O PDCA como elemento integrador das normas ABNT 27001, 27002 e 27003

Emmanuel G. Souza[1]

[1]Sistema de Informação – Universidade Federal da Paraíba: Campus IV (UFPB)
Caixa Postal 58297-000 – Rio Tinto – PB – Brazil

emmanuel.souza@dce.ufpb.br

Resumo – *Neste trabalho será estudado o PDCA (Plan-Do-Check-Act) como elemento de integração as normas ABNT 27001, 27002 e 27003, que se unem num sistema para auxiliar os gestores na analise de dados para determinar os riscos que rodeiam a estrutura da empresa e que possam causar deterioração na sua base estrutural, tal como queda no crescimento comercial do ramo em que atue. Tendo assim, uma maior integração e iteração dos setores que estruturam a empresa, buscando o auxilio das tecnologias da informação visando a ciação de sistemas de gestão de segurança da informação findadas nas ISOs regidas nas normas para ter uma estrutura mais elaborada e que atenda a todas as necessidades da (s) organição (s), tendo assim um maior controle dela.*

Palavras-chaves: Tecnologias, Empresa, Gestão, Segurança, ISO.

Abstract - *In this work is studied the PDCA (Plan-Do-Check-Act) as an integrating element ABNT 27001 standards 27002 and 27003, which come together in a system to assist managers in data analysis to determine the risks surrounding the structure enterprise which can cause deterioration in its structural base, such as decline in trade growth in the industry in which it operates. Having thus, greater integration and iteration of the sectors that structure the company, seeking the help of information technologies for the ciation of information security management systems findadas the ISOs governed the rules to have a more elaborate structure that meets all the needs organizations, thus having a greater control of it.*

Keywords: Technology, Business, Management, Security, ISO.

1. INTRODUÇÃO

A estrutura cíclica PDCA (*Plan-Do-Check-Act*) busca criar um ambiente que auxilie no gerenciamento da estrutura de gerenciamento das organizações, auxiliando os gestores a elaborar seus planos de riscos para que se tenha integridade e maior segurança no manuseio e contenção da informação e dos dados que se encontram no banco de dados das empresas, auxiliando ainda na criação de Sistema de Gestão de Segurança da Informação (SGSI) com base nas normas ISO 27001, 27002 e 27003, fazendo uma análise dos requisitos exigidos

Trabalho de Conclusão de Curso apresentado pelo aluno **Emmanuel Gomes Souza** sob a orientação da professora **Adriana Z. Clericuzi** como parte dos requisitos para obtenção do grau de Bacharel em Sistemas de Informação na UFPB Campus IV.

pelas normas para se manter um padrão de controle e garantir maior confiança e segurança para os seus parceiros e clientes.

Tendo tal normalização aplicada a todos os tipos de organizações e de todos os tamanhos, inclusive empresas comerciais, agências governamentais e organizações sem fins lucrativos. Tendo em vista que a complexidade e os riscos de cada instituição são únicos e os seus requisitos específicos irão direcionar e auxiliar na implantação do SGSI.

Sendo assim, torna-se possível a elaboração de planos que tenham um ciclo de vida iniciado com base nos dados gerados a partir do resultado final, obtido ao fim de cada ciclo. Tendo seguido cada processo sem ter pulado nenhum dos passos exigidos pelas normas ISO com o embasamento da estrutura cíclica PDCA, sendo voltada para a criação do SGSI.

2. OBJETIVO

Propor uma metodologia para auxiliar os gestores na análise de dados determinando os riscos que cercam e ameaçam a estrutura da empresa através da utilização do PDCA, como meio determinístico para a geração de resultados que venham a ser úteis com relação a segurança e na tomada de decisões, como também na segurança dos próprios dados.

3. DESENVOLVIMENTO TEÓRICO

Durante o desenvolvimento deste trabalho vamos estudar e analisar os conceitos e especificações que abrangem a ISO 27001, 27002, 27003 e a estrutura cíclica PDCA para criar um grau de qualificação e eficácia no gerenciamento das atividades criadas no plano pelo gestor, para que as empresas tenham um maior índice de melhoramento nos seus processos, podendo ser usado nos mais variados portes de organização.

A partir daí será buscado uma base e fundamentação que mostre de forma especifica e abrangente os pontos abordados no trabalho, para que posteriormente seja feita a explanação e aprofundamento de uma estrutura baseada nos fatores estudados e que esteja co-relacionado ao setor de segurança das organizações.

3.1 ISO 27001

A ISO 27001 é o padrão e a referência Internacional para a gestão da Segurança da informação, como também a ISO 9001 é referência Internacional da certificação de gestão em Qualidade.

Podemos assim ver que tal norma tem vindo de forma continua a ser remodelada com o passar do tempo, e tendo sido originado de um conjunto de normas anteriores, sendo uma delas conhecida e intitulada como BS7799 (*British Standards*). Tendo sua origem e registro

em um documento publicado em 1992 por um departamento do governo Britânico que buscava estabelecer um código de práticas relacionadas a gestão da segurança da informação.

No passar dos anos, milhares de profissionais ajudaram e contribuíram com o seu *know-how* e experiência para a criação e fundamentação de um Standard mais estável e maduro, que de tal modo tende a continuar a evoluir com o passar do tempo e dos dados gerados e coletados para o seu aperfeiçoamento. Ainda podemos dizer, que a norma tem como princípio de maneira geral a adoção de um conjunto de requisitos pelas empresas, como também processos e um controle de objetivos, para assim, mitigar e gerar um controle de risco da organização.

Há milhões de entidades no mundo que se estruturam e usam tais práticas documentadas no *Standard* além de usufruir dos benefícios da sua adoção, sendo que, se assim desejarem ainda podem se certificarem mostrando assim de forma concreta que cumprem os requisitos e processos exigidos pela norma. Algumas organizações, determinam e obrigam que os seus fornecedores ou parceiros detenham certificações, especificamente a ISO 27001, para ter uma garantia do cumprimento dos princípios estabelecidos por tal norma, proporcionando assim para seus clientes e parceiros um bom nível de segurança da informação e conforto para se proceder nos negócios das empresas. Sendo assim, as organizações que se certificam nesta norma adquirem uma atribuição especial e de grande importância para com a proteção dos dados de seus clientes e parceiros.

3.1.1 Serventia e Benefícios na adoção da ISO 27001

A adopção desta norma ISO serve para que as organizações sigam e adotem um modelo que seja adequado para o estabelecimento, desenvolvimento, controle, vistória, revisão e gestão do Sistema de Gestão de Segurança da Informação (SGSI). O SGSI tem como base os princípios que regem a norma ISO 27001, num modelo que busca compreender de forma global a abordagem da Segurança sem depender precisamente de marcas e fabricantes tecnológicos.

É de compreensão global ter uma abordagem 360º à Segurança da Informação, fazendo uma correlação de múltiplos temas, tais como as telecomunicações, segurança aplicacional, proteção do meio físico, recursos humanos, etc. Independente de fabricantes a norma se destina ao estabelecimento de processos e procedimentos que podem ser materializados a situação de cada organização de forma distinta e com especificação de cada ambiente tecnológico e organizacional.

Independentemente das organizações ou empresas se certificarem ou não, a necessidade de adoção das práticas apresentadas pela norma gera um conjunto de benefícios, que podemos listar alguns deles da seguinte forma: ter um compromisso dos Executivos da Organização para com a segurança da informação; aumentar a viabilidade e a segurança da

informação dos sistemas, em termos de confidencialidade, disponibilidade e integridade; ter uma garantia de investimentos com mais eficiência e orientados a riscos, ao invés de se basear nas tendências; acrescentar alguns níveis de contribuição, participação e motivação dos colaboradores da Organização para com a Segurança da Informação; Identificar e determinar de forma continua as oportunidades para melhorias dos processos; aumentar a confiança e satisfação dos clientes e parceiros, tendo como provimento um aumento na realização de mais negócios; implementar controles com base na norma que contenham uma análise de risco, melhorando assim o desempenho operacional das organizações; e adotar na organização um sistema de controlo da gestão, incrementando a eficácia da organização.

3.2 ISO 27002

A ISO 27002 foi publicada originalmente como uma renomeação da norma ISO 17799 existente, e é conhecida como uma norma para os códigos de práticas para gestão de segurança da informação. Referindo-se aos requisitos que devem ser implementados pelas organizações, sendo ainda um guia que auxilia na utilização dos controles de segurança para garantir maior proteção da informação e construir a confiança em atividades dentro das organizações, tendo ainda como base a orientação fornecida dentro da ISO 27001.

Esta ISO contém as diretrizes estabelecidas e os princípios para começar, executar, manter e modificar melhorias na gestão da segurança da informação dentro de uma organização padrão. Tendo assim, os controles sendo listados em um padrão que visa atender a necessidades especificas das organizações, identificando tais fatores através de uma avaliação de risco formal. Como sabemos que os vários campos que regem uma organização sempre andam juntos, sendo eles o setor de tecnologia, pessoas, gestão, processos, segurança e negócios, nada mais coerente do que os projetos de TI estarem focados nas melhores práticas de gestão em segurança da informação, até porque a informação é definida como a alma do negócio, pois não se faz necessário apenas ser o detentor dela, mas principalmente, saber como gerenciá-la e lidar com os chamados ativos da informação, provendo assim, os seus princípios elementares: integridade, confidencialidade e disponibilidade.

