UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS ARARANGUÁ

CURSO DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

MICHEL BORTOLUZZI

ANÁLISE CRÍTICA DA APLICAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) EM EMPRESA DO SETOR FINANCEIRO: UM ESTUDO DE CASO

Araranguá, 08 de julho de 2016

MICHEL BORTOLUZZI

ANÁLISE CRÍTICA DA APLICAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) EM EMPRESA DO SETOR FINANCEIRO: UM ESTUDO DE CASO

Trabalho de Curso submetido à Universidade Federal de Santa Catarina como parte dos requisitos necessários para a obtenção do Grau de Bacharel em Tecnologias da Informação e Comunicação. Sob a orientação do Professor Dr. Paulo Cesar Leite Esteves.

Araranguá, 2016

Michel Bortoluzzi

ANÁLISA CRÍTICA DE POLÍTICA DE SEGURANÇA EM EMPRESA DO SETOR FINANCEIRO: UM ESTUDO DE CASO

ANÁLISA CRÍTICA DE POLÍTICA DE SEGURANÇA EM EMPRESA DO SETOR FINANCEIRO: Um Estudo de Caso Trabalho de Curso submetido à Universidade Federal de Santa Catarina como parte dos requisitos necessários para a obtenção do Grau de Bacharel em Tecnologias da Informação e Comunicação

Orientador
Prof. Dr. Paulo Leite Esteves/Universidade Federal de Santa Catarina

Examinador
Prof. Adriano de Oliveira/Universidade Federal de Santa Catarina

Solange Silva

Examinador
Prof .ª Dr.ª Solange Maria da Silva/Universidade Federal de Santa Catarina

Araranguá, 08 de julho de 2016

Este trabalho é dedicado a Deus, aos professores, minha família e minha esposa.

AGRADECIMENTOS

Agradeço em primeiro lugar ao meu professor orientador Paulo Cesar Leite Esteves e co-orientador Adriano de Oliveira pelo apoio na orientação desse trabalho, agradeço também a minha família, esposa e amigos pelo apoio e paciência nos momentos difíceis.

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Bortoluzzi, Michel
ANÁLISE CRÍTICA DA APLICAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) EM EMPRESA DO SETOR FINANCEIRO: UM ESTUDO DE CASO / Michel Bortoluzzi ; orientador, Paulo Cesar Leite Esteves ; coorientador, Adriano de Oliveira. - Araranguá, SC, 2016.
112 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Araranguá. Graduação em Tecnologias da Informação e Comunicação.

Inclui referências

1. Tecnologias da Informação e Comunicação. I. Cesar Leite Esteves, Paulo. II. de Oliveira, Adriano. III. Universidade Federal de Santa Catarina. Graduação em Tecnologias da Informação e Comunicação. IV. Título.

A verdadeira motivação vem da realização, desenvolvimento pessoal, satisfação no trabalho e reconhecimento.

(Frederick Herzberg)

RESUMO

O crescimento organizacional aliado ao desenvolvimento das TICs – Tecnologias da Informação e Comunicação vem criando um cenário propício ao aumento no número de ativos de informação. Esses ativos, por sua vez, estão cada vez mais vulneráveis às ameaças oriundas, tanto do ambiente lógico, quanto do ambiente físico. As organizações estão buscando, cada vez mais, uma autodefesa contra essas ameaças. Essa proteção vem sendo desenvolvida sob a forma de uma Política de Segurança da Informação – PSI, que tem por objetivo criar métodos eficazes de defesa, aplicando regras e diretrizes com o intuído de mitigar ou diminuir os efeitos de ataques contra a informação. Diante desse cenário, o presente trabalho desenvolve uma análise do alinhamento e conformidade entre os modelos teóricos e a implantação de uma Política de Segurança da Informação em uma empresa do setor financeiro, para obter subsídios necessários a uma análise crítica referente ao tema. Surge então, a necessidade de desenvolver um estudo de caso, objetivando identificar os principais conceitos e modelos, efetuando assim uma análise comparativa entre a política aplicada na organização em contrapartida aos modelos teóricos pesquisados.

Palavras-chaves: Segurança, informação, organizações, normas.

ABSTRACT

The organizational growth together with the development of ICTs - Information and Comunication Tecnologies - is creating a setting leading to an increase in the number of information assets. These assets in turn, are increasingly vulnerable to threats arising from both the logical environment as the physical environment. In turn, organizations are seeking, increasingly self-defense against these threats. This protection has been developed in the form of a Security Policy information - PSI which aims to create effective methods of defense applying rules and guidelines with the intuited to mitigate or reduce the effects of attacks against information. In this scenario, this paper develops an analysis of alignment and conformity between the theoretical models and the implementation of a Security Policy Information in a financial company, to get the subsidies needed for a critical analysis about the issue. Then comes the need to develop a case study in order to identify the main concepts and models, making this way a comparative analysis of the policy applied in the organization in contrast to theoretical models researched.

Key-words: security, information, organizations, standards

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

TIC – Tecnologias da Informação e Comunicação

TI – Tecnologias da Informação

SI – Segurança da Informação

PSI – Política de Segurança da Informação

ISO – International Organization for Standardization

CVE – Common Vulnerabilities and Exposures

PDCA – Plan – Do – Check – ACT

RH – Recursos Humanos

PCN – Política de Continuidade do Negócio

SUMÁRIO

1. INTRODUÇÃO

Essa pesquisa é direcionada à conclusão do Curso de bacharelado em Tecnologias da Informação e Comunicação pela Universidade Federal de Santa Catarina, Campus Araranguá. O currículo do curso é estruturado para atender as Diretrizes Curriculares Nacionais para o ensino de graduação brasileiro, definidos pelo Conselho Nacional de Educação (CNE) (Resolução n° 2 de 18 de junho de 2007) e nos Referenciais Orientados para os Bacharelados Interdisciplinares e Similares de Novembro de 2010. Tem por objetivo, a reorganização do processo de formação em torno de novos valores como competência, aprendizagem, participação e envolvimento de todos os agentes implicados, propondo uma educação integrada e flexível para atender diferentes perfis e orientações. (Universidade Federal de Santa Catarina - UFSC, 2013).

No decorrer dos anos tem sido percebido um expressivo crescimento tecnológico. Evolução que vem ocorrendo nas organizações no que diz respeito às tecnologias da informação e Comunicação. Segundo a consultoria IDC (SISMEMA, 2016), o setor de TICs deverá manter, em 2016, um faturamento superior a US$ 60 bilhões, tendo um crescimento na base de 2,6% em relação a 2015.

Uma nova tendência em tecnologia vem surgindo para mudar a maneira como as organizações executam suas atividades, impressora 3D, por exemplo, já pode ser considerada um avanço em processos de produção, contribuindo para a confecção de produtos numerosos e com menor custo. As melhorias nos sistemas de comunicação também contribuem para esse crescimento tecnológico, assim como as melhorias nos sistemas de redes que auxiliam na mobilidade e troca de informações e dados. Todos esses avanços trazem novos produtos e novas

formas de se gerar ativos de informação contribuindo para a necessidade de sistemas cada vez mais eficazes no que diz respeito à segurança dessas informações.

O crescimento no número de empresas também é um fator importante no que diz respeito às Políticas de Segurança da Informação. As pequenas e médias empresas tiveram um aumento de faturamento de R$ 144 bilhões para R$ 599 bilhões nos últimos 10 anos, respondendo, assim, por mais de um quarto do produto interno bruto brasileiro (PIB) segundo dados do Serviço Brasileiro de Apoio ás Micros e Pequenas Empresas (SEBRAE, 2014). Ainda segundo SEBRAE, as micro e pequenas empresas são responsáveis por 53,4% do PIB do setor.

O crescimento tecnológico, juntamente com crescimento das organizações, acrescido do aumento no número de colaboradores, cada vez mais informatizados, são fatores que fazem com que o número de ativos de informação cresça, proporcionalmente, deixando as organizações mais vulneráveis aos riscos inerentes às falhas de segurança da informação.

Segundo COELHO et al. (2014, p. 2):

> A informação pode existir em diversos formatos: impressa, armazenada eletronicamente, falada, transmitida pelo correio convencional de voz ou eletrônico etc. Seja qual for o formato ou meio de armazenamento ou transmissão, recomenda-se que ela seja protegida adequadamente. Sendo assim, é de responsabilidade da segurança da informação protegê-la de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar riscos e maximizar o retorno dos investimentos.

No decorrer dos anos, já é possível notar uma maior conscientização por parte das organizações, que já conseguem enxergar os ativos de informações como valores e entendem os problemas gerados pela sua vulnerabilidade. A segurança da informação é garantia de competitividade dos negócios, lucratividade e compreensão dos aspectos legais, juntamente com uma garantia de imagem para a organização, tanto no setor público quanto para o setor privado.

A segurança da informação é a proteção dos ativos de informação de todo tipo de ameaças com o objetivo de garantir a integridade e a continuidade do negócio. Diminuir riscos e garantir a prosperidade do negócio também deve ser considerado quando se trata de segurança da informação. Para garantir que isso aconteça faz-se necessário criar um ou vários conjuntos de controle, unindo políticas, criando processos e procedimentos a serem implementados e tratados na organização em questão.

Conforme cita COELHO et al. (2014, p. 2)

> Em particular, os controles necessitam ser estabelecidos, implementados, monitorados, analisados e continuamente melhorados, com o intuito de atender aos objetivos do negócio e de segurança da organização. A identificação de controles adequados requer um planejamento detalhado.

Diante do exposto, esse trabalho visa mostrar, de forma comparativa e crítica, a aplicação de uma Política de Segurança da Informação (PSI) em uma organização, citando os pontos positivos e negativos, falhas e acertos quando comparados às bibliografias específicas.

A ideia principal é analisar, pesquisar e expor as diferentes aplicações de políticas presentes em pesquisas e normas utilizadas atualmente e, com isso, buscar informação necessária para comparar de forma positiva e negativa a aplicação da Política de Segurança da Informação em uma organização específica, por meio de um estudo de caso.

O propósito dessa pesquisa surgiu a partir da necessidade de implementação de uma PSI – Política de Segurança da Informação - que atenda aos requisitos necessários para funcionamento em uma organização, agindo de forma organizada, que engaje os membros e que não seja uma forma de bloquear as funções, mas sim, de unir a organização como um todo diante da política.

O objetivo geral é analisar o alinhamento e conformidade entre os Modelos teóricos de implantação de uma Política de Segurança da Informação (PSI) e o Modelo implantado em uma empresa do setor financeiro.

Para que isso seja alcançado, será necessário o cumprimento dos seguintes objetivos específicos:

1. Identificar os principais conceitos e modelos presentes na literatura ao estabelecimento de uma política de segurança da informação (PSI) eficaz

2. Compreender a implantação de PSI na empresa selecionada para o estudo de caso.

3. Efetuar uma análise comparativa com a PSI aplicada na empresa selecionada frente aos modelos.

4. Indicar as características presentes nos Modelos de PSI, que foram consideradas na empresa.

Os resultados podem servir para medir o quanto uma Política de Segurança da Informação pode afetar a rotina de uma organização? Qual o verdadeiro impacto provocado na implantação e no decorrer dos trabalhos após a implantação da mesma? A pesquisa pode contribuir de forma positiva para as organizações que desejam implantar uma PSI, para que saibam quais os impactos e o que realmente deve ser feito para obter um melhor resultado na sua implantação.

Para a organização selecionada para o estudo de caso, pode ser uma forma de ratificar o que está em acordo com as proposições dos modelos teóricos e, caso necessário, promover a correção de gaps, de forma a contribuir para a efetividade da PSI na empresa. Também será possível gerar uma fonte de pesquisa e consulta para quem tiver interesse no tema, graduandos, profissionais da área e outros interessados poderão buscar referências para novas pesquisas e artigos relacionados ao assunto.

Para o desenvolvimento desse trabalho faz-se necessário, primeiramente, criar uma fundamentação teórica baseada em uma pesquisa exploratória relacionada ao tema. Também é necessário desenvolver um procedimento metodológico, incluindo pesquisa em geral e comparações entre os dados levantados durante a pesquisa. Sendo assim, para contextualização do trabalho, a pesquisa está voltada a estudos bibliográficos e documentais das normas aplicadas para desenvolvimento de Políticas de Segurança da Informação.

A pesquisa bibliográfica é efetuada por meio artigos científicos relacionados ao tema. Também são utilizadas as normas ISO relacionadas à Segurança da Informação (ISO/IEC 27001 e ISO/IEC 27002).

ISO/IEC 27001: Norma de certificação para formalidade documental e organizacional.

ISO/IEC 27002: Norma de certificação para controle de segurança da informação.

Por meio desses instrumentos de pesquisa visa-se coletar dados suficientes para o desenvolvimento, interpretação e conclusão do presente trabalho, mostrando qual o comportamento de uma empresa durante o processo de implantação, treinamento e continuidade do negócio, criando críticas positivas e negativas sobre todo o processo de implantação de uma PSI na organização.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 O que é informação

A informação está presente no dia a dia de qualquer ambiente, seja público ou privado, seja em casa ou em uma organização, os ativos de informação circundam o ambiente, tanto de forma lógica quanto de forma física. “Pode estar disponível de forma impressa, armazenada eletronicamente, falada, transmitida pelo correio convencional ou eletrônica [..]” (COELHO et al, 2014, p.2).

A informação é um ativo de essencial importância, por esse motivo deve ser devidamente protegida, principalmente, nos ambientes de maior relevância como as áreas de negócio por exemplo. O aumento da conectividade trouxe grandes riscos para as organizações trazendo consigo uma diversidade de ameaças e vulnerabilidades.

Dentro do contexto da produção da informação, a operacionalização pode ser feita por meio de práticas devidamente especificadas, representando seguintes atividades: reunir, selecionar, codificar, reduzir, classificar e armazenar a informação. Essa organização visa criar um controle de estocagem da informação para uso no presente ou no futuro.

Desde os primórdios, a informação move o mundo de diversas maneiras, é ela que dá a dimensão da evolução que se vive no universo. O conjunto imenso de informação é transformado em conhecimento e utilizado pelo ser humano em sua sobrevivência. “A informação é muito mais que um conjunto de dados. Transformar esses dados em informação é transformar algo com pouco significado em um recurso de valor para a nossa vida pessoal e profissional” (FONTES, 2006, p. 2).

2.1.1. A importância da informação

A informação tem muita importância na vida e na sociedade, conforme Barreto (1994, p. 1):

> A informação sintoniza o mundo. Como onda ou partícula, participa na evolução da revolução do homem em direção a sua história. Como elemento organizador, a informação referência o homem ao seu destino; mesmo antes de seu nascimento, através de sua identidade genética, e durante a sua existência pela sua competência em elaborar a informação para estabelecer a sua odisseia individual no espaço e no tempo. A importância que a informação assumiu na atualidade pós-industrial recoloca para o pensamento questões sobre a sua natureza, seu conceito e os benefícios que pode trazer ao indivíduo e no seu relacionamento com o mundo em que vive.

De forma geral, a informação na sua forma correta e segura pode aumentar o conhecimento intelectual permitindo desempenhar atividades com maior segurança, seja essa atividade operacional, utilizada taticamente ou, estrategicamente.

Conforme nos fala Messias (2005, p.9):

> A informação é o recurso que movimenta a economia global, sendo o principal elemento de produção das sociedades desenvolvidas. A fonte de renda e poder não é mais representada pela moeda, mas pela quantidade de informação acumulada, organizada e transformada em valor monetário.

Pode servir como uma ferramenta estratégica para os negócios, é necessário saber coletar as informações, saber onde encontrar, como mostrar e, principalmente, como usá-la a favor dos negócios. Analisando por esse lado, a informação pode ser um instrumento útil para solucionar problemas na administração das organizações e, sendo bem utilizada por seus gestores, pode auxiliar e destacar o negócio frente à concorrência.

2.2. As TICs

No contexto da informação as TICs (Tecnologias da Informação e Comunicação), tem uma abordagem referente as políticas de segurança da informação, sob o ponto de vista da gestão. Não se pode pensar nas TICs apenas como uma unidade tecnológica responsável pelas aplicações de informática dentro da organização, o objetivo principal desse setor é desenvolver conhecimentos, gerando melhorias nos sistemas de informação, melhorando processos, auxiliando nas atividades e consequentemente otimizando os negócios.

"Tecnologia da Informação pode ser conceituada como recursos tecnológicos e computacionais para geração e uso da informação [..]" (REZENDE; 2005 p.32).

Fazem parte das TICs alguns componentes importantes, que que aliados ao recurso principal, que é o humano, fazem com que a tecnologia ganhe funcionalidade. Segundo Rezende (2005, p.33) esses componentes são:

- Hardware e seus dispositivos e periféricos;
- Softwares e seus recursos;
- Sistemas de telecomunicações;
- Gestão de dados e informação;

2.3. Conceituando Segurança da Informação

A segurança da informação tem por objetivo proteger ativos de informação garantindo a sua integridade, disponibilidade e confidencialidade.

Coelho et.al (2014, p.6) conceitua as três propriedades acima como:

> 1. **Integridade:** trata da garantia contra os ataques ativos por meio de alterações ou remoções não autorizadas. É relevante o uso de um esquema que permita a verificação da integridade dos dados armazenados e em transmissão. A integridade pode ser considerada sob dois aspectos: serviço sem recuperação ou em recuperação. Uma vez que os ataques ativos são considerados no contexto, a detecção, em vez de prevenção, é o que importa; então, se o comprometimento da integridade é detectado, pode-se reportá-lo e o mecanismo de recuperação é imediatamente acionado. A integridade também é um pré-requisito para outros serviços de segurança. Por exemplo, se a integridade de um sistema de controle de acesso e um Sistema operacional for violado, também será violada a confidencialidade de seus arquivos, a perda de integridade surge no momento em que uma determinada informação fica exporta ao manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário da informação.
> 2. **Disponibilidade:** determina que recursos estejam disponíveis par aceso por entidades autorizadas, sempre que solicitadas, representando a proteção contra perdas ou degradações. A perda de disponibilidade acontece quando a informação devia estar acessível para quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ou, equipamento ou por ação não autorizada de pessoas ou sem má intenção.
> 3. **Confidencialidade:** compreende a proteção de dados transmitidos contra os ataques passivos, isto é, conta acesos não autorizados, envolvendo medidas como controle de aceso e criptografia. A perda da confidencialidade ocorre quando há uma quebra de sigilo de uma determinada informação, por exemplo, a senha de um usuário ou

> administrador de sistema permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.

Conforme a norma ABNT ISSO/IEC 17799 (2005), outras propriedades também podem ser incluídas no processo de segurança da informação, tais como: a autenticidade, responsabilidade, não repúdio e confiabilidade.

Um princípio importante, além de todos os citados até então, refere-se à comunicação. Segundo BEAL (2005), a comunicação é o processo de transmissão da informação concluída quando um emissor envia uma mensagem a um receptor, utilizando algum tipo de canal comum entre os dois.

Quando se fala em segurança da informação também pode-se falar sobre segurança da comunicação, considerada proteção ponto a ponto, do ponto de vista do envio da informação do emissor para o receptor. Essa proteção tem por objetivo preservar:

- **Integridade do conteúdo:** A mensagem deve chegar de forma exata e completa até o receptor.

- **Irretratabilidade da comunicação**: visa garantir que tanto o emissor quanto o receptor não possam negar que a informação não chegou até o destino como deveria ocorrer.

- **Autenticidade do emissor e receptor:** visa garantir que tanto emissor quanto receptor sejam quem realmente devem ser.

- **Confidencialidade do conteúdo:** garante que o conteúdo seja utilizado somente a quem foi endereçado.

- **Capacidade de recuperação do conteúdo pelo receptor:** o conteúdo deve ter garantias de recuperação original. É necessário expor essa questão quando, por exemplo, uma mensagem é enviada criptografada, nesse caso o receptor deve ter garantias de que conseguirá visualizar a mensagem. Esse princípio está diretamente ligado aos protocolos de comunicação utilizados.

A segurança da informação visa proteger os ativos de informação de diversos tipos de ameaças, garantindo, assim, a continuidade do negócio, diminuindo riscos, aumentando os retornos de investimento e criando oportunidades. Para isso, é necessário criar diversos controles que incluem políticas, procedimentos, processos estruturas de organização e funções computacionais logica e fisicamente. Conforme a norma ABNT ISO/IEC 17799 (2005) menciona, os controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados [...], com o objetivo de garantir que os objetivos de negócio e segurança sejam atendidos [...].

"Os regulamentos (políticas, normas e regras) de segurança da informação tem como objetivo fazer com que o uso da informação na organização aconteça de uma forma estruturada, possibilitando que o negócio não seja prejudicado por um mau uso da informação: seja por erro ou por acidente. " (FONTES, 2006, p.2):

Assim, entende-se que a segurança da informação engloba um conjunto regras com o objetivo de preservar a informação de diversos riscos nocivos ao negócio, regras essas que vão além das TICs, pois envolvem diversas outras áreas da organização.

Conforme Brasil (2008, p. 2):

> A gestão da informação é entendida como: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento de informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, a tecnologia da informação e comunicações.

2.4. Proteção dos ativos de informação

Não existe uma forma extremamente padronizada para classificação dos ativos de informação, porém, Beal (2005 apud Kovacich, 1998, p.59) propõe três categorias: informação pessoal, informação de segurança nacional e informação de negócio.

1. **Informações pessoais:** trata-se da preservação de informações pessoais, do cuidado que se deve ter com informações de funcionários, clientes e demais indivíduos. Algumas das preocupações, nesses casos são as de respeitar a privacidade das pessoas e manter o sigilo das informações de cada um.

2. **Informação de segurança nacional:** O objetivo dessa categoria é garantir a segurança dos ativos do Estado e da sociedade e possuem legislações especiais para classificar os ativos de acordo com risco para a segurança nacional.

