UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
UNIDADE ACADÊMICA GARANHUNS

SAMIR JOSUÉ LARANJEIRA SOARES

Análise e Proposta de Diretrizes para um Sistema de Gerenciamento de Segurança da Informação no Instituto Nacional do Seguro Social de Garanhuns – INSS/GEXGAR

GARANHUNS
2019

SAMIR JOSUÉ LARANJEIRA SOARES

Análise e Proposta de Diretrizes para um Sistema de Gerenciamento de Segurança da Informação no Instituto Nacional do Seguro Social de Garanhuns – INSS/GEXGAR

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação da Unidade Acadêmica de Garanhuns da Universidade Federal Rural de Pernambuco.

Orientador: Assuero Fonseca Ximenes

GARANHUNS

2019

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Biblioteca Ariano Suassuna, Garanhuns-PE, Brasil

S676a Soares, Samir Josué Laranjeira
Análise e Proposta de Diretrizes para um Sistema de Gerenciamento de Segurança da Informação no Instituto Nacional do Seguro Social de Garanhuns – INSS/GEXGAR / Samir Josué Laranjeira Soares. - 2019.
55 f. ; il.

Orientador: Assuero Fonseca Ximenes.
Trabalho de Conclusão de Curso (Graduação em Ciência da Computação)-Universidade Federal Rural de Pernambuco, Departamento de Ciência da Computação, Garanhuns, BR-PE, 2019.
Inclui referências e anexo(s).

1. Segurança da informação 2. Sistemas de segurança 3. Sistemas de informação gerencial 4. Computação I. Ximenes, Assuero Fonseca, orient. II. Título

CDD 004

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação da Unidade Acadêmica de Garanhuns da Universidade Federal Rural de Pernambuco, aprovada pela comissão examinadora que abaixo assina.

_____

Prof. Dr. Assuero Fonseca Ximenes - Orientador

UAG

UFRPE

_____

Prof. Dr. Ryan Ribeiro de Azevedo - Examinador

UAG

UFRPE

_____

Prof. Dr. Rodrigo Gusmão Carvalho Rocha - Examinador

UAG

UFRPE

GARANHUNS

2019

AGRADECIMENTOS

Agradeço primeiramente a Deus, por tudo que ele tem me proporcionado na minha vida.

Aos meus pais, Socorro Laranjeira e João da Cruz, por acreditado em mim e terem sido meus primeiros professores e me guiar em caminho de valores. E minha família, irmã, tios e tias, primos e primas, pelo apoio sempre que precisava estavam prontos a me ajudar e me escutar.

A minha namorada, Yamuna Jaya, pela paciência e puxões de orelha para me incentivar.

Aos meus professores, em especial ao meu orientador Assuero Ximenes e Rodrigo Rocha, pela troca de conhecimento, incentivo, paciência e a confiança depositada em mim para a realização desse trabalho.

Aos chefes, André Ponte e Rogério Souza, por permitir que esse trabalho fosse executado na Gerência Executiva Garanhuns, me enviando os documentos, perguntando sobre o andamento da pesquisa, mesmo envolvendo uma burocracia. Aos servidores que responderam o questionário, a equipe de comunicação que enviou os e-mails.

Aos meus amigos, que de alguma forma contribuíram para a realização de trabalho.

RESUMO

A proteção da informação tornou-se um fator crítico para as organizações. Com o crescimento tecnológico e, principalmente, com o advento da Internet se criou um ambiente propício ao desenvolvimento de ameaças, as quais se aproveitam da ausência de um ambiente seguro e da deficiência de políticas de segurança para trazer prejuízos às organizações. Portanto, devido a essa ausência de segurança, surgiu à necessidade de investimento em Segurança da Informação, o que se deu por meio da criação de políticas de segurança da informação. Este trabalho trata-se de uma pesquisa descritiva e bibliográfica de natureza qualitativa apresenta uma análise da situação atual da segurança da informação em uma organização pública federal feita por meio de questionário e observação sistemática e, por meio desta análise, propor diretrizes de um Sistema de Gestão de Segurança da Informação – SGSI, em conformidade com as normas ABNT NBR ISO/IEC 27001 e 27002. A proposta tem como planejamento criar uma comissão com a alta direção e coordenação local, treinamento sobre as normas para os envolvidos no planejamento e implantação do SGSI, criação do escopo e política do SGSI, identificação de ativos e riscos, análise dos riscos, classificação da informação, criação da declaração de aplicabilidade, criação de novos e documentações dos controles existentes através de procedimentos, políticas e manuais, criação de indicadores, realizações de reuniões críticas e auditorias internas, e conscientização para todos envolvidos no SGSI da instituição. Desta forma, por meio da proposta, será possível classificar a informação, identificar os riscos relevantes que atingem as informações, selecionar controles das normas e construir um plano de ação para a implantação do SGSI.

Palavras-chave: Segurança da informação, Política de Segurança da Informação, Sistema de gestão de Segurança da Informação.

