadb(this)\" >";
        echo "<option value=\"-1\">Alternativas</option>";
        echo "<option value=\"3\">Sim</option>";
        echo "<option value=\"1\">Não</option>";
        echo "<option value=\"2\">Parcial</option>";
        echo "<option value=\"0\">Não Aplica-se</option>";
        echo " </select>";
 return;}
```

Figura 14 – Função que cria o menu de opção de resposta.

Fonte: Própria do autor

A variável *$nome*(figura 14) é importante ao ponto que no momento que o usuário selecionar a opção de resposta, esta utilizará a função chamada no evento *onChange*, e passará por parâmetro para a função *atualizadb* (figura 15) o nome da pergunta e o valor de sua resposta através do método *serializeArray*() (figura 15) com a função de criar um *array* de objetos JavaScript, sendo que este elemento opera em um objeto JQuery representado por um conjunto de elementos de formulário.

5.5.JQuery e AJAX

O JQuery é um *framework* do JavaScript, ou seja, é um conjunto de métodos e funções a serem utilizados com sintaxe simples comparado ao JavaScript, pode ser considerado um novo método de se programar, um novo estilo (Thiago Belem, 2010). O JQuery pode ser usado para construções de páginas, adição de efeitos, requisições em AJAX. Para que se possa utilizar o JQuery é necessário que se tenha no código da página, a sua biblioteca de funções adicionadas, sendo esta disponibilizada na própria *Web Page* do JQuery.

A utilização do JQuery no projeto foi sua biblioteca de funções, utilizadas pela técnica AJAX, que significa *Asynchronous JavaScript and* XML(JavaScript *and* XML Assíncronos), muito utilizado para criar aplicações Web interativas. O AJAX é um código executado no próprio navegador da máquina cliente, não necessita de requisições HTML para sua execução, não efetuando assim o recarregamento da página do navegador, ou seja, no ato de responder ao questionário o usuário efetuara a escolha de uma opção disposta no *SelectBox* (figura 12). Após esta seleção, não é efetuado um recarregamento da página.

Como exemplificação de funcionamento do AJAX pode-se citar, por exemplo, ao se efetuar um cadastro em que necessitamos digitar o CEP (Código de Endereçamento Postal) do local em que residimos, nota-se que automaticamente as informações de nome da rua, cidade e estado são preenchidas, isto se deve ao fato do uso da técnica AJAX para efetuar esta ação.

Para definições do trabalho, necessitou-se de uma função que obtivesse os dados de resposta do usuário no momento da seleção da resposta, não atualizando a página, e assim enviado estas informações de resposta para um banco de dados para posteriormente serem tratadas.

A função utilizada para envio de informações foi a seguinte:

```
function atualizadb(obj){
      $.ajax({ url: 'form.php',
         data: { iduser: "<?php echo $_SESSION['idusuario']; ?>", chave:
"destaques", valor: $(obj).serializeArray()},
         type: 'post',
         responseType: 'json',
               success: function(output) {
               //console.log(output);
               }
      });
               //console.log(obj);
}
```

Figura 15 – Função JQuery que captura e envio das respostas do usuário.

Fonte: Própria do autor

Inicialmente foi criada uma *function*(função) chamada *atualizadb* (figura15), esta função é chamada a cada vez que o usuário seleciona uma opção do *SelectBox* (figura 12), através do evento *onChange* (figura 14). Por seguinte a técnica *$.ajax*(figura 15) é chamada para efetuar o envio das informações referentes as respostas e o valor da resposta, para a *url:form.php* (figura 15) que tem por função tratar os dados recebidos e ajusta-los ao banco de dados.

A *tag data* (figura 15) tem por função o envio de informações ao servidor, onde converte os valores para uma *string.* Neste caso foram usados para a passagem de parâmetros os seguintes dados, *iduser* (figura 15) que refere-se ao identificador do usuário corrente, ou seja, quem está respondendo ao questionário naquela seção, e um "valor" passando por parâmetro o que é recebido pela função *atualizadb(obj)* (figura 15), neste caso o "*obj*" são os valores da pergunta e o valor da resposta, utilizando o método *serializeArray* (figura 15) do JQuery para criar uma lista de vetores a serem enviados para a página de tratamento *form.php*, enviando-os com o *type post* (figura 15) para uma melhor interação com a página de tratamento de dados.

O *json* (figura 15) é um tipo de *string* para tratamento de dados, sendo que estes podem ser armazenados e recuperados posteriormente pela técnica AJAX para serem processados. No projeto ele foi utilizado para que os dados fossem tratados da melhor forma se utilizado com o método *serializeArray*.

Para exemplificação, temos a seguir uma captura de tela da ferramenta de desenvolvedor, do navegador, que nos mostra como os dados são processados, e o envio de

informações fica transparente ao usuário, ou seja, as informações de resposta e identificador de pergunta já foram salvas no banco de dados:

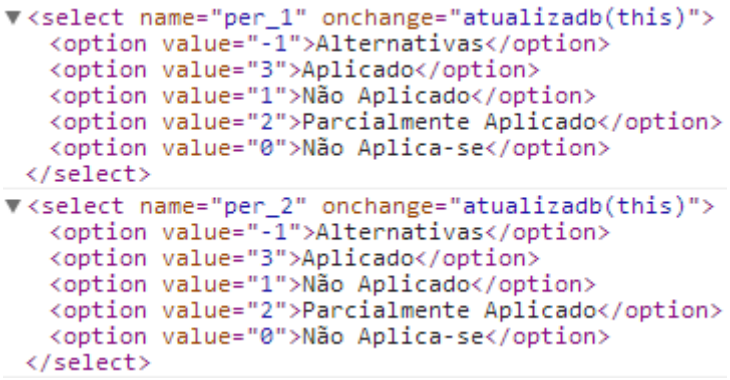


Figura 16 – Função *criaselect* mostrada pela ferramenta de desenvolvedor

Fonte: Captura de tela de própria autoria com Ferramenta de desenvolvedor Google Chrome

Para tratamento das respostas de cada questão, foi criado um sistema que recebe estas informações para adicioná-las ao banco de dados, porém para os requisitos de elaboração do projeto de banco de dados, optou-se por adicionar valores numéricos, tanto para o valor da pergunta, quanto para o valor da resposta.

Para exemplificação, cada pergunta do questionário seguiu a seguinte numeração, per_1, per_2, per_3, per_4,....., per_298, per_299, onde ao enviar os dados a função AJAX envia o valor do *name*(atributo da *tag select*(figura 14)). Conforme o mostrado, para facilitar a adição e utilização destas informações das respostas para eventos posteriores, optou-se por utilizar uma função do PHP chamada de *substr* que é utilizada para retornar parte extraída da *string*, por exemplo:

$retorno = *substr*(“projeto”, 1); //retorno e “rojeto” retira a primeira letra;

$retorno = *substr*(“projeto”, -1); //retorno e “projet” retira a última letra;

$retorno = *substr*(“projeto”, 4); //retorno e “eto”; retirou as 4 primeiras;

No caso do projeto, foi utilizando da seguinte forma:

```
$_POST['valor'][0]['name'] = substr($_POST['valor'][0]['name'], 4);
```

Figura 17 – Função *substr* utilizado no projeto

Fonte: Própria do autor

Esta linha de código (figura 17) foi utilizada para pegar o valor enviado pela função *atualizadb* (figura 15), ou seja, no ato de envio da *tag data* (figura 15), com o *serializeArray*, o valor da pergunta e a resposta, foram enviados concomitantemente, porém cada um com seu valor. O *name* (figura 14) refere-se ao nome da pergunta per_1, per_2, per_3..... , e para que se pudesse guardar somente o identificador da pergunta, o número dela, foi utilizado na função do PHP, *substr* (figura 17), com o valor de corte 4 para que a parte "per_" seja retirada a cada vez que uma pergunta for adicionada ao banco, acrescentando somente o identificador único dela, ou seja, seu número.

Posteriormente ao tratamento do valor da pergunta, é executada a adição dos valores de identificador de usuário, identificador de pergunta e o valor da resposta de cada pergunta ao banco de dados. Os valores são adicionados ao banco inicialmente através de um *insert into* (figura 22), que é uma função do MySql que insere valor ao banco de dados, onde envia-se por parâmetros os campos à adicionar, e em seguida os valores de cada campo, exemplificado pela imagem a seguir:

```
$sql->Queryorupdate
("INSERT INTO respostas (idusuario, pergunta, resposta)
 VALUES (".$_SESSION['idusuario']."', '".$_POST['valor'][0]['name']."',
'".$_POST['valor'][0]['value']."');"
```

Figura 18 – Inserção da resposta no banco de dados.

Fonte: Própria do autor.

Os campos a serem inseridos são *idusuario*, *pergunta* e *resposta* (figura 18) com seus respectivos valores, ou seja, o campo *idusuario* receberá o valor do usuário que está naquela seção, em seguida o campo adicionado e o *pergunta* que recebe o valor enviado pelo método *serializeArray* da *tag data* da função *atualizadb* (figura 15), com o valor de *name* (figura 14) que foi definido na criação da pergunta, sendo que este valor é um número inteiro que foi

transformado pela função *substr* do PHP, e por seguinte o campo *resposta* recebe o valor *value* que foi definido na *tag select* na criação da função *criaselect* (figura 14), que também é um valor inteiro.