3. **Informações de negócio:** Essa categoria trata das informações importantes para as organizações, tais como informações, financeiras, planos técnicos, marketing, planos estratégicos. Esses exemplos de ativos podem exigir maior segurança quando falamos em integridade, confidencialidade e disponibilidade.

Para a que seja possível alcançar uma proteção adequada para os ativos de informação é necessário fazer o inventário dos mesmos e também identificar os seus devidos proprietários e consequentemente responsáveis. O proprietário, por sua vez, é o responsável pelo ativo, ele pode efetuar implementações ou delegar essa função de implementação, porém a responsabilidade será sempre sua.

Conforme descreve a norma ABNT 17799 (2005, p. 21):

> Convém que a organização identifique todos os ativos e documente a importância desses ativos. Convém que o inventário do ativo inclua todas as informações necessárias que permitam recuperar de um desastre, incluindo o tipo do ativo, formato, localização, informações sobre copias de segurança, informações sobre licenças e a importância do ativo para o negócio. Convém que o inventário não duplique outros inventários desnecessariamente, porém ele deve assegurar que o seu conteúdo está coerente.

É importante para a classificação do ativo, que este esteja identificando o seu proprietário e o tipo de informação, tudo isso documentado para cada tipo de ativo. É necessário, então, criar classificações e impor os níveis de segurança proporcionais ao ativo, de acordo com a sua importância, seu real valor para organização e o seu grau de segurança. A norma ABNT 17799 (2005, p.21) aponta alguns tipos de ativos (Quadro 1) cuja classificação se faz necessária:

Ativos de Informação	**Ativos de software**	**Ativos físicos**	**Serviços**	**Pessoas**	**Intangíveis**
Base de dados de arquivos	Aplicativos	Equipamentos computacionais	Computação	Qualificações	Reputação da organização
Contratos e acordos	Sistemas	Equipamentos e comunicação	Comunicações	Habilidades	Imagem da organização

Documentação de sistema	Ferramentas de desenvolvimento	Mídias removíveis	Aquecimento	Experiências	
Pesquisas	Utilitários	Equipamentos em geral	Iluminação		
Manuais de usuários			Eletricidade		
Material de treinamento			refrigeração		
Procedimentos de suporte ou operação					
Planos de continuidade do negocio					
Procedimentos de recuperação					
Trilhas de auditorias					
Informações armazenadas					

Quadro 1 **- Ativos e suas classificações Fonte: ABNT NBR 17799 (2005)**

Para facilitar a classificação dos ativos de informação, é interessante criar modelos relacionados a essa classificação assim com para outros pontos do processo de implementação de uma política de segurança da informação. Santos (2012, p.36) cita em seu modelo de gestão dos Ativos algumas atividades necessárias segundo seu ponto de vista:

- Identificar os ativos.
- Estruturar e manter o inventário de todos os ativos importantes.
- Documentar a importância de cada ativo.
- Realizar a valoração dos ativos.
- Avaliar o impacto causado pelo incidente de segurança ocorrido em cada ativo.

- Assegurar a existência de um proprietário, responsável por cada ativo identificado.

- Identificar, documentar e implementar regras quanto ao uso das informações e de seus ativos associados.

- Classificar a informação de acordo com o seu valor, requisitos legais, sensibilidade e criticidade.

- Definir e implementar procedimentos para rotulação e tratamento da informação de acordo com a sua classificação.

2.5. Definição de controles

A definição de controles é efetuada após terem sido identificados os riscos e os requisitos de segurança da informação. O objetivo da definição de controles é justamente criar ações que diminuam o risco a níveis favoráveis para a organização. A norma ABNT 17799 (2005, p. 10) pondera que:

> [...] a seleção de controles de segurança da informação depende das decisões da organização baseados nos critérios para aceitação do risco, na opção do tratamento do risco e no enfoque geral à gestão do risco aplicado à organização e, convém que também esteja sujeito a todas as legislações e regulamentações nacionais e internacionais relevantes.

A própria norma ABNT 17799 (2005, p.11) aponta alguns controles considerados essenciais do ponto de vista legal:

- Proteção de dados e privacidade de informações pessoais;
- Proteção de registros organizacionais;
- Direitos de propriedade intelectuais.

A norma ABNT 17799 (2005, p. 11) também aponta os controles considerados como práticas da segurança da informação.

- Documento da política de segurança da informação;
- Atribuição de responsabilidade para a segurança da informação;

- Conscientização, educação e treinamento em segurança da informação;
- Processamento correto das aplicações;
- Gestão de vulnerabilidades técnicas;
- Gestão da continuidade do negócio
- Gestão de segurança da informação e melhorias;

2.6. Tratamento de incidentes

O tratamento de incidentes em segurança da informação diz respeito às atitudes e medidas para a proteção contra os incidentes na organização. Beal (2005) cita como exemplo a inclusão de firewalls de rede e internet, scanners para varredura da rede e de sistemas, detectores de abusos e anomalias, software para filtragem de conteúdo, antivírus e programas de auditoria como algumas das formas para se prevenir e detectar os problemas de segurança em uma organização.

Brasil (2009) define tratamento de incidentes de segurança em redes computacionais como sendo "Serviço que consiste em receber, filtrar, classificar e responder solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências".

Os tratamentos de incidentes em segurança consistem na tarefa de produzir suporte necessário para processos de análise e recuperação e também para análise de ataques. Além disso, é possível formar análises quantitativas e qualificativas referente aos ataques. Miani (2013, p.52) afirma que, "[...]. Os dados podem ser usados para correlação de eventos e determinação de tendências, melhorando a percepção acerca de problemas de segurança da organização [...]. ".

Conforme a norma ABNT 17799 (2005) informa, é conveniente que seja estabelecido um procedimento de notificação formal para incidentes de segurança, estabelecendo assim, as ações necessárias ao receber qualquer evento. Para isso pode ser necessário e conveniente a criação de um ponto de contato para as devidas notificações, que esse ponto seja divulgado para toda a organização e que esteja sempre disponível quando necessário gerar uma resposta

adequada. A norma acrescenta também que todos os funcionários, fornecedores e terceiros estejam alertados sua responsabilidade de notificar qualquer evento de segurança da informação o mais rápido possível.

É desejável que as notificações de incidentes sigam alguns critérios. A norma ABNT 17799 (2005, p. 98) afirma que é importante que os procedimentos incluam:

- Processos adequados para realimentação para assegurar que os eventos de segurança da informação relatados sejam notificados referente aos resultados após a questão ter sido conduzida e concluída.
- Formulário para apoiar a ação de notificar um evento de segurança da informação e a ajudar as pessoas a lembrar das ações necessárias para a notificação do evento.
- O comportamento correto no caso de um evento de segurança da informação, como por exemplo:
    - Anotar todos os detalhes importantes imediatamente (por exemplo, tipo de não-conformidade ou violação, mau funcionamento, mensagens na tela, comportamento estranho);
    - Não tomar nenhuma ação própria, mas informar imediatamente o evento ao ponto de contato.
    - Referência para um processo disciplinar estabelecido para lidar com funcionários, fornecedores ou terceiros que cometam violação da segurança da informação.

São alguns exemplos de eventos e incidentes de segurança da informação, segundo ABNT NBR ISO IEC 17799 (2005):

- Perda de serviço, equipamentos ou recursos;
- Mau funcionamento ou sobrecarga do sistema;
- Erros humanos;
- Não-conformidade com políticas e diretrizes;
- Violação de procedimentos de segurança física;
- Mudanças descontroladas de sistema;
- Mau funcionamento de software e hardware;

- Violação de acesso.

Os incidentes, dependendo do seu aspecto em relação aos riscos de segurança da informação podem servir como aprendizado por meio de treinamentos ou outras formas de estudo, além disso, os ataques podem servir de apoio a novas correções, porém devem ser detectados e catalogados o mais rápido possível.

2.7. Gestão de risco em segurança da informação

> "[...]. Gestão do risco é o conjunto de processos que permite às organizações identificar e implementar as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação, e equilibra-los com os custos operacionais e financeiros envolvidos. " (BEAL, 2005, p.11).

O processo de gestão de risco pode ser iterativo para o processo de avaliação de riscos ou para o seu tratamento. Um enfoque iterativo na execução do processo de avaliação de risco torna possível aprofundar e detalhar a avaliação em cada repetição permite minimizar o tempo e o esforço despendido na identificação de controles e, ainda assim, assegura que o risco de alto impacto ou de alta probabilidade possam ser adequadamente avaliados. (ABNT NBR ISO/IEC 27005, 2011).

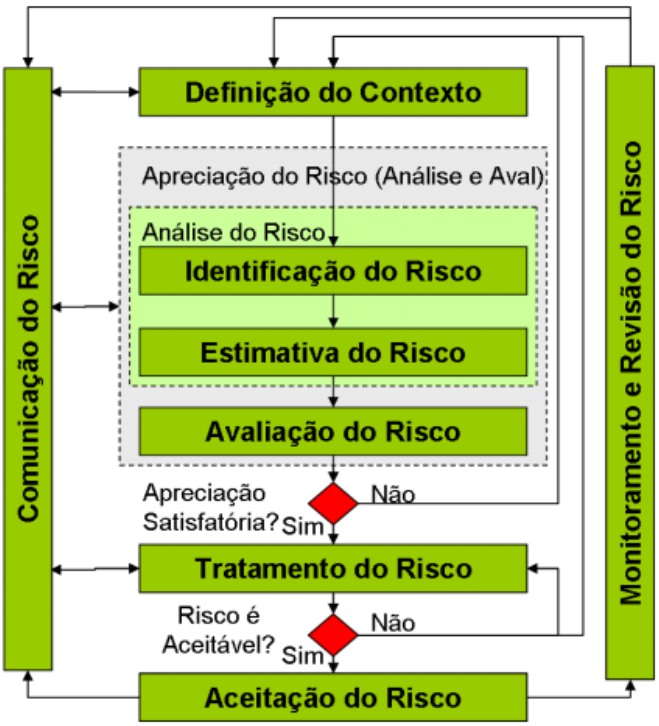

Figura 1. Processo de gestão de risco
Fonte: ABNT NBR ISO/IEC 27005 2011

É de extrema importância que, durante o processo de gestão do risco, os tratamentos dados e os riscos sejam informados às pessoas responsáveis, como gestores por exemplo. Tendo em mãos a informação de risco com antecedência, é possível utilizá-la para reduzir os incidentes e evitar perdas financeiras e materiais. A conscientização por parte dos gestores traz benefícios para a gestão de risco, pois torna mais plausível o trabalho com os incidentes e eventos mais imprevisíveis.

Beal (2005, p.11) cita alguns termos básicos relacionados à gestão do risco:

- **Consequência:** resultado de um evento
- **Critérios de risco:** termos de referência pelo quais a relevância do risco é avaliada.
- **Evento:** ocorrência de um conjunto particular de circunstancias, que caracteriza uma única ocorrência ou uma serie delas.
- **Fonte:** item ou atividade associada a uma consequência potencial.
- **Gestão do risco:** Coordena atividades para direcionar e controlar uma organização com relação ao risco. A gestão do risco normalmente inclui avaliação do risco, tratamento do risco, aceitação do risco e comunicação do risco.
- **Probabilidade:** Associada a um evento é calculada para determinado período de tempo, e é definida como número real na escala de 0 a 1 de ocorrência relativa de longo prazo ou a um grau de confiança de que um evento irá ocorrer para um alto grau de confiança na ocorrência, a probabilidade é próxima a 1.
- **Risco:** combinação da probabilidade de um evento e sua consequência.

O autor também cita os termos relacionados às pessoas ou organizações afetadas pelo risco:

- **Comunicação do risco:** troca ou compartilhamento da informação sobre o risco feita entre o tomador de decisão e outros stakeholders. A informação pode estar relacionada a existência, natureza, forma, probabilidade, gravidade, aceitabilidade, tratamento ou outros aspectos do risco.

- **Parte interessada:** pessoa ou grupo que possui interesse no desempenho ou sucesso de uma organização. Exemplos: clientes, proprietários, integrantes da organização, fornecedores, bancos, sindicatos, parceiros, sociedade.

- **Percepção do risco:** maneira pela qual o stakeholder vê um risco, com base em um conjunto de valores ou preocupações.

- **Stakeholder:** qualquer indivíduo. Grupo ou organização que pode influir sofrer influência ou perceber-se como sendo afetado por um risco.

Ainda sobre os termos o autor cita os relacionados à avaliação de risco:

- **Analise de risco:** uso sistemático de informação, dados históricos analise teórica, opiniões fundamentais, preocupações dos stakeholders para identificar fontes e estimar o risco. A análise de risco oferece uma base para a avaliação, o tratamento e a aceitação do risco.

- **Avaliação do risco:** comparação do risco estimado com determinado critério de risco para determinar sua relevância. A avaliação do risco pode ser usada para subsidiar a decisão de aceitar e tratar um risco.

- **Estimativa do risco:** atribuir valores à probabilidade e às consequências de um risco. A estimativa do risco pode considerar custo, benefícios, preocupações de stakeholders e outras variáveis apropriadas para a avaliação do risco.

- **Estudo do risco:** processo global de análise e avaliação do risco.

- **Identificação do risco:** processo de localizar, listar e caracterizar elementos do risco. Os elementos podem incluir fonte, evento, consequência e probabilidade.

E, por fim, o autor cita os termos relacionados ao tratamento e controle do risco:

- **Aceitação do risco:** decisão de aceitar um risco.

- **Atenuação:** limitação de quaisquer consequências negativas de um evento em particular.

- **Controle do risco:** ações para implementação das decisões de gestão do risco. O controle do risco pode envolver monitoração, reavaliação e conformidade com decisões.

- **Evasão do risco:** decisão de não se envolver, ou ação de fuga de uma situação de risco.

- **Otimização do risco:** processos relacionados a um risco para minimizar as consequências negativas e maximizar as consequências positivas e suas respectivas probabilidades.
- **Redução do risco:** ações tomadas para reduzir a probabilidade, as consequências negativas ou ambas, associadas a um risco.
- **Risco residual:** risco remanescente após o tratamento do risco.
- **Transferência do risco:** compartilhamento com um terceiro do prejuízo da perda ou benefício do ganho em relação a determinado risco, A transferência do risco pode ser feita por meio de seguros ou outros tipos de acordo.
- **Tratamento do risco:** processo de seleção e implementação de medidas para modificar o risco. A expressão tratamento do risco é as vezes utilizada para se referir às próprias medidas de proteção usadas para atenuar, reduzir, transferir ou evitar o risco.

2.7.1. Análise, avaliação e tratamento de risco em segurança da informação.

A análise de risco é um dos processos da gestão da informação e é iniciado por meio da identificação dos seus elementos e riscos. Esses riscos e elementos são classificados em: alvos, agentes, ameaças, vulnerabilidades, impactos. (BEAL, 2005).

Dentro dos conceitos principais em análise de risco estão as ameaças, vulnerabilidades e impactos, Beal (2005) trata esses conceitos como:

- **Ameaça:** um acontecimento que pode ocorrer de forma acidental ou proposital, causado por algum tipo de agente que pode afetar o ambiente, o ativo ou sistema de informação.
- **Vulnerabilidade:** é a fragilidade que poderia ser explorada por uma ameaça para concluir o ataque.
- **Impacto:** os danos ou consequências causadas por um ataque ou incidente. O conceito de impacto está ligado a ameaça e a vulnerabilidade.

Coelho (et al. 2014, p. 3) em seu conceito sobre esses termos cita que:

- **Ameaça:** qualquer evento que explore a vulnerabilidade. Causa potencial de um acontecimento indesejado, que pode resultar em dano para um sistema ou organização.

- **Vulnerabilidade:** Qualquer fraqueza que pode ser explorada e comprometer a segurança de sistemas de informação. Fragilidade de ativos ou grupos de ativos que pode ser explorada por uma ou mais ameaças. São falhas que permitem o surgimento de deficiências na segurança geral de computadores ou rede. Configurações incorretas no computador ou na segurança também permitem a criação de vulnerabilidades. A partir dessas falhas, as ameaças exploram a vulnerabilidade que quando concretizadas resultam em dano? Para o computador, para organização ou para os dados pessoais.

- **Impacto:** consequência avaliada de um evento em particular.

Conforme Beal (2005), outros conceitos podem ser úteis para a gestão do risco e em consequência para a análise de risco:

- **Agente:** é a fonte produtora do evento que pode ter efeitos sobre os ativos de informação, podem ser funcionários, meio ambiente, hackers, etc.

- **Alvo:** ativo que pode ser atacado pode ser banco de dados, equipamentos de hardware, sistemas de informação, serviços de comunicação.

- **Ataque:** o evento que explora uma vulnerabilidade, ou seja, quando uma ameaça atinge a vulnerabilidade, pode ser uma digitação incorreta por parte do usuário, um vazamento de agua, uma fraude por exemplo.

- **Incidente:** é a consequência negativa de um ataque, como exemplo pode-se citar dados armazenados incorretamente, pagamentos indevidos, etc.

A análise e avaliação do risco busca critérios para que o risco possa ser aceito e posteriormente tratado, conforme a norma ABNT 17799 (2005, p. 6) afirma:

> Convém que as analises/avaliações do risco identifiquem, quantifiquem e priorizem os riscos com base em critérios para aceitação dos riscos e dos objetivos relevantes para organização. Convém que os resultados orientem e determinem as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação, e para implementação dos controles selecionados, de maneira a proteger contra esses riscos. O processo de avaliar os riscos e selecionar os controles pode precisar ser realizado várias vezes, de forma a cobrir diferentes partes da organização ou de sistemas de informação específicos.

Devido às mudanças ocorridas no ambiente, a análise de risco não pode ser uma tarefa executada apenas uma vez, ela deve ser realizada periodicamente, assim atendendo às mudanças ocorridas e que não foram detectadas na análise anterior. Além de periódica, a análise e avaliação de risco deve seguir um escopo definido e, pode estar interligada com outras áreas quando necessário. Esse escopo pode englobar toda a organização, parte dela ou um sistema

específico. Isso vai depender, exclusivamente, da necessidade da aplicação. (ABNT 17799, 2005).

Quanto ao tratamento de risco em segurança da informação, é necessário que antes de executar qualquer tratamento, sejam avaliados os critérios em relação ao risco ser aceito ou não. Para cada risco identificado deve se tomar uma decisão, algumas delas segundo a ABNT 17799 (2005) são:

- Aplicar controles apropriados para reduzis os riscos;
- Conhecer e aceitar o risco reconhecendo que eles fazem parte da organização;
- Não permitir ações que podem causar risco;
- Transferir o risco, quando, por exemplo, ele é repassado para seguradoras ou a fornecedores.

Existem diversas classificações para medir a proteção que se deve gerar para tratar o risco, ou seja, para diminuir ou mitigar esses riscos. Conforme Beal (2005) uma possível classificação é:

- **Medidas preventivas:** Controlar ou reduzir a probabilidade de uma ameaça agir, ou também, diminuir a vulnerabilidade, evitando assim que a ameaça consiga de alguma forma agir;
- **Medidas corretivas ou reativas:** diminuir o impacto causado, então esse tratamento é dado após um possível ataque ou evento.
- **Métodos defectivos:** gerar ataques e incidentes com o objetivo de testá-los e criar reações contra os mesmos.

A norma ABNT NBR ISO/IEC 27001 (2013) aponta os objetivos do tratamento do risco para o processo de segurança da informação:

- Utilizar a avaliação de risco para selecionar opções de tratar os mesmos.
- Determinar os controles necessários para o tratamento dos riscos.
- Efetuar comparações entre os controles escolhidos para o tratamento do risco.
- Confeccionar o plano de tratamento de risco.

- Obter a aprovação dos responsáveis dos riscos escolhidos.

2.7.2. Análise de vulnerabilidade

A vulnerabilidade em segurança da informação pode ser considerada como a fragilidade onde uma ameaça pode atacar de alguma forma, nesse caso é necessário identificar essas vulnerabilidades e saber como elas estão abertas, ou seja, vulneráveis. Conforme Coelho (et al. 2014), é necessário levantar as probabilidades de cada ativo estar vulnerável a ameaças. Portanto, deve-se atentar para o compromisso elegendo as prioridades, e para garantir a segurança no que se refere a confidencialidade, integridade, disponibilidade.

O resultado de uma análise, contemplando as ameaças, vulnerabilidades e impactos devem servir como guia para adoção de medidas de segurança que atendam aos requisitos da organização, considerando os custos, nível de proteção e facilidade de uso. (COLELHO et al., 2014).

A seguir, são mostrados exemplos de vulnerabilidades, segundo a norma ABNT ISO/IEC 27005 (2011):

- **Hardware:** manutenção insuficiente, instalação defeituosa de mídia de armazenamento, falta de rotina de substituição periódica, sensibilidade a umidade, poeira e sujeira, inexistência de controle eficiente de mudança de configuração, sensibilidade a variação de voltagem, sensibilidade a variação de temperatura, armazenamento não protegido, falta e cuidado durante o descarte, realização de copias não controladas.
- **Software:** testes insuficiente ou existentes, não logout ao deixar estação de trabalho, não remoção de dados ao descartar mídias, atribuições errôneas de controles de acesso, software amplamente distribuído, interface de usuário complicada, documentação inexistente, configuração de parâmetros incorretas, datas incorretas, inexistência de mecanismos de autenticação de usuários, tabelas de senhas desprotegidas, gerenciamento de senhas mau feito, serviços desnecessários habilitados, softwares imaturos, inexistência de um controle eficaz de mudança, download e uso não controlado de software, inexistência de backup, inexistência de proteção físicas, portas e janelas, inexistência de relatórios de gerenciamento.
- **Rede:** inexistência de firewall, linhas de comunicação desprotegidos, trafego sensível desprotegido, ponto único de falha, arquitetura insegura de rede, transferências de se-

nhas erroneamente, gerenciamento inadequado do roteamento, conexões de rede desprotegidos.