Sendo uma norma que não é utilizada para auditorias e tirar certificações, porém a maior parte que constitui seu framework consiste em uma diversidade de boas práticas na gestão de projetos, organização de processos e pessoas, como também na estruturação de ferramentas adequadas para o seu embasamento. Dessa maneira, podemos notar que o gerenciamento de projetos, tem elementos adequados e que se enquadram a ISO 27002, por exemplo, trata-se a comunicação quando se trabalha a gestão de riscos, tendo os ativos e todo ciclo de vida que rege um projeto através da informação, pois tal maturidade levará a conseguir constituir de forma menos traumática a formação do SGSI, que é parte integrante para fundamentar de forma concreta tal norma.

Podemos assim dizer que todo este conjunto de sistemas se acoplam para originar este projeto de SGSI, podendo então listar algumas das razões básicas para se adotar a ISO 27002, sendo as seguintes:

1. Possui uma governança corporativa nos seus fundamentos de aplicação;
2. Cria uma melhoria na Segurança da Informação de forma mais eficaz;
3. Gera um diferencial de mercado;
4. Atende aos requisitos das partes interessadas e clientes;
5. É uma norma única que tem aceitação global;
6. Busca a redução potencial no valor do seguro;
7. Têm foco nas responsabilidades dos funcionários;
8. Essa norma cobre TI como também a organização, o pessoal e as instalações;
9. Condiz e segue a legislações.

Portanto o fato de conhecer a existência desta ISO, deveria se torna um fato obrigatório para os gestores das empresas, pois antes de se exigir o resultado final, teria que ter uma compreensão melhor do porquê do fato não ter alcançado o objetivo que se esperava, tendo em vista que o simples fato de às vezes se subestimar os processos utilizados para criar o mapeamento dos riscos, ignorando a implantação de normas e políticas de segurança da informação, fazendo com que não haja uma classificação devida dos ativos da informação produzindo um quadro crítico do negócio, dentre outros aspectos ignorados durante o processo, fazendo necessário a utilização da norma para se ter um maior controle e estabilidade no desenvolvimento das atividades nas organizações.

3.3 ISO 27003

A ISO 27003, busca focar nos aspectos críticos e necessários para a implantação de projetos bem-sucedidos de um Sistema de Gestão da Segurança da Informação. A norma representa o processo de especificação de um projeto de SGSI, desde a fase de concepção até a elaboração dos planos de implantação, também descreve o processo para obter a aprovação da direção para implementação do SGSI, como também define um projeto para implementar um SGSI, fornecendo direções sobre como planejar o projeto, como também os resultados que devem ser alcançados em um plano final para ter a implantação do SGSI.

Sendo assim, a implementação de um SGSI além de ser um processo importante e normalmente feito em uma organização na forma de um projeto, possuindo uma inicialização na fase de planejamento o que proporciona uma maior estabilidade para a definição do projeto, podemos então categorizar o processo de planejamento em 5 fases:

a) Obtenção da aprovação gerencial para dar início ao projeto.
b) Definição da estrutura do projeto, juntamente com eu escopo e de sua política.

c) Execução de uma análise da organização.
d) Criação e aplicação de uma avaliação de riscos contendo um o tratamento dos riscos encontrados na organização.
e) Criação de um modelo que servira como referência de controle para a aplicação e gerenciamento dos riscos (modelagem).

Portanto cada fase acima é representada por uma clausula que possui: a definição dos objetivos a serem alcançados em determinada fase; e as atividades necessárias que são executadas para se alcançar os objetivos definidos. Tendo que cada atividade por sua vez é e pode ser definida em subcláusulas que define o que deve ser feito, sendo elas:

Entrada: têm os dados necessários, como documentos, até mesmo documentos de saídas que foram resultados de outras atividades já finalizadas.
Guia: possui informações especificas e que auxilia e possibilita na entrega das atividades.
Saída: constitui os resultados que podem ser entregues ao termino de uma atividade.
Outras informações: constitui qualquer informação com fundamentação que auxilie na realização da tarefa, como de outras atividades que virão a surgir.

Onde a certificação de tal norma geralmente envolve um processo de auditoria em dois passos, caracterizados a seguir: no primeiro, é realizado uma revisão da existência e da complexidade da documentação chave que constitui a organização contendo a sua política de segurança, declaração de aplicação e o plano de tratamento de risco; já no passo dois, é realizado uma auditoria detalhada que envolva a existência e efetividade do controle das práticas de segurança contidas na declaração de aplicação e no plano de tratamento do risco, bem como a sua documentação de suporte. Dessa maneira, o processo descrito na ISO 27003 fornecerá apoio para a implantação de tal norma, tendo em vista a preparação de um plano para implantação do SGSI na organização, através da definição da estrutura organizacional do projeto já aprovada, sendo feito a estruturação das atividades que devem ser executados para atender tanto ao próprio SGSI como suprir os requisitos da ISO 27001.

3.4 PDCA

A estrutura cíclica PDCA é uma ferramenta que busca gerenciar e conseguir resultados eficazes e confiáveis em atividades que regem dentro de uma organização. Sendo um eficiente modo de desenvolver uma melhoria no processo, atuando de maneira padrão sobre as informações do controle da qualidade, evitando assim os erros lógicos nas análises, o que torna os dados gerados mais fáceis de serem entendidos. Podendo ainda ser utilizado para melhorar e tornar fácil a mudança para um estilo de administração direcionada, gerando uma melhoria continua, como também é aplicado para se obter resultados dentro de sistema

de gestão, podendo assim ser utilizado em qualquer empresa com a finalidade de gerar sucesso dos negócios.

Um fato curioso sobre tal estrutura, é que ele também pode ser conhecido como ciclo de *Deming* ou ciclo de *Shewhart*. Isso devido em 1930, Walter Shewhart ter apresentado uma estrutura que é aplicável no setor de administração da qualidade, sendo este o PDCA. No entanto, só no decorer dos anos 50, por meio de William Edwards Deming e suas explicações e fundamentações apresentadas em palestras no Japão, a estrutura PDCA veio se tornar conhecida nos demais continentes do mundo todo.

Depois de ter tido sua aplicação e exploração no Japão, o primeiro ciclo de Shewhart foi a partir daí bem visto, apesar que sua ideia original ainda era alvo de objeções. Ishikawa (1986) observou e determinou que o *plan-do-see* não era adequo ao povo japonês, pois na sua visão, o significado do verbo see (ver/olhar), "... propicia a atitude passiva de apenas se manter em expectativa". Mais Moen e Norman (1987) relatam uma curiosidade sobre a história que foi relatada pelo Dr. Noriaki Kano, sobre tal versão do fato, onde Deming havia ensinado para os japoneses que o verdadeiro significado de see não é restritamente ver ou revisar, mas sim tomar uma ação, ou *take action* no inglês.

Assim como esta ideia para eles parecia mais concreta, os japoneses decidiram integrar action ao modelo, omitindo take, conforme relembra Kano (1984) no seu relato. Tendo que o modelo adotado no Japão passou a ser o *Plan-Do-Check-Action*, que é o PDCA utilizado nos dias atuais como estrutura base para o desenvolvimento dos planos de gerenciamento, onde a sigla tem o seguinte significado: Plan (Planejar), Do (Executar/Desenvolver), Check (Verificar/Checar) e Act (Agir/Atuar).

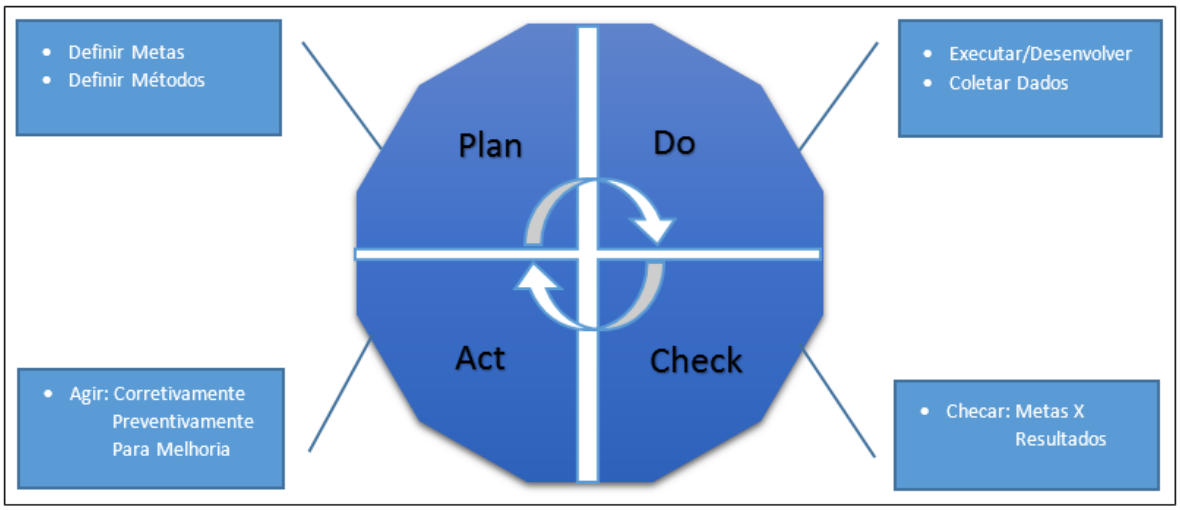

Figura 1 Modelo de Estrutura PDCA

Fonte: Próprio Autor

Plan (Planejar): Neste ponto, o gestor determina as metas identificando os elementos causadores de problemas que possam impedir o objetivo que se espera conquistar com as metas, sendo necessário se fazer a análise dos fatores que venham a influenciar nesse problema, como também identificar possíveis causas que o geram. Afinal, o gestor precisa ter e definir um plano que tenha uma ação eficiente.