SUMÁRIO

INTRODUÇÃO 6
1 – REFERENCIAL TEÓRICO 9
1.1 – GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO 9
1.2 – GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO 11
1.3– GESTÃO DA SEGURANÇA DA INFORMAÇÃO 14
1.4 – SEGURANÇA DA INFORMAÇÃO 15
1.5 – ABNT NBR ISO/IEC 27001:2013 18
1.6 – ABNT NBR ISO/IEC 27002:2013 21
1.7 – ANÁLISE DO CENÁRIO ATUAL 22
1.8 – A POLÍTICA DE SEGURANÇA DA INSTITUIÇÃO 23
2 – PERCURSO METODOLÓGICO 27
3 – APRESENTAÇÃO E INTEGRAÇÃO DOS DADOS 29
3.1 – DETALHAMENTO DA ANÁLISE E PROPOSTA DO SGSI 38
CONSIDERAÇÕES FINAIS 45
REFERÊNCIAS BIBLIOGRÁFICAS 47
ANEXO I 51

Introdução

Na atualidade, a área de Tecnologia da Informação (TI) desempenha um papel insubstituível nas organizações, visto que a tecnologia tornou-se indispensável aos registros das informações necessárias para qualquer atividade, tanto no ambiente interno como externo das organizações.

Por causa deste crescimento tecnológico que traz benefícios, também traz um problema que preocupa tanto pessoas quanto organizações, de um modo geral, que é a segurança da informação. Este termo tem sido usado por especialistas da área de tecnologia de informação nas últimas décadas, mas pouco se tem feito para assegurar uma real proteção contra invasões e ataques cibernéticos que estão em evolução contínua e ocorrem a todo o momento em escala mundial, que torna informações de suas vítimas expostas ao público.

Com o passar dos anos, a informação tornou-se um bem econômico ou ativo organizacional e as maneiras de obter, lidar e utilizar a informação passaram a ser objeto de pesquisa com a finalidade de potencializar os benefícios inerentes a este ativo (LORENS, 2007). Seguindo este contexto, surgiu então a necessidade de manter esta informação segura, inclusive como um modo de proteger a organização.

Em face disto, a informação é considerada fonte de riqueza e, portanto, um dos principais ativos a serem protegidos. Por isso, subestimar a importância da segurança pode custar a sobrevivência da organização no mercado (NIMER, 1998).

Desta forma, a Informação é o elemento mais importante dentro da organização e envolve os aspectos técnicos, humanos e organizacionais e, por isso, é fundamental a definição de uma política para a segurança das informações. Assim, torna-se necessário elaborar políticas de segurança a fim de se evitar riscos que possam comprometer as organizações.

Em face a esses riscos, a segurança da informação vem sendo considerada uma necessidade real nas empresas e nas instituições, visto que a informação é o bem ativo mais valioso. Por isso, a segurança passa a ser um requisito estratégico, que interfere na capacidade das organizações de realizar negócios e no valor de seus produtos e serviços no mercado.

Por isso, uma política de segurança da informação deve ser composta por regras claras, praticáveis e sintonizadas com a cultura e o ambiente tecnológico da empresa e não apenas proteger as informações confidenciais, mas motivar as

pessoas que as manuseiam, mediante a conscientização e envolvimento de todos com a finalidade de garantir a segurança organizacional que, atualmente, representa um desafio e que passa por todas as pessoas envolvidas direta e indiretamente em relação as informações.

Nesse contexto, as informações nas organizações são protegidas, mas não de forma adequada e, por isso, expõe os ativos adotando práticas antigas, e não possuem um gerenciamento correto como o proposto por um Sistema de Gestão de Segurança da Informação (SGSI) que fornece controle das melhores práticas em relação a segurança da informação.

O SGSI é o resultado da aplicação planejada de objetivos, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para a segurança da informação.

Portanto, segurança representa a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não-autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança nas organizações.

Para tanto, foi traçado o seguinte objetivo geral que será analisar as normas de segurança da informação do INSS/GEXGAR (Instituto Nacional do Seguro Social/Gerência Executiva Garanhuns) comparando-as com as recomendações das normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013 e, com isso, propor diretrizes de um SGSI definindo regras e responsabilidades de acordo com a instituição. E como objetivos específicos foram mapear os processos e descrição das atividades a serem realizadas, baseado nas normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013, analisar as normas utilizadas pelo INSS para a segurança da informação, comparar a norma utilizada com as normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013, propor diretrizes um SGSI, definir regras e responsabilidades na organização para implementação do SGSI.

Neste sentido, este trabalho está organizado da seguinte maneira: no referencial teórico serão apresentados alguns fatores que motivaram a governança de TI, após nas subseções será discutida a gestão de riscos, gestão em segurança da informação, segurança da informação e a ABNT NBR ISO/IEC 27001 e a ABNT NBR ISO/IEC 27002. Posteriormente, na próxima seção, será abordado o percurso metodológico, no qual será elucidado o tipo de pesquisa, o sujeito, o campo e

instrumentos utilizados. Na seção seguinte será feita uma análise do cenário atual da organização.