- **Recursos humanos:** ausência de recursos humanos, recrutamento inadequado, treinamento insuficiente em segurança, uso incorreto de software e hardware, falta de conscientização em segurança, inexistência de mecanismos de monitoramento, não supervisão de pessoal terceirizado, inexistências de políticas para uso de telecomunicação e troca de mensagens.

- **Local e instalações:** uso inadequado de controles de acesso físico, localização a áreas suscetíveis a inundações, fornecimento de energia instáveis, inexistência de proteção física para portas e janelas.

- **Organização:** inexistência de registro formal para registro e remoção de usuários inexistência de processo formal para análise de direitos de acesso, provisões insuficientes ou inexistentes, em contratos com clientes e terceiros.

Não monitoramento das instalações de processamento de informações inexistência de auditorias periódicas, inexistência de análise e avaliação de risco, respostas inadequadas de serviços de manutenção, inexistência de controles de mudança, inexistência de procedimento formal para controle de documentação e supervisão dos registros do SGSI, inexistência de um processo formal para autorização das informações disponíveis publicamente, atribuição inadequada das responsabilidades pela segurança da informação, inexistência de um plano de continuidade, inexistência de política de uso de e-mails e também para instalação de software em sistemas operacionais, ausência de registro de arquivos de auditorias (log), inexistência de procedimentos para manipulação de informações classificadas provisões insuficientes ou inexistentes, em contratos com funcionários assim como a ausência das responsabilidades de segurança da informação disponíveis nos cargos e funções, inexistência de política formal para uso de computadores moveis, assim como de controle de ativos fora das dependências, política de mesa e telas limpas, inexistência de mecanismos estabelecidos para monitoramento de violação de segurança, inexistência de analises críticas e periódicas por parte da direção, inexistência de procedimentos para o relato de fragilidades ligadas a segurança assim como pra garantir a conformidade com os direitos de propriedade intelectual.

A vulnerabilidade, por si só, não causa danos, ela precisa estar ligada a uma ameaça que possa explorá-la, sendo assim uma vulnerabilidade que não possui ameaça não requer um controle imediato, porém a mesma deve ser monitorada. Também é possível notar que um controle sendo operado de forma errada, implementado incorretamente ou com mau funcionamento pode ser considerado uma vulnerabilidade. (ISO/IEC 27005, 2011).

O padrão conhecido pela indústria para identificação de vulnerabilidades de ambientes computacionais é chamado CVE– Common Vulnerabilities and Exposures, esse padrão pode ser considerado um dicionário das vulnerabilidades e tem por objetivo a identificação e o desenvolvimento de ferramentas voltadas à busca das vulnerabilidades no ambiente. Conforme cve.mitre.org (2016) CVE, essa sigla pode significar:

- Um nome para uma vulnerabilidade ou exposição.
- Uma descrição padronizada para cada vulnerabilidade ou exposição.
- Um dicionário em vez de um banco de dados.
- Fazer bases de dados e ferramentas falarem a mesma língua.
- Caminho para melhor segurança sem falhas e interrupções.
- Base para avaliação entre ferramentas e base de dados.
- Software gratuito.
- Certificado através de CVE Naming Authorities, CVE Editorial Board e CVE-Compatible Products.

Lançado em 1999 para suprir a necessidade da época em relação à padronização das vulnerabilidades sistêmicas, CVE se tornou um padrão para nomes de vulnerabilidades. O padrão acabou criando nomes CVES, números CVES, CVEs-Ids ou CVEs como ponto de referência para a troca de informação a respeito de vulnerabilidades (CVE.MITRE.ORG, 2016).

Para testes de vulnerabilidades de ambientes computacionais é possível utilizar ferramentas de auditoria, um exemplo é o NESSUS, uma ferramenta de auditoria que serve para identificar e efetuar correções de vulnerabilidade em redes. O objetivo da ferramenta é varrer a rede identificando as portas TCP, simulando possíveis invasões e assim detectando vulnerabilidades existentes para possíveis correções (MORINOTO, 2011).

Conforme Tenable (2016), o objetivo da ferramenta NESSUS é responder às perguntas que são necessárias à respeito de uma determinada rede, por exemplo, compatibilidade entre dispositivos, detecção de vírus na rede, informações privadas. Dentre as funcionalidades no NESSUS é possível:

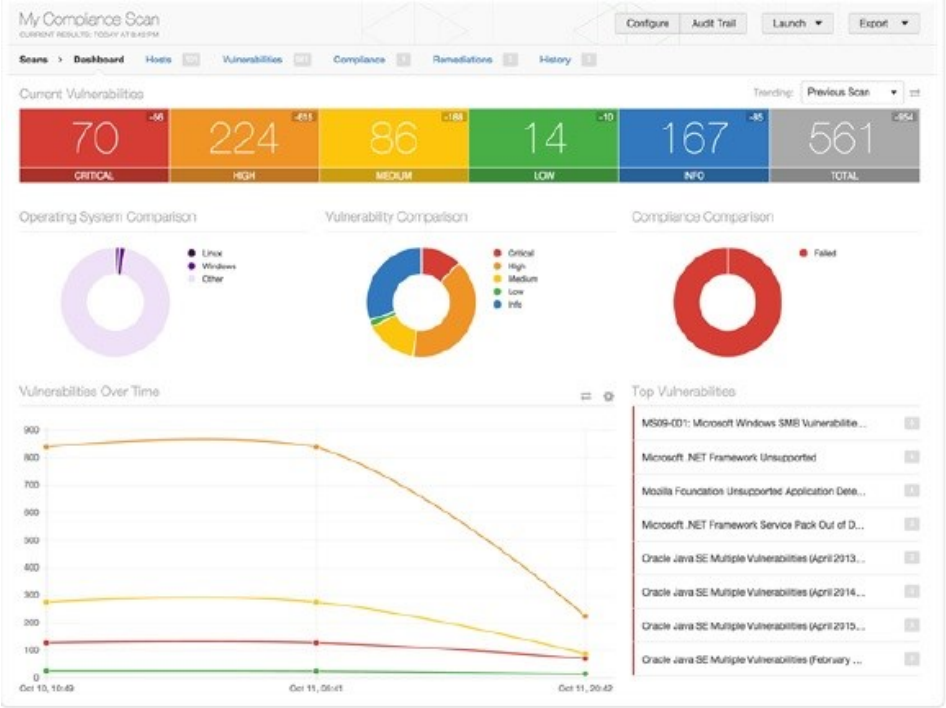

Figura 2. Dashboard Nessus
Fonte: Tenable network security

- Compartilhar scanners, cronogramas, políticas e resultados de varreduras possibilitando soluções rápidas entre equipes.
- Fazer interligações de SIEMs (Gerenciamento de eventos e informações de segurança), barreiras contra malwares, gerenciamento, firewalls e sistemas virtualizados.
- Identificar dados sensíveis na web.

  Atualizar dados sobre ameaças avançadas, vulnerabilidades e novas configurações regulamentadas.

Quanto as vulnerabilidades técnicas a norma ABNT ISO/IEC 27002 (2013) trata algumas diretrizes necessárias para o gerenciamento dessas vulnerabilidades:

- Estabelecer funções e responsabilidades a respeito das vulnerabilidades técnicas com monitoramento, avaliação de risco, correções e acompanhamento dos ativos.
- Recursos para gestão de vulnerabilidades, devidamente, identificados e atualizados.
- Definir prazos para reação em caso e identificação de vulnerabilidades.
- Analisar os riscos inerentes e ações tomadas após identificar a vulnerabilidade técnica.

- Analisar os riscos inerentes de correções novas quanto a sua instalação.
- Mantes registro de auditoria dos procedimentos realizados.
- Monitoramento e avaliação periódica do processo de gestão de vulnerabilidade.
- Aliar o processo de gestão de vulnerabilidade técnica com o de gestão de incidentes.
- Procedimentos necessários para vulnerabilidades identificadas, mas que não tenham um controle eficaz.

A norma ABNT ISO/IEC 27002 (2013) fala também sobre a restrição da instalação de software, que é uma funcionalidade que traz grande vulnerabilidade para a organização. A norma cita diretrizes como, a política de restrição de instalação para certos tipos de software, onde a organização pode definir quais tipos de softwares podem ou não ser instalados nos computadores. Outra medida é a política de privilégio que pode ou não permitir que um usuário tenha permissão para instalar softwares. A medida relacionada à política de instalação de software é necessária, pois a instalação descontrolada pode causar vulnerabilidades e automaticamente ferir os princípios de segurança da informação.

2.8. Política de Segurança da Informação - PSI

A PSI ou Política de Segurança da Informação é um dos passos principais na gestão de segurança da informação. Essa política é composta de uma documentação representando as delegações que a organização escolheu para gerir a política de segurança. O objetivo desse documento além do processo de arquivamento do que foi definido, também deve ser disponibilizado a todos os colaboradores da organização mostrando as diretrizes, normas e restrições e deve ser aplicada a todos os sistemas e processos da organização. Conforme a norma ABNT 27002 (2013) a política deve ser definida e aprovada pela direção, deve ser publicada e comunicada a todos os colaboradores e partes externas interessadas. A própria norma ABNT 27002 (2013) cita os requisitos que a política precisa contemplar que são as estratégias de negócio, regulamentação, legislação e contratos, as ameaças atuais e futuras no ambiente de segurança da informação.

Segundo Costa (2009, p. 48):

> A política por definição é um documento de alto nível, e com isso, não deve conter normas ou procedimentos. Ela deve estabelecer regras de alto nível sobre os recursos tecnológicos da organização e o que deve ser feito e por que ser feito, nunca o "como fazer". Deve-se criar um documento que os usuários assinem, dizendo que leram, entenderam e concorram com a política estabelecida. Esta é uma parte importante do processo.

É conveniente que a PSI possua um gestor responsável pelo desenvolvimento, analise e avaliação da política. É conveniente também que a análise crítica contemple a avaliação de melhorias para a PSI, assim como da organização e que tenha foco no gerenciamento das mudanças do ambiente organizacional, nos negócios, na legalidade e no ambiente. Conforme Coelho et.al (2014). O gestor se torna responsável geral pela segurança da organização, também auxiliando no processo de implantação e treinamento da PSI, é necessário que o gestor esteja sempre engajado no processo, se atualizando em relação aos riscos inerentes a organização, analisando as adequações da PSI e os processos adotados para a implantação da política de segurança da informação.

A norma ABNT ISO/IEC 17799 (2005, p. 9) aponta algumas informações importantes para a análise crítica de PSI, são elas:

- Realimentação das partes interessadas.
- Resultado de analises críticas independentes
- Situação de ações preventivas e corretivas
- Resultados de analises críticas anteriores feitas pela direção
- Desempenho do processo e conformidade com a política de segurança da informação.
- Mudanças que possam mudar o enfoque da organização para gerenciar a segurança da informação, incluindo mudanças no ambiente organizacional, nas circunstâncias do negócio na disponibilidade e dos recursos, nas questões contratuais, regulamentares e de aspecto legais ou no ambiente técnico.
- Tendências relacionadas com a as ameaças e vulnerabilidades.
- Relato sobre incidentes de segurança da informação
- Recomendações fornecidas por autoridades relevantes

Em se tratando das saídas de análise crítica a norma cita ações relacionadas a:

- Melhoria do enfoque da organização para gerenciar a segurança da informação e seus processos.
- Melhoria dos controles e dos objetivos de controles.
- Melhoria na alocação de recursos ou de responsabilidade.

A norma ABNT ISSO/IEC 27002 (2013) contempla alguns pontos relacionados às PSIs com tópicos especiais, dentre eles estão:

- Controles de acesso
- Classificações e tratamento dos ativos de informação
- Segurança física
- Tópicos relacionados a usuários finais
- Uso correto dos ativos
- Política de mesa e tela limpa
- Transferência de informações
- Dispositivos moveis e trabalho remoto
- Restrição de uso e instalação de software
- Uso e administração de backup
- Proteção contra códigos maliciosos
- Vulnerabilidades técnicas
- Controles de criptografias
- Segurança de comunicação
- Privacidade de identificação pessoal

Para confecção da política a organização pode escolher algumas formas de construção. Uma delas é a escolha de um consultor ou de uma consultoria, mais frequentes para empresas de menor porte, nesse caso a consultoria efetua a elaboração do documento que é repassado para avaliação da diretoria da organização. Em outros casos a empresa cria um grupo de elaboração da política interna. Depois de elaborado o documento pelo grupo ele deve ser

devidamente revisado pela diretoria, que deve avaliar a coerência com as diretrizes da organização no que diz respeito a missão, visão, valores e objetivos (BEAL, 2005).

2.9. Continuidade do negócio

Para que a gestão ocorra de maneira correta é necessário um entendimento em relação aos riscos, desastres e o que isso pode causar, como interrupções ou perdas de informações. O processo utilizado pode se assemelhar com a análise de risco, porém enfatizando-os impactos que a organização pode sofrer e, assim criando um plano que visa recuperar e dar continuidade ao negócio.

Continuidade do negócio diz respeito às estratégias e táticas de uma organização pública ou privada de criar planejamento e dar respostas rápidas a incidentes e interrupções que podem ocorrer, com o objetivo de minimizar os impactos e prover a recuperação das perdas de informação, sendo assim mantendo as operações funcionais, conforme definido no planejamento (GSI/CDN, 2015).

É importante contemplar alguns pontos para a elaboração do plano de continuidade do negócio, dentre eles estão a identificação das responsabilidades juntamente com a concordância com os procedimentos; a aceitação da perda da informação; implementar métricas de recuperação da perda mantendo prazos e mantendo atenção no ambiente externo e contratos; documentar os procedimentos e processos; testar e atualizar os planejamentos; treinamento adequado, tanto nos processos quanto no gerenciamento de crise (ABNT NBR ISO/IEC 17799, 2005).

As indisponibilidades de ativos de informação, serviços e software aumentam com o passar dos anos, é importante que o planejamento de continuidade produza projetos de redução do tempo de inatividade diminuindo assim o impacto provocado na organização (BEAL, 2005).

Existem técnicas a se utilizar para elaboração do plano de continuidade, objetivando a operação do plano no mundo real e atendendo à demanda corretamente. Testes com objetivo de recuperações de diferentes interrupções e em diferentes locais, simulações, testes de servi-

ços disponibilizados por terceiros, testes gerais com a organização para avaliar se todos estão preparados para algum tipo de interrupção.

2.10. Auditorias Internas de Sistemas de Segurança da Informação

A auditoria de sistemas de informação garante a conformidade dos sistemas quanto à sua segurança, integridade e disponibilidade. Pode ser considerado também uma garantia de continuidade do negócio já que esse processo ajuda a monitorar as diretrizes da PSI na organização, se estão sendo realmente cumpridos em todos os ambientes e normas.

A realização de testes auxilia nas revelações de falhas e vulnerabilidades de segurança tanto nos sistemas quanto nos recursos humanos, ambos podem estar vulneráveis e consequentemente sofrerem ameaças de exploração, nesse caso a auditoria pode servir para prevenir um desastre antes que ele ocorra (ENGEBRETSON, 2011).

A norma ABNT NBR ISO/IEC 27001 (2013) indica alguns pontos onde a auditoria interna deve se concentrar e ser planejada, com o objetivo de indicar se a organização possui os requisitos de acordo com a sua política de gestão da informação; se todos os requisitos estão seguindo a norma estabelecida; se está sendo seguido um cronograma de auditoria indicando a frequência, os método e requisitos necessários e, principalmente, se o que está sendo detectado nas auditorias está realmente sendo tratado e, por último, escolher auditores que conduzam de forma correta o processo de auditoria. Também deve se assegurar que a auditoria está sendo repassado para os gestores da organização para que possam tratar juntos as inconformidades, e assegurar que a documentação referente as evidencias esteja sendo devidamente arquivado com segurança.

Todas as ferramentas relacionadas à auditoria e aos testes realizados durante esse processo devem estar devidamente protegidos, arquivos de dados devem estar separados de outros em execução, documentos devem ser disponibilizados como semente leitura para evitar alterações indevidas, deve-se também ter muito cuidado em relação a terceiros que venham a estar atuando na auditoria, é necessário analisar os riscos e manter um controle de acesso físico para uso das ferramentas de auditoria, manter também cuidado em relação ao uso de senhas internas da organização por parte destes.

Enfim, a auditoria interna faz parte do processo de concepção da PSI e é o passo importante para que a Política siga as diretrizes que foram estudadas, documentadas e praticadas.

2.11. Classificação e Controle dos Ativos da Informação

Um dos objetivos da classificação e controle em segurança da informação é dar ênfase para que a informação mantenha um nível aceitável de segurança de acordo com o seu nível de importância para a organização. Nesse processo é estabelecido o nível de importância do ativo de informação quanto ao seu impacto para a gestão dos negócios, ou seja, quanto maior a importância da informação maior também será a sua importância. Para a classificação é importante que ocorra de acordo com o seu valor, requisitos legais, sensibilidade e criticidade com o objetivo de evitar o vazamento e modificações não autorizadas (ABNT NBR ISO/IEC 27002, 2013).

Para o tratamento da informação classificada, são criadas ações referente ao processo que podem ser de recepção, classificação, utilização, acesso, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação em qualquer grau de sigilo. (DECRETO Nº 7.845, 2012).

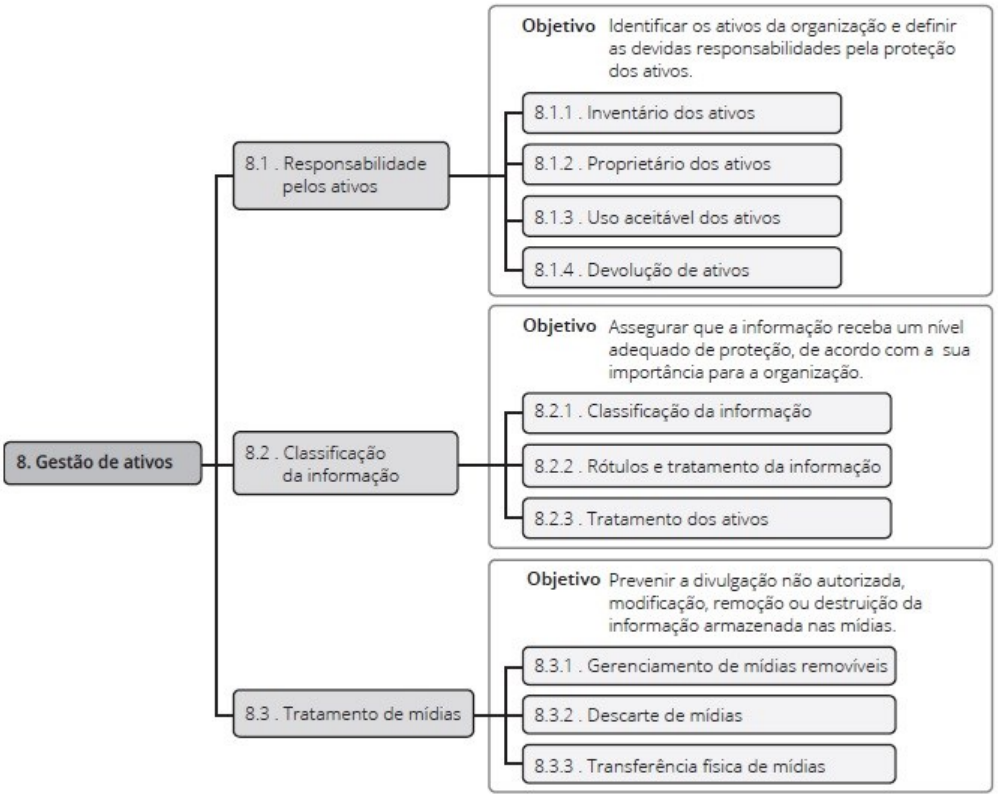

Figura 3. Gestão de ativos de informação
Fonte: Coelho et.al (2014)

O processo de classificação da informação pode ter sua avaliação voltada para sua confiabilidade, integridade e disponibilidade dentre outros requisitos analisados pela organização. A classificação da informação para a organização deve seguir critérios em relação ao que pode ou não ser compartilhado, também é necessário que além da classificação, a reclassificação seja efetuada ao longo do tempo para que seja mantida sempre atualizada nesse processo, essa reclassificação deve ser feita de preferência pelo proprietário do ativo. Durante a classificação é importante também que não seja criado um sistema muito complexo, que dificulte o entendimento além de aumentar os custos, também se faz importante criar nomes para a classificação que sejam passíveis de entendimento por todos os interessados. (ABNT NBR ISO/IEC 17799, 2005).

Na classificação da informação a nomeação para cada classe de ativo é chamada de rotulo, para efetuar a rotulação é possível seguir alguns critérios. A norma ABNT ISO/IEC 17799 (2005) aponta que a classificação deve abranger tanto os ativos no formato físico como os lógicos, é importante também que as informações sensíveis ou críticas tenham uma classi-

ficação especial e para cada nível de informação os procedimentos a se seguir contemplando a armazenagem, transmissão, reclassificação e destruição, é importante também classificar as informações oriundas de terceiros mas que afetem a organização, para esses casos deve-se identificar os rótulos dessas organizações.

2.12. Aspectos humanos

Em segurança da informação, os recursos humanos trazem um ponto muito importante para o processo. De nada adiantaria a PSI possuir as diretrizes de segurança se a diretoria, os colaboradores, e todos os demais envolvidos com a PSII estivessem desinformado ou desengajados do propósito de implantação desse processo.

Não basta somente a confiança quando se fala em recursos humanos, é necessário verificar, ou seja, fazer uma análise do comportamento humano na organização, pois apesar de normalmente ser dada mais atenção às invasões vindas de fora, a maioria dos desastres de segurança são causados por pessoas ligadas diretamente à organização, seja, involuntariamente, ou com a intenção de causar algum tipo de dano a mesma (BEAL, 2005).