Do (Executar/Desenvolver): A partir daqui, é aconselhável realizar todas as atividades que foram determinadas e estabelecidas dentro do plano criado pelo gestor e ainda coletar dados que serão usados na próxima etapa de verificação dos processos.

Check (Verificar/Checar): Depois de temos planejado e posto em prática, o gestor a partir deste momento necessita monitorar e avaliar de forma constante os resultados e dados obtidos com a realização das atividades. Fazendo assim, uma avaliação dos processos e resultados, comparando-os com o que foi determinado no planejamento, alcançando os objetivos, especificações e resultados finais desejados, podendo assim, consolidar as informações e posteriormente criar relatórios mais específicos.

Act (Agir/Atuar): Por fim, é necessário tomar as providências geradas nas avaliações e relatórios criados sobre os processos, para que assim, se torne possível o gestor traçar novos planos de ação para melhoria da qualidade do procedimento, tendo em vista a correção da maior porcentagem de falhas e o continuo aprimoramento dos processos que regem a empresa.

Depois de analisarmos a estrutura PDCA e determinar para que ela serve, podemos assim, dizer que o objetivo desta ferramenta é garantir que com base nos resultados controlados seja possível aumentar o grau de eficiência de cada resultado seguinte, para que assim se encontre cada vez melhor e eficaz na aplicação de melhorias para o desenvolvimento da empresa. Sendo assim, qual a empresa que não quer implantar esta prática e aperfeiçoar todos os processos? Devido a esta grande utilidade e ainda ao fato de ajudar na prevenção de erros, o PDCA é considerado uma ferramenta de qualidade, podendo ser utilizada em empresas de porte micro, pequena, média ou grande, sendo um método que possui rapidez e eficácia na solução de problemas das organizações.

3.4.1 Vantagens e cuidados na utilização do Ciclo PDCA

Considerado o fato de ser uma das primeiras ferramentas de gestão da qualidade, o Ciclo PDCA auxilia de forma otimizada e constante na análise e controle sobre diversos processos existentes dentro de uma empresa. Tendo esta ferramenta um método amplo e aplicado para aumentar a confiabilidade e a eficiência das atividades e crescimento de uma organização, com sua estrutura de gestão baseada em quatro únicos passos, o que torna o ciclo uma das mais simples dentre as diversas ferramentas de qualidade criadas.

Têm um modelo perceptivo que torna fácil de aplicar e ainda gera ganhos reais para toda ou qualquer empresa que usá-lo. De forma geral, devemos recordar que o PDCA se trata de uma estrutura cíclica, portanto deve continuamente girar e dar procedimento a novos outros ciclos. E para isso se proceder, todas as etapas nela contida deve ter execução, pois a omissão de qualquer uma das fases pode causar consequências e erros nos processos como um todo.

Tendo em vista isso, ao se fazer a aplicação e elaboração do plano gestor com base na estrutura cíclica PDCA, deve-se evitar atitudes como: executar sem planejar; parar o ciclo depois de completar uma volta; planejar, executar, verificar, mas não agir de forma corretiva; como também determinar metas as pessoas que irão executa-las sendo que as mesmas não se encontram preparadas para a execução dessas metas sem saber como fará ou os métodos que irá usar para atingi-las.

Sendo assim, podemos criar e estimular o melhoramento e ainda alterar as diretrizes de controle, pois o Ciclo PDCA pressupõem que as coisas podem ter sempre um melhoramento a partir dos parâmetros em que já se encontra a estrutura para dar início a um novo ciclo. Por tal fator, deve-se estar atento as possíveis curvas e extraviamentos de qualidade ruim em relação ao planejamento pré-elaborado. Em caso de ocorrer isso, a equipe que faz utilização e aplicação do PDCA deverá buscar agir de modo que devesse manter o andamento do ciclo ao máximo do planejado, a fim de se ter mais eficiência com relação ao aperfeiçoamento dos processos organizacionais. Vale ressaltar também que para alcaçar as vantagens na utilização do ciclo, o mesmo pode ser usado de forma conjunta com outras ferramentas de gerenciamento de qualidade, por exemplo, a utilização da Análise de **SWOT**[1] e o **5W2H**[2].

4. MODELO ESTRUTURAL PDCA DE SEGURANÇA

Após vermos toda essa definição mais especifica, vamos ver neste setor do trabalho a análise da estrutura PDCA mais abaixo, voltada para os Sistema de Gestão de Segurança da Informação (SGSI), tendo ainda como base desta análise os assuntos discutidos no decorrer deste trabalho, envolvendo as normas ISO 27001, 27002 e 27003 que são essenciais para se ter uma maior garantia de eficácia e confiabilidade no manuseio da informação e de sua proteção, proporcionando um ambiente mais planejado e projetado para os parceiros e clientes das organizações.

1 O termo "**SWOT**" é as siglas iniciais das palavras *strengths*, *weaknesses*, *opportunities* e *threats,* que significam respectivamente: forças, fraquezas, oportunidades e ameaças.

2 Representa os termos *What* (o quê), *Who* (quem), *Why* (por quê), *Where* (onde), *When* (quando), *How* (como) e *How Much* (quanto) da língua inglesa, que são simples perguntas e que servem de apoio ao planejamento.

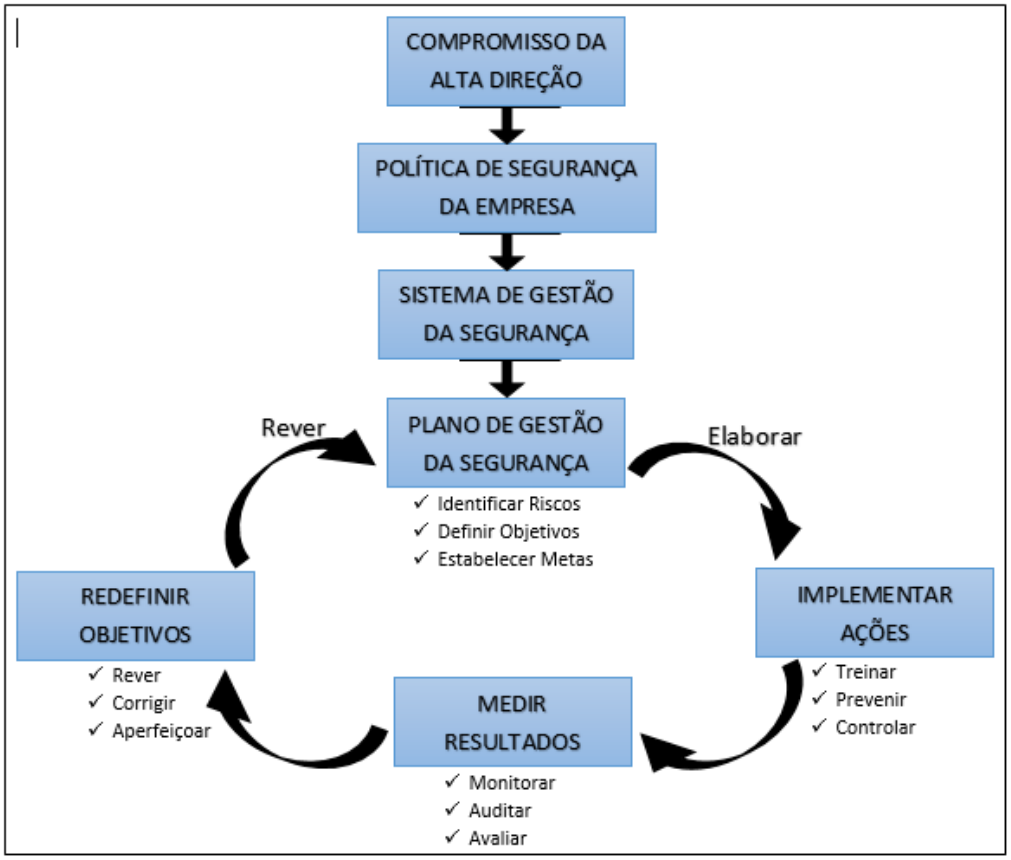

Figura 2 Modelo de Estrutura PDCA da Segurança

Fonte: Próprio Autor

4.1 Compromisso da alta direção

É necessário que haja um comprometimento da alta direção para que esses processos funcionem excepcionalmente bem. Deve ser dado atenção ao ciclo do PDCA para que seja bem executado, e para isso é preciso que se tenha um envolvimento das pessoas, como também reuniões, onde os colaboradores coordenam as atividades, se reunindo para propor melhorias em toda a organização.