Dando continuidade, na seção seguinte, será feito a apresentação e integração dos dados, ou seja, serão analisados os dados obtidos nas observações e no questionário referentes a segurança da informação com a finalidade de demonstrar as categorias resultantes deste processo de análise. Seguindo na próxima seção, será feito um detalhamento da análise e benefícios com a adoção de um SGSI baseado nas normas ABNT NBR ISO/IEC 27001 e a ABNT NBR ISO/IEC 27002. Para finalizar este trabalho, as considerações finais e as referências.

1 – Referencial Teórico

1.1 – Governança de tecnologia da informação

A Governança de TI surgiu no início dos anos 1990 como um subconjunto da Governança Corporativa para justificar a necessidade de se obter maior controle e clareza sobre os gestores corporativos. Ela concentra-se na estrutura das relações e processos para desenvolver, dirigir e controlar os recursos de TI de modo a alcançar os objetivos da organização por meio de um equilíbrio entre risco versus retorno sobre ativos de TI.

A Governança de TI é o termo usado para descrever a forma como as pessoas responsáveis pela governança de uma organização considerarão a TI em supervisão, monitoramento, controle e direção (ITGI, 2003). Ou seja, desenvolver o controle e direcionar o uso atual e futuro da TI significa avaliar e direcionar o uso da TI para dar suporte à organização e supervisionar seu uso para realizar os planejamentos, além de incluir a estratégia e as políticas de uso da TI dentro da organização.

Weill e Ross (2006) colocam que a Governança de TI é a definição dos direitos determinantes e do framework utilizado que estimulam comportamentos desejáveis na utilização da TI. O principal objetivo da Governança de TI é alinhar o setor de TI aos requisitos do negócio, considerando soluções de apoio, assim como a garantia da continuidade dos serviços e a mitigar a exposição do negócio aos riscos (FERNANDES; ABREU, 2014).

De acordo com Costa *et. al.* (2013), a TI assumiu um papel extenso na sociedade de um modo geral e sua decorrente evolução ao longo dos últimos 30 anos mudou o modo como as atuais organizações pensam e trabalham em seus processos administrativos, financeiros, logísticos, etc. Contudo, ao mesmo tempo em que a TI tem representado um importante avanço para as organizações, ela se mostra geradora de conflitos pela ausência do conhecimento adequado para sua aplicabilidade. Neste sentido, é importante avaliar o contexto atual das empresas desenvolvedoras de software de modo a definir estratégias que sejam adequadas para o seu desenvolvimento, tanto do ponto de vista do cliente como da empresa. Assim, serão observados especialmente os parâmetros pela Governança de TI. (BATISTA, 2015)

Existe hoje dentro das organizações um maior número de informações em formatos digitais, o que faz a TI desempenhar papeis mais importantes dentro das organizações, por exemplo: gerenciamento de ativos de TI, controles, transparências e previsões que antes era pouco gerenciada passaram a ser desempenhadas de forma sistêmica com base na governança de TI, garantindo, assim, maior transparência para seus investidores.

Para Batista (2015), a área de TI faz parte da realidade de praticamente toda organização na atualidade, mas nem sempre serão capazes de montar e manter uma equipe para preencher as suas necessidades nos processos. Desta forma, ao se tratar de uma área que vem sendo discutida e defendida por diversos teóricos como um dos principais ativos de uma organização constituindo importante vantagem competitiva, é que tem crescido a necessidade de *Outsourcing*. No entanto, muitas empresas, até aquelas que prestam serviços terceirizados de TI, se mostram despreparadas e enfrentam sérias dificuldades em seu exercício porque fogem dos requisitos básicos salientados pela governança de TI.

Assim, de acordo com Tarouco e Graeml (2011), a TI tornou-se essencial para que as empresas mantenham um processo de decisões efetivo, bem como um melhor controle em suas operações. Entretanto, essa revolução tecnológica trouxe processos relacionados à sua gestão e manutenção, exigindo que aspectos relativos à sua qualidade, bem como eficiência, eficácia e efetividade das informações, sejam devidamente controlados.

Uma boa governança de TI dentro das organizações não é só mais questões de garantir a conformidade da TI com o negócio da empresa ou controlar o ROI (*Return on investment*), retorno sobre seus investimentos, mas sim garantir a segurança das informações. Hoje em dia muitas organizações têm informações sigilosas quanto o cofre de um banco, onde que se essas informações caírem em mãos erradas a competitividade da empresa estará comprometida, podendo até perder ações no mercado. (MALLMANN, 2018)

Há várias ferramentas que têm por objetivo auxiliar as corporações durante o processo de planejamento e implantação da Governança, como a ITIL[1], o COBIT[2], a família ISO[3] 27000, o CMMI, dentre outros.

[1]Information Technology Infrastructure Library
[2]ControlObjectives For Information andRelated Technology
[3]International Organization for Standardization

É importante salientar a diferença entre os termos Gestão de TI e Governança de TI. Segundo Peterson (2004), existe uma clara diferença entre elas. A Gestão de TI tem como foco o fornecimento interno de serviços de TI e gerenciamento de suas operações atuais, enquanto