Segundo a norma ABNT NBR ISO/IEC 17799 (2005), o objetivo é assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, reduzindo os riscos de ações fraudulentas, furtos de informação e má utilização dos recursos.

De acordo com Beal (2005, p. 72):

> A segurança dos ativos de informação baseados em TI depende da colaboração permanente dos funcionários da organização, que precisam atuar tanto na prevenção, desempenhando as funções de segurança de que foram incumbidos, como por exemplo, escolher senhas difíceis e mantê-las em sigilo, quando na reação a eventuais problemas de segurança, reatando falhas nos controles e incidentes observados. O procedimento de segurança de responsabilidade dos usuários finais de informação deve estar associado a regras claras, de obediência obrigatória, e a punições em caso de seu descumprimento, e ser adequadamente divulgados para evitar que seu desconhecimento diminua a eficácia dos controles existentes.

A Segurança em recursos humanos visa garantir a segurança da informação em três momentos diferentes da vida profissional do servidor na organização, que são antes da contratação, durante a contratação e no encerramento ou mudança de contratação (MONTEIRO, 2009, p.26)

2.12.1. Processo de Seleção

No processo de seleção é importante que sejam realizadas as verificações de acordo com as leis, regulamentações e éticas, proporcionalmente, aos requisitos do negócio, a classificação das informações e aos riscos detectados (ABNT NBR ISO/IEC 17799, 2005).

Durante o processo de seleção é importante buscar informações das pessoas, tais como referencias profissionais e pessoais para analisar o comportamento da pessoa antes da contratação, verificação curricular, qualificações acadêmicas, verificações criminais como fichas policiais e também de credito junto aos órgãos de proteção ao cliente por exemplo. Também é importante buscar informações de terceiros e fornecedores quando na contratação, é conveniente uma análise junto aos órgãos responsáveis, assim como as especificações claras da política de segurança da informação da organização, especificações essas que podem ser devidamente incluídas em contrato. Desse modo é necessário que tanto funcionário, terceiros ou fornecedores assinem termos de responsabilidade quanto a PSI durante o processo de contratação e após terem recebido devido treinamento (ABNT NBR ISSO/IEC 17799, 2005).

2.12.2. Contratações

Com os funcionários, terceiros e fornecedores contratados o trabalho de conscientização da política continua. Eles devem estar cientes das suas obrigações quanto a organização e devem seguir todas as normas estabelecidas. Cabe à direção ter a responsabilidade de garantir que a segurança da informação está sendo aplicada de forma correta e se necessário aplicar as punições necessárias.

É conveniente que todos os funcionários da organização, fornecedores e terceiros sejam treinados para assumir as responsabilidades de segurança na organização, é importante também que recebam treinamento de atualizações advindas dos procedimentos organizacionais relevantes à função que exercem (ABNT NBR ISO/IEC 17799, 2005).

2.12.3. Encerramento ou mudança

Quando um funcionário, terceiro e fornecedor deixa a organização é importante assegurar que a devolução de equipamentos pertencentes à organização, sejam feitos e que to-

dos os acessos dos mesmos sejam bloqueados ou excluídos. Quanto às mudanças, é importante que organização mantenha a gerência das funções dos colaboradores de acordo com o cargo que o mesmo vai exercer.

É importante que para o processo de encerramento de atividades sejam incluídos requisitos e responsabilidades apropriadas e que os acordos de confidencialidade, condições de trabalho tenham prazo maior do que o período em que o funcionário, terceiro ou fornecedor exerceu na organização, caso algo após esse período ocorra. Para mudanças ocorridas na organização é importante manter a gerência quanto ao encerramento das atividades atuais e o controle das novas atividades exercidas pelos mesmos (ABNT NBR ISO/IEC 27002, 2013).

2.13. Segurança física

A segurança física corresponde proteção que abrange os ativos tangíveis da organização, que podem ser desde ambiente físico, como portas e janelas como equipamentos, fitas de backup, documentos, dentre outros. O objetivo é manter a prevenção de acessos não autorizados, possíveis danos em instalações e, informações da organização.

É conveniente a criação de barreiras, como paredes, portões, salas cofres e controles de entrada como cartões, biometria, senhas dentre outras com objetivo de manter os ativos de informações protegidos contra acessos físicos (ABNT NBR ISO/IEC 17799, 2005).

A norma ABNT NBR 27002 (2013) cita algumas diretrizes importantes para as barreiras de segurança física, controles de entrada física e proteções prediais, são elas:

2.13.1. As barreiras físicas

- As barreiras devem ser definidas e sua localização, assim como sua resistência, depende do tipo de ativo que compõe o ambiente interno desse local.
- Construções sólidas para locais que contenham processamento de dados com barreiras reforçadas em paredes robustas evitando qualquer tipo de invasão.
- Implantação de recepção para visitantes e locais internos seja somente para acessos autorizados.
- Portas corta-fogo sejam compostas de alarme, monitoramento e devidamente testadas.

- Sistemas de detecção, alarmes devem ser instalados e testados regularmente.
- Instalações de processamento de dados sejam separados do ambiente de acesso a terceiros.

2.13.2. Controles de entrada física

É conveniente seguir diretrizes referente a entrada em ambientes físicos, o registro de data e hora de entrada e saída de visitantes por exemplo, garantir a supervisão dos visitantes durante toda visita e instruir os mesmos referente as regras de PSI do local onde estão acessando.

2.13.3. Segurança predial

Para acesso a salas, escritórios e locais de instalação é necessário criar regras como por exemplo a proteção que se deve dar a chaves das salas, que os edifícios onde ocorram algum tipo de atividade que envolva processamento de dados sejam discretos, ou seja, sem identificações, placas e logomarcas a fim de evitar a curiosidade e garantir sigilo do local.

2.13.4. Ameaças externas

Quando se fala em ameaças externas a PSI deve tratar realmente de vários fatores relevantes, explosões, terremotos, enchentes por exemplo, devem ser devidamente tratados para a segurança física do ambiente. No caso de equipamentos de backup, que sejam armazenados em ambiente seguro para evitar possíveis intemperes do meio ambiente, para o uso de sites backups que sejam criados em ambientes diferentes respeitando s normas e garantindo a segurança dos locais, também se faz necessário ter todos os equipamentos ante incêndio em dia para garantir a segurança evitando surpresas desagradáveis.

2.13.5. Áreas seguras

As áreas seguras, como salas cofres, sites backups dentre outros sejam protegidos de forma a evitar fatos que quebrem os regulamentos de acesso físico. O local só deve ser revelado caso haja necessidade de atendimento, as pessoas devem ser devidamente autorizadas e monitoradas e não deve ser permitido o uso de equipamentos que possam registrar o local,

como câmeras fotográficas, dispositivos moveis, etc., a não ser que sejam devidamente autorizados.

2.13.6. Áreas de carregamento

As áreas de carregamento correspondem a locais de acesso a público muitas vezes não autorizadas, para esses locais é necessário criar diretrizes como a restrição de entrada, isolamento dessa área das demais, portas devidamente protegidas, por exemplo, quando a interna estiver aberta a interna esteja fechada, todos os materiais sejam analisados antes da entrada, que todos os ativos sejam gerenciados, ou seja, qualquer material que chegue tem que ser identificado de acordo.

2.13.7. Equipamentos

Quanto aos equipamentos presentes na organização é necessário criar diretrizes para a proteção dos mesmos, como local de armazenamento, controles contra furtos ou desastres naturais, proteção para áreas restritas como de processamento de dados, também é necessário proteger equipamentos contra danos elétricos. Ainda falando de equipamentos, cabeamentos de energia e telecomunicação devem seguir diretrizes de segurança tais como proteções para cabeamento de redes para evitar interceptações ou paradas não autorizadas, utilizar as marcações necessárias nos cabeamentos, etc.

Coelho et.al (2014) cita a restrição de acesso a equipamentos de hardware, para que esse acesso seja feito somente por funcionários competentes, devidamente registrado de acordo com as necessidades da organização. O autor cita a possibilidade de adaptação dessa diretriz para a aplicação nas organizações.

No que se refere à manutenção de equipamentos da organização, as diretrizes falam sobre o cuidado que se deve ter com as autorizações de manutenção de equipamento, registros de falhas e que sejam delimitados períodos para manutenção preventiva de equipamentos. A retirada de equipamentos para fora das dependências da organização também devem ter cuidados especiais, como equipamentos portáteis, por exemplo. Eles devem estar previamente registrados e, autorizados para retirada, seguindo os requisitos da análise e avaliação de riscos imposta na organização.

Em relação ao descarte e à reutilização de equipamentos é necessário tomar cuidado em relação a equipamentos de armazenamento, pendrives, HDs, etc. Convém que esses equipamentos sejam analisados e, que seja descartado de forma segura, todo o armazenamento que contém, a fim de evitar riscos de roubos de dados e uso não autorizado das informações.

2.13.8. Dispositivos móveis

Um estudo do IBGE (Instituído Brasileiro de Geografia Estatística) revelou um crescimento no número de dispositivos moveis como Smartphones, Tablets, TVs. Pela primeira vez esse número ultrapassou a quantidade de usuários de computadores pessoais. Até 2013 os computadores eram maioria, já em 2014 caíram para segundo lugar. Ainda segundo a pesquisa, a cada cinco casas pesquisadas quatro utilizam telefone móvel para se conectarem a internet, um avanço muito significativo para a inclusão digital e também para o crescimento dos BYOD – Bring Your Own Device.

Tablets, notebooks, iPhone e Android já fazem parte do cotidiano das organizações, diversos colaboradores em praticamente todos os cargos utilizam algum tipo de dispositivo móvel, diante desse cenário a organização acaba tendo um corpo de funcionários que participam do que é denominado BYOD, que é o termo para quem utiliza o dispositivo móvel tanto para fins pessoais como profissionais (ADDED.COM.BR, 2016).

A utilização de dispositivos móveis nas dependências da organização é um ponto que chama a atenção pelo risco eminente que esses trazem para o local. A norma ABNT NBR ISO/IEC 27002 (2013) fala desses riscos e cita alguns pontos importantes referentes aos usos desse tipo de equipamento como, o registro de dispositivos, a proteção física dos equipamentos, a restrição quanto à instalação de softwares e atualizações, proteção contra conexão a serviços que contenham informações, controles de acesso e criptografias, desativações e bloqueios remotos quando necessário, dentre outros.

Os recursos que possam ser utilizados para processamento e armazenamento de dados sejam eles privados ou pessoais, necessitam de implementações de acordo com o tipo, nesses casos é importante criar diretrizes para uso autorizado dos dispositivos dentro da organização (ABNT NBR ISSO/IEC 17799, 2005).

2.14. Segurança Lógica

A segurança lógica em TI previne outro segmento de ativos intangíveis da organização. O acesso lógico corresponde a uma vulnerabilidade maior inclusive do que a segurança física. Nos dias atuais, o crescimento da conectividade aliada ao crescimento dos dispositivos de conexão portáteis ou não, tornou o sistema cada vez mais vulnerável, promovendo assim a necessidade de um estudo aprofundado em relação às Políticas de Segurança da Informação. O controle de acesso lógico diz respeito às medidas de proteção contra acessos não autorizados e inclui a implantação de controles informatizados para proteção dos ativos lógicos e a dar os privilégios necessários para usuários do sistema.

Conforme Beal (2005, p. 91):

> Para cada tecnologia emergente implementada para dar apoio ao negócio, novas ameaças e vulnerabilidades precisam ser consideradas em relação ao ambiente SI/TI. Mesmo novas medidas criadas, para a proteção dos ativos informacionais muitas vezes produzem novos requisitos de segurança, é o caso, por exemplo, dos controles para proteção das chaves secretas de criptografias usadas para salvaguardar informações sigilosas: não faz sentido aplicar processos de codificação da informação se a chave ou frase –senha que permite a decodificação estiver facilmente num arquivo de computador ou num pedaço de papel pregado no monitor.

Em relação ao acesso lógico a norma ABNT NBR ISO/IEC 17799 (2005) pondera que o uso de segurança da informação deve garantir as restrições necessárias para acesso ao ambiente lógico. Para isso devem-se criar controles de acesso definidos para esse fim, controlar a autorização de softwares de uso da organização em geral, controlar os sistemas operacionais e controlar também softwares maliciosos.

> Para implementação de um controle de acesso lógico é conveniente a criação, documentação e análise crítica de uma política de acesso lógico baseadas na segurança da informação estabelecida. Essa analise deve estabelecer controles de acesso, direitos de acesso, restrições para diferentes tipos de cargo ou de usuários, com o objetivo de mitigar os riscos inerentes dos acessos mal-intencionados e riscos de incidentes involuntários. É conveniente que a delimitação de acesso seja documentada e repassada aos usuários para que esses estejam cientes da política (ABNT NBR 27002, 2013).

A norma ABNT NBR 27002 (2013) indica alguns itens interessantes a se levar em consideração em relação à criação do controle de acesso lógico:

- Segurança de aplicativos individuais
- Conhecer e ser autorizado

- Direitos de acesso e política de acordo com a implantação
- Legislação e obrigações contratuais.
- Diferenciar os tipos de controles, pedido, bloqueio, administração de acesso.
- Autorização forma para pedido de acesso
- Analise periódica dos direitos de acesso
- Remoção de direitos de acesso
- Arquivamento dos registros de acesso
- Regras de privilégio

2.14.1. Segurança das redes

A segurança de redes diz respeito não somente aos ataques já conhecidos, como hackers, falhas ou crimes humanos e a incidência de malware. A segurança das redes garante novas oportunidades de negócio quando promovem a correta disponibilidade do recurso, ou quando passam confiabilidade, flexibilidade e são fáceis de operar, ou seja, a segurança em redes significa prevenção, monitoração e respostas rápidas a eventuais incidentes de forma a passar confiança a quem as utiliza (NAKAMURA; GEUS, 2007).

A norma ABNT NBR ISO/IEC 27002 (2013) aponta algumas diretrizes importantes na formulação da política de acesso à rede:

- A política deve incluir redes e serviços que são permitidos os acessos.
- Autorizações para quem tem permissões de acesso.
- Gerenciamento de acesso a rede
- Que contemple meio utilizados para acessar as redes.
- Autenticação de usuários
- Monitoramento

Esses controles são importantes pois é necessário que se tenha segurança nos acessos a redes e sistemas críticos garantindo a integridade e o acesso correto. O acesso não autoriza-

do ou não monitoramento pode causar sérios danos a organização em relação a segurança da informação.

Outro ponto importante na segurança de redes são os registros e cancelamentos de usuários, que devem seguir diretrizes quanto ao processo tanto para conceder acessos quanto para bloquear. A norma ABNT NBR 27002 (2013) aborda a necessidade de controles documentais, para registro e cancelamentos de usuários, com a utilização de IDs únicos, os acessos devem corresponder ao seu cargo dentro da organização, a remoção imediata em caso de mudança ou desligamento, a segurança de que permissões não sejam dadas a usuários incorretamente, dentre outros.

2.14.2. Firewall

Firewall pode ser considerado um ponto entre duas ou mais redes, único ou em conjunto que gerencia todo o trafego de rede que por ele passa, gravando registros, autenticações de todo o trafego realizado. Esse componente possui funções de proteção de uma rede confiável, de uma rede pública não confiável e também pode gerenciar sub redes, grupo de trabalhos e LANs na organização (NAKAMURA; GEUS, 2007).

Whitman; Mattord (2012) conceituam firewall como um dispositivo responsável por separar seletivamente o fluxo de informação dentro e fora da organização, pode ser um dispositivo de computação ou configurado em um computador capaz de permitir ou impedir acessos onde as regras são implementadas. São normalmente dispostos em barreiras de segurança atrás ou como parte de um gateway. Os autores ponderam que existem vários tipos de firewall, desde filtragens de pacotes, proxy, níveis de aplicação e são geralmente classificados de acordo com o tipo de informação que tem a capacidade de filtrar.

Firewalls podem ser considerados Gateways seguros conforme a norma ABNT NBR 17799 (2005) cita, sendo conveniente a utilização desse componente para filtrar o trafego entre domínios e efetuar bloqueios necessários para a segurança da rede.

2.14.3. Os softwares maliciosos e o uso de antivírus

Medidas de proteção devem ser implementadas para prevenir o acesso de softwares maliciosos no sistema da organização, conforme Beal (2005, p. 97):

> O problema com softwares maliciosos se estende para muito além dos relacionados ao download de anexos contaminados por usuários de correio eletrônico. Mesmo discos de distribuição de software originais de fabrica ou produzidos por um parceiro confiável podem conter vírus, bombas logicas e cavalos de troia, a equipe de tecnologia não tem como inspecionar esses programas para averiguar e existe ou não algum código malicioso presente.

A norma ABNT NBR 17799 (2005) estabelece alguns pontos importantes para a detecção de códigos maliciosos:

- Proibição de softwares não autorizados
- Proteção contra importação de arquivos e softwares, externos ou não
- Analises críticas para detectar a presença de arquivos e softwares não autorizados
- Utilizar aplicações para detecção de softwares maliciosos e manter essas aplicações atualizadas.
- Definir responsabilidades
- Manter-se atualizado quanto a novos códigos maliciosos detectados pelo mundo
- Conscientizar os usuários sobre códigos maliciosos utilizando materiais atualizados e de fonte segura.

Para prevenir a ação de códigos maliciosos, vírus, dentre outros é essencial a presença de um bom antivírus, pois o mesmo ajuda a impedir o ataque desses códigos mantendo uma análise periódica dos arquivos detectando mudanças inesperadas, analise de base de dados de vírus para saber se existe algo parecido no ambiente de instalação.

2.14.4. Mensagens e correio eletrônico

As mensagens eletrônicas correspondem a uma parcela significativa nas vulnerabilidades de segurança da informação. O tratamento desse meio de comunicação é diferente do dado à segurança física de documentos, a vulnerabilidade nesse caso é bem maior. Em muitos casos o tratamento deve ser dado de uma forma remetente e receptor, pois os tratamentos

normais de rede não são suficientes para barrar uma possível adulteração de um documento durante o seu trajeto.

Em casos onde a situação exige, ou seja, onde os impactos causados por corrupção aos conteúdos transportados podem causas sérios danos organização, como e-mails com mensagens confidenciais ou transferência eletrônica de fundos, é imprescindível a aplicação de métodos de proteção mais eficazes, como é o caso da criptografia e assinatura digital, por exemplo. (BEAL, 2005).

A norma ABNT NBR ISO/IEC 27002 (2013) cita algumas diretrizes importantes em relação a política de envio de mensagens por meio eletrônico, são eles:

- Proteção das mensagens contra acesso não autorizado, alteração ou não aplicação do serviço.
- Garantir endereçamento de transporte correto.
- Confiabilidade e disponibilidade.
- Aspectos legais
- Formalização e aprovação para serviços públicos, como mensagens instantâneas e compartilhamento de arquivo.
- Autenticação com alto nível de controle.

Outra recomendação para o uso correto de correio eletrônico é citada pelo site Serasaexperian.com.br, como por exemplo.

- Leitores de e-mail sempre atualizados.
- Desativar a visualização via HTML.
- Desativar a execução de anexos automaticamente.
- Desativar a execução de JavaScript e java.
- Antivírus atualizando automaticamente.

A transferência de informações contempla a necessidade de se estabelecer políticas de segurança que visem a proteção da informação contra copias, interceptações, modificações,

destruição, proteção contra códigos maliciosos, uso correto de informações com anexos, da responsabilidade de colaboradores e terceiros que possam comprometer a organização, o uso de técnicas de criptografias, normas de exclusão e retenção da informação, restrições ligadas a retransmissão automática de mensagens, a conscientização referente a utilização correta dos canais de comunicação e requisitos legais referente aos serviços de transferências de informação (ABNT NBR ISO/IEC 27002, 2013).

2.14.5. Mídias removíveis

As mídias removíveis são componentes presentes na PSI devido ao seu alto risco para a organização, vazamentos, perdas, fraudes, vírus são alguns dos fatores que fazem desses equipamentos fortes instrumentos de vulnerabilidade para a segurança da informação. Devido a esses fatores vem a necessidade de prevenção contra divulgação, modificação, repasse e destruição da informação armazenada. “As mídias magnéticas como discos, fitas, DVDs/CD, etc. e documentações devem ser protegidos contra ameaças por interrupções, interceptação, modificação e fabricação. ” (COELHO, et.al, 2014, p. 118).

A norma ABNT NBR ISO/IEC 27002 (2013) cita diretrizes importantes para o correto controle das mídias, tais como a destruição de conteúdos inutilizados, autorização para retirada de mídias da organização, proteção para guarda desses equipamentos, utilização e técnicas de criptografias quando a informação for de cunho sigiloso e ofereça grande risco a organização, a monitoração das informações transitadas.

Também é muito importante para organização manter o correto controle de descarte dessas mídias, fatores importantes como a destruição ou incineração de componentes inutilizados, documentação das mídias destruídas para fins de auditoria, escolha de organizações que tenham experiência na coleta desse tipo de equipamento para descarte, dentre outros. (ABNT NBR ISO/IEC 27002, 2013).

2.14.6. Propriedade intelectual

Diz respeito à propriedade intelectual, todos os ativos que possuam direitos autorais e também propriedades industriais. A segurança desses ativos de necessita controles bem definidos para esse fim. Para a segurança da informação eles dizem respeito, principalmente, ao

cumprimento das leis, aos contratos firmados, aos direitos regulamentados e a outros deveres relacionados aos ativos com características intelectuais.

São incluídos no controle de propriedade intelectual os direitos a softwares ou documentos, projetos, marcas, patentes e licenças de software e códigos. Alguns produtos, como softwares são fornecidos sob licença, com restrições especificas, então o controle é executado de acordo com o que o contrato explica, as violações de direitos de propriedade intelectual podem acarretar processos criminais e ações legais contra a organização (ABNT NBR ISO/IEC 27002, 2013).