Sendo necessário a participação ativa da alta direção da empresa no apoio à equipe de trabalho, fazendo o acompanhamento da realização das ações e incentivando os envolvidos na busca de resultados melhores para o projeto, sendo que para os resultados serem alcançados deve-se ter comprometimento tanto dos dirigentes e funcionários de todos os níveis e funções, como em especial os da alta direção.

4.2 Política de Segurança

A abundância de ferramentas e tutoriais disponíveis na internet permite qualquer pessoa, a realizar ataques a infraestrutura de TI de uma organização e com o número crescente

de roubos de dados esse assunto é tratado com extrema importância nas organizações atualmente.

É constante o aumento do risco de roubo de dados confidenciais e estratégicos dentro das organizações, pelos ataques de *hackers* e pela espionagem das organizações concorrentes. Visando eliminar os riscos que enfrentam as organizações estão investindo em equipamento de segurança, tendo a inserção de uma política de segurança juntamente com sua manutenção.

Para elaborar as políticas de segurança da organização, o comitê deve ter embasamento nos padrões e normas supramencionadas, entre eles a BS7799/ISO17799 (Beal, 2008), onde a Política de segurança é um documento que descreve as práticas de segurança, as responsabilidades, as normas e as recomendações. Mas não existe uma política de segurança padrão, pois a política deve ser apropriada às características de cada organização. A construção de uma política é bastante complexo e precisa de um constante monitoramento e também ser revisada e atualizada. E os seus resultados só serão conhecidos a médio e longo prazo.

Segundo a (ISO/IEC 17799:2005) "Convém que a direção estabeleça uma política clara e demonstre apoio e comprometimento com a segurança dos dados e informação através da emissão e manutenção de uma política de segurança da informação para toda a organização".

Para a possibilidade de garantir os princípios básicos da segurança da informação, integridade, disponibilidade e confiabilidade, não adianta somente a criação de uma política de segurança, mas sim que ela seja realmente uma referência aos colaboradores.

"A simples utilização de mecanismos de segurança para a proteção dos recursos de um sistema de informação não é suficiente para garantir que os serviços de segurança desejados sejam alcançados. Sem a compreensão de todos os aspectos envolvidos na segurança de um sistema, todo o trabalho pode estar comprometido (Beal,2008) ".

O comitê criado deverá propor as políticas para a gestão da segurança da informação e seus recursos, devendo realizar a implantação, o acompanhamento e as revisões. A política de segurança dever estar adequada a ISO/IEC 17799 e deverá estar de acordo com a legislação e cláusulas contratuais, estabelecendo as responsabilidades e as consequências das violações. Ela também deverá listar os seguintes tópicos:

- Controle de acesso: Cada pedido de acesso deverá ser documentado. É importante evitar a separação de função e a manutenção das auditorias registradas no sistema.

- Gerência de usuários e senha: Cada usuário é responsável pela sua senha, ela deve ser individual e trocada periodicamente.

● Propriedade da informação: Determina-se o responsável pela informação, o colaborador que poderá definir quem poderá ter acesso às informações e o nível de acesso permitido, também deve estabelecer a periodicidade necessária para se realizar o backup destes dados ou da própria informação.

● Desenvolvimento ou compra de sistemas: Com foco na integridade, disponibilidade e confiabilidade é importante determinar o fluxo interno da organização.

● Classificação da informação: Classificação pelo gestor das informações em relação aos princípios básicos da segurança (integridade, disponibilidade e confiabilidade).

● Segurança Física: Permissão de acesso a áreas de servidores deverá ser só com autorização. E deverá existir um controle de pessoas e equipamentos e entrarem e saírem.

● Plano de continuidade de negócios: Uma das fases de mais importância na política de segurança, onde será recomendado a elaboração de controles e padrões que especificarão os detalhes quanto ao plano de contingência e de continuidade dos negócios.

● Definição do escopo: Nessa fase é incluso o cálculo dos ativos que serão envolvidos. De acordo com a evolução do projeto ele deve ser revisado baseado no escopo. E fixar limites no escopo é de muita importância.

As políticas elaboradas devem ser entendidas e obedecidas por todos que fazem parte da organização e servir como referência e guia para a segurança da informação.

4.3 Sistema de gestão de segurança da informação

Nos dias de hoje a maioria dos dados nas organizações são trocadas e armazenadas entre vários sistemas automatizados. Logo, as decisões são tomadas a partir dessas informações contidas nos dados e passam por esses sistemas.

Um sistema de gestão de segurança da informação (SGSI) é um conjunto de processos e procedimentos, baseado em normas e legislação, que uma organização implementa para prover segurança no uso de ativos tecnológicos (Sêmola, 2003). O SGSI deve ser colocado em prática por todos que se relacionam com a infraestrutura de TI da organização (parceiro, colaboradores, terceirizados e etc.)

Para a implantação de um SGSI é realizada uma análise de riscos na infraestrutura de TI, onde é identificada as falhas nos sistemas e onde são vulneráveis. O usuário é um ponto fraco para invasão de sistemas, pelo fato do pouco conhecimento dos métodos realizados para as invasões. Por isso no SGSI é muito importante para sua implantação um programa de

treinamento e conscientização dos usuários em relação a segurança da dos dados que contém as informações.

A implementação de um SGSI começa definindo quais dos itens especificados em cada padrão devem ser implementados na organização. Visto que é necessário definir se os itens do padrão estão adequados às características da organização.

Assim, temos que o SGSI é um sistema de gestão sujeito a certificação através das evidências do conjunto de controles implantados e que devem ser constantemente executados e registrados. Sendo esse modelo de gestão baseado no ciclo com melhoria contínua PDCA.

Tendo o ciclo sido citado na BS7799 como "meio de facilitar o gerenciamento do projeto de segurança da informação". O ciclo se inicia com a fase *Plan*, depois passa para fase *Do*, passando subsequentemente para fase *Check* e depois a fase *Act*. Com o objetivo que o processo seja realizado constantemente e a cada novo ciclo, o sistema seja revisado e aperfeiçoado.

Sendo assim, nas duas primeiras fases do ciclo PDCA, que são as fases *Plan* e *Do*, é onde ocorre a implantação do SGSI, as outras duas fases, *Check* e *Act*, ocorre a verificação das medidas de segurança que foram especificadas e se estão sendo executadas as soluções para se ter uma melhoria contínua durante a sua utilização.

4.4 Etapas do Processo PDCA

Plano de Gestão da Segurança

Essa é a fase de planejamento do processo PDCA, é onde se estabelece os objetivos, os processos, a política e os procedimentos do SGSI, que são muito importantes para a melhoria da segurança e a gestão de riscos para que seus resultados sejam de acordo com as políticas e objetivos de uma organização.

a. Objetivo: Essa fase enxerga proteger os dados contra-ataques, com a finalidade de garantir que os serviços sejam contínuos e que sejam minimizados os riscos, por isso seu objetivo é criar uma política de segurança que seja de acordo com a missão e visão da organização.

b. Metas: Realizar o plano de gestão da segurança da informação no período de mais ou menos um ano. Com os seguintes programas: Programa de treinamento de pessoas: realizar treinamentos para os colaboradores da organização e adotar políticas de bom relacionamento e de motivação; Programa de segurança da informação: unir um grupo, formado por pessoas de todos os níveis para criar o plano de gestão da segurança. E esse grupo terá o papel de planejar, controlar, implementar e avaliar as políticas de segurança; e

também um Programa de capacitação de gestores: onde será realizado a capacitação dos gestores da organização e adotado políticas de bom relacionamento e de motivação.

Implementar Ações

A segunda fase do ciclo PDCA é onde se executa o planejamento, ou seja, coloca o plano de gestão da segurança que foi elaborado na fase anterior em prática, exatamente de acordo como foi estabelecido. Com a execução do plano, as mudanças no processo e as observações, deve ocorrer a coleta dos dados para a próxima etapa do ciclo.

a. Treinar e Prevenir: Examinar o que foi levantado na primeira fase do ciclo e executar as mudanças necessárias; realizar um levantamento de possíveis mudanças de funcionalidades de segurança do sistema; e executar um treinamento e capacitação para os colaboradores da organização.

b. Executar: Examinar relatórios de acessos aos sistemas, situação de equipamentos, backups, etc. Apurar aspectos positivos e negativos. Examinar dados das pesquisas e fazer uma comparação com o planejamento feito.

Medir Resultados

O terceiro passo do PDCA é realizar uma análise ou verificação dos resultados alcançados e dados coletados. Ela pode ocorrer concomitantemente com a realização do plano quando se faz a verificação do trabalho que está sendo feito e se da forma devida, ou após a execução, quando são feitas análises estatísticas dos dados e verificação dos itens de controle. Nesta fase podem ser detectados erros ou falhas. A partir dos dados coletados na execução deve-se comparar o resultado alcançado com a meta planejada.

a. Monitorar e Avaliar: Monitorar o que foi realizado e se os procedimentos foram claramente entendidos; como também se os processos estão sendo realizados de acordo com o que foi planejado; e verificar ainda se a execução dos processos está sendo feita corretamente e bem executada.

b. Auditar: As auditorias internas de qualidade também são necessárias para avaliar os resultados e se estão de acordo com o que foi planejado e realizado, tendo a seguinte avaliação: se atendem aos requisitos desta Norma e à legislação ou regulamento pertinentes; se atendem aos requisitos de segurança da informação identificados; se estão mantidos e implementados eficazmente; e se forão executados conforme o esperado.