Sendo assim as respostas referentes ao questionário estão salvas no banco de dados, podendo ser acessadas pelo sistema de *feedback*, onde vai constar ao usuário uma média referente as suas respostas do questionário, recebendo um *feedback* em relação ao seu nível de segurança da informação.

6. SISTEMA DE *FEEDBACK*

Dentre os objetivos do projeto, um deles é proporcionar ao usuário ou organização que respondeu o questionário um *feedback*, ou seja, uma informação ao usuário como está seu nível de segurança. Proporcionar uma pontuação que possa auxiliar o gestor de segurança da informação da organização a observar seus pontos fortes como também seus pontos fracos, auxiliando como um direcionamento para o estabelecimento de novos controles de segurança da informação encontrados na norma ABNT NBR ISO/IEC 27002.

Para definição da escala de pontuação, foram utilizadas quatro variáveis que demonstram situação bem diretas em relação a pergunta aplicada. Onde todo o julgamento das respostas, das perguntas, deve ser feito por um gestor que possua conhecimento da organização, pois o resultado final dependerá desta análise. Cada pergunta pode ser respondida através de uma das opções da escala de valores, sendo elas:

Aplicado: este termo refere-se que a organização possui aplicado o controle de segurança da informação, mostrando também que o controle está implementado, aumentando assim a segurança da informação.

Parcialmente Aplicado: leva em consideração em ter o controle incluso, porém de forma que o gestor de segurança da informação julgue que o item não foi implementado levando em consideração todos os requisitos do negócio, podendo causar brechas na segurança da informação.

Não Aplicado: diz respeito a não implementação do controle de segurança podendo assim proporcionar falhas de segurança que podem ser exploradas com a finalidade de prejudicar os negócios da organização.

Não Aplica-se: como a própria norma ABNT NBR ISO/IEC 27002:2005 relata que nem todos os controles são aplicáveis as organização, e tudo depende dos requisitos do negócio, esta opção de resposta foi imposta ao questionário para omitir do *feedback* perguntas que não se referem aos requisitos do negócio da organização.

Por questões de tratamento dos dados com banco de dados, foi determinado que cada alternativa de resposta possuísse valores numéricos, ou seja, cada alternativa iria possuir uma pontuação que iria variar de 0 a 3, onde 0(zero) seria a pontuação mínima ou insignificante e 3 a pontuação máxima, mais significante, atribuindo a cada uma das opções de resposta a sua pontuação. A opção Aplicado passou a contar pela pontuação igual 3, mais significante no que refere-se a ter um controle maior de segurança. A opção Não Aplicado possuiria a pontuação

igual a 1, por ter valor baixo e não possuir a segurança da informação. A opção Parcialmente Aplicado com a pontuação igual a 2, como um termo intermediário entre a melhor e a pior opção, não desprezando o que está aplicado e o não aplicado em relação a segurança de informações. E a opção Não Aplica-se com pontuação igual a 0(zero) definido com uma pontuação insignificante, que não altera nada em relação a segurança da informação na organização.

Para realização do *feedback* utilizando os valores impostos, isto é um retorno em relação a pontuação feita após responder ao questionário, foram feitos alguns estudos das médias que poderiam ser utilizadas para calcular a pontuação que qualificasse a segurança da informação da organização, dentre elas foram estudadas, moda, mediana, média aritmética e média ponderada.

Moda: neste método estatístico o valor selecionado para definição da pontuação, e o valor que mais aparece em um conjunto de valores, como por exemplo:

Ex: pontuação {1, 1, 3, 2, 1, 3, 1, 3, 2, 1, 2}

Neste conjunto de elementos, o valor que mais aparece é o valor 1, sendo ele a moda deste conjunto. Que por requisitos do projeto, trabalhando com pesos para as questões, não é a mais apropriada.

Mediana: neste método utiliza-se o elemento intermediário de um conjunto de elementos, como por exemplo:

Ex: pontuação {1, 1, 3, 2, 1, 3, 1, 3, 2, 1, 2}

Onde: pontuação {1, 1, 1, 1, 1 , 2, 2, 2, 3, 3, 3}

No caso do exemplo, a mediana refere-se ao número 2, pois ele é o termo intermediário do conjunto de números. Caso o conjunto de números for ímpar conforme o exemplo acima, utiliza-se o valor intermediário, porém se o conjunto de números é par, utiliza-se a média aritmética dos dois números intermediário para se definir a mediana.

Média Aritmética: é uma das medias mais simples, onde soma-se todos os elementos, dividindo a soma pelo número de elementos que foram somados, obtendo-se assim a média dos valores:

Ex: 1 + 2 + 1 + 3 +2 + 1 / 6 = 10/6 = 1.66

Por questão de definição do trabalho, onde cada questão foi definida com um peso de resposta, uma das medias mais apropriadas, foi a Média Ponderada, que diferentemente da Média Aritmética, trabalha com questões de ponderação, ou seja, com o peso relativo de cada questão, melhorando assim a precisão das respostas. Por exemplo:

Ex: Utilizando as respostas do questionário, por exemplo, onde o número de respostas para a opção:

Aplicado (peso 3) = 3 respostas

Parcialmente Aplicado (peso 2) = 5 respostas

Não Aplicado (peso 1) = 2 respostas

Não Aplica-se (peso 0) = 1 resposta (resposta insignificante)

Para o cálculo da Média Ponderada utiliza-se o número de ocorrência (frequência em que as respostas aparecem) vezes o peso de cada resposta, por exemplo:

[(3(Aplicado)*3(Respostas)) + (2(Parcialmente Aplicado)*5(Respostas)+ (1(Não Aplicado)*2(Respostas))]

Então assim, divide-se pelo somatório das frequências de cada resposta:

(3(Respostas Aplicado) + 5(Respostas Parcialmente Aplicado) + 2 (respostas Não Aplicado))

Calculando então:

[(3(Aplicado)*3(Respostas)) + (2(Parcialmente Aplicado)*5(Respostas) + (1(Não Aplicado)*2(Respostas))] / (3(Respostas Aplicado) + 5(Respostas Parcialmente Aplicado) + 2 (respostas Não Aplicado))

= {(3*3) + (2*5) + (1*2)} / {(3+5+2)} = {9+10+2}/10 = 21/10 = 2.1 como Média Ponderada.

Com esse cálculo realizado obtemos o valor de 2,1, ou seja, um valor mais preciso em relação às respostas do questionário, ficando próximo da opção de resposta, Parcialmente Aplicado. Para que o usuário que respondeu ao questionário possa ter um *feedback* mais compreensível, foi elaborado um sistema onde em uma faixa de valores o usuário recebe uma mensagem que relata como está o nível de segurança da informação, no item especifico.

Para regras de arredondamento dos valores utilizou-se regras da norma NBR 5891 “o algarismo imediatamente seguinte ao último algarismo a ser conservado for superior a 5, ou, sendo 5, for seguido de no mínimo um algarismo diferente de zero, o último algarismo a ser conservado deverá ser aumentado de uma unidade”.

Por exemplo:

1,666 6 arredondado à primeira decimal tornar-se-á: 1,7 ; 4,850 5 arredondados à primeira decimal tornar-se-ão : 4,9.(NBR 5891)

Onde no projeto para retorno de *feedback* utilizou-se a seguinte descrição:

Valor de resposta entre 1 e 1,490, pertence a valores mais próximos do resposta Não Aplicado, onde o nível de segurança da informação e bem crítico e necessita ser melhorado rapidamente, aconselha-se:

A organização não segue boas práticas de segurança da informação em relação a este item, pois a pontuação obtida foi muito baixa;

Valor de resposta entre 1.5 e 1,990, onde este valor está quase no nível Parcialmente Aplicado, ou seja, existe algo implementado, porém nada que seja suficiente para atingir a segurança da informação, aconselha-se:

Sua organização obteve uma pontuação intermediária/baixa, é necessário uma reavaliação de alguns termos de segurança;

Valor de resposta entre 2 e 2,490, este valor pertence ao item Parcialmente Aplicado, porém com algumas falhas na segurança da informação, aconselha-se:

O nível de segurança está quase bom, é necessário a busca da norma para melhorar controles de segurança da informação;

Valor de resposta entre 2.5 e 3, refere-se a ter um bom nível de segurança da informação, onde as melhorias dependem dos requisitos do negócio, e do nível de segurança que a organização pretende atingir, aconselha-se:

A organização segue boas práticas de segurança da informação, melhoras dependem somente dos requisitos do negócio da organização;

Este sistema foi aplicado através de uma página onde estas informações são processadas e apresentadas ao usuário. Para o mecanismo de cálculos, foram utilizadas busca no banco de dados selecionando um conjunto de respostas referentes a cada item de segurança, ou seja, o item de Política da Segurança da Informação é calculado separado do item de Organizando a Segurança da Informação, e assim sucessivamente para os demais itens, cada um com seu *feedback*, como mostrado anteriormente.