Beal (2005, apud Santos, 2001, p.151) destaca que:

> Ao se falar em propriedade intelectual pode se destacar duas categorias distintas: propriedade industrial e direitos autorais. A primeira categoria, da propriedade industrial, compreende as invenções, as marcas registradas e os desenhos industriais. Do outro lado, os direitos autorais estão compreendidos no campo da literatura e das artes e podem ser expressos em diferentes formas: através de palavras, símbolos, músicas, quadros, objetos tridimensionais, ou através de combinações deles. As leis de proteção ao direito autoral regulam trabalhos literários (livros, poemas, contos...), músicas coreografias, artísticos (pintura, escultura, desenho...), fotográficos, audiovisuais (filmes, desenhos animados, peças de teatro, programas de televisão ...), além de mapas e desenhos técnicos.

De acordo com a norma ABNT NBR ISO/IEC 27002 (2013), podem ser considerados alguns controles que visam proteger aos ativos que contenham propriedade intelectual, o uso legal de softwares e de ativos de informação, aquisição de softwares originais, reconhecer e monitorar os ativos, arquivar as provas em relação às aquisições efetuadas de produtos que contenham propriedade intelectual, não extrapolar o número de licenças por usuário, instalar somente softwares originais com autorização e, manter o direito de propriedade intelectual, acima de tudo.

2.14.7. Controle de acesso

O controle de acesso tanto para o ambiente físico ou lógico e concessão de direitos de acesso é um ponto importante para a política de segurança da informação, nesse ponto são criadas as diretrizes necessárias para preservação e controle dos ativos de informação na organização. Possibilita alcançar bons objetivos quanto a confidencialidade, integridade e disponibilidade da informação.

> [...] pode se considerar que o acesso é a habilidade de realizar algo com recursos computacionais e a autorização e a permissão dada direta ou indiretamente pelo sistema ou pelo dono do recurso para a utilização do mesmo. A autenticação é a responsável pela garantia de que o usurário é realmente quem ele declara ser. O controle de acesso logico, designado ao controle realizado sobre as informações referente aos recursos computacionais, cuidando do acesso aos diversos níveis existentes. (NAKAMURA; GEUS, 2007, p. 375).

Nakamura; Geus (2007) citam também algumas responsabilidades do controle de acesso lógico:

- Proteger os ativos contra modificações ou utilização sem autorização.
- Garantir a integridade e a disponibilidade, ou usar restrições necessárias.
- Manter sigilo das informações.

É conveniente a implementação de uma política devidamente documentada a respeito do tema. É necessário identificar os pontos a se liberar e bloquear, onde o proprietário do ativo será responsável pelas regras de controle analisando e, concedendo direitos e restrições. O objetivo é garantir que a política de segurança da informação seja preservada e os acessos sejam concedidos de acordo com o perfil de cada usuário. É conveniente que sejam considerados os controles de acesso físico e lógico conjuntamente e, que a política implementada seja divulgada aos colaboradores e aos demais envolvidos de forma direta e indireta na organização (ABNT NBR ISO/IEC 27002, 2013).

2.14.8. Serviços terceirizados

É imprescindível que medidas sejam tomadas quanto ao acesso de terceiros logicamente e fisicamente a organização, medidas essas que tem por objetivo evitar incidentes de segurança da informação, procedimentos implementados para reduzir a vulnerabilidade nas operações efetuadas por terceiros interno e externamente, controles que podem ir desde registros de acesso físico a canais criptografados para acesso lógico (MONTEIRO, 2009).

Quanto as informações providas de terceiros que participem direta ou indiretamente da organização, é importante que sejam devidamente classificados e rotuladas de acordo com o seu nível crítico e de sensibilidade do ativo, é importante manter o compartilhamento seguro das informações, cuidando com a rotulação de ativos de terceiros e tomando o devido cuidado com o armazenamento da informação (ABNT/CB, 2012).

A norma ABNT NBR ISO/IEC 17799 (2005) fala da importância do controle de entrega efetuado por terceiros, objetivando a continuidade do negócio e o serviço justo executado pela mesma. Também é mencionado a questão de monitoramento dos serviços realizados por terceiros, como nível de desempenho, conscientizar os terceiros referente a PSI implantada na organização. A norma menciona também importância de escolher um profissional ou equipe capacitada para atender os serviços terceirizados objetivando a regulamentação e o acompanhamento referente às responsabilidades dos terceirizados junto à organização.

3. METODOLOGIA DA PESQUISA

3.1. Metodologia e levantamento de dados

Conforme Marconi e Lakatos (2003) mencionam, a pesquisa é sistêmica e permite mensurar novos dados. A pesquisa é um procedimento formal com uma mentalidade reflexiva e um cunho científico que permite a descoberta parcialmente da verdade. Os autores expõem os passos para o desenvolvimento de uma pesquisa como:

a. Seleção de tópicos ou problema para a investigação.
b. Definição e diferenciação de um problema
c. Levantamento e hipótese do trabalho
d. Coleta, sistematização e classificação dos dados
e. Relatório do resultado da pesquisa

Os levantamentos das informações utilizadas nessa pesquisa foram feitos em uma organização do sistema financeiro, utilizando os métodos a seguir:

Pesquisa bibliográfica: para efetuar a fundamentação teórica em questão, fez-se a opção pelo método da pesquisa bibliográfica. Conforme MARCONI e LAKATOS (2003), a pesquisa bibliográfica ou pesquisa de fontes secundárias abrange todo material público em relação à pesquisa efetuada, desde publicações, boletins, jornais, revistas, livros, etc, tendo por finalidade colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou filmado sobre determinado assunto.

Pesquisa documental: Para aprofundar o estudo do projeto de política de segurança da informação implantado na organização, foi necessário efetuar uma pesquisa documental, cedido pela organização e obedecendo a sua política de segurança e ética. A pesquisa documen-

tal pode ser feita através de documentos públicos ou particulares e utilizada conjuntamente com a pesquisa bibliográfica, uma vez que ela também lida com fontes documentais, tem por característica a fonte de dados restrito a documentos, escritos ou não, constituindo o que se chama de fonte primária. (MARCONI; LAKATOS, 2003)

Entrevista: para fins de entendimento da política da organização pesquisada, fez-se necessário a utilização de entrevista, efetuada de forma não estruturada e informalmente, permitindo assim, explorar mais amplamente as questões abordadas na pesquisa. (MARCONI; LAKATOS, 2003).

A entrevista semiestruturada ou não estruturada tem por característica o uso de poucas questões deixando o entrevistado mais à vontade em colocar suas opiniões quando necessário. Tem como vantagem a flexibilidade na obtenção das informações, é uma entrevista mais universal, atingindo de maneira mais fácil vários segmentos da população e é eficaz a obtenção de dados mais profundamente (MARTINS; BARBA).

Questionários: foram utilizados questionários encaminhados aos colaboradores e ao gestor de SI, com o objetivo de coletar informações referentes ao conhecimento e prática da política de segurança da informação implantada na organização. Para uso desses questionários foram utilizadas técnicas conforme MARCONI; LAKATOS (2003), utilizando o método avaliativo, onde o julgamento é emitido através de escalas de grau de intensidade e as respostas indicam um grau crescente ou decrescente de acordo com a intensidade empregada.

O objetivo geral da pesquisa foi analisar criticamente e o projeto de PSI da organização. Marconi e Lakatos (2003) citam que a pesquisa qualitativa "é o conteúdo interno do processo de desenvolvimento, da conversão e das mudanças quantitativas em mudanças qualitativas".

3.2. A organização

A organização analisada atua na área financeira como banco cooperativo, foi fundada em meados de 1989, atuando em 17 municípios catarinenses, possui 150 funcionários e geograficamente está distribuída em 19 pontos chamados de agência e 1 ponto principal chamado

de Sede Administrativa. Essa pesquisa foi realizada na sede da empresa localizada no município de Turvo – SC, no sul do estado de Santa Catarina.

Fisicamente, a Sede Administrativa está dividida em um prédio de três andares com média de 400m² de área em cada andar, comportando assim o ambiente administrativo, comercial e tecnológico. Cada agência possui em média 300m² comportando o ambiente comercial e tecnológico. Ao todo a organização possui 274 computadores distribuídos em todos os setores organizacionais, sendo utilizados diretamente ou indiretamente.

Logicamente, a organização possui um sistema virtualizado utilizando a ferramenta VMware, utiliza sistema AD – Active Directory interligando a organização ao centro de processamento de dados. Quanto à distribuição de rede, a organização utiliza sistema de VPN para interconectar a organização ao centro de processamento de dados.

4. ANÁLISE

4.1. A implantação da PSI na organização

O processo de implantação da PSI na organização começou a ganhar força quando a central de onde a organização é membro, conforme explicado na METODOLOGIA, sentiu a necessidade de implantar o projeto de segurança da informação em suas singulares, pensando no presente e no futuro da organização, assim como na correta estratégia de negócio que a PSI viria a oferecer. Nesse ponto, mais precisamente em meados de 2011, o projeto de segurança da informação da organização citada começou a ser implementado.

Dentro do seu ramo de atividade, constata-se, por meio desse estudo, que a organização pesquisada segue algumas diretrizes de segurança da informação, porém, esses processos não são devidamente documentados e, consequentemente, não monitorados corretamente. Por exemplo, o controle de acesso existe, porém em certos momentos há falhas e liberações indevidas, o sistema de CFTV fazia o monitoramento necessário, porém em certos problemas ocorriam e não eram detectados, o compartilhamento de senhas também era um fator de exemplo de como a falta de diretrizes e de uma PSI causavam problemas para a organização objeto da pesquisa.

De acordo com a entrevista, constata-se que a organização escolheu os seus gestores de SI, que ficaram encarregados de participar dos treinamentos propostos, adequar a PSI e implantar a mesma na organização. Eles foram submetidos a treinamentos, passando pela análise de risco e vulnerabilidade, política de segurança da informação e continuidade do negó-

cio, com o intuito de ganharem conhecimento necessário para trazer a implantação da política para a sua organização de origem.

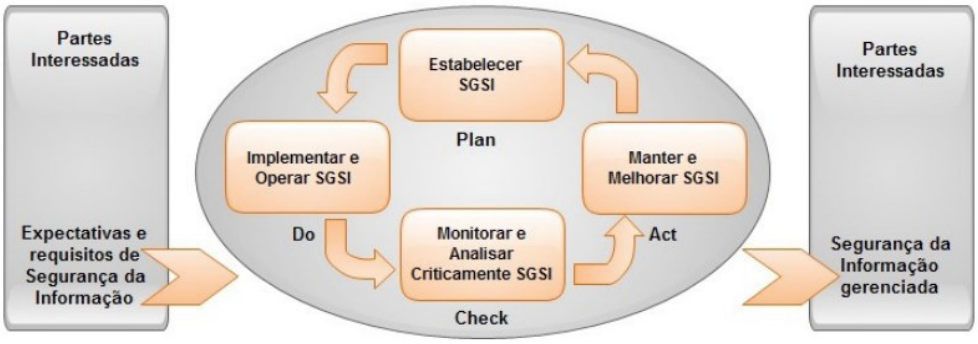

Figura 4. Processos PDCA para gestão da segurança da informação
Fonte: ABNT NBR ISO/IEC 27001 (2006)

4.2. Processo de treinamento

Para o processo de treinamento foi escolhido, em uma gama de empresas de consultoria, uma em questão, que ficou responsável pelo treinamento dos gestores de SI. Essa empresa criou um cronograma de treinamentos, dividido em 8 encontros de 2 dias cada, durante o período de 1 ano. Nesse período, foram efetuados treinamentos referentes aos processos de implantação da PSI, relatados nas próximas seções desse trabalho. Essa mesma empresa ficou responsável pela consultoria direta na organização e, também, pela auditoria aplicada anualmente em cada unidade.

4.3. Aplicação da análise de vulnerabilidade

A análise de vulnerabilidade na organização se dá a partir da identificação dos recursos de hardware, software e de serviços, com o objetivo de levantar subsídios suficientes para identificar os requisitos de confiabilidade, integridade e disponibilidade. Dentro da análise buscou-se identificar as várias classificações de vulnerabilidades, desde físicas, naturais, hardware, software, humana e de organização. Nesse momento, foram então implementadas as técnicas necessárias para a identificação e gestão das vulnerabilidades da organização.

4.3.1. Buscando e identificando as vulnerabilidades

Essa fase também conhecida como Coleta de Vulnerabilidades ou Coleta de Informações é o processo de utilização de métodos necessários para levantar quais são as vulnerabilidades existentes no ambiente, qual o grau de risco que elas oferecem e qual a melhor maneira de tratar as mesmas. Por meio da coleta das vulnerabilidades foi possível criar as diretrizes necessárias para os próximos passos do projeto de PSI da organização. No que diz respeito a essa questão foram seguidos os seguintes passos:

- Para base de vulnerabilidades foi utilizado o padrão CVE, que conforme cve.mitre.org (2016), pode ser considerado um dicionário de vulnerabilidades que tem por objetivo padronizar os tipos de vulnerabilidades nos ambientes computacionais e de redes;
- Para efetuar a coleta das vulnerabilidades sistêmicas e de redes foi utilizada a ferramenta NESSUS. A ferramenta NESSUS pode ser utilizada para fazer a varredura da rede em busca de possíveis vulnerabilidades. Com o levantamento desses dados é possível criar práticas de correção e prevenção relacionadas a esses fatores;
- O próximo passo foi a confecção e preenchimento do *checklist*, utilizando o sistema de banco de dados Microsoft ACCESS para locação dos processos de TI, nesse quesito foram levados em consideração alguns processos, tais como:
  - ✓ Procedimentos operacionais
  - ✓ Responsabilidades operacionais
  - ✓ Planejar e aceitar os sistemas
  - ✓ Códigos maliciosos e móveis
  - ✓ Backups
  - ✓ Segurança de rede
  - ✓ Troca de informações
  - ✓ Utilização de mídias
  - ✓ E-commerce
  - ✓ Monitoramento

O passo seguinte foi a análise do ambiente físico da organização levando-se em conta as barreiras de segurança física. Para esse quesito foram levados em conta algumas barreiras, tais como:

- Planejamento: funções e responsabilidades, treinamento, inspeção, controle de incidentes.
- Ambiente externo: iluminação, portões e grades, detecção de invasores, áreas restritas, equipamentos de TI, controle dos ativos, armários e gavetas, dentre outros.
- Controle de acesso: identificação, acessos, chaves e cadeados, dentre outros.
- Controles gerais: sistema de monitoramento por câmeras e CFTV, vigilância patrimonial.

Em seguida, foram verificadas as questões voltadas à política de usuários, onde foram analisados quesitos, desde controles de acesso até as notificações, conforme demonstrado abaixo:

- Contas e senhas
- Malwares, vírus e spans
- Gerenciadores de e-mails
- E-mails
- Navegadores
- Sistema de troca de mensagens (chats)
- Compartilhamento de sistemas e arquivos
- Backups
- Transações em geral
- Uso de dados pessoais na navegação web
- Cuidado com armazenamento de dados em disco
- Navegação wireless e bluetooth
- Notificação de incidentes

4.4. Aplicação da análise de risco

Quanto à aplicação da análise de risco, a empresa adotou o método de *checklist*, onde o projeto destacou os conceitos fundamentais de risco tratando a identificação dos Ativos, Ameaças e Vulnerabilidades para ganhar subsídios suficientes para a criação da Análise de Risco e suas consequências. Com a análise devidamente desenvolvida o próximo passo foi o tratamento dos riscos de acordo com o seu grau de prioridade.

4.4.1. Identificação e avaliação dos ativos

Para a identificação e avaliação dos ativos foram levados em consideração os requisitos de Confidencialidade, Integridade e Disponibilidade, obedecendo a uma escala para a avaliação, conforme apresentado no quadro 2:

GRÁU NOMINAL	GRÁU NUMÉRICO
1 – CRÍTICO	4
2 – ALTO	3
3 - MODERADO	2
4 – BAIXO	1
5 - NULO	0

Quadro 2 - Classificação dos ativos

Fonte: dados da empresa

4.4.2. As ameaças para a organização

Conforme explorado no capítulo Análise, Avaliação e Tratamento de Risco em Segurança da Informação, as ameaças são consideradas eventos intencionais ou não, que exploram as vulnerabilidades do ambiente. As ameaças têm a característica de tentar quebrar a confidencialidade, a integridade e a disponibilidade dos ativos, o conceito de confidencialidade, integridade e disponibilidade foram abordados no capítulo, Conceituando Segurança de Informação.

Durante o processo as ameaças foram classificadas como:

- Externas
- Internas
- Intencionais
- Acidentais

O grau de exposição das ameaças seguiu o critério conforme escala apresentada no quadro x a seguir:

GRÁU NOMINAL	GRÁU NUMÉRICO
1 – CRÍTICO	4
2 – ALTO	3
3 - MODERADO	2
4 – BAIXO	1
5 - NULO	0

Quadro 3 - Definição do grau das ameaças

Fonte: dados coletados junto à organização

4.4.3. A avaliação das vulnerabilidades para organização

A avaliação das vulnerabilidades ocorre de acordo com o seu grau de deficiência seguindo a mesma escala apresentada para as ameaças e a identificação dos ativos conforme apresentado no quadro número 4, a seguir:

GRÁU NOMINAL	GRÁU NUMÉRICO
1 – CRÍTICO	4

2 – ALTO	3
3 - MODERADO	2
4 – BAIXO	1
5 - NULO	0

Quadro 4 - Definição do grau de vulnerabilidades

Fonte: dados coletados junto à organização

Para o desenvolvimento do checklist foram implementados critérios para avaliação de acordo com o seu nível de prioridade:

- Atendimento total
- Atendimento parcial
- Atendimento informal
- Não atende
- Não relevante

A utilização dos critérios e checklist tiveram como objetivo buscar o grau de deficiência dos ativos, avaliando assim as boas práticas, ou seja, como é feito o tratamento do ativo avaliado. Em relação às tecnologias, a avaliação também seguiu critérios de como os controles sobre os ativos são utilizados. Todos esses dados juntos dentro de um sistema de checklist passaram por uma avaliação automática tornando possível saber o grau de risco de cada ativo avaliado. Todo o preenchimento do checklist referente à análise de risco foi feito através do banco de dados ACCESS da Microsoft.

4.4.4. Calculando os riscos encontrados

O Cálculo do risco obedeceu aos critérios de medição do grau de risco e de impacto apresentado, anteriormente, formando assim uma matriz de risco, responsável por calcular o grau de cada ativo inserido no checklist. A base de cálculo para o risco segue o parâmetro descrito a seguir:

A seguir no quadro 5 está a Matriz de Risco utilizada para o cálculo de risco dos ativos:

MATRIZ DE RISCO						
IMPACTO	PROBABILIDADE	1-CRITIA	2-ALTA	3-MODERADA	4-BAIXA	5-NULA
	1-CRÍTICA	4	3,5	3	2,5	2
	2-ALTA	3,5	3	2	2	1,5
	3-MODERADA	3	2,5	1,5	1,5	1
	4-BAIXA	2,5	2	1	1	0,5
	5-NULA	2	1,5	0,5	0,5	0

Quadro 5 - Matriz do Risco

Fonte: dados coletados junto à organização

4.4.5. Efetuando o tratamento de riscos

O objetivo nesse ponto foi procurar as vulnerabilidades que ofereceriam maior risco para o tratamento adequado desse ativo de informação. Foi definido, então, a maneira como o risco deveria ser tratado, o risco pode ser modificado, retido, evitado ou compartilhado.

4.4.6. Definição do plano de ação

Nesse ponto, foram definidos os planos de ações voltados aos riscos identificados. Por exemplo, escolhendo a opção APLICAR CONTROLE podem ser definidas ações voltadas a esse processo, como incluir uma melhoria ou não tomar nenhuma ação.

Os controles a serem aplicados na organização seguiram a norma ABNT ISO/IEC 27001 e foram utilizados na aplicação da política, como, por exemplo, a própria política de segurança da informação, a organização da segurança da informação, a gestão dos ativo, a segurança em recursos humanos, a segurança física e lógica do ambiente, o gerenciamento da comunicação, controles de acesso, aquisição, desenvolvimento e manutenção de sistemas de

informação, a gestão de incidentes e a continuidade do negócio (ABNT NBR ISO/IEC 27001, 2013).

4.5. A aplicação da PSI na organização

O primeiro passo para implantação da política de segurança da informação na organização foi demonstrar os conceitos de PSI apontando o que a mesma determina, suas regras, a gerência da informação, sua amplitude e simplicidade, da necessidade de revisões contínuas e da busca pelo apoio da alta diretoria. Ainda em relação aos conceitos básicos, são colocadas algumas diretrizes para caracterizar o que a PSI define, como a definição de objetos, responsabilidades, punições, escopo e regulamentos.

4.5.1. Política de ordem específica

Foram conceituados os temas de ordem especifica para a política de segurança da informação, que trata de questões detalhadas, por exemplo, um determinado serviço utilizado por determinado usuário e quais a diretrizes devem ser tomadas quanto a esse serviço. Ex: e-mail, chats, dispositivos móveis.

4.5.2. Política de ordem de sistemas

Nesses conceitos foram definidos os temas de ordem direcionados aos sistemas, como sistemas operacionais, banco de dados, softwares específicos, dentre outros. Para esses sistemas foi necessário mostrar como os mesmos devem estar de acordo com a política da organização.

4.5.3. Comitê de segurança da informação

Durante o processo de implantação da PSI uma das diretrizes foi a criação de um comitê de segurança da informação, integrado por 5 pessoas, representantes de todos os setores da organização. O objetivo principal desse comitê foi discutir a definição das políticas para compor o documento.

Com a representação de um gestor da política de segurança da informação, nesse caso um membro de TI, conjuntamente, com os integrantes dos outros setores, o comitê de segu-

rança seguiu orientações para a criação de regras da PSI, coerentes com o ambiente organizacional, na tentativa de não criar regras genéricas, discriminatórias, inseguras, ilegais e inviáveis, ou seja, que as regras criadas para o documento deveriam seguir as diretrizes de segurança da informação da forma mais coerente possível.