Redefinir Objetivos

Esta é a última fase do PDCA onde é realização ações corretivas, ou seja, a correção das falhas encontradas no passo anterior. Após realizada a investigação das causas das falhas

ou desvios no processo, deve-se repetir, ou aplicar o ciclo PDCA para corrigir as falhas (através do mesmo modelo, deve-se planejar as ações, fazer, checar e corrigir) de forma a melhorar cada vez mais o sistema e os métodos de trabalho.

a. Rever e Corrigir: é preciso rever os todos os passos que foram realizados a fim de verificar se as metas propostas foram atingidas. Se durante a checagem ou verificação for encontrada alguma anormalidade, onde este será o momento de agir corretivamente, atacando as causas que impediram que o procedimento fosse executado conforme planejado.

b. Aperfeiçoar: assim que as falhas forem localizadas, as contramedidas deverão ser adotadas, isto é, as ações que vão evitar que o erro ocorra novamente. Em alguns casos, essas medidas podem virar normas, novos procedimentos, padrões, e etc.

5. METODOLOGIA

Teremos neste trabalho a utilização da metodologia PDCA para a integração das normas ABNT para segurança da informação, tendo em vista a busca pelo aumento do desenvolvimento da empresa, após ter feito todo um estudo na informação que a mesma detem para a geração de um plano de riscos que deve ser seguido para minimizar os problemas que a ameaçam.

Sendo assim com base em tal metodologia estrutural com integração de tais normas ISOs, podemos determinar através de etapas bem definidas por onde os dados passam se fazendo uma análise meticulosa, visando não deixar que nenhuma informação deixe de ser checada, pois ao final do ciclo teremos uma estrutura de riscos bem estabelecida que busca auxiliar a organização de forma continua e gradativa.

Mantendo, de tal maneira, a segurança em excelência através do documento de riscos gerado, que sempre irá evoluir no decorrer que o ciclo recebe cada vez mais informações para o aperfeiçoamento dos métodos que serão aplicados para se manter e estabelecer uma qualidade de eficácia e eficiência cada vez maior, tanto com a empresa como também com a informação que sempre estará em constante utilidade de serventia, como também segura.

Em vista disso, podemos determinar que no decorer do trabalho houve um bom embasamento teórico e uma boa fundamentação com base em várias fontes bibliográficas, gerando uma definição sólida sobre o PDCA e o conjunto das normas prospostas, solidificando o conceito de segurança dos dados e informação nas empresas. Após isso, o que se verá até a fase final deste trabalho numa posterior versão, será a validação através de um questionário da proposta apresentada neste trabalho juntamente com a citação de projetos paralelos a este que tenham um perfil parecido com o proposto aqui, e que venham a comprovar o que foi explanado nesta aplicação sobre a segurança da informação e suas soluções, como também um plano criado usando o PDCA e a ideia apresentada pelas normas, mostrando que atráves dessas ferramentas apresentadas e com a sua integração podem se tornar uma ótima arma de combate a incidentes de segurança para as organizações.

6. RESULTADOS

Neste ponto fica exposto a explanação da aplicação feita em uma empresa local de Mamanguape/PB, com nome de **G2 Soft**, atuante na área de desenvolvimento de software, cujo o dono se chama senhor **Paulo**, onde foi feito a aplicação de um questionário (apêndice 1) sobre o assunto abordado neste trabalho, como também foi passado o conhecimento contido no mesmo sobre as certificações tanto para dono como para os funcionários da empresa, destacando como tudo isso é importantes para gerar mais qualidade dos serviços e produtos, como também do próprio marketing, deixando em foco principal o quesito referente a segurança e como se pode usar o PDCA em conjunto com as ISOs para criar um plano que auxilie em sua gestão.

A seguir veremos as figuras gráficas geradas das questões aplicadas e uma breve explicação sobre cada uma delas. Vejamos os gráficos abaixo:

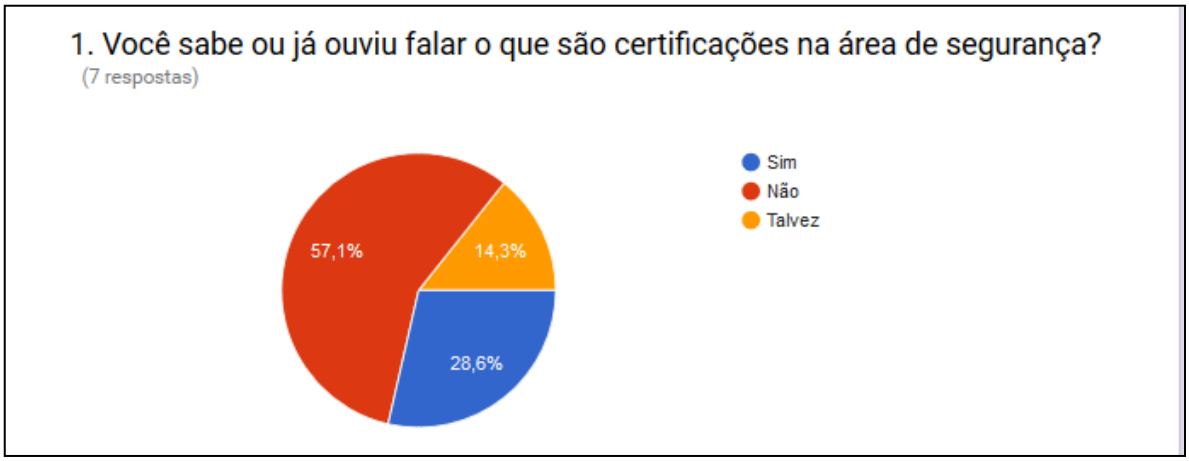

Figura 3 Gráfico Gerado da Questão 1

Fonte: Próprio Autor

Na questão 1 apresentada na figura acima, buscou-se saber se o pessoal da empresa possuía conhecimento sobre certificações, em foco na área de segurança, o que foi obtido como reposta foi uma grande porcentagem de 57,1% de pessoas que trabalham lá mais não possuem conhecimento sobre as certificações, tendo somente 28,6% que conhecem e responderam “sim”, deste modo fica claro a necessidade de se passar o conhecimento para a organização e deixa-los mais aptos sobre esse assunto e sua importância para o crescimento comercial.

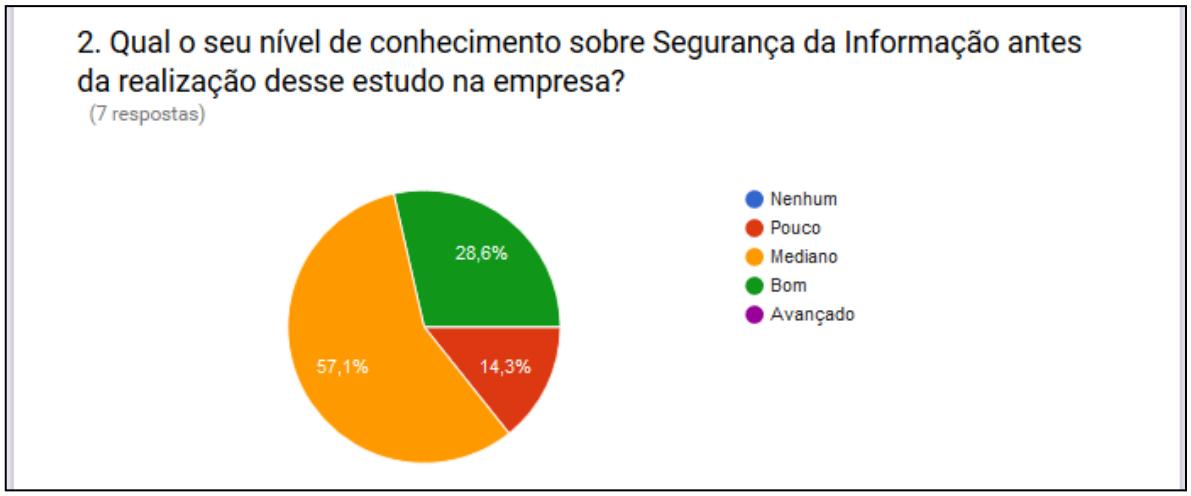

Figura 4 Gráfico Gerado da Questão 2

Fonte: Próprio Autor

Na sequência temos a questão 2 na figura acima, que teve o objetivo de coletar a informação sobre o conhecimento de modo geral sobre a seguranra da informação, que é um fator fundamental para se evitar incidentes na empresa, sendo obtido o valor de 57,1% pessoas que tem um conhecimento mediano e 28,6% que possuem um bom conhecimento sobre o assunto e técnicas gerenciais, o que fica visível um bom amadurecimento no quesito sobre a segurança.