Para a seleção das questões e suas respectivas respostas, para os cálculos, foram utilizadas funções da linguagem SQL, mais especificamente, *Select's*, com objetivo de selecionar algo, a função *SUM* que faz um somatório de algum campo de uma tabela, o *COUNT*, a contagem de quantos registros possuem o campo especificado, e juntamente a função *WHERE*

e *BEETWEN* para delimitações de campos e valores sucessivamente. Para melhor entendimento, um exemplo na imagem a seguir:

```
SELECT SUM(resposta) FROM respostas WHERE
(idusuario=".$_SESSION['idusuario']."
AND (resposta=3 AND idpergunta BETWEEN 1 and 10);
```

Figura 19 – Utilização da função SUM do MySQL

Fonte: Própria do autor

Neste exemplo (figura 19) é efetuado um somatório do campo "resposta" , da tabela "respostas" onde o *idusuario*, é o que está com a seção iniciada, e onde a "resposta = 3"(valor da resposta APLICADO), e o identificador da pergunta esteja entre 1 e 10. Para todos os outros valores do campo "resposta" (APLICADO = 3, PARCIALMENTE APLICADO = 2 e NÃO APLICADO = 1) foram criadas consultas para a seleção dos dados para posteriores cálculos. Utilizou-se também para os cálculos além da função *SUM* a função *COUNT*, alterando os parâmetros citados acima, salvando em variáveis diferentes para cálculos posteriores, como exemplo para a função *COUNT*:

```
SELECT COUNT(resposta) FROM respostas WHERE
(idusuario=".$_SESSION['idusuario']."
AND (resposta=3 AND idpergunta BETWEEN 1 and 10);
```

Figura 20 - Utilização da função COUNT do MySQL

Fonte: Própria do autor

Após efetuar a seleção de valores e salva-las em diferentes variáveis para cálculos, estes, são apresentado na aba de "resultado" da página Web (Apêndice F). Tendo o item de segurança com seu respectivo valor de resposta, e logo abaixo, adicionou-se o sistema de *feedback* das mensagens, auxiliando assim o usuário com a identificação dos pontos fortes e fracos. Em seguida foi direcionado um caminho a ser seguido para buscar implementações de controles de segurança da informação que estão na norma ABNT NBR ISO/IEC 27002 no site da Associação Brasileira de Normas Técnicas, referenciado por um link na página dos "resultado".

Sendo assim, a página de aplicação do questionário está finalizada e em condições de receber usuários interessados em verificar o nível de segurança da informação, podendo perceber qual ou quais podem ser os pontos fracos, onde a organização pode sofrer perdas de informações importantes para continuidade do negócio.

7. CONCLUSÃO

Nota-se que, o desenvolvimento de um projeto capaz de auxiliar organizações na proteção das informações se torna cada vez mais necessário, devido a este mundo globalizado, onde muitas informações são processadas e armazenadas e compartilhadas todos os dias. A necessidade de melhorias relativas à segurança de informações se torna cada vez mais importante, pois são estas informações que auxiliam o desenvolvimento e sustentabilidade de uma organização.

Com a evolução dos meios de comunicação, é fundamental que estas informações trafeguem de forma mais segura e rápida, não importando qual o meio e por onde ela trafegue, sendo internamente ou externamente nas organizações. A todo o momento são criadas novas maneiras de se burlar algum mecanismo de segurança para acesso a informações sigilosas, e estes mecanismos de segurança devem ser revisados e melhorados proporcionando assim maior segurança às informações importantes.

Como objetivo, este projeto propõe as organizações interessadas a verificarem o seu nível de segurança de informações, sendo este nível testado com um questionário baseado em uma norma internacional de segurança da informação, que por sua vez foi adaptada para o português brasileiro pela Associação Brasileira de Normas Técnicas, a ABNT NBR ISO/IEC 27002:2005 Tecnologia da Informação – Técnicas de Segurança – Código de pratica para a gestão da segurança da informação, proporcionado assim a toda e qualquer organização, sugestões que auxiliam a adição de novos controles de segurança da informação.

Com base na delimitação do projeto, os objetivos foram alcançados. O questionário foi baseado nas seções de segurança da informação da norma ABNT NBR ISO/IEC 27002:2005. Elaborado com enfoque nos controles que a norma adota como metas para atingir a segurança da informação, constando com 299 questões relacionadas as seções de Política de Segurança da Informação, Organizando a Segurança da Informação, Gestão de Ativos, Gestão em Recursos Humanos, Segurança Física e do Ambiente e Gerenciamento das Operações e Comunicação. A partir deste questionário, foi criada uma página Web com capacidade de aplicação das questões, constando também com um sistema de *feedback*, onde o usuário que respondeu ao questionário será informado com uma pontuação e um conselho de como está a segurança da informação em sua organização.

Dentre as funções de um profissional de redes de computadores, um dos objetivos é a manutenção da segurança das informações dentro do ambiente de trabalho, proporcionando

métodos capazes de auxiliar na manutenção e integridade dos dados importantes para o desenvolvimento do sistema da organização, ajudando no aumento de receitas e geração de lucros.

Contudo, é necessário salientar a importância de levar ao ambiente de trabalho, sistemas capazes de auxiliar a detecção de falhas, sendo importante ao ponto de preveni-las, diminuindo os riscos de perda de informações sensíveis, tudo isso aliado a uma norma que tem por objetivo auxiliar na implementação de mecanismos capazes de reduzir a perda de informações importantes, que é a norma ABNT NBR ISO/IEC 27002:2005.

Outro fator importante foi a criação de um mecanismo com capacidade de aplicar um questionário de perguntas, sendo disponibilizado em um página na Internet, onde a todo o momento as pessoas estão conectadas, facilitando o acesso e a resolução deste questionário. Desenvolvido através de linguagem conhecidas como HTML, PHP, JavaScript e também com novas técnicas que facilitam a programação Web, baseadas em JavaScript como JQuery e AJAX.

Com a norma ABNT NBR ISO/IEC 27002:2005 auxiliando as organizações na manutenção da segurança da informação, foi criado um questionário para verificar qual o nível de segurança da informação em uma organização, e disponibilizar este questionário em uma página Web para que possa ser respondido por organizações interessadas, torna o trabalho importante ao ponto de que essas organizações busquem a sua melhoria no que diz respeito a toda segurança da informação, através da adição de controles de segurança que estão presentes na norma.

7.1.Sugestões para pesquisas futuras

O questionário possibilita uma ampla visão dos requisitos de segurança da informação, auxiliando na verificação de pontos fracos e fortes, porém neste projeto não foi abordado todas as seções de segurança da informação presentes na norma ABNT NBR ISO/IEC 27002:2005, deixando passar outros pontos importantes, como os já abordados.

Para tanto é necessário um mecanismo mais completo, o qual leva em consideração todos os requisitos de segurança da informação, para tornar a verificação da segurança da informação na organização, mais aperfeiçoada, reduzindo os riscos de perda de informações importantes. E, em pesquisas futuras criar um mecanismo que possa após o questionário

respondido, levar em consideração os pontos fracos, na criação de um sistema que promova sugestões de melhoramento neste processo.

Dentro deste mecanismo de sugestões, que poderia oferecer aos usuários algumas dicas de implementação de controles de segurança da informação, sendo estas dicas baseadas nos pontos fracos conforme a pontuação obtida, auxiliando no domínio e manutenção da segurança da informação.

8. REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 5891**: Regras de Arredondamento na Numeração Decimal. Rio de Janeiro, 1977.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2006** Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão de Segurança da Informação. Rio de Janeiro, 2006.

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

CESPEDES. G. J.; Medidas Resumo. SlideShare. **Anais Eletrônicos.** Disponível em: < http://pt.slideshare.net/ArielRChaves/aula-3-medidas-resumo-parte-1>. Acesso em: 26 nov.2013.

CLASSIFICAÇÃO e cálculo da média de classificação. **Survey Monkey Help Center.** Disponível em: < http://help.surveymonkey.com/articles/pt_BR/kb/What-is-the-Rating-Average-and-how-is-it-calculated >. Acesso em: 29 nov.2013.

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.

CRIARWEB.COM; **O que é HTML**. Disponível em: <http://www.criarweb.com/artigos/7.php >. Acesso em: 12 jan. 2014

DOCUMENTAÇÃO. **PHP NET**. Disponível em:< http://www.php.net/manual/pt_BR/>. Acesso em: 04 nov. 2013.

GONDIM, J. J. C; **Gerenciamento das Operações e Comunicação**. GSIC602 2009-2011. v. 1.

CONSULT CORP. **Segurança da Informação-Códigos Móveis**. Disponível em: < http://www.consultcorp.com.br/noticias/noticias-gerais/191-seguranca-da-informacao-codigos-moveis>. Acesso em: 10 jan.2014.

GRUPO DE RESPOSTAS A INCIDENTES DE SEGURANÇA(GRIS). Notícias. **Boas práticas para garantir a segurança física da informação.** Disponível em:< http://www.gris.dcc.ufrj.br/news/boas-praticas-de-seguranca-fisica-da-informacao/>. Acesso em 02 out.2013.

INTEL. DiálogoTI/*Next Generation Center*. **Segurança da Informação**. Disponível em: , <http://www.nextgenerationcenter.com/detalle-curso/Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o.aspx>. Acesso em: 09 set.2013.