4.5.4. Estrutura da Política de Segurança da Informação

4.5.4.1. Introdução

4.5.4.1.1. Apresentação

A apresentação visou mostrar de forma geral qual a importância do documento descrevendo as condutas adequadas para manipulação dos ativos de informação. Também teve por objetivo demonstrar para quem a política foi destinada, no caso todos os usuários em geral e também aos recursos de informação da organização.

4.5.4.1.2. Objetivos

Mostrar quais os objetivos da PSI para organização, do comportamento dos usuários e ativos, da conscientização quanto ao uso dos ativos de informação e das ações e responsabilidades necessárias para gerencia da informação.

4.5.4.1.3. Declaração da diretoria

Essa declaração visou demonstrar o engajamento da diretoria da organização para com a segurança da informação. Nesse campo os próprios diretores deram a sua declaração de ciência da política visando garantir os princípios de confidencialidade, integridade e disponibilidade comprometendo-se na implantação, continuidade e auditoria da PSI.

4.5.4.1.4. Documentação relacionada

Esse campo visou demonstrar que a PSI está relacionada com outros documentos de conduta da organização e que ela é um complemento das políticas já utilizadas no processo de convivência no ambiente organizacional.

4.5.4.1.5. Definições

O objetivo das definições foi identificar teorias descritas no documento que pudessem de alguma forma não ser entendidas pelos leitores, nesse caso buscou-se falar desses temas referenciando as normas ABNT necessárias.

4.5.4.1.6. Autores

Foram informados da autoria do documento. Como descrito anteriormente, a responsabilidade pelo desenvolvimento do documento ficou a cargo do comitê de segurança da informação, conjuntamente, com a assessoria de uma empresa especializada. Também foi destacada a responsabilidade do comitê de segurança quanto à aplicação e manutenção da PSI dentro da organização.

4.5.4.1.7. Divulgação/Distribuição

A divulgação tratou principalmente de demonstrar que a PSI deve ser divulgada a todos os usuários da organização e também da responsabilidade do comitê de segurança da informação por essa divulgação. Também deixou clara a responsabilidade de se manter um programa de conscientização contínuo, voltada à política, divulgando notícias e informações sobre boas práticas, dentre outras informações.

4.5.4.1.8. Versão e revisão

Campo responsável por mostrar a versão do documento e, o período de homologação da mesma. Também destacou a necessidade de revisão do documento e o desenvolvimento de uma versão mais atual, caso ocorressem mudanças em ativos de informação, criação de novos ativos ou dentro do período de 24 meses, que é quando uma nova versão deve ser desenvolvida, atualizando as diretrizes da PSI.

4.5.4.1.9. Manutenção da segurança da informação

A manutenção de segurança demonstrou quais as diretrizes em relação ao tema devem ser tomadas pela organização para o efetivo controle e manutenção da PSI:

- Demonstrou as responsabilidades do comitê de segurança da informação em relação à gestão da segurança nos aspectos físicos e lógicos. Destacou a responsabilidade do

coordenador de TI quanto à responsabilidade pela segurança lógica e física do ambiente;

- Destacou a necessidade de manter um plano de continuidade do negócio sob responsabilidade do comitê de segurança da informação e das necessidades de criação de planos preventivos e corretivos para a organização;

- A necessidade de manter um sistema de classificação dos ativos também foi destacada, e da responsabilidade do comitê de segurança da informação em relação ao sistema de classificação. Já a classificação, propriamente, dita ficou sob a responsabilidade do gestor de cada setor. Foi destacada também a conduta correta em relação à classificação, mantendo foco nos aspectos legais e de confidencialidade de ativos que demonstrassem essa característica;

- A necessidade da análise de risco também foi destacada, sendo estabelecida a periodicidade de pelo menos 18 meses para cada analise. Foi destacado nesse ponto as responsabilidades quanto a segurança lógica e física ficando a cargo de cada coordenador, lógico e físico efetuarem a análise.

- Outro ponto importante destacado foi o treinamento e conscientização sobre a PSI dando responsabilidade para o comitê de segurança da informação, gestão de pessoas e coordenador de TI, quanto a aplicação dos treinamentos de conscientização. Também foi destacada a questão dos novos colaboradores, que devem passar por treinamento durante o processo de contratação.

- O último ponto deu destaque à auditoria interna, responsabilizando o setor de TI pela gerência das auditorias. Foram delimitados prazos para esse processo, sendo de 6 meses para auditorias internas e de 18 meses para as auditorias externas.

4.5.5. Segurança lógica

4.5.5.1. Acesso à internet

Quanto ao acesso à internet foram destacados pontos quanto às boas práticas de uso e às diretrizes necessárias para controle do acesso pelos usuários:

- **Monitoramento:** os conteúdos acessados com monitoramento através de firewall.

- **Controle de acesso:** bloqueios de acesso a sites utilizando controles específicos.

- **Autenticação de usuário:** os acessos à internet feitos por usuários autenticados.

- **Conteúdos imorais e ilícitos:** conscientização para o não acesso desses conteúdos.

- **Acesso a visitantes:** controle de acesso autorizado para visitantes.
- **Dispositivos móveis:** destaque para não utilização de dispositivos moveis nas dependências da organização
- **Uso liberado de internet:** somente para fins profissionais e com autorização do responsável de segurança lógica. Destaque para a não utilização de internet fora do horário de expediente.

4.5.5.2. Rede interna

Para o acesso a rede interna foram criadas diretrizes específicas referente a sua utilização:

- **Monitoramento:** trata do direito da organização em monitorar os acessos à rede
- **Horário de expediente:** trata do acesso à rede corporativa somente em horário de trabalho.
- **Autenticação de usuário:** trata do acesso à rede interna somente com autenticação.
- **Dispositivos pessoais:** trata das conexões de dispositivos pessoais, como notebooks, smartphones, tablets na rede interna, na qual, segundo a PSI, ficou proibido o acesso.
- **Rede de visitantes:** trata do acesso à rede por visitantes o qual deve ser feito apenas por pessoas externas, devidamente, autorizadas e, para fins profissionais. Esse item trata ainda a questão de monitoramento da rede e da desautorização de qualquer visitante a acessar a rede interna da organização, ou seja, qualquer informação interna necessária deve ser passada, somente, por usuários internos autorizados.

4.5.5.3. Armazenamento

Tratou do uso adequado dos locais de armazenamento lógico, como discos, pastas de setor e pastas de usuários dentre algumas diretrizes para restrição de armazenamento:

- **Armazenamento adequado:** tratou do armazenamento adequado das informações corporativas nos locais previamente definidos, locais esses com segurança de Backup e replicação de informação, como são os casos dos servidores de arquivos.
- **Informações pessoais:** tratou das informações pessoais, demonstrando diretrizes para o armazenamento adequado das informações relacionadas ao trabalho e a restrição contra informações pessoais não relacionadas ao trabalho.

- **Uso de dispositivos móveis:** tratou da questão de uso de dispositivos como notebooks corporativos, porém conectados à rede armazenamento de dados e das responsabilidades pelo uso dessas ferramentas.

- **Compartilhamento de informação:** esse item tratou a questão do compartilhamento de arquivos na organização demonstrando as diretrizes necessárias para as boas práticas, como o não compartilhamento de arquivos entre usuários exigindo que seja feito através do servidor de arquivos; da responsabilidade do setor de TI em gerenciar os compartilhamentos de servidor; da responsabilidade do coordenador ou gestor de setor no compartilhamento que lhe compete. Também foram tratados, nesse ponto, questões relacionadas ao acesso público de informações que deve ser temporário e devidamente gerenciado.

- **Backup de informações:** quanto ao uso de backup a política explana o fato de que os usuários não devem efetuar backup por conta própria, ao contrário disso, o setor de TI é responsável pelo backup das informações armazenadas nos locais devidamente especificados.

4.5.5.4. As propriedades intelectuais

A propriedade intelectual é algo preocupante para as organizações e, para esse item, foram deliberadas diretrizes específicas para evitar e conscientizar aos usuários à respeito de:

- **Armazenamento:** quanto ao armazenamento foram criadas diretrizes restringindo o armazenamento de dados de música ou vídeos nas estações de trabalho assim como nas pastas de servidor de arquivo;

- **Softwares:** para garantir a não violação da propriedade intelectual foram deliberadas restrições quanto a instalação de softwares nas estações de trabalho, tanto com medidas aplicadas nas estações como com a conscientização dos usuários. A garantia de conformidade com as instalações ficou sob a responsabilidade do setor de TI. Somente esse setor teria autorização para instalação de softwares no ambiente corporativo.

- **Referências:** trata-se do uso de materiais, como fotos, vídeos, textos para uso corporativo como apresentações por exemplo, da importância de referenciar a autoria dos materiais.

4.5.5.5. Sistemas corporativos

Esse item tratou dos controles com os sistemas corporativos que a organização possui, das boas práticas e, das restrições necessárias para o uso desses sistemas, a saber:

Direito de acesso: trata dos direitos concedidos de acordo com os setores que a organização possui, ou seja, é uma segregação de funções através do sistema para que cada usuário tenha acesso somente ao que é de sua alçada. Esse ponto também tratou da revisão de acessos, impondo prazos, nesse caso de 12 meses, para a revisão dos direitos de acesso de todos os usuários e setores.

Autenticação de usuário: tratou da questão de autenticação de usuários através de login e senha para os sistemas corporativos e da importância do não compartilhamento de senhas para o correto andamento da política.

4.5.5.6. Utilização de e-mails

As diretrizes de uso de e-mails foram tratadas na PSI da organização com o objetivo de criar controles e conscientizar os usuários em relação ao uso dessa ferramenta:

- **E-mail corporativo:** tratou da conscientização demonstrando que os e-mails são monitorados. Também foi tratado o controle de envio e recebimento de e-mails de fora do ambiente corporativo, controle esse que objetiva bloquear esse envio e recebimento sendo liberado apenas para usuários devidamente autorizados.
- **E-mails não corporativos:** tratou da conscientização para o uso de e-mail exclusivamente para fins profissionais.
- **Cadastro de e-mails**: nesse caso foram traçadas diretrizes de conscientização para o não cadastramento de e-mails corporativos na web sem fins profissionais, por exemplo, em fóruns, sites de compras, dentre outros. Também foram conscientizados a não utilizar as contas de e-mails corporativos em dispositivos fora da organização.
- **E-mail pessoal**: tratou da questão de uso de e-mail pessoal no ambiente corporativo, uso esse permitido com devida autorização do gestor do usuário. Previamente a política conscientiza contra o risco de arquivos maliciosos que podem advir de e-mails pessoais, além de proibir o uso do e-mail pessoal para comunicação profissional.

4.5.5.7. Utilização de senhas

A utilização de senhas no ambiente corporativo certamente é um item preocupante para segurança da informação, para esse fim foram criados diretrizes de responsabilidade pela utilização das senhas na organização:

- **Responsabilidades**: tratou de demonstrar a responsabilidade das senhas, conscientizando de que as senhas são pessoais e intransferíveis, ou seja, não devem ser emprestadas nem compartilhadas com outros usuários.

- **Facilidade das senhas:** tratou da conscientização sobre como elaborar uma senha segura sem a utilização de dados pessoais ou sequencias simples, já que o objetivo da senha é justamente evitar qualquer tipo de acesso que seja o detentor da mesma.

4.5.5.8. Troca de mensagens

Dentro da PSI a organização específica tratou das diretrizes a respeito dos sistemas para troca de mensagens como Chats por exemplo, indicando os controles e instruções para a boa pratica de uso desses sistemas:

- **Sistema de troca de mensagens:** tratou diretrizes referente a homologação por parte da organização dos sistemas para troca de mensagens, conscientizando os usuários que somente sistemas desse nível poderiam ser utilizados para troca de mensagens.

- **Criação de contas:** tratou das responsabilidades pela criação e manutenção das contas para troca de mensagens, nesse caso o setor de TI ficou responsável por essa tarefa.

- **Monitoramento:** tratou da questão de monitoramento dos sistemas de troca de mensagens para fins de auditoria.

- **Utilização:** tratou a questão de uso da ferramenta, especificando o uso somente para fins profissionais, da proibição e controle para não cadastramento de contatos por usuários não autorizados e a limitação para uso externo somente para usuários também autorizados.

4.5.6. Segurança física

4.5.6.1. Gestão de segurança

A gestão da segurança visou criar diretrizes para a gerencia do ambiente físico focando na conscientização, inspeções e analise dos controles inerentes ao tema, conforme a PSI da organização.

- **Checklist:** tratou-se da criação de um checklist referente a segurança física contemplando os ativos a serem examinados, essa analise teve periodicidade estabelecida onde cada 4 meses deveriam ser realizados novas analises auxiliadas pelo checklist.

- **Conscientização:** outra diretriz para a gestão de segurança física foi o treinamento e conscientização para novos colaboradores.

- **Inventário de chaves:** tratou da implantação de um inventário de todas as chaves da organização, identificando os usuários e efetuando a manipulação e troca de chaves no ambiente físico.

- **Sistema de CFTV:** tratou das diretrizes referentes à vigilância de vídeo onde ficou definido o monitoramento em tempo real por empresa especializada. Ao mesmo tempo, foram implantadas diretrizes estabelecendo direitos para a organização manter monitoramento de todos, tanto no ambiente interno quanto externo, para fins legais.

- **Vigilância:** as diretrizes criadas impuseram a utilização de um checklist a ser seguido pelos responsáveis pela vigilância do ambiente físico.

- **Controles de segurança física:** contemplou o controle de porta e janelas prediais, com diretrizes apontando a importância de serem mantidas fechadas. A segurança externa, fora do horário de trabalho, também foi contemplada, especificando a necessidade de vigilância humana durante todo o período.

4.5.6.2. Ambiente de segurança

Na PSI da organização esse tópico foi criado para especificar todo o ambiente físico, desde o ambiente interno ao externo e, as diretrizes a serem seguidas de acordo com a política:

- **Ambiente externo**: foi destacada a necessidade de existir monitoramento vídeo 24x7. Também foi destacada a questão de iluminação que dever ser adequada para permitir o monitoramento humano dos ambientes.

- **Ambiente interno:** foram destacadas as diretrizes voltadas aos perímetros, como a prevenção de portas e janelas fechadas quando ninguém utilizar o recinto, necessidade de manter o recinto, devidamente, trancado, quando no fim de expediente, ou em horários dos intervalos. Foi destacado também a necessidade de monitoramento por vídeo do ambiente administrativo, pois é uma área também de circulação de terceiros onde também abordado a questão do arquivo morto que deve permanecer trancado.

- **Instalações:** foi dado destaque aos ativos que ficam em instalações, como documentos e equipamentos de processamentos de dados, com o objetivo de controlar o acesso somente para pessoas autorizadas, também foi dado ênfase para a prevenção contra sinistros ou catástrofes naturais.

4.5.6.3. Os controles

Os controles de acesso físico tratam das medidas necessárias para manter os ativos físicos protegidos na organização, para esse item foram criadas diretrizes referentes às políticas de acesso e autorizações:

- **Visitantes**: esse item tratou das medidas necessárias para o acesso de visitantes dentro das dependências da organização, diretrizes como o aceso somente com registro prévio identificado o período e o responsável por receber a visita, e a necessidade de o visitante estar identificado para poder adentrar ao ambiente.
- **Administrativo**: o setor administrativo da organização também teve diretrizes implementadas referente aos controles de acesso, como controles digitais com registro de log para acesso no ambiente, a restrição de cadastro apenas para usuários autorizados para acesso ao ambiente administrativo e a responsabilidade pela gestão do controle de acesso, nesse caso ficando a cargo do setor de TI da organização.
- **Controle de retirada de equipamentos**: esse item tratou das questões de retirada de equipamentos de tecnologia de informação das dependências da organização, delimitando a retirada somente pelo setor de TI, ou em caso de terceiros retirarem equipamentos, que esses sejam devidamente acompanhados e relacionados como responsáveis pela retirada, o motivo e a data da retirada e retorno do equipamento. Por fim tratou o fato de ser proibido a retirada de qualquer equipamento das dependências da organização para fins pessoais.
- **Retirada de documentos**: referente a retirada de documentos as diretrizes deram responsabilidades aos gestores de cada setor da organização, para que esses mantenham o controle de armazenamento e retirada dos documentos das dependências de seus ambientes físicos. Foi destacada a necessidade de se manter o registro de todos os documentos retirados com os devidos responsáveis.

4.5.6.4. Utilização de alarmes prediais

O uso de alarme predial foi um item voltado ao controle de segurança dos ambientes físicos da organização, onde foram implementadas diretrizes voltadas a responsabilidades e boas práticas para os usuários autorizados a utilizarem o controle:

- **Cadastro de senhas**: para esse item foram definidas as responsabilidades em relação ao cadastro e remoção das senhas de alarme, nesse caso ficando o setor de TI responsável pela tarefa, também foram implementadas diretrizes a respeito da periodicidade

de revisão dos cadastros de senha, nesse caso ficando no período a cada 6 meses para revisão dos cadastros.

4.5.7. Incidentes e punições

4.5.7.1. Das notificações e incidentes

Nesse ponto da PSI foram tratadas as questões relacionadas às notificações, que são as "denuncias" efetuadas referentes as boas práticas, aos controles, a gestão dentre outras questões que envolvam risco de incidente ou de evento prejudicial as informações da organização.

- **Denúncias:** a PSI deixa claro nesse ponto a necessidade de todos os envolvidos na organização efetuarem as notificações referente a incidentes que lhe tragam preocupações relacionadas a política implantada. Destaque também para disponibilização de um canal de denuncia garantido a confidencialidade da identidade de quem efetua a notificação.
- **Relevâncias:** a relevância do incidente define qual é o destino que ele deve tomar, caso a relevância seja alta o setor de TI, que é quem recebe as notificações deve repassar para comitê de segurança da informação, que reunidos e analisando o conteúdo darão o destino correto para fato, ou seja, definem a necessidade de algum tipo de punição.

4.5.7.2. Das punições

Sabe-se que a conscientização é o melhor passo para que o processo da PSI ocorra bem na organização, porém em alguns casos faz-se necessário aplicar algum tipo de punição para que o processo volte a ocorrer corretamente dentro das diretrizes criadas e documentadas.

Deliberações: esse ponto trata das responsabilidades em deliberar as punições, no caso ficando a cargo do comitê de segurança da informação auxiliados pelo setor de gestão de pessoas da organização.

Graus de punições: esse ponto mostra os graus de punições a serem executados de acordo com a análise efetuada pelo comitê de segurança da informação e gestão de pessoas. Foram definidos então cinco níveis conforme demonstrado abaixo:

- **Advertência informal:** para esse tipo de advertência ficou definido a chamada advertência verbal ou no máximo com o encaminhamento de uma mensagem auxiliando sobre as diretrizes criadas referentes ao incidente praticado.
- **Advertência formal:** a advertência formal está um nível acima da informal, com a necessidade de um documento de advertência devidamente assinado pelo praticante do incidente, onde ficou definido que para cada três advertências formais de um usuário o nível de punição aumenta.
- **Suspenção do uso:** essa deliberação trata da suspenção de direito ao uso ou acesso ao recurso, por exemplo, o acesso à internet, caso seja detectado o acesso a conteúdo imorais ou ilícitos para quem está devidamente autorizado a ter o acesso liberado, esse recurso pode ser imediatamente bloqueado caso seja deliberado durante a análise de punições.
- **Punições trabalhistas:** na punição trabalhista cabe uma análise mais profunda do incidente, essas punições podem acontecer quando o usuário retrocede ao erro após ter sido notificado formalmente ou dependendo da gravidade do incidente causado. A punição pode ocorrer imediatamente após a análise do comitê de segurança da informação conjuntamente com a gestão de pessoas da organização.
- **Outras punições:** as punições destacadas, anteriormente, são de cunho judicial. Caso analisado que o incidente causado fere a organização de forma que seja necessário acionar a justiça e que a punição seja a altura do incidente provocado, por exemplo, o roubo de uma informação de grande importância para a organização, há casos em que pode existir a necessidade de acionar as autoridades para proceder com punições no nível do incidente.

4.5.8. Aprovação da diretoria

A última parte da política de segurança da informação trata da declaração de ciência referente ao documento da PSI, devendo estar devidamente reconhecida, aceita e assinada pelos membros integrantes da alta administração da organização demonstrando o período de assinatura (data).

4.6. A continuidade do negocio

A última parte do projeto de PSI implantado na organização foi o desenvolvimento do plano de continuidade do negócio, tendo por objetivo auxiliar no desenvolvimento de práticas para evitar paradas e proteger os processos, também tendo por objetivo garantir a retomada rápida dos procedimentos organizacionais em caso de desastre.

4.6.1. Analise de impacto

Primeiramente foi estabelecida a base para a política de continuidade do negócio, a análise de impacto, que tem por objetivo escolher os processos considerados essenciais e analisar os impactos causados em caso de uma interrupção. Foram definidos durante esse processo alguns passos importantes como classificação dos processos, a identificação dos impactos, os requisitos de contingências, o nível máximo aceitável para interrupções e as dependências dos processos.

Também foram estipuladas questões importantes como a importância da aceitação da alta gestão da organização em relação à PCN e a definição de um responsável pelo processo. Para dar início ao projeto e aplicar os passos foi destacado a importância de reuniões, questionários e entrevistas voltados ao processo de implantação da PCN.