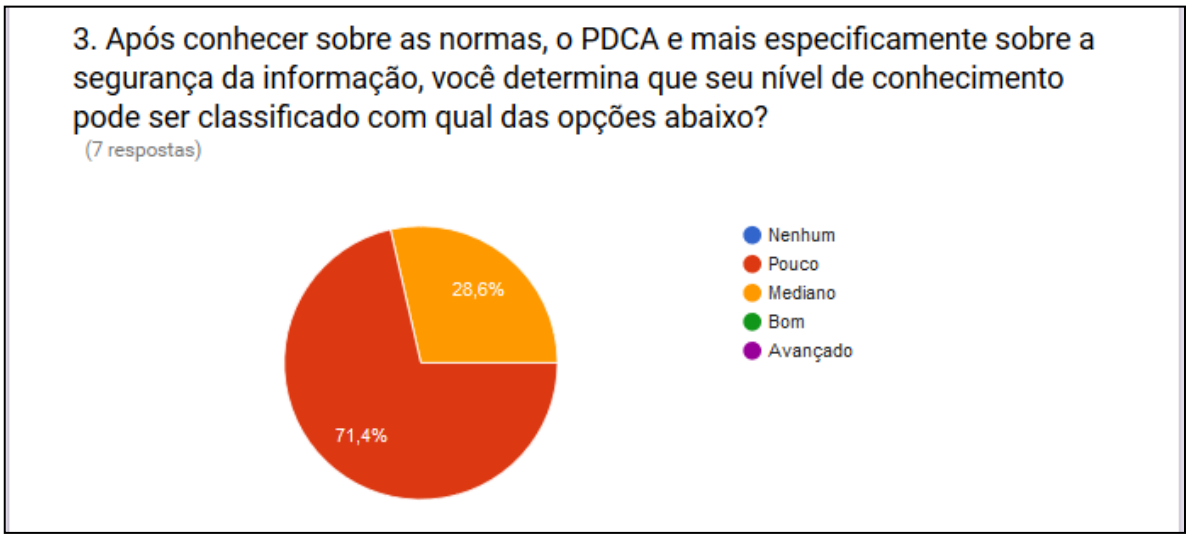

Figura 5 Gráfico Gerado da Questão 3

Fonte: Próprio Autor

Já no caso da questão 3 na figura acima, após uma explicação sobre o que este trabalho aborda foi feito essa pergunta para saber o quanto de conhecimento que antes era nulo foi adquirido com a explanação desse conteúdo e conceitos novos, sendo obtido 71,4% que agora possuem pouco conhecimento e 28,6% que adquiriram um conhecimento mediano sobre o assunto e o que ele quis passar para agregar um valor substâncial para a empresa.

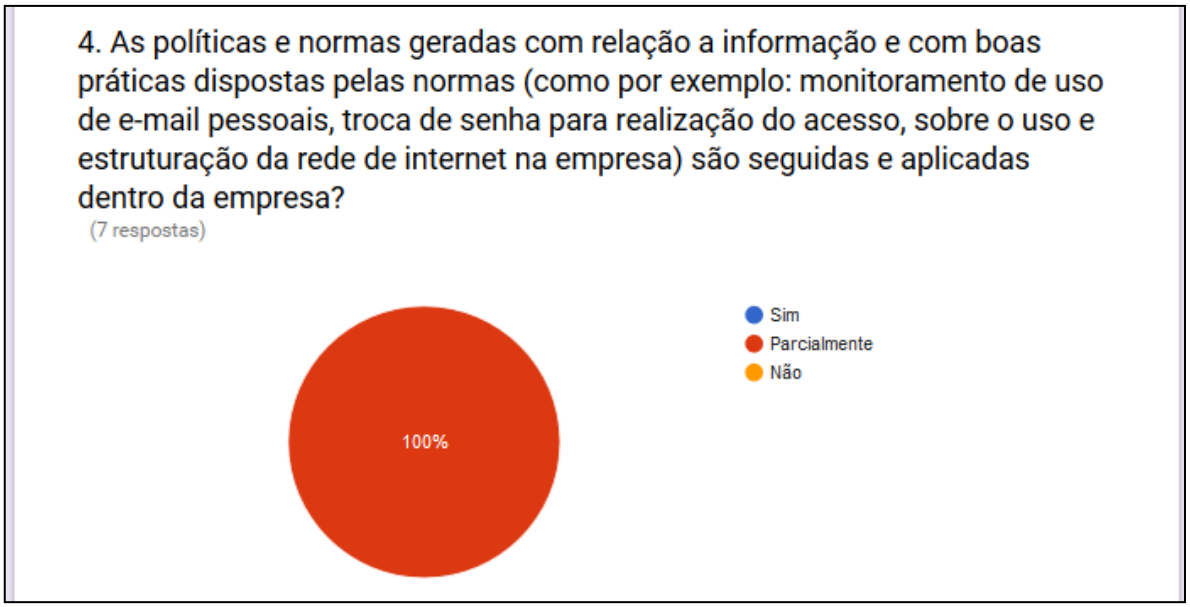

Figura 6 Gráfico Gerado da Questão 4

Fonte: Próprio Autor

Em seguida foi feito a questão 4 na figura acima, buscando-se coletar informações sobre práticas de segurança que aplicadas na empresa e que estão interligadas diretamente com alguns fatores expostos pelas ISOs desse trabalho, sendo adquirido 100% com resposta “parcialmente”, pois já aplicam algumas boas práticas para garantir a segurança dos dados, informações e do próprio produto da empresa. Identificando logo de cara como resposta do pessoal o gerenciamento superficial que é feito da rede de internet, evitando a invasão no sistema da empresa e garantido mais qualidade para realização de serviços propostos pela empresa, como por exemplo, o atendimento via internet de um técnico ao computador de um cliente para a realização de manutenção.

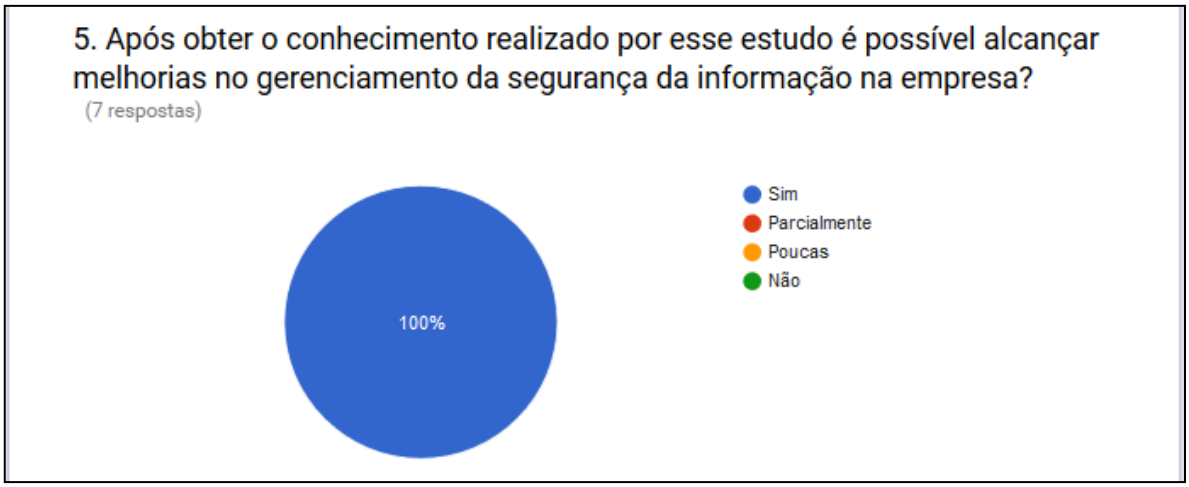

Figura 7 Gráfico Gerado da Questão 5

Fonte: Próprio Autor

Já na questão 5 na figura acima, foi buscado saber se a partir do estudo e conhecimento adquirido sobre o que este trabalho aborda e se torna possível a realização de melhorias na gestão de segurança da empresa, e como resultado tivemos 100% das respostas "sim", o que gera uma grande satisfação de trabalho realizado e como a disseminação desse estudo pode ser útil não só para o conhecimento como também para criar novas práticas na empresa.

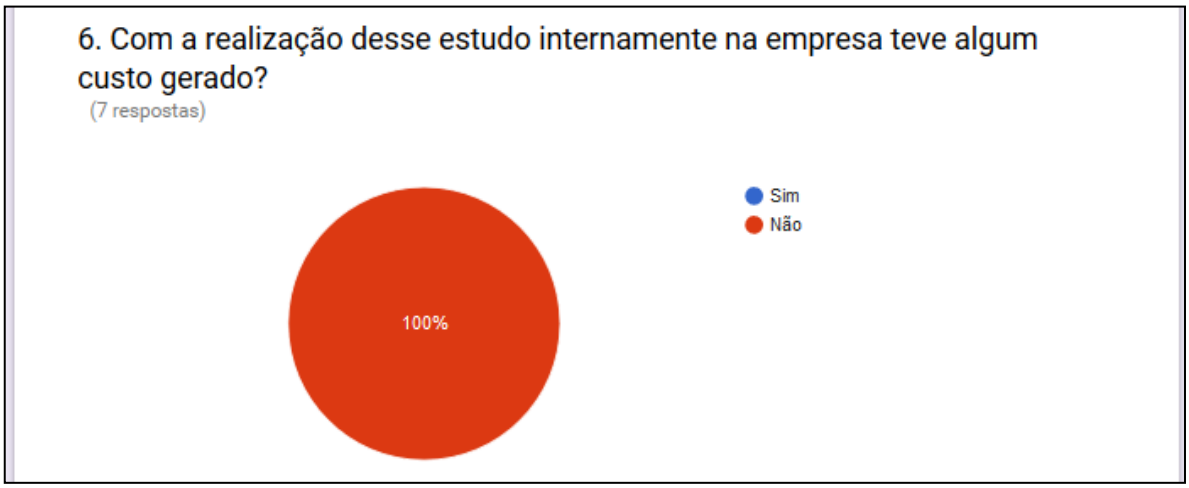

Figura 8 Gráfico Gerado da Questão 6

Fonte: Próprio Autor

Temos no sequencial a questão 6 na figura acima, que só teve a finalidade de avaliar se com a aplicação deste trabalho houve algum prejuízo financeiro momentâneo para a empresa e como resultado obteve-se 100% de respostas "não", o

que fica visível que além de auxiliar a empresa em seu crescimento e foi possível fazer isso sem gerar gastos ou perdas para a mesma.