JAVASCRIPT - *Select* - *OnChange.* **Stackoverflow.** Disponível em: <http://stackoverflow.com/questions/11877527/javascript-select-onchange>. Acesso em: 18 nov.2013.

JQuery.ajax().**Jquery – Write less, do more.** Disponível em: < http://api.jquery.com/jQuery.ajax/ >. Acesso em: 15 nov.2013.

LISTA (*SELECT BOX*) PHP + JQUERY (AJAX). **PHP Tech.** Disponível em: < http://www.phptech.com.br/lista-select-box-php-jquery-ajax/>. Acesso em: 18 nov.2013.

MÉDIA PONDERADA. **Mundo Educação**. Disponível em: <http://www.mundoeducacao.com/matematica/media-ponderada.htm>. Acesso em: 02 dez.2013.

MODULO. Soluções. **Gestão de Ativos – Automatize os processos da sua empresa**. Brasil, 2013.

MYSQL WORKBENCH. **MySQL**. Disponível em: <http://www.mysql.com/products/workbench/>. Acesso em: 11 out.2013.

NAKAMURA, E. T.; GEUS, P. L. de. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec Editora, 2007.

O IDENTIFICADOR SELECT. **FORMS.** UFRGS/EDU. Disponivel em: < http://penta.ufrgs.br/edu/forms/tut22.html>. Acesso em: 28 out.2013.

PASS array to ajax request in $.ajax() [duplicate]. **Stackoverflow**. Disponível em: <http://stackoverflow.com/questions/8890524/pass-array-to-ajax-request-in-ajax>. Acesso em: 28 nov.2013.

PEIXOTO, M. C. P; **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

PORTAL NACIONAL DO DOCUMENTO ELETRÔNICO. Técnicas & Definições. **O que significa Não-Repudio?**-2005-2013. São Paulo, 2013.

PINHEIRO, J. M. Dos S.; **Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar**. 5. ed. Rio de Janeiro: UniFOA, 2007.

PROGRAMAÇÃO E *DESING*. **WP Masters.** Disponível em: < https://www.youtube.com/user/canalwpmasters?feature=watch>. Acesso em: 04 nov.2013.

HEUSER C. A.; **Projeto de Banco de Dados**. 6º. ed. Porto Alegre: Artmed Editora SA, 2010.

SCR19: Utilizar um evento *onchange* num elemento *select* sem provocar uma alteração de contexto. **W3C Working Group Note.** Disponível em: <http://www.acessibilidade.gov.pt/w3/TR/WCAG20-TECHS/SCR19.html>. Acesso em: 05 dez.2013.

SYMANTEC. *Content*. ***Internet Security Threat Report 2013***. Volume 18. United States, 2013. Disponível em: <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf>. Acesso em: 16 set.2013.

SOUSA. R. H. de.; Gestão de Ativos – A Organização nas mãos da TI. **Infra Magazine**. n. 11. DevMedia. Disponível em: <http://www.devmedia.com.br/gestao-de-ativos-a-organizacao-nas-maos-da-ti-revista-infra-magazine-11/27895>. Acesso em: 22 out. 2013.

THE ISO 27000 DIRECTORY. ***History***. Reino Unido, 2013. Disponível em: <http://www.27000.org/thepast.htm >. Acesso em: 20 ago, 2013.

THIAGO BELEM. **O que é e como funciona o JQuery**. Disponível em: <http://blog.thiagobelem.net/o-que-e-e-como-funciona-o-jquery/ >. Acesso em: 20 dez.2013.

XAMPP. **ApacheFriends**. Disponível em: <http://www.apachefriends.org/pt_br/xampp.html>.Acesso em: 02 set.2013.

APÊNDICES

APÊNDICES

Apêndice A – Questionario completo, a abordando as seções trabalhadas no projeto.

5 Política de Segurança da Informação
5.1 Política de Segurança da Informação
5.1.1 Documento da política de segurança da informação
a)Na organização, existe um documento relacionado a política de segurança da informação?
b)Este documento tem apoio da direção?
c)Todos as pessoas envolvidas com a organização tem acesso a este documento?
d)O documento declara as metas da organização com a segurança da informação?
5.1.2 Analise crítica da política de segurança da informação
a) A política de segurança e reavaliada em intervalos planejados?
b) Esta avaliação provê oportunidades de melhoria na política de segurança?
c)A análise é feita com base em relatos sobre incidentes de segurança da informação?
d) A análise crítica inclui informações sobre mudanças que possam afetar o enfoque da organização?
e) E mantido um registro sobre a análise crítica?
f)O documento final da análise crítica é revisado, e a aprovação é realizada pela direção?

6 Organizando a segurança da informação
6.1 Organização interna
6.1.1 Comprometimento da direção com a segurança da informação
a) A direção apoia ativamente a segurança da informação?
b)A direção evidência um claro comprometimento, reconhecendo responsabilidades perante a segurança da informação?
c) A direção tem ciência das metas perante a segurança da informação?
d)Estas metas atendem os requisitos da organização?
e)A direção aprova sistemas que mantem a conscientização da segurança da informação?
6.1.2 Coordenação da segurança da informação
a) Existem atividades relacionadas à segurança da informação, como por exemplo, um sistema de troca de ideias e dúvidas?
b)Estas atividades são compostas por pessoas de diferentes setores da organização?
c)As atividades envolvem discussão de processos relativos a organização?
d)A atividade promove a educação, treinamento e conscientização perante a segurança da informação?
6.1.3 Atribuição de responsabilidades para a segurança da informação
a)Existe um inventário de atribuição de responsabilidades pela segurança da informação?
b) Existe um inventário, que atribua responsabilidades pela proteção dos ativos?
c) Existe uma inventário, que atribua responsabilidades pela proteção de processos de segurança da informação?
6.1.4 Processo de autorização para recursos de processamento de informações
a) Existe um processo para autorização de processamento de informações?
b)Esta autorização e obtida através da supervisão de um gestor de segurança da informação?
c) Existe um inventário relativo ao uso de equipamentos privados ou pessoais?
6.1.5 Acordos de confidencialidade
a) Existe um documento que declare políticas de acordo de privacidade?
b)Este documento explicita todos os termos do acordo, tanto na abertura, quanto no fechamento de contratos?
c)O documento especifica o tempo de duração do contrato de confidencialidade?
d)Os requisitos de confidencialidade estão de acordo com as leis vigentes?
6.1.6 Contato com autoridade
a) Existe procedimento para acionamento de autoridades(bombeiros, autoridades fiscalizadoras)?
b) Existe procedimento para acionamento e apoio do serviço de provedor de internet em caso de ataques?
6.1.7 Contato com grupos especiais
a)Existem contatos com grupos ou fóruns relacionados a área de segurança da informação?
b)Este contato proporciona o recebimento de alertas, aconselhamentos e correções relativas à segurança da informação?

c)Esta troca de informações está dentro dos requisitos de segurança da política de segurança da informação?

6.1.8 Análise crítica independente de segurança da informação

a)E feita uma análise, em intervalos planejados, quando ocorrem mudanças significativas relativas a implementação da segurança da informação?

b)Esta análise crítica, e executada por pessoas independentes da área avaliada?

c)A análise e comunicada a direção da organização?

d)São mantidos registros desta análise?

6.2 Partes Externas

6.2.1 Identificação dos riscos relacionados as partes externas

a)São implementados controles de risco antes do acesso de partes externas a informações da organização?

b)Na análise de riscos, foram identificados possíveis vulnerabilidades que partes externas possam explorar no momento ou após a concessão de acesso?

c)Esta análise de riscos, envolveu acesso físico a salas de equipamentos, acesso lógico ao banco de dados e sistemas de informação?

d)A análise de riscos envolveu diferentes controles quando a parte externa estiver armazenado, processando, comunicando ou compartilhando informações?

6.2.2 Identificando a segurança da informação, quando tratando com os clientes

a)Existem requisitos de segurança antes de permitir o acesso de clientes a informações da organização?

b)Existem procedimentos caso ocorrer perdas de dados ou comprometimento de equipamentos ao conceder acesso aos clientes?

c)Existem restrições em relação a cópia e divulgação de informações?

d)Há mecanismos de acesso com uso de identificadores únicos, para a concessão de acesso e privilégios?

e)Existem declarações de que acessos não autorizados, são proibidos?

f)Existe descrição de serviços prestados e serviços inaceitáveis por parte da organização?

6.2.3 Identificando a segurança da informação nos acordos com terceiros

a)Em acordos envolvendo terceiros, assegura-se que não existe mal-entendido entre a organização e o terceiro?

b)Existem procedimentos de treinamento de terceiros?

c)Existem acordos de revogação de acesso caso os sistemas sejam comprometidos?

7 Gestão de Ativos

7.1 Responsabilidades pelos ativos

7.1.1 Inventário dos ativos

a)Existe um inventário de todos os ativos?

b)Os ativos estão claramente identificados?

c)Este inventário e mantido atualizado?

7.1.2 Proprietário dos ativos

a) Todos os ativos identificados, tem uma pessoa ou entidade associada?

b)Ativos relacionados a recursos de processamento estão adequadamente identificados?