4.6.2. Processo essenciais

Quanto aos processos ou atividades essenciais o objetivo foi definir quais os mais importantes quanto ao fornecimento de produtos e serviços, identificando as suas caraterísticas de funcionamento normal e correto. Após essa identificação o objetivo foi efetuar a classificação do processo quanto ao seu grau critico, conforme apresentado no quadro 6:

PROCESSO	Processo 1	Processo 2	Processo 3
1 – Não considerável			

2 - Relevante			
3 - Importante			
4 - Crítico			
5 - Vital			

Quadro 6 - Classificação dos processos quanto a sua criticidade

Fonte: dados coletados junto à organização

Também foi apontada a necessidade de classificação dos níveis mínimos referentes a produtos e serviços para garantia que os mesmos possam permanecer em funcionamento, mesmo que não seja em sua carga total. Pontos de restauração também foram apontados, tendo por objetivo orientar a uma retomada aceitável dos processos, caso esses sejam interrompidos de alguma forma.

4.6.3. Definindo impacto

A avaliação do impacto, nesse caso, trata de como o processo seria prejudicial durante o seu tempo sem realizar as atividades que lhe competem. Nesse ponto foram definidos os tipos de impactos que podem ocorrer na organização, de ordem financeira, operacional e de imagem.

Outra definição importante para o processo de PCN, foi a IMA e o TOR:

IMA (Interrupção Máxima aceitável): tratou do período em que o impacto pode tornar-se altamente prejudicial.

TOR (Tempo objetivo de recuperação): tratou do tempo necessário para o processo ser iniciado novamente por inteiro ou em um estado de contingência.

A classificação do impacto ocorreu conjuntamente com a IMA, os impactos que ultrapassassem o valor da IMA deveriam ser classificados seguindo a tabela apresentada no quadro 7:

GRÁU NOMINAL	GRÁU NUMÉRICO
1 – CRÍTICO	4
2 – ALTO	3
3 - MODERADO	2
4 – BAIXO	1
5 - NULO	0

Quadro 7 - Classificação de impacto

Fonte: dados coletados junto à organização

4.6.4. Identificando as dependências

A identificação das dependências teve por objetivo associar os processos às suas respectivas dependências, por exemplo, um processo poderia estar ligado a um software, hardware ou às pessoas.

4.6.5. Formulário da PCN

Com o conceito devidamente implementado, o próximo passo foi desenvolver o formulário referente à PCN contendo a identificação dos processos, as métricas e as dependências dos processos. Esse formulário foi desenvolvido no ambiente ACCESS da Microsoft para posterior estudo das estratégias atuais e das estratégias para alcançar o objetivo da IMA.

4.7. Analisando criticamente a PSI da organização

A primeira análise refere-se à relação entre o projeto de PSI implantado e a pesquisa exploratória conforme demonstrado no *quadro 8*. O objetivo foi encontrar os fatores positivos e negativos no projeto de PSI da organização em comparação com a pesquisa bibliográfica efetuada. O *quadro 8* contempla os processos gerais para formação da política de segurança

da informação da organização. Foram considerados positivos quando também são apresentados pela literatura utilizada na pesquisa.

PROCESSOS	POSITIVO	NEGATIVO
1. IMPLANTAÇÃO		
1.1. Processo de implantação	X	
1.2. Escolha do gestor de SI	X	
2. PROCESSO DE TREINAMENTO		
2.1. Escolha de uma empresa de consultoria	X	
2.2. Perda do gestor de SI		X
3. ANALISE DE VULNERABILDIADES		
3.1. Processo de análise	X	
3.2. Base de dados de vulnerabilidade	X	
3.3. Coleta das vulnerabilidades	X	
3.4. Processos de TI	X	
3.5. Ambiente físico	X	
3.6. Gestão dos usuários	X	
3.7. Falta de engajamento dos usuários em responder aos questionamentos		X
3.8. Uso da ferramenta ACCESS		X
4. ANALISE, AVALIAÇÃO E TRATAMENTO DE RISCO		
4.1. Identificação e avaliação dos ativos	X	
4.2. Identificação das ameaças	X	
4.3. Avaliação das vulnerabilidades	X	

4.4. Calculo de risco	X	
4.5. Tratamento de risco	X	
4.6. Utilização da ferramenta ACCESS		X
4.7. Engajamento dos setores		X
5. CONTINUIDADE DO NEGOCIO		
5.1. Processo de continuidade do negocio	X	
5.2. Analise de impacto do negocio	X	

Quadro 8 - Processos gerais de formação da PSI contemplando a análise crítica

Fonte: autor da pesquisa

O quadro 9 contempla as diretrizes formadas no documento da PSI da organização, também demonstrando os fatores positivos e negativos se comparado à pesquisa bibliográfica:

DIRETRIZES	**POSITIVO**	**NEGATIVO**
1. **ESTRUTURA DA PSI**		
1.1. Estrutura inicial		
1.1.1. Comitê de segurança da informação	X	
1.1.2. Estrutura em geral	X	
1.2. Segurança lógica		
1.2.1. Acesso à internet	X	
1.2.2. Rede interna	X	
1.2.3. Armazenamento de informações	X	
1.2.4. Propriedades intelectuais	X	
1.2.5. Sistemas corporativos	X	
1.2.6. E-mails e troca de mensagem	X	

1.2.7. Política de senhas	X	
1.2.8. Falhas de firewall		X
1.2.9. Dificuldade de monitoramento de ações de armazenamento		X
1.2.10. Uso incorreto de senhas		X
1.3. Segurança física		
1.3.1. Barreiras de segurança física	X	
1.3.2. Retirada de equipamentos	X	
1.3.3. Controle de acesso de terceiros	X	
1.4. Incidentes e punições		
1.4.1. Notificações de incidentes	X	
1.4.2. Punições	X	
1.4.3. Conscientização dos usuários em notificar incidentes		X

Quadro 9 - Documento da PSI contemplando análise critica

Fonte: Autor da pesquisa

Gráfico 1. Representação dos Processos Gerais e PSI Documental conforme tabela 8 e 9
Fonte: autor da pesquisa

O *gráfico 1* destaca os valores quantitativos da tabela 8 e 9 relacionados aos fatores positivos e negativos, conforme demonstrado. O projeto de PSI tanto nos processos gerais quanto no documental obteve êxito em relação a análise crítica efetuada. Nos PROCESSOS GERAIS a contagem quantitativa de fatores atingiu 76,19% de pontos positivos contra 23,80% de pontos negativos, já a PSI DOCUMENTAL atingiu 77,77 % de pontos positivos contra 22,22% de pontos negativos.

Foram efetuadas 7 perguntas relacionadas aos processos demonstrados conforme *quadro 10*, com o objetivo de saber se os processos relacionados atingiram de forma positiva o projeto de implantação da PSI na organização. Para avaliação, o entrevistado, que é gestor de SI da organização, votou utilizando uma pontuação de 1 (não atende) a 10 (atende totalmente) sendo que o peso da maior nota equivaleu a 100%.

O objetivo nessa análise foi justamente saber se o projeto de segurança da informação atingiu os seus objetivos de acordo com a opinião do principal articulador da política dentro da organização, que é o Gestor de SI.

PROCESSO	PONTUAÇÃO 1 (não atende) a 10 (atende totalmente)	PERCENTU-AL
1. IMPLANTAÇÃO DA PSI	10	100%
2. TREINAMENTO	10	100%
3. ANALISE DE VULNERABILIDADE	7	70%
4. ANALISE, AVALIAÇÃO, TRATAMEN-TO DE RISCO	7	70%
5. ESTRUTURA DA PSI DA ORGANIZA-ÇÃO	8	80%
5.1. SEGURANÇA LÓGICA	10	100%
5.2. SEGURANÇA FÍSICA	10	100%
6. INCIDENTES E PUNIÇÕES	3	30%
7. CONTINUIDADE DO NEGOCIO	9	90%

Quadro 10 - Análise atribuída ao gestor de SI para avaliação do projeto

Fonte: Autor da pesquisa

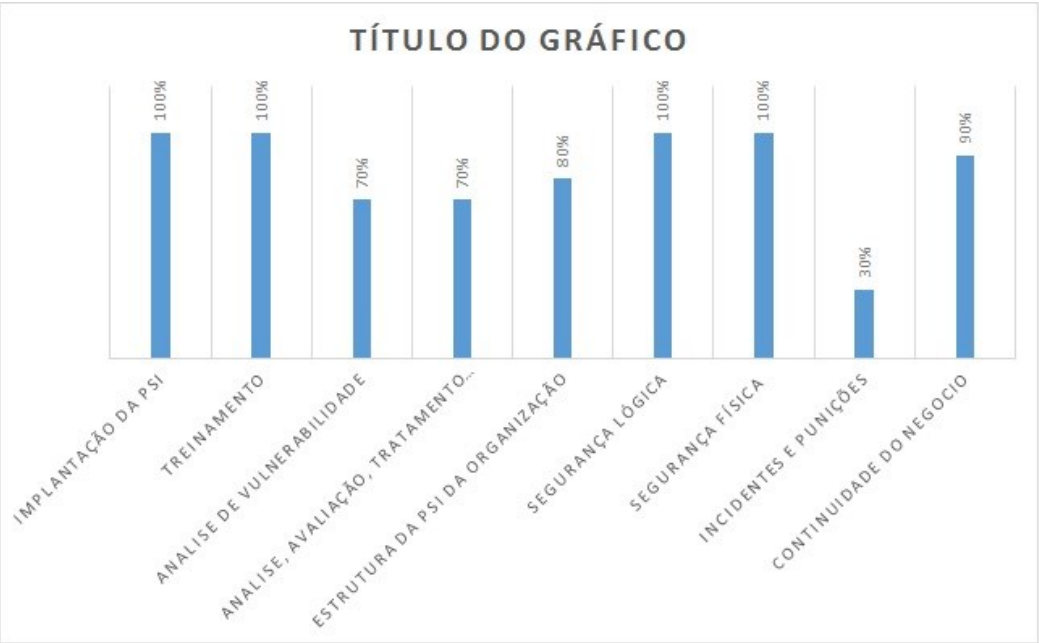

Gráfico 2. Representação da análise do projeto de PSI segundo o gestor de SI
Fonte: autor da pesquisa

Nota-se conforme o *gráfico 2*, e segundo informação do gestor de SI que os processos de implantação e treinamento não foram um obstáculo para o projeto. Já a análise de vulnerabilidade e risco foi um ponto mais crítico em relação aos trabalhos, justamente, por envolver mais processos e fatores. A norma ABNT NBR ISO/IEC 17799 (2005) fala que a análise de risco envolve a identificação, quantificação e priorização dos riscos criando critérios de aceitação e tratamento. Todos esses processos foram julgados pelo entrevistado como uma dificuldade atingindo 70% da avaliação em relação à nota máxima.

As diretrizes de segurança lógica e física não foram um ponto impactante, visto que a organização já contava com diretrizes de proteção de ambos os processos. O ponto mais crítico, segundo a entrevista, foi o dos incidentes e punições, relatando a dificuldade em conscientizar os usuários da necessidade de identificar e relatar os incidentes de segurança da informação. Beal (2005) cita em seu livro a necessidade de colaboração dos funcionários em relação as políticas de segurança da informação, demonstrando que os mesmos precisam ser atuantes na prevenção e desempenho, assim como na necessidade de relatar as falhas nos controles e incidentes observados. A continuidade do negócio não recebeu nota máxima devido às dificuldades nos processos já relatados, anteriormente.

Foram entrevistados 20 colaboradores da organização escolhidos, aleatoriamente, para efetuar uma pesquisa referente ao conhecimento da PSI e do conteúdo constatado na mesma. Foram utilizadas 15 questões avaliadas de acordo com uma nota de 1 a 5, onde 1 (não atendeu) e 5 (atendeu totalmente), os questionários foram encaminhados e recebidos eletronicamente via e-mail. Dos 20 colaboradores entrevistados 16 retornaram o questionário sendo que não foram obtidas respostas de 4 questionários.

O objetivo dessa etapa da pesquisa foi analisar criticamente como a PSI atingiu os usuários, se foi formulada com fácil entendimento e se foi repassada a todos os membros da organização. As respostas estão mencionadas no quadro *11*.

DIRETRIZES	**FREQ.**	**MEDIA**	**PERCENTUAL**

1. INTRODUÇÃO	70	4,37	87,4%
2. SEGURANÇA LÓGICA			
2.1. Acesso à internet	71	4,43	88,6%
2.2. Rede interna	66	4,12	82,4%
2.3. Armazenamento	73	4,56	91,2%
2.4. Propriedades intelectuais	64	4	80%
2.5. Sistemas corporativos	66	4,12	82,4%
2.6. Utilização de e-mails	74	4,62	92,4%
2.7. Utilização de senhas	73	4,56	91,2%
2.8. Troca de mensagens	69	4,31	86,2%
3. SEGURANÇA FÍSICA			
3.1. Gestão de segurança	69	4,31	86,2%
3.2. Ambiente de segurança	70	4,37	87,4%
3.3. Controles	67	4,18	83,6%
3.4. Utilização de alarmes prediais	70	4,37	87,4%
4. GERENCIAMENTO DE TERCEIROS	68	4,25	85%
5. INCIDENTES E PUNIÇÕES			
5.1. Notificações e incidentes	70	4,37	87,4%
5.2. Punições	72	4,5	90%

Quadro 11 - Conhecimento da PSI segundo os colaboradores da organização específica

Fonte: autor da pesquisa

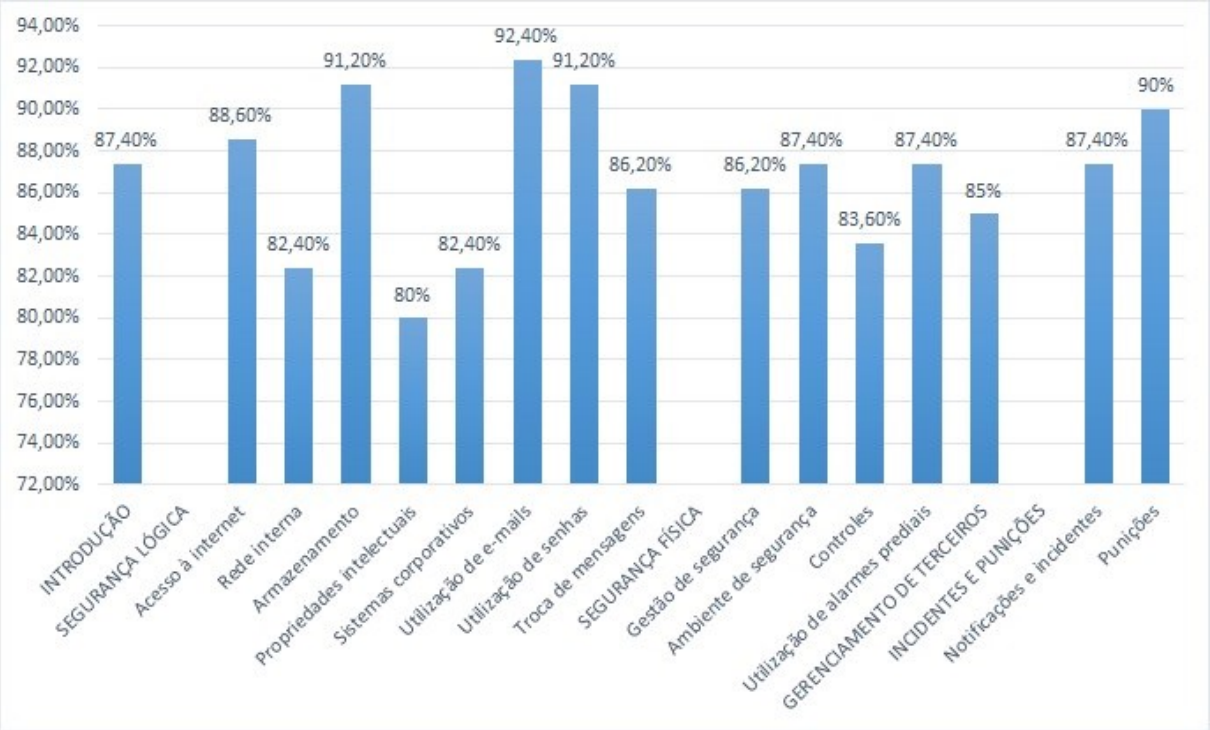

Gráfico 3. Representação da análise de conhecimento da PSI conforme colaboradores
Fonte: autor da pesquisa

O *gráfico 3* demonstra que, no geral, a política de segurança da informação atingiu aos objetivos no que diz respeito ao conhecimento e conscientização dos usuários, mantendo uma alta porcentagem em relação ao entendimento das diretrizes impostas na PSI. A porcentagem mais baixa foi registrada quanto ao entendimento das propriedades intelectuais relacionadas à segurança lógica. Nota-se assim uma dissonância cognitiva em relação aos usuários entrevistados e o gestor de SI. Entende-se por dissonância cognitiva, o esforço do ser humano para manter as suas cognições ou opiniões, quando outra pessoa tem uma opinião ou crença diferente, então assim é gerado a dissonância cognitiva (PORATALDAEDUCAÇÂO.COM.BR, 2013). As maiores porcentagens ficaram relacionadas à segurança lógica, nas diretrizes de armazenamento, utilização de e-mails e senhas, também pode ser notado uma alta porcentagem no que se refere aos incidentes e punições, relacionado a diretriz punição com 90% de entendimento, demonstrando mais uma vez uma dissonância cognitiva entre os colaboradores e o gestor de SI quanto ao entendimento da diretriz Punições.

O quadro *12* demonstra a análise da aplicação da PSI como um todo, das diretrizes que foram atendidas e não atendidas, que devem ser melhoradas ou que ficaram fragilizadas devido às falhas na aplicação da política de segurança da informação. Essa análise foi baseada na primeira auditoria de segurança da informação efetuada na organização com auxílio do gestor de SI, efetuando-se uma pesquisa quantitativa das não conformidades, ações futuras, sugestões de melhoria e conformidades encontradas, armazenando-as em uma tabela e aplicando um gráfico para mensurar os dados.

DIRETRIZES	NÃO CONFORME	AÇÃO FUTURA	SUJ. DE MELHORIA	CONFORME
Análise de Risco	**1**	**1**	**-**	**2**
Análise de impacto, ameaças e vulnerabilidades: Desenvolvimento				
Plano de ação aos principais riscos: Criação				
Execução e revisão do plano de ação: execução das ações				
Periodicidade da análise de risco: periodicidade				
Organização da segurança da informação	**1**	**5**	**6**	**6**
Divulgação, Distribuição e revisão da PSI: Divulgação				
Divulgação, Distribuição e revisão da PSI: Distribuição				
Divulgação, Distribuição e revisão da PSI: Revisão da PSI				
Comitê de Segurança da informação: Formação do comitê de segurança da informação				
Comitê de Segurança da informação: Reuniões periódicas do comitê				
Comitê de Segurança da informação: Aprovação do comitê de segurança da informação				
Classificação dos ativos de informação: classificação				

Plano de continuidade do negócio: plano de ação				
Análise de risco: Desenvolvimento da análise de risco				
Treinamento de conscientização da PSI: Treinamento da PSI				
Treinamento de conscientização da PSI: Avaliação dos usuários da PSI				
Treinamento de conscientização da PSI: Termo de ciência da PSI				
Treinamento de conscientização da PSI: Campanha de conscientização da PSI				
Auditoria de segurança da informação: Plano de ação da auditoria anterior				
Incidentes e punições: registro e tratamento de incidentes				
Incidentes e punições: medidas disciplinares				
Incidentes e punições: Conscientização sobre registros de incidentes				
Gerenciamento de serviço de terceiros: Dependência de terceiros				
Política de segurança lógica	**2**	**-**	**3**	**18**
Acesso de internet: monitoramento de acessos				
Acesso de internet: bloqueios de acesso				
Acesso de internet: uso adequado da internet				
Acesso a rede interna: controle de acesso				
Acesso a rede interna: dispositivos moveis				
Armazenamento e manuseio lógico: controle de acesso				
Armazenamento e manuseio lógico: conformidade das permissões de acesso				
Armazenamento e manuseio logico: armazenamento corporativo				
Armazenamento e manuseio logico: armazenamento de documentos pessoais				

Armazenamento e manuseio logico: remoção de acesso de colaboradores desligados				
Propriedade intelectual: utilização de software pirata				
Propriedade intelectual: Presença de arquivos piratas				
Uso de e-mails: monitoramento de e-mail				
Uso de e-mails: uso de e-mail corporativo				
Uso de e-mails: uso de e-mail pessoal				
Uso de sistemas corporativos: procedimento de liberação de acesso				
Uso de sistemas corporativos: revisão de direitos de acesso				
Uso de sistemas corporativos: conformidade dos acessos				
Uso de sistemas corporativos: remoção dos direitos de acesso				
Uso de senhas: uso adequado				
Sistemas de troca de mensagens: monitoramento				
Sistemas de troca de mensagens: uso adequado				
Política de segurança física	**-**	**-**	**3**	**5**
Controles físicos de segurança: monitoramento de CFTV				
Controles físicos de segurança: Checklist de segurança física				
Controles físicos de segurança: Acesso predial				
Controles físicos de segurança: Datacenter				
Controles físicos de segurança: Arquivo morto				
Controle de documentos e equipamentos: Controle de documento				
Controle de documentos e equipamentos: controle de equipamentos				

Armazenamento e manuseio de documentos: armazenamento				
Uso de chaves e alarmes: inventário de ambos				
Políticas de tecnologias da informação	**-**	**-**	**2**	**4**
Processos: backup				
Processos: ferramenta de helpdesk				
Controles tecnológicos preventivos: uso de antivírus				
Controles tecnológicos preventivos: ferramenta de firewall				
Controles tecnológicos preventivos: ferramenta de controle de SPAN				
Monitoramento de recursos: monitoramento				
Plano de continuidade do negocio	**-**	**4**	**-**	**-**
Análise de impacto de negócio: analise de impacto				
Estratégia de continuidade: estratégia				
Treinamento e testes de continuidade: treinamento e testes				
Revisão periódica do plano de continuidade: revisão periódica				
Auditorias de segurança da informação	**-**	**3**	**-**	**-**
Periodicidade das auditorias: periodicidade				
Tratamento das não conformidades: tratamento				
Tratamento das sugestões de melhorias: tratamento				

Quadro 12 - Análise baseada na auditoria de PSI da organização com apoio do gestor de SI

Fonte: Pesquisa Documental em dados da organização objeto da pesquisa

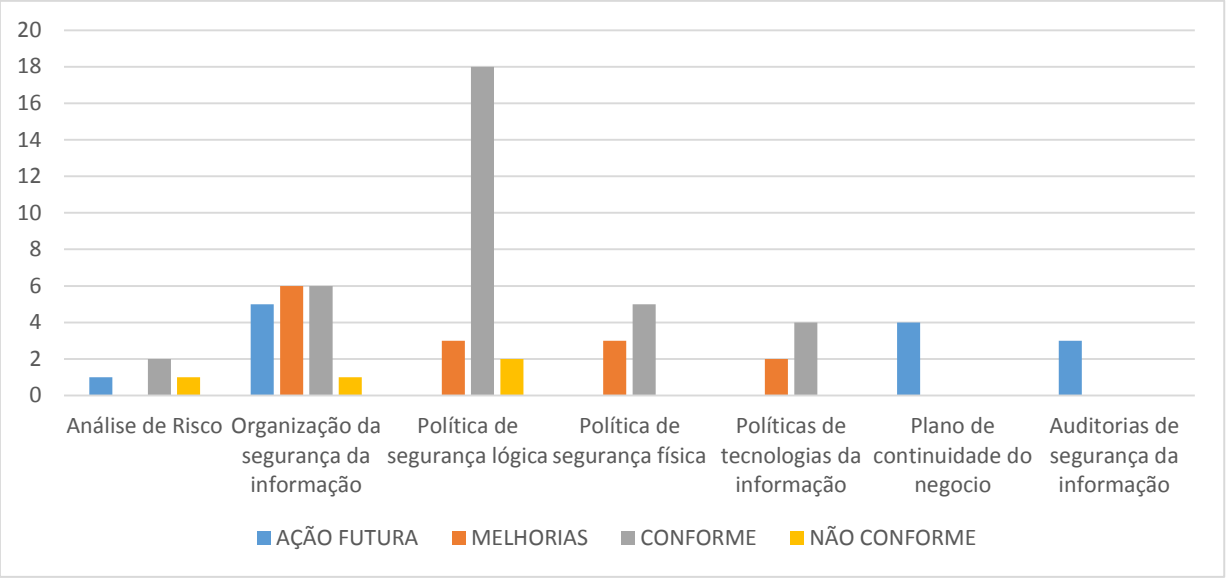

Gráfico 4. Representação da análise conforme tabela 12
Fonte: autor da pesquisa

O *gráfico 4* demonstra os dados da *tabela 12* devidamente organizados, apesar de não apresentar muitas inconformidades, o projeto após sua implantação, necessita de melhorias e ações futuras, o grupo **Organização da Segurança da Informação** deixa isso bem claro, pois as conformidades encontradas contrastam com as necessidades de melhorias. Os dois últimos grupos estão demonstrando somente ações futuras, isso se deu, pois segundo informação do gestor de SI, foram grupos que não passaram por intenso treinamento, portanto não foram caracterizados como inconformidades, mas sim como ações futuras a serem implementadas até a próxima auditoria de segurança da informação.