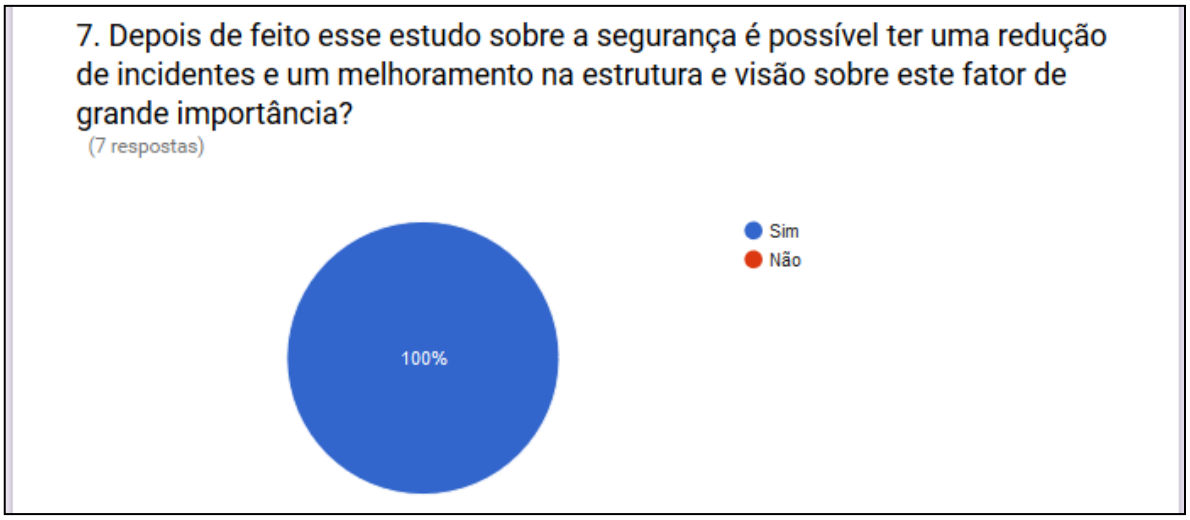

Figura 9 Gráfico Gerado da Questão 7

Fonte: Próprio Autor

A questão 7 na figura acima, tem como objetivo analisar se com a obtenção desse conhecimento fica possível a redução de incidentes na empresa e a busca de melhorias, onde se teve como resultado 100% de respostas "sim" ficando visível o grande aproveitamento do estudo para a empresa e para o amadurecimento do pessoal que constitue sua estrutura.

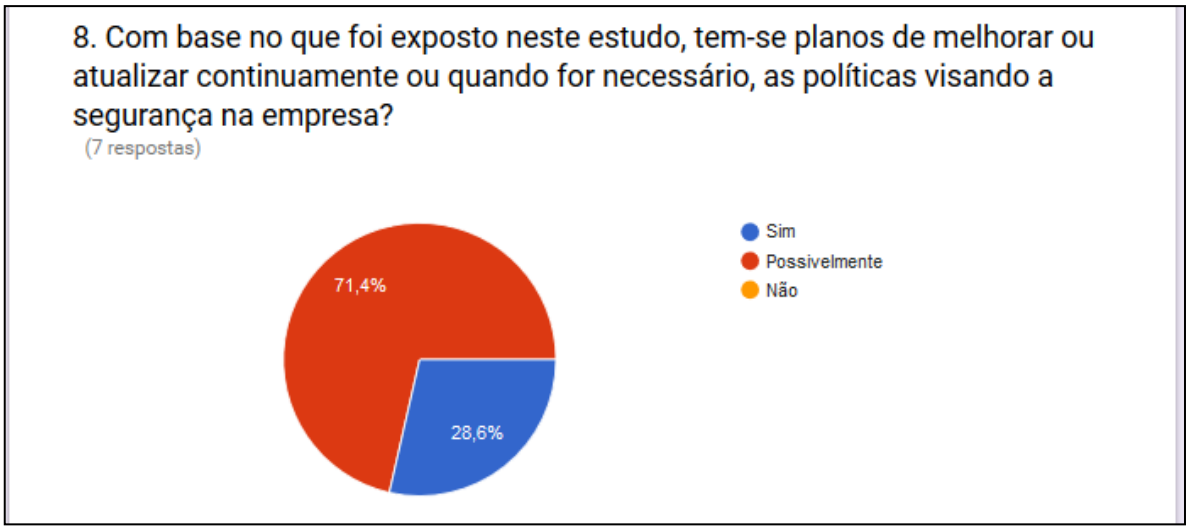

Figura 10 Gráfico Gerado da Questão 8

Fonte: Próprio Autor

Na questão 8 mais acima, foi feito a análise sobre um melhoramento continuo sobre as politicas relacionadas a segurança e suas práticas dentro da empresa para seu constante crescimento, onde tivemos como resultado 71,4% de respostas “possivelmente” e 28,6% de respostas “sim”. Deixando claro como a aplicação atingiu positivamente a empresa que antes possui um valor nulo com relação a utilização dessas práticas voltadas para a segurança.

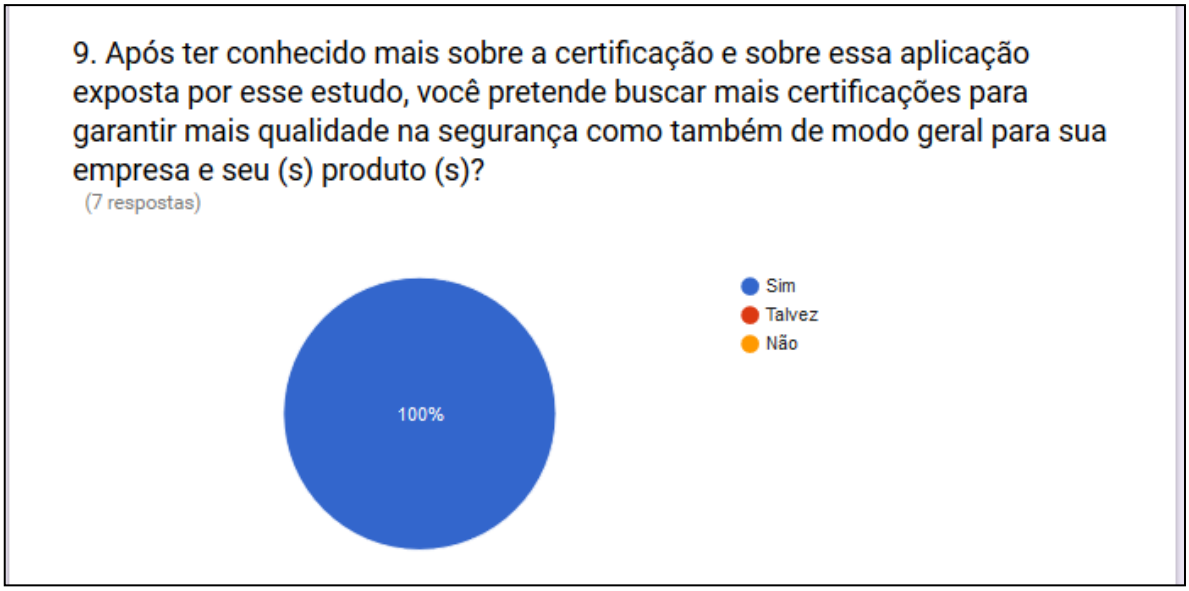

Figura 11 Gráfico Gerado da Questão 9

Fonte: Próprio Autor

E por fim a questão 9 na figura acima, que se objetivou em despertar na empresa o desejo de buscar certificações, se possível as apresentas neste trabalho para gerar um diferencial no ramo em que atua, tendo como resultado 100% das respostas “sim”. O que deixa uma grande satisfação de trabalho realizado e que fará com que a empresa cresça cada vez e alcance um destaque em seu mercado comercial atuante.

Sem mais delongas, vimos que com a aplicação foi possível passar um bom conhecimento para a empresa sobre o assunto abordade neste trabalho como também despertar a vontade de se buscar melhorar suas práticas voltados a segurança, como também buscar certificações para aumentar a qualidade garantida da empresa. Tendo ainda a geração de um primeiro plano PDCA voltado para a segurança com base nas ISOs e no que foi estudado no decorer desse trabalho, que pode ser visto ao final deste trabalho (apêndice 2).

7. TRABALHOS RELACIONADOS

Neste ponto fica explicito alguns links de trabalhos de mesma natureza ou similares ao que foi realizado e explanado neste trabalho, buscando mostrar que existe a preocupação e busca do conhecimento sobre a segurança da informação, como também a criação de politicas que auxiliem em sua gestão com base nas ISOs e em estruturas (ferramentas) auxiliadoras para sua implantação.