c)Os ativos são regularmente inspecionados pela sua autoridade responsável?

7.1.3 Uso aceitável dos ativos

a)No uso dos ativos, são implementadas e documentadas regras?

b)Existem regras para o uso dos ativos por parte e funcionários, fornecedores e terceiros?

7.2 Classificação da informação

7.2.1 Recomendações para classificação

a) A informação e classificada conforme criticidade e vulnerabilidade?

b)A classificação de informações e avaliada em intervalos regulares?

c) A classificação leva em consideração os objetivos do negócio?

7.2.2 Rótulos e tratamento de informações

a)O tratamento e rotulação de informações é feito conforme os requisitos de classificação adotados pela organização?

b)Existem procedimentos para tratar diferentes níveis de informação?

c)Acordos de compartilhamento de informações são tratados conforme sua classificação de criticidade?

8 Segurança em recursos humanos

8.1.1 Papeis e responsabilidade

a)Em contratos, estão definidos as responsabilidades pela segurança da informação conforme a política de segurança da informação?

b)Nestes papeis constam como implementar e agir com os recursos conforme a política de segurança?

c)Nestes papeis constam requisitos de controle de acesso não autorizado?

d)Estes papéis e responsabilidades são comunicados as partes interessadas?

8.1.2 Seleção

a)São efetuadas verificações dos históricos dos candidatos, fornecedores e terceiros?

b)Estas verificações estão de acordo com as legislações vigentes?

c)São efetuados testes no processo de seleção?

8.1.3 Termos e condições de contratação

a) Os termos e condições de trabalho estão declarados?

b)Estes termos estão em conformidade com a política de segurança?

c)Existem ações a serem tomadas caso funcionários, fornecedores ou terceiros violarem os requisitos de segurança da informação?

8.2 Durante a contratação

8.2.1 Responsabilidades da direção

a)A direção instrui funcionários, fornecedores e terceiros em relação a política de segurança da informação?

b)A direção assegura que funcionários, fornecedores e terceiros estão cientes de suas responsabilidades?

c)A direção garante que funcionários, fornecedores e terceiros tem a habilidade e qualificação apropriada?

8.2.2 Conscientização, educação e treinamento em segurança da informação

a)Existem procedimentos para treinamento de funcionários, fornecedores e terceiros?

b)Estes treinamentos tratam de questões de conscientização, atualização de informações relativas a política e procedimentos operacionais?

c)Este treinamento e realizado antes da concessão de acesso a informações da organização?

8.2.3 Processo disciplinar

a)Após o funcionário cometer algum delito, existem procedimentos formais disciplinares para ele?

b)O processo disciplinar foi formalmente especificado no contrato de admissão?

c)Caso o funcionário seja culpado de cometer violações, os direitos de acesso e privilégios, são removidos?

8.3 Encerramento e mudanças da contratação

8.3.1 Encerramento de atividades

a) Encerramento ou mudança de atividades estão formalmente dispostas em um contrato?

b)Este contrato revoga todos os direitos concedidos no momento da admissão?

c)As responsabilidades e obrigações de funcionários, fornecedores ou terceiros permanecem validas após o encerramento do contrato?

8.3.2 Devolução dos ativos

a)Existem um procedimento formal para a devolução dos ativos após encerramento das atividades?

b)Estes ativos que devem ser devolvidos, estão claramente identificados?

c)Caso o funcionário compre equipamentos com seus próprio recurso, e os utilize para o trabalho, são adotas procedimentos formais para esta ação?

8.3.3 Retirada dos direitos de acesso

a)Existe uma processo formal que revoga todos os direitos de acesso após o encerramento das atividades?

b)Na análise de riscos, foi observado se é necessária a retirada dos direitos de acesso antes do encerramento total das atividades?

c)Os funcionários, fornecedores e terceiros são informados para não efetuar compartilhamento de informações com a pessoa ou entidade que foi desvinculada da organização?

9 Segurança física e do ambiente

9.1 Áreas seguras

9.1.1 Perímetro e segurança física

a)Existem controles de acesso físico, como portões de entrada ou recepcionistas para proteger salas de processamento de informações?

b)A capacidade de resistência de cada perímetro está definido e conforme a os resultados obtidos na análise de riscos?

c)Informações sensíveis como sala de equipamentos estão bem protegidas por perímetros de proteção sólidos?

d)Locais de acesso restrito, são monitorados adequadamente?

e)Portas corta-fogo são monitoradas para que o nível de segurança seja aceitável e de acordo com as leis vigentes?

f)Todos os tipos de acesso a parte interna da organização, estão protegidos e de acordo com as leis vigentes?

g)As instalações de processamento de informação ficam separadas das que são utilizadas por terceiros?

9.1.2 Controle de entrada física

a)Existe um controle para que se tenha somente acesso autorizado a salas de processamento de informações?

b)São registrados data e hora de entrada e saída de visitantes?

c)As visitas são supervisionadas por pessoal autorizado?

d)Todo o tipo de pessoa, seja funcionário, fornecedor ou terceiro, e claramente identificado por um crachá ou documento?

e)Os direitos de acesso concedidos, são revisados e atualizados em intervalos regulares?

9.1.3 Segurança em escritórios, salas e instalações

a)Os perímetros de segurança, levam em consideração os regulamentos e norma de saúde?

b)A lista de funcionários e guia telefônico, e localização de instalações sensíveis são protegidas do acesso público?

9.1.4 Proteção contra ameaças externas e do meio ambiente

a)Existem procedimentos de proteção contra desastres naturais ou desastres humanos?

b)São levados em consideração, desastres que podem ocorrer nas proximidades da organização?

c)Matérias inflamáveis, são guardados em locais seguros e a uma distância aceitável conforme as leis vigentes?

d)Equipamentos de backup são armazenados em locais separados da organização?

e)Existem equipamentos para prevenção e combate a incêndios?

9.1.5 Trabalhado em áreas seguras

a)Somente as pessoas autorizadas, tem o conhecimento da existência da área segura?

b)O trabalho nestes locais e supervisionado?

c)Nestes locais, o uso de equipamentos como, maquinas fotográficas, gravadores de vídeo ou áudio entre outros, não são permitidos?

9.1.6 Acesso do público, áreas de entrega e de carregamento

a)Áreas de acesso de entrega e carregamento de informações, são devidamente supervisionadas e protegidas?

b)O acesso a área de entrega e carregamento e controlada somente para que pessoas autorizadas tenham acesso?

c)Os matérias que entram e saem são supervisionados para detectar possíveis ameaças ou perda de informações importantes?

9.2 Segurança de equipamentos

9.2.1 Instalação e proteção de equipamentos

a)Equipamentos sensíveis estão seguros e em local protegido?

b)O local que os equipamentos estão alocados, possuem um controle de acesso e segurança rígida?

c)No local em que dados sensíveis são processados, existem bloqueios visuais para pessoas não autorizadas?

d)Na análise de riscos, foram analisados todos os riscos potências que estes equipamentos podem sofrer?

e)Foram estabelecidas regras quanto a se alimentar próximo a equipamentos sensíveis?

9.2.2 Utilidades

a)Os equipamentos são protegidos caso falte energia elétrica?

b)Equipamentos que fazem uso da água para elaboração de atividades, são protegidos contra a falta dela?

c)Os sistemas de calefação e refrigeração estão de acordo com os requisitos do negócio?

d)Estes sistemas são analisados e testados em intervalos regulares?

e)A organização possui um sistema de geradores para suprir energia, caso os requisitos do negócio exijam?

f)As chaves de desligamento geral de energia ficam localizadas próximas as saídas de emergência?

g)Existe iluminação indicando as saídas de emergência?

h)Os equipamentos de telecomunicação são ligados a rede pública, por no mínimo duas linhas separadas?

i)Existe mais de uma linha de energia ligada a rede pública?

9.2.3 Segurança do cabeamento

a) Cabeamento de energia e dados estão protegidos contra interceptações?

b)Os cabos ligados a equipamentos, estão claramente identificados para que não ocorra erro no manuseio, e para que não sejam conectados no locais errados?

c)Cabos de dados e energia estão posicionados a certa distância, para que não ocorra interferência?

d)Todas as conexões são mantidas em um documento?

e)Em sistemas sensíveis, são utilizados conduítes blindados?

f)Em sistemas sensíveis, são utilizadas vias alternativas de comunicação?

g)Em sistemas sensíveis, existe acesso controlado aos painéis de conexões e a salas de cabos?

9.2.4 Manutenção de equipamentos

a)Os equipamentos possuem manutenção correta e apropriada?

b)A manutenção e efetuada em intervalos regulares recomendados pelo fornecedor?

c)A manutenção e realizada somente por pessoal autorizado?

d)São mantidos registros de falhas e operações realizadas?

9.2.5 Segurança de equipamentos fora das dependências da organização

a)A operação de equipamentos de processamento de informações fora das dependências da organização, são autorizados pela direção?

b)Equipamentos com informações sensíveis, são transportados de forma disfarçada?

c)Equipamentos utilizados fora das dependências da organização, são protegidos por algum tipo de seguro?

9.2.6 Reutilização e alienação segura de equipamentos

a)Os equipamentos que contem mídias de armazenamento, são analisados antes do descarte?

b)Os dados armazenados são removidos e sobregravados por qualquer outros dados?

c)Dispositivos com informações sensíveis são destruídos por meios técnicos que tornem essas informações irrecuperáveis?

9.2.7 Remoção de propriedade

a)Equipamentos e informações são supervisionados e retirados dos seus locais somente com autorização?

b)Funcionários, fornecedores e terceiros que possuem a permissão de remoção dos ativos dos seus locais, são claramente identificados e registrados?

10 Gerenciamento das operações e comunicação

10.1.1 Documentação dos procedimentos de operação

a)Os procedimentos de operações são documentados e mantidos em constante atualização?

b)Estes procedimentos são disponibilizado a todos as pessoas que necessitarem deles?

c)Os procedimentos de processamento e tratamento de informações possuem um informativo de como serão executados?

d) Os procedimentos de backup possuem um informativo de como serão executados?

e)Nestes procedimentos constam o horário de início e término?

f)Existem procedimentos caso ocorra um problema e o sistema necessite ser reiniciado e recuperado?

10.1.2 Gestão de mudanças

a)Existe um controle para execução de mudanças?

b)Ao ocorrerem mudanças nos recursos de processamento, essas mudanças são devidamente documentadas e registradas?

c)Nestas mudanças, todas as partes envolvidas são comunicadas?

10.1.3 Segregação de funções

a)Existe pessoal especializado para cada área?

b)Existe algum tipo de controle para impedir que pessoas não utilizem recursos sem autorização?

c)Caso não exista segregação de funções, a organização possui um procedimento para monitoração de atividades?

10.1.4 Separação dos recursos de desenvolvimento, teste e de produção

a)As fazes de desenvolvimento, testes e produção são processados de maneira separada?

b)Ao se efetuar a transferência de um processo, de uma faze para a outra, esta transferência e documentada?

c)Os ambientes de testes emulam de forma mais real possível o resultado do produto final?

d)Os testes são efetuados em ambientes estáveis e apropriados para o tipo de processo?

10.2 Gerenciamento de serviços terceirizados

10.2.1 Entrega de serviços

a)Nos acordos de serviço estão incluídos controles de segurança, definições de serviço e níveis de entrega?

b)A organização possui um planejamento adequado para este tipo de serviço, protegendo as informações sensíveis?

10.2.2 Monitoramento e análise crítica de serviços terceirizados

a)Em serviços terceirizados, os serviços prestados, relatórios e registros são analisados regularmente?

b)No monitoramento, é analisado o nível de desempenho do serviço?

c)Este nível de desempenho está de acordo com os contratos estabelecidos?

d)São efetuadas reuniões para a discussão sobre o nível de progresso do serviço?

e)Após a entrega do serviço, são efetuadas analises críticas para a busca de possíveis falhas?

f)A responsabilidade do relacionamento entre o terceiro e a organização e atribuída a um indivíduo designado ou a uma equipe de gerenciamento de serviço?

10.2.3 Gerenciamento de mudanças para serviços terceirizados

a)Existe um processo que gerencie a mudança de serviços terceirizados?

b) Na mudança da terceirização de serviços, são incluídos no processo, restrições criadas na análise de riscos?

c)Na mudança do serviço de terceiros estão incluídos o uso de novas tecnologias, adoção de novos produtos?

10.3 Planejamento e aceitação dos sistemas

10.3.1 Gestão de capacidade

a)Existem planos para a aceitação de novos recursos afim garantir o desempenho requerido?

b)Os requisitos de capacidade são claramente identificados para que o sistema não seja sobrecarregado?

c)Os requisitos de capacidade também estão identificados para atividades em andamento?

d)São implementados controles de detecção para se identificar e prevenir possíveis problemas?

e)No monitoramento dos sistemas, são aplicados ajustes de forma a melhorar a disponibilidade e eficiência dos sistemas?

10.3.2 Aceitação de sistemas

a)Existem critérios para a aceitação, atualização e uso de novas versões de sistemas?

b)São efetuados testes nos sistemas durante o desenvolvimento e após aprovação?

c)Os critérios de aceitação de novos sistemas estão devidamente definidos, acordados e documentados?

d)Para a aceitação formal, são verificados o desempenho e capacidade de processamento de informações neste novo sistema?

e)Os critérios estão em concordância com os controles de segurança?

f)Existem evidenciados que o uso do novo sistema não afetara os sistemas existentes?

g)Possíveis operadores destes sistemas estão devidamente treinados para exercer a função?

10.4 Proteção contra códigos maliciosos

10.4.1 Controle contra códigos maliciosos

a) E implementado algum tipo de controle e proteção contra códigos maliciosos?

b)Existem procedimentos de conscientização dos usuários sobre os perigos dos códigos maliciosos?

c)A proteção contra códigos maliciosos e efetuada por softwares de detecção e reparo?

d)São estabelecidas políticas sobre o uso de softwares não-licenciados?

e)Existem políticas para proteção contra riscos relativos ao download de arquivos e softwares de redes externas?

f)São feitas analises críticas dos softwares e dados dos sistemas, para a detecção não aprovada?

g)Os softwares de proteção contra códigos maliciosos efetuam a verificação de códigos maliciosos antes do uso, no caso de correios eletrônicos e em páginas web?

h)Existem planos de recuperação em caso de falhas ou roubo de informações?

10.4.2 Controles contra códigos maliciosos

a)Existem políticas para uso de códigos moveis?

b)Estas políticas estão de acordo com a política de segurança da informação?

c)Os códigos moveis são executados em ambientes isolados?

10.5 Copias de segurança

10.5.1 Cópias de segurança das informações

a)Existem políticas de cópias de segurança de informações e softwares?

b)Estas cópias são regularmente testas para a verificação de integridade?

c)Existe uma nível de prioridade para cada cópia de segurança das informações?

d)Existem procedimentos documentados sobre a realização destas cópias de segurança?

e)O local em que estas cópias estão mantidas, refletem os requisitos de segurança física avaliados na análise de riscos?

f)Copias de segurança com informações sensíveis, utilizam algum tipo de encriptação de dados?

10.6 Gerenciamento da segurança em redes

10.6.1 Controles de redes

a)As redes de comunicações são gerenciadas e controladas por pessoas qualificadas?

b)São implementados controles que garantam a segurança da informação e a proteção dos serviços utilizados pela rede?

c)Existem políticas de separação da responsabilidade da redes para com os recursos computacionais onde é necessária uma maior proteção?

d)Existe uma política sobre responsabilidades e procedimentos sobre o gerenciamento de equipamentos remotos?

e)Existem mecanismos que façam o registro e monitoração para aplicar a gravação de ações relevantes a segurança?

f)Existem processos para que o gerenciamento seja coordenado para otimizar o desempenho dos serviços?

10.6.2 Segurança dos serviços de rede

a)Em acordos de serviço de redes, são incluídos características de segurança, níveis de serviço e requisitos para o gerenciamento destes serviços?

b)Existem acordos para a monitoração dos serviços realizados por provedores de serviço?

c)E realizada uma checagem para assegurar que o provedor de serviço cumpra com seus deveres?

10.7 Manuseio de mídias

10.7.1 Gerenciamento de mídias removíveis

a)Existem políticas implementadas e documentados para o uso de mídias removíveis?

b)Quando uma mídia removível e retirada da organização, existem uma autorização documentada sobre esta ação?

c)As mídias removíveis são guardadas em local seguro conforme especificações do fabricante?

d)Informações que precisam ficar armazenadas por muito tempo na mesma mídia, possuem uma cópia autorizada para manutenção da integridade da informação?

e)Estas mídias são todas registradas para evitar a possível perda de dados?

10.7.2 Descarte de mídias

a)O descarte de mídias e executado por meio de procedimentos formais?

b)Estes procedimentos são regularmente revisados e atualizados?

c)O descarte de itens sensíveis e registrado para que se possa manter trilhas de auditoria?

d)Mídias com informações sensíveis são destruídas por incineração ou trituração, ou pela remoção das informações por outra aplicação segura?

10.7.3 Procedimentos para tratamento de informações

a)Existem procedimentos para tratamento e armazenamento de informações?

b)Estes procedimentos são regularmente revisados e atualizados?

c)A organização possui um registro formal de todas os destinatários que possam vir a receber dados?

d)Existe uma proteção para a expedição e impressão de forma consistente dos dados?

e)Existe uma identificação de todas as cópias das mídias para prevenir possíveis alterações dos destinatários autorizados?

f)E efetuada regulamente uma análise da lista de destinatários autorizados?

10.7.4 Segurança da documentação dos sistemas

a)Existe uma proteção adequada dos documentos dos sistemas contra acesso não autorizado?

b)O número de pessoas com acesso autorizado a estes documentos e controlado?

c)E efetuada uma proteção adequada da documentação do sistema que e fornecida através de uma rede pública?

10.8 Troca de informações

10.8.1 Políticas e procedimentos para a troca de informações

a)Existem politicas documentadas para a troca de informações por qualquer meio de comunicação?

b)Há procedimentos seguros de trocas em meio de recursos eletrônicos a fim de proteger os dados contra cópia, interceptação e modificação dos dados?

c)Existem procedimentos para proteção de informações sensíveis enviadas em forma de anexo?

d)Existem procedimentos para o uso de comunicação wireless, levando em conta os riscos deste tipo de comunicação?

e)A organização possui diretrizes para reter e descartar informações de negócios, incluindo mensagens com regulamentações e legislação local e nacional?

f)Existem políticas para não deixar informações sensíveis em equipamentos de impressão, copiadoras e aparelhos de fax?

g)Existe um controle para reter a transmissão automática de mensagens por correio eletrônico?

h)A organização orienta os funcionários para tomarem precauções ao falar de assuntos relacionados a organização em locais públicos ou em casa?

i)A organização orienta os funcionários a não deixarem mensagens com informações sensíveis em secretarias eletrônicas?

j)A organização orienta as pessoas, para que evitem deixar as informações pessoais gravadas em softwares ou em páginas web?

10.8.2 Acordos para a troca de informações

a)Existem acordos documentados para a troca de informações softwares dentro da organização e com terceiros?

b)Nos acordos, está estabelecido a responsabilidade do gestor pelo controle e notificação de transmissão, expedição e recepção?

c)Nos acordos existem procedimentos para rastrear eventos e o não-repudio?

d)Nos acordos de troca da informações estão definidos responsabilidades e obrigações pela perda de dados?

10.8.3 Mídias em transito

a)Existem políticas para a proteção de mídias em transito?

b)Existem termos de declaração de confiabilidade com o serviço de transporte?

c)Existem procedimentos para a identificação dos transportadores?

d)Os equipamentos são embalados de forma adequada para se proteger contra danos físicos?

e)Os equipamentos são embalados de forma que se perceba possíveis tentativas de rompimento do lacre?

10.8.4 Mensagens eletrônicas

a) Existem métodos para a proteção de mensagens que trafegam em meios eletrônicos?

b)O serviço de mensagens e confiável e está a maior parte do tempo disponível?

10.8.5 Sistemas de informações do negocio

a)Existem procedimentos desenvolvidos e implementados para proteger informações que são usadas em interconexão de sistemas?

b)Na interconexão de sistemas, são tratadas possíveis vulnerabilidades no compartilhamento de informações entre os diferentes setores?

c)A organização possui uma política de exclusão de categorias de informações sensíveis, caso o sistema não possua o nível adequado de proteção?

d)Existem mecanismos para procedimentos de recuperação e em casos de eventualidades?

10.9 Serviços de comercio eletrônico

10.9.1 Comercio eletrônico

a) Em comunicações que transitam na rede pública, existe algum tipo de proteção contra atividades fraudulentas, disputas contratuais e divulgação e modificação não autorizada?

b)Para a o estabelecimento de comunicações, existem mecanismos de autenticação que comprovem a identidade de ambas as partes?

c)Nos processos de autorização, existe uma entidade que determina preços, emite e assina documentos-chave na negociação?

d)Existem garantias que os parceiros comerciais estão cientes de suas autorizações?

e)Nos contratos de licitações e contratação, foram determinados e atendidos os requisitos de confidencialidade, integridade e evidenciados na emissão e recebimento os documentos-chave destes processos?

f)Existem procedimentos apropriados para a verificação de pagamento de um cliente?

g)Foram selecionadas as melhores maneiras de se efetuar pagamentos, para prevenir possíveis fraudes?

h)Foi selecionado o melhor nível de proteção para manter os requisitos de confidencialidade e integridade das informações dos pedidos?

i)Os termos comerciais são divulgados a seus clientes?

10.9.2 Transações online

a)Existem mecanismos de segurança para que se proteja transações online, prevenindo-se de transmissões incompletas, erros de roteamento, alterações não autorizadas, divulgação não autorizada, ou duplicação?

b)A organização faz uso de assinaturas eletrônicas para transações online?

c)Existem mecanismos seguros de autenticação?

d)São utilizados mecanismos de criptografia de dados para transmissões seguras?

10.9.3 Informações publicamente disponíveis

a)Existem mecanismos para se prevenir modificações não autorizadas dos dados que estão disponibilizados publicamente?

b)Os sistemas antes de serem acessíveis ao público, são testados para se prevenir possíveis falhas?

c)Existem processos formais para que as informações não sejam expostas antes de receberem a devida autorização?

d)Os sistemas que estão disponíveis para o acesso público, possuem um gerenciamento e proteção adequado?

10.10 Monitoramento

10.10.1 Registros de auditoria

a)São produzidos registros(logs) de auditoria contendo atividades dos usuários, e eventos de segurança da informação?

b)Os registros, incluem a identificação dos usuários, datas, horários e detalhes-chave do evento?

c)Os terminais de acesso são identificados e localizados corretamente?

d)Existem registros de tentativas de acesso aceitas e rejeitadas?

e)Existem registros de possíveis alterações do sistema?

f)Existem registros dos tipos de arquivos acessados?

g)Existem registros de tentativa de ativação ou desativação dos sistemas de antivírus ou sistemas de detecção de intrusão?

10.10.2 Monitoramento do uso de sistemas

a)Existem procedimentos de monitoramento do uso de recursos acessados relacionado a processamento de informações?

b)Estes acessos são analisados criticamente?

c)Existe supervisão para pessoas com acesso privilegiado(root) do sistema?

d)Os resultados do monitoramento envolvem criticidade dos processos, valor e sensibilidade das informações envolvidas?

10.10.3Proteção das informações dos registros

a)Os registros e informações dos registros são protegidos contra acesso não autorizado?

b)Os registros são protegidos contra alterações ou exclusão?

c)Os mecanismos de armazenamento possuem tamanho suficiente para o armazenamento dos registros?

10.10.4 Registros(log) de administrador e operador

a)Atividades desenvolvidas por administradores e operadores são registradas de forma segura?

b)São armazenados a hora, data e informações dos arquivos utilizados no evento?

c)E identificada a conta do administrador ou operador que estava envolvido?

d)As atividades desenvolvidas pelos operadores, são analisadas em intervalos regulares?

10.10.5 Registros(log) de falhas

a)Os registros são coletados por pessoas com competência e habilidade na área?

b)Todas as falhas ocorridas são registradas e analisadas?

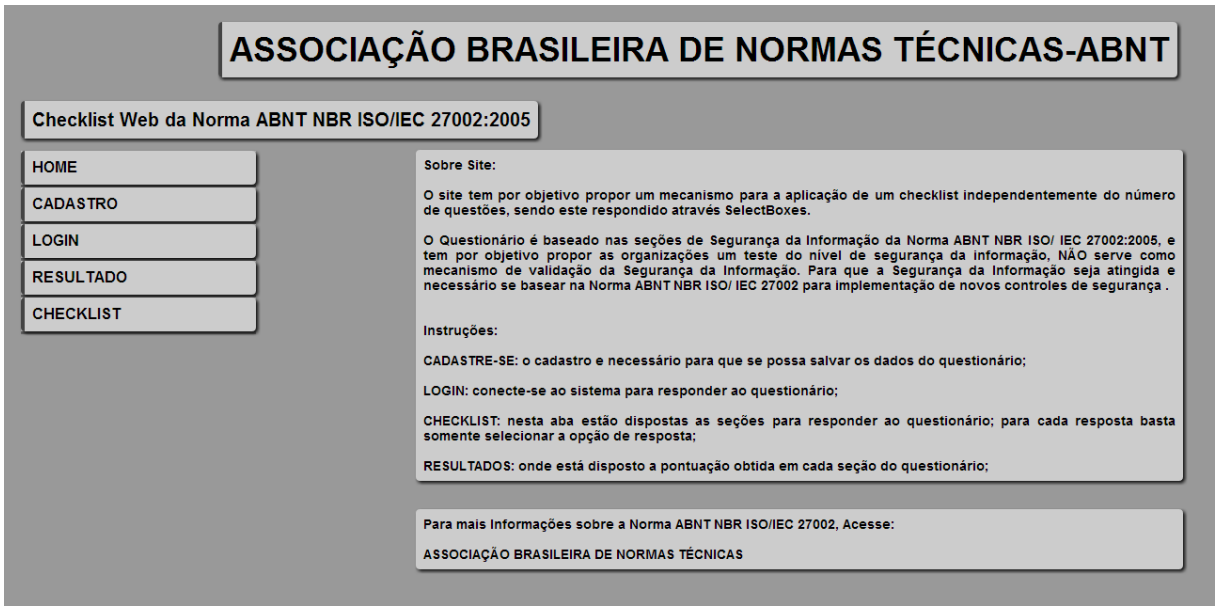
c)Existem registros das medidas corretivas adotadas para a resolução da falha?

10.10.6 Sincronização dos registros

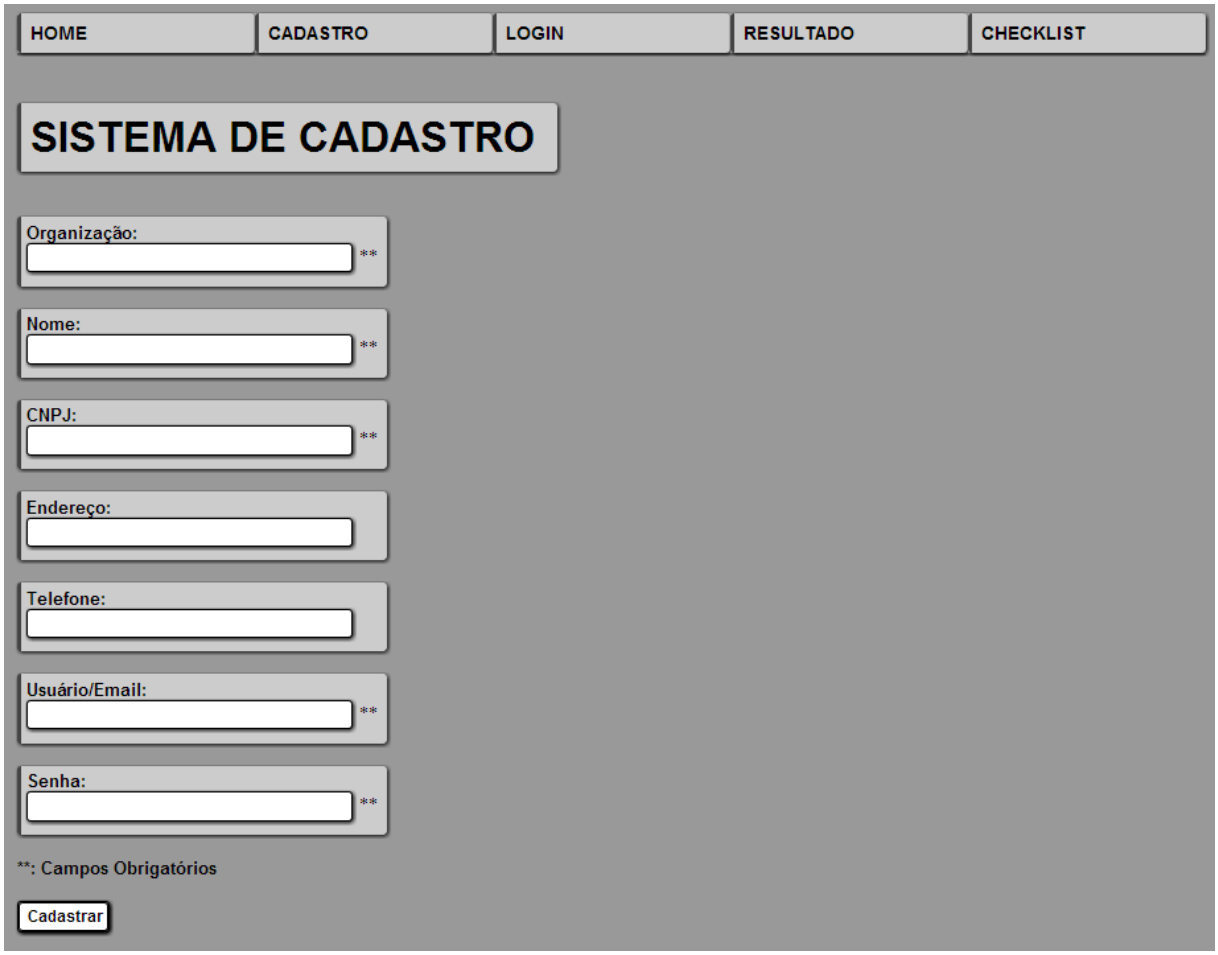
a)Os relógios dos sistemas da organização são sincronizados por uma fonte segura?

b)Existem métodos para a correção, caso o relógio não esteja de acordo com o sistema?

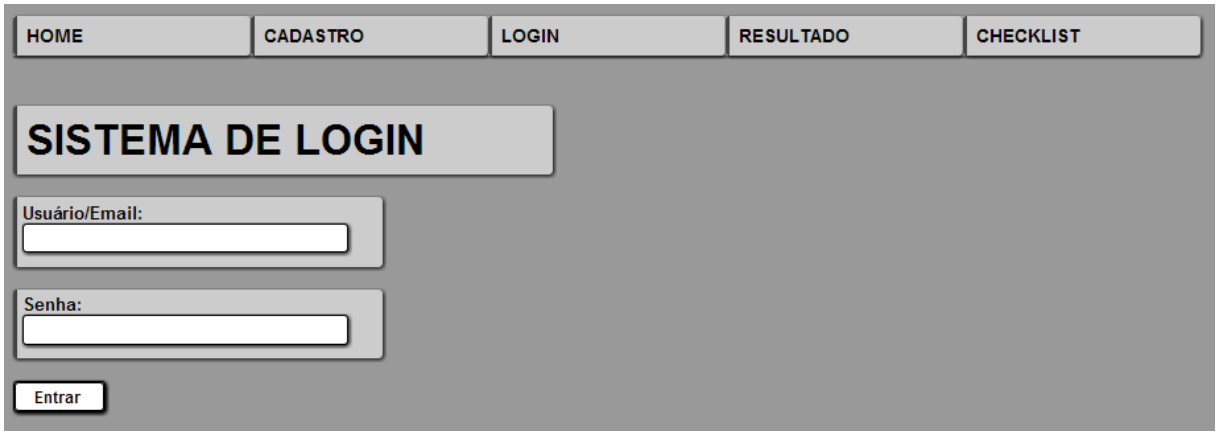
Apêndice B – Capturas de Tela da Página Web – Página Inicial



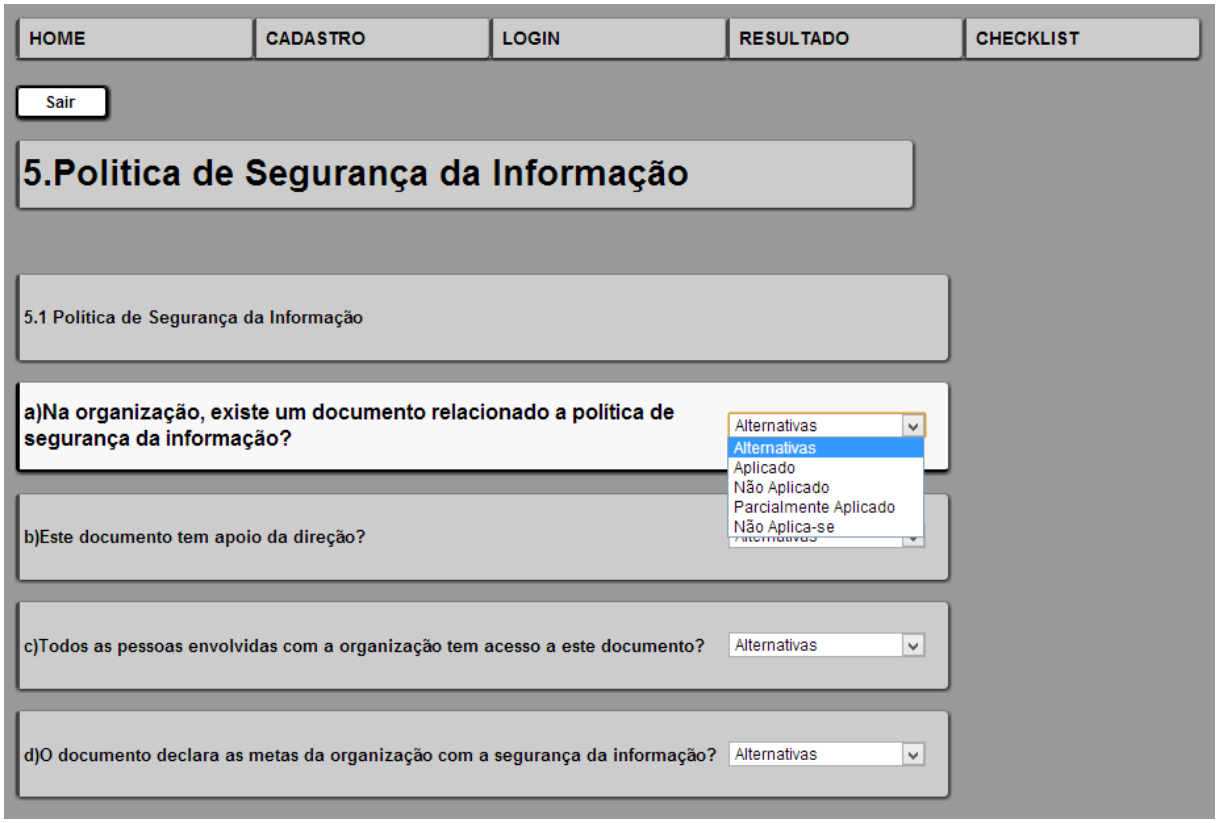
Apêndice C – Capturas de Tela da Página Web – Página de Cadastro



Apêndice D – Capturas de Tela da Página Web – Página de Login



Apêndice E – Capturas de Tela da Página Web – Página do Questionario/Checklist



Apêndice F– Capturas de Tela da Página Web – Página do Resultado