Em comparação aos gráficos números 8 e 9 nota-se uma discordância entre algumas diretrizes consultadas. Nota-se que a auditoria segmentou mais os assuntos em relação ao projeto de PSI da organização. Essa segmentação pode ter relação com o número alto de melhorias e ações futuras analisadas, que podem não ter sido inteiramente aplicadas devido à falta de entendimento no momento da implementação do projeto de PSI.

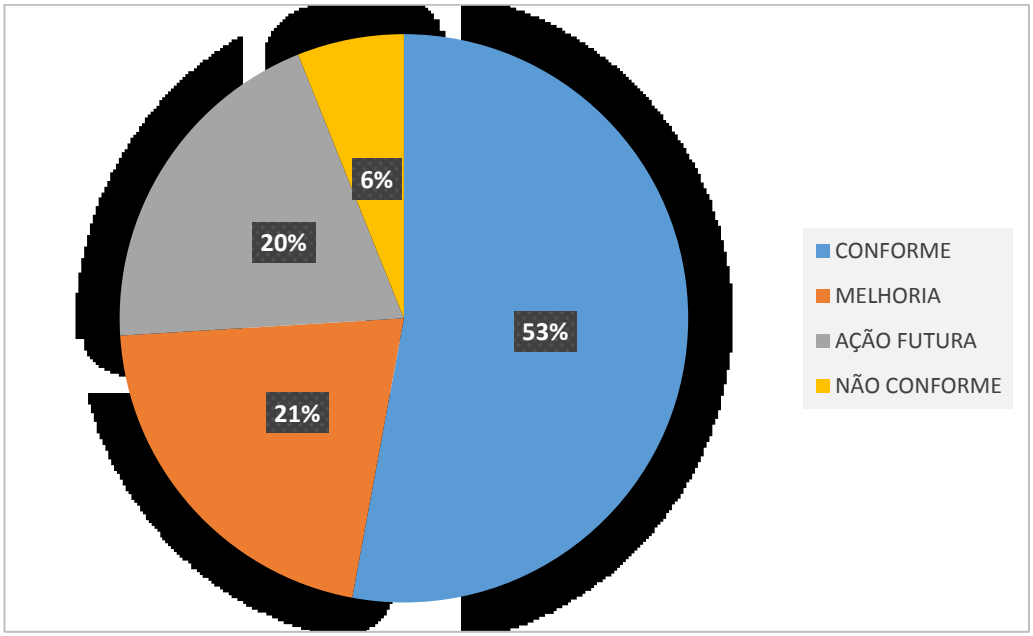

Gráfico 5. Representação em percentual da tabela 12.
Fonte: autor da pesquisa

O *gráfico 5* demonstra as ações de acordo com sua porcentagem. Conforme demonstrado em azul, as **conformidades** foram maioria com 53% enquanto as **não conformidades** atingiram 6%. Mesmo com esse ganho é necessário analisar as **ações futuras** com 20% e as **sugestões de melhorias** com 21%, pois existe a necessidade de implementar esses grupos para que se tornem futuras conformidades e atendam às expectativas da organização em relação ao projeto de PSI implantado e, em relação à pesquisa exploratória efetuada.

5. CONSIDERAÇÕES FINAIS

Dentro do conceito de informação, do crescimento organizacional e das TICs, é possível perceber o quanto as organizações estão ficando cada vez mais vulneráveis aos impactos causados pelos eventos que ferem a segurança da informação.

Considera-se, de acordo com a pesquisa exploratória e, a análise crítica efetuada, que a organização seguiu diretrizes para implementação da PSI e, que se utilizou de ferramentas que customizaram o processo de implementação do projeto. É notório a necessidade da organização em assegurar que os ativos não sofram impactos que prejudiquem a gestão estratégica do negócio.

A análise também demonstrou que, mesmo com os fatores tecnológicos envolvidos em um planejamento de PSI, o fator humano conta muito no processo de implantação da política. As dissonâncias cognitivas encontradas na análise demonstram claramente que é preciso manter foco nos usuários e obter a aceitação em relação ao projeto implantado na organização. Essa aceitação pode ser melhor absorvida através de programas intensivos de conscientização, como treinamentos periódicos, ou com a criação de canais de conscientização utilizando ferramentas de TICs, como e-mails educativos, vídeo-aulas ou outros meios de transmitir informações a respeito do assunto.

Por último, a análise realizada em referência à auditoria, demonstra que a organização alcançou um nível aceitável de conformidades em relação ao projeto como um todo, porém faz-se necessário analisar as sugestões de melhoria e ações futuras que também alcançaram níveis relevantes. A análise demonstra a necessidade de melhoria no que diz respeito às diretrizes impostas e às cobranças efetuadas em auditoria, para que os gestores possam traba-

lhar as diretrizes de forma mais correta melhorando a estrutura do projeto e assim alcançar aos níveis desejados de conformidades. O desafio é ajustar esses fatores para que se tornem futuras conformidades e façam a organização atingir níveis máximos de segurança em todos os setores e serviços disponíveis.

6. TRABALHOS FUTUROS

- Nesta seção estão listadas algumas propostas para trabalhos futuros:
- Fazer um estudo referente aos impactos e riscos relacionados a falta de projetos de PSI.
- Fazer uma avaliação de como alcançar as melhorias e ações futuras encontradas na pesquisa.
- Avaliar o nível de aceitação de PSI em organizações de dimensões parecidas.

7. REFERÊNCIAS

ABNT. ABNT NBR ISO/IEC 17799. **Tecnologias da informação - Código de pratica para gestão de segurança da informação**. ABNT. Rio de Janeiro, 2005, 120 p.

ABNT. ABNT NBR ISO/IEC 27001. **Tecnologias da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos**. ABNT. Rio de Janeiro, 2013, 32 p.

ABNT. ABNT NBR ISO/IEC 27002. **Tecnologias da informação - Código de pratica para controles de segurança da informação**. ABNT. Rio de Janeiro, 2005, 112 p.

ABNT. ABNT NBR ISO/IEC 27005. **Tecnologias da informação – Técnicas de segurança – Gestão de riscos de segurança da informação**. ABNT. Rio de Janeiro, 2011, 87 p.

ADDED. **Desafios diários para gerir dispositivos móveis nas empresas**. Disponível em: <http://www.added.com.br/#!-CIOs-desafios-di%C3%A1rios-para-gerir-dispositivos-m%C3%B3veis-nas-empresas/c1xb4/2F27329D-CC58-4728-AF45-DF73BCDA60FE>. acesso em 10/04/2016

BARRETO, A.A. **A questão da informação**. Fundação Seade. Revista São Paulo. v. 8, n 4, 1994.

BEAL, A. **Segurança da Informação**. Princípios e melhores práticas para a proteção dos ativos de informação nas organizações. 1. Ed. São Paulo: Editora Atlas S.A. 2005. 175 p.

BRASIL. **Instrução normativa GSI/PR nº 1, de 13 de junho de 2008.** Disponível em: < http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf >. Acesso em: 26 abril 2016.

BRASIL. Presidência da república. Gabinete de segurança nacional. **Estratégia de segurança da informação e comunicação e de segurança cibernética da administração pública federal 2015-2018**, versão 1.0. Gabinete de segurança institucional, Secretária-executiva, Departamento de segurança da informação e comunicações. Portaria No. 14, de 11 de maio de 2015, publicada no DOU No. 88 de 12/05/2015.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. Brasília, 2007. 71 p.

CARNEIRO, L.E.S; ALMEIDA, M.B. **Gestão da informação e do conhecimento no âmbito das práticas de Segurança da informação: o fator humano nas organizações**. Minas Gerais, v.18, n. 37, 2013. Disponível em: <https://periodicos.ufsc.br/index.php/eb/article/view/26466> Acesso em: 17 março 2016.

COELHO, F.E.S; ARAUJO, L.G.S; BEZERRA, E.K. **Gestão da segurança da informação**. 2. ed. Rede nacional de ensino e pesquisa, 2014. 198 p.

COSTA, D.R. **Fatores críticos de sucesso para elaboração de uma política de segurança da informação e comunicação no âmbito da administração pública federal**. [Monografia de especialização]. Brasília: Universidade de Brasília, 2009.

CVE.MITRE.BR. **Sobre o CVE.** Disponível em: <http://cve.mitre.org>. Acesso em: 20 abril 2016.

ENGEBRETSON. P. **The Basics of Hacking and Penetration Testing**. Ethical Hacking and Penetration Testing Made Easy. Walthman. Elsevier. 2011. 159 p.

FIORENTINO. G.; BROSSI. L.; AMELOG. I.; CAMPANATTI. C. **As oito grandes tendências de crescimento até 2020**. Disponível em: <http://www.bain.com/offices/saopaulo/pt/Images/The_great_eight_POR.PDF>. Acesso em: 16 março. 2016.

FONTES, E. **Segurança da informação.** O usuário faz a diferença. 1. Ed. São Paulo: Saraiva. 2006. 172 p.

GLOBO.COM. **Internet chega pela 1ª vez a mais de 50% das casas no Brasil, mostra IBGE**. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/04/internet-chega-pela-1-vez-mais-de-50-das-casas-no-brasil-mostra-ibge.html>. Acesso em 10/04/2016

GOMES.R.A Importância da informação. Disponível em: <http://www.administradores.com.br/producao-academica/a-importancia-da-informacao/2820/>

IBGE. **Política de segurança da informação e comunicações do IBGE, 2016**. Rio de Janeiro, 2016. 35 p.

MARCONI, M.A; LAKATOS, E.M. **Fundamentos de metodologia científica**. 5. Ed. São Paulo: Editora Atlas S.A. 2003. 311 p.

MESSIAS, L.C.S. **Informação: um estudo exploratório do conceito em periódicos científicos brasileiros na área de ciência da informação**. 2005. 206 f. Dissertação (Pós Graduação em Ciência da Informação) – Faculdade de Filosofia e Ciências Campus Marilia, Universidade Estadual Paulista, Marília, 2005.

MIANI, R.S. **Um estudo sobre métricas e quantificação em segurança da informação**. 2013. 202 f. Dissertação (Doutorado em Engenharia Elétrica) – Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, São Paulo, 2013.

MONTEIRO, I.L.C. **Proposta de um guia para elaboração de políticas de segurança da informação e comunicação em órgãos da administração pública federal**. 2009. 67 f. Monografia (Especialização em gestão de segurança da informação e comunicações) – Especialização em gestão de segurança da informação e comunicações, Universidade de Brasília, Brasília, 2009.

MORINOTO. C.E; **Usando NESSUS**. Disponível em: <http://www.hardware.com.br/guias/seguranca-linux-windows/usando-nessus.html>. Acesso em 20 abril 2016.

NAKAMURA, E.T; GEUS, P.L. **Segurança de redes em ambientes corporativos**. 4. ed. São Paulo: Novatec Editora, 2010. 288 p.

PLANALTO. **LEI Nº 9.609 , DE 19 DE FEVEREIRO DE 1998** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9609.htm> Acesso em 13/04/2016

PORTALDAEDUCAÇÃO. **Teoria da dissonância cognitiva.** Disponível em <http://www.portaleducacao.com.br/psicologia/artigos/41439/teoria-da-dissonancia-cognitiva>. Acesso em: 07 junho 2016.

REZENDE, D.A. **Engenharia de software e sistemas de informação**. 3. Ed. São Paulo: Brasport. 2005. 316 p.

REZENDE, D.A; ABREU, A.F. **Tecnologia da informação.** Aplicada a sistemas de informação empresariais. 5. Ed. São Paulo. Editora Atlas S.A. 2008. 303 p.

SANTOS, V.O; **Um modelo de sistema de gestão da segurança da informação baseados nas normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008. 2012**. 127 f. Dissertação (Mestrado em Engenharia Elétrica) – Faculdade de engenharia elétrica e de computação, Universidade Estadual de Campinas, Campinas, 2012.

SEBRAE. **Em dez anos, os valores da produção gerada pelos pequenos negócios saltaram de R$ 144 bilhões para R$ 599 bilhões.** Disponível em: http://www.sebrae.com.br/sites/PortalSebrae/ufs/mt/noticias/Micro-e-pequenas-empresas-geram-27%25-do-PIB-do-Brasil. Acesso em: 16 de março. 2016

SEBRAE. **Sobrevivência das empresas no Brasil. Brasília**. GEOR – Gestão Estratégica Orientada a Resultados. Disponível em: <http://www.sebrae.com.br/Sebrae/Portal%20Sebrae/Anexos/Sobrevivencia_das_empresas_no_Brasil=2013.pdf>. Acesso em: 16 de março 2016.

SERASA. **Correio eletrônico** <http://www.serasaexperian.com.br/quem-somos/seguranca/correio-eletronico/> Acesso em 13/04/2016

SISNEMA. **Mercado de TI no Brasil deverá crescer 2,6% em 2016, segundo IDC**. Disponível em: < http://sisnema.com.br/noticia/02/02/2016/mercado-de-ti-no-brasil-devera-crescer-em-2016-segundo-idc>. Acesso em: 15 março. 2016.

TENABLE NETWORK SECURITY. **Nessus user guide**. 2016, 356f. Disponível em <http://static.tenable.com/documentation/nessus_6.4_user_guide.pdf> Acesso em: 07 maio 2016.

TENABLE.COM. **Proteja sua rede localmente e na nuvem com Nessus**. Disponível em: <http://www.tenable.com/pt-br/nessus/ Acesso em 20 Abril 2016>. Acesso em: 20 abril 2016.

UNIVERSIDADE FEDERAL DE SANTA CATARINA – **UFSC. Projeto pedagógico do curso de bacharelado em tecnologias da informação e comunicação**. Araranguá. 2013. 117 p.

WHITMAN, M.E; MATTORD, H.J. **Principles of information security**. Boston: Course Tecnology, 2012. 617 p.

8. APÊNDICE

QUESTINÁRIO GESTOR DE SI

A pontuação segue as notas de 1 a 5 onde 1 (não atendeu) e 5 (atendeu totalmente)

1. IMPLANTAÇÃO DA PSI
   1.1. O processo de implantação da PSI ocorreu de acordo com o projeto implementado?
      A. 1
      B. 2
      C. 3
      D. 4
      E. 5
      F. 6
      G. 7
      H. 8
      I. 9
      J. 10
2. TREINAMENTO
   2.1. O processo de treinamento implementado pelo projeto da organização auxiliou na implantação e gestão da PSI da organização?
      A. 1
      B. 2
      C. 3
      D. 4
      E. 5
      F. 6
      G. 7
      H. 8
      I. 9
      J. 10
3. ANÁLISE DE VULNERABILDIADE
   3.1. Foi possível identificar todas as vulnerabilidades do ambiente utilizando o projeto de PSI da organização?

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6
G. 7
H. 8
I. 9
J. 10

4. ANÁLISE, AVALIAÇÃO, TRATAMENTO DE RISCO

4.1. A análise de risco gerou subsidio suficiente para encontrar, avaliar e tratar os riscos na organização.

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6
G. 7
H. 8
I. 9
J. 10

5. ESTRUTURA DA PSI DA ORGANIZAÇÃO

5.1. A estrutura da PSI contemplando todos os pontos implementados na mesma foram suficientes para a atender a segurança da informação da organização.

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6
G. 7
H. 8
I. 9
J. 10

5.1. Ainda quanto a estrutura da PSI, a política de segurança lógica ficou claramente esclarecida para a implementação da PSI na organização?

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6
G. 7

H. 8
I. 9
J. 10

5.2. Ainda quanto a estrutura da PSI, a política de segurança física ficou claramente esclarecida para a implementação da PSI na organização?

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6
G. 7
H. 8
I. 9
J. 10

6. INCIDENTES E PUNIÇÕES

6.1. Quanto aos incidentes e punições, você acha que são medidas suficientes para mitigar os riscos inerentes aos incidentes da política de segurança da informação?

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6
G. 7
H. 8
I. 9
J. 10

7. CONTINUIDADE DO NEGOCIO

7.1. O plano de continuidade do negócio auxilia na gestão futura da PSI na organização?

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6
G. 7
H. 8
I. 9
J. 10

QUESTINÁRIO COLABORADORES

Necessitamos da sua opinião referente a PSI – Política de Segurança da Informação implantada na organização. Esse questionário é voltado a um estudo para um projeto de defesa de TCC e sua opinião além de muito importante será mantida em sigilo, não é necessário à sua identificação nesse documento.

Avalie as questões abaixo dando uma nota de 1 a 5, sendo 1 (não atendeu) e 5 (atendeu totalmente):

1. A PSI começa com o primeiro título sendo a **INTRODUÇÃO**, ficou claro o conteúdo apresentado nessa parte do documento?
   A. 1
   B. 2
   C. 3
   D. 4
   E. 5

2. A PSI deixou claro as questões inerentes a **SEGURANÇA LÓGICA** conforme as diretrizes abaixo?
   2.1. Política de acesso à internet
      A. 1
      B. 2
      C. 3
      D. 4
      E. 5

   2.2. Acesso a rede interna
      A. 1
      B. 2
      C. 3
      D. 4
      E. 5

   2.3. Armazenamento de informações
      A. 1
      B. 2
      C. 3
      D. 4
      E. 5

   2.4. As propriedades Intelectuais
      A. 1
      B. 2
      C. 3

D. 4
E. 5

2.5. Uso de sistemas corporativos
A. 1
B. 2
C. 3
D. 4
E. 5

2.6. Utilização de e-mails
A. 1
B. 2
C. 3
D. 4
E. 5

2.7. Política de uso de senhas
A. 1
B. 2
C. 3
D. 4
E. 5

2.8. Sistemas de troca de mensagem
A. 1
B. 2
C. 3
D. 4
E. 5

3. A PSI deixou claro as questões inerentes a **SEGURANÇA FÍSICA** conforme as diretrizes abaixo?
3.1. Gestão da segurança física
A. 1
B. 2
C. 3
D. 4
E. 5

3.2. Ambiente de segurança física
A. 1
B. 2
C. 3
D. 4
E. 5

3.3. Controles de acesso físico
   A. 1
   B. 2
   C. 3
   D. 4
   E. 5

3.4. Uso de alarmes prediais
   A. 1
   B. 2
   C. 3
   D. 4
   E. 5

4. A PSI deixou claro as responsabilidades e o cuidado quanto aos **SERVIÇOS TERCEIRIZADOS** conforme descrito no documento?
   A. 1
   B. 2
   C. 3
   D. 4
   E. 5

5. A PSI deixou claro as questões inerentes aos **INCIDENTES E PUNIÇÕES** conforme as diretrizes abaixo?

   5.1. Notificações e incidentes
      A. 1
      B. 2
      C. 3
      D. 4
      E. 5

   5.2. Punições
      A. 1
      B. 2
      C. 3
      D. 4
      E. 5