- Links:

- **Título do trabalho:** Aplicação das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 em uma média empresa. http://www.periodicos.unifacef.com.br/index.php/resiget/article/download/1065/848
- **Título do trabalho:** Fatores que Influenciam a Aceitação de Práticas Avançadas de Gestão de Segurança da Informação: um estudo com gestores públicos estaduais no Brasil. https://repositorio.ufrn.br/jspui/bitstream/123456789/12138/1/AnnaCSN.pdf
- **Título do trabalho:** Segurança da Informação. http://www.trabalhosfeitos.com/ensaios/Seguran%C3%A7a-Da-Informa%C3%A7%C3%A3o/677567.html
- **Título do trabalho:** Questões PDCA. http://www.trabalhosfeitos.com/ensaios/Quest%C3%B5es-Pdca/340814.html

Após se consultar os links acima pode-se notar que o assunto abordado neste trabalho já é uma preocupação presente em outros ambientes e nas empresas, que visam melhorar a segurança dos dados e garantir uma maior integridade e qualidade de seu manuseio e sua preservação.

8. CONSIDERAÇÔES FINAIS

Podemos assim determinar com base no que foi pesquisado neste trabalho que a estruturação de um PDCA com a integração das normas ISO 27001, 27002 e 27003 têm como finalidade auxiliar no gerenciamento dos risco que a organização sofre no setor de segurança da informação, provendo a criação de um SGSI que siga as especificações exigidas dentro dos parâmetros apresentados e que venha a proporcionar um crescimento quantitativo da empresa no mercado em que atua, fazendo com que seus negócios sejam mais bem gerenciados e administrados pelo gestor, seguindo o plano de riscos por ele criado.

Sendo fundamental para que as empresas adquiriram uma estruturação mais estável de suas atividades com base no que foi visto, podendo gerar um maior controle do escopo da

organização, além de prover uma garantia de segurança maior da informação, que proporciona uma maior confiabilidade para que os parceiros e clientes da empresa possam investir e confiar seus dados sem ter medo de perde-los (serem roubados), como também terem um controle do gerenciamento deles.

REFERÊNCIAS

BEAL, Adriana. **Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações** – São Paulo: Atlas, 2008.

ISHIKAWA, Kaoru. TQC – **Total Quality Control: estratégia e administração da qualidade**. Trad. Mário Nishimura. São Paulo: IMC, 1986.

KANO, N. et al. **Attractive quality and must-be quality**, Hinshitsu, v.14, n.2, p.147-56, 1984.

LAUREANO, Marcos Aurelio Pchek. **Uma Abordagem Para a Proteção de Detectores de Instrução Baseadas em Máquinas Virtuais.** Dissertação de Mestrado apresentado ao Programa de Pós-Graduação em Informática Aplicada da Pontifícia Universidade Católica do Paraná, 2004.

Moen, R. and Nolan, T. 1987. **Process Improvement, Quality Progress**, Sept. 1987, page 65.

NBR ISO/IEC 17799:2005 – **Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Associação Brasileira de Normas Técnicas – Rio de Janeiro: ABNT, 2005.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma visão Executiva**. – Rio de Janeiro: Campus, 2003.

APÊNDICE 1: QUESTIONÁRIO

UFPB: CAMPUS IV LITORAL NORTE

CENTRO DE CIÊNCIAS APLICADAS E EDUCAÇÃO

BACHARELADO EM SISTEMA DE INFORMAÇÃO

O PDCA como elemento integrador das normas ABNT 27001, 27002 e 27003

Emmanuel Gomes Souza
Orientadora: Prof.ª Dr.ª Adriana Z. Clericuzi

Este trabalho está sendo feito com o objetivo de se fazer uma análise a respeito da aplicação de boas práticas, que através desse questionário será feito a coleta de informações a respeito da segurança modelado e estruturado pelo PDCA com base no que diz as ISOs 27001, 27002 e 27003, como também sobre o conhecimento das certificações.

Peço que por favor, façam o preenchimento deste questionário, levando as considerações o que se está sendo imposto por cada questão abaixo. Desde já agradeço por sua ajuda, muito obrigado!

Questões

1. Você sabe ou já ouviu falar o que são certificações na área de segurança?
   ( ) Sim.
   ( ) Não.
   ( ) Desconheço.

2. Qual o seu nível de conhecimento sobre Segurança da Informação antes da realização desse estudo na empresa?
   ( ) Nenhum. ( ) Bom.
   ( ) Pouco. ( ) Avançado.
   ( ) Mediano.

Trabalho de Conclusão de Curso apresentado pelo aluno **Emmanuel Gomes Souza** sob a orientação da professora **Adriana Z. Clericuzi** como parte dos requisitos para obtenção do grau de Bacharel em Sistemas de Informação na UFPB Campus IV.

3. Após conhecer sobre as normas, o PDCA e mais especificamente sobre a segurança da informação, você determina que seu nível de conhecimento pode ser classificado com qual das opções abaixo?

   ( ) Nenhum. ( ) Bom.

   ( ) Pouco. ( ) Avançado.

   ( ) Mediano.

4. As políticas e normas geradas com relação a informação e com boas práticas dispostas pelas normas (como por exemplo: monitoramento de uso de e-mail pessoais, troca de senha para realização do acesso, sobre o uso e estruturação da rede de internet na empresa) são seguidas e aplicadas dentro da empresa?

   ( ) Sim.

   ( ) Parcialmente.

   ( ) Não.

5. Após obter o conhecimento realizado por esse estudo é possível alcançar melhorias no gerenciamento da segurança da informação na empresa?

   ( ) Sim, muitas.

   ( ) Parcialmente.

   ( ) Poucas melhorias.

   ( ) Não, nenhuma.

6. Com a realização desse estudo internamente na empresa teve algum custo gerado?

   ( ) Sim.

   ( ) Não.

7. Depois de feito esse estudo sobre a segurança é possível ter uma redução de incidentes e um melhoramento na estrutura e visão sobre este fator de grande importância?

   ( ) Sim.

   ( ) Não.

8. Com base no que foi exposto neste estudo, tem-se planos de melhorar ou atualizar continuamente ou quando for necessário, as políticas visando a segurança na empresa?

( ) Sim.

( ) Possivelmente.

( ) Não.

9. Após ter conhecido mais sobre a certificação e sobre essa aplicação exposta por esse estudo, você pretende buscar mais certificações para garantir mais qualidade na segurança como também de modo geral para sua empresa e seu (s) produto (s)?

   ( ) Sim.

   ( ) Talvez.

   ( ) Não.

APÊNDICE 2: PLANO PDCA VOLTADO À SEGURANÇA

Plano: G2 Soft

➔ Elaboração do primeiro ciclo do plano da empresa para melhoramento da segurança.

- **Pontos iniciais para garantir criação do plano**:

- Atuação de toda a hierarquia da empresa na definição e identificação de fatores para a criação desse primeiro plano;
- Análise da existência de uma politica de segurança já existente: identificado uso de segurança DHCP da internet e não uso de computadores da empresa para a realização de aceso pessoal;
- Não possue um sistema de gestão especifico de segurança na empresa.

- **Plano de Gestão da Segurança**:

- Definir um período para a mudança de senhas mais constante na empresa para acesso do sistema interno e da própria rede de internet;
- Usar um programa de monitoramento de rede que resolva o problema antes que os usuários percebam que está indisponível, por exemplo, o solarwinds;
- Evitar o uso de ferramentas de transporte de dados e arquivos (pen-drive) pessoas de próprio uso em outros ambientes nos computadores da empresa;

- **Implementar Ações**:

Neste ponto fizemos uma análise dos pontos determinados anteriormente no planejamento para ver o que era possível ser executado de imediato para aumentar a segurança na empresa e o que ficaria para uma nova rotação do ciclo em sua versão seguinte. Sendo feito a aplicação da mudança de senha; como também a suspenção do uso de ferramentas pessoas na empresa nos computadores.

- **Medir Resultados**:

Com base no que foi definido no planejamento e colocado em ação na implementação, foi possível a realização e aplicação dos seguintes pontos propostos com base na estrutura de segurança que a empresa possui, sendo eles:

- Definir um período para a mudança de senhas mais constante na empresa para acesso do sistema interno e da própria rede de internet;
- Evitar o uso de ferramentas de transporte de dados e arquivos (pen-drive) pessoas de próprio uso em outros ambientes nos computadores da empresa;

- **Redefinir Objetivos**:

Após a aplicação desse primeiro ciclo do plano, o único ponto pendete e que não foi executado por motivos de necessitar ser feito um estudo mais a fundo sobre ferramentas e qual a mais eficiente, sendo o ponto não executado e pedente para uma nova versão do ciclo o seguinte:

- Usar um programa de monitoramento de rede que resolva o problema antes que os usuários percebam que está indisponível, por exemplo, o solarwinds;
- Definir novos pontos para aplicação na empresa na segunda versão do ciclo...

Trabalho de Conclusão de Curso apresentado pelo aluno **Emmanuel Gomes Souza** sob a orientação da professora **Adriana Z. Clericuzi** como parte dos requisitos para obtenção do grau de Bacharel em Sistemas de Informação na UFPB Campus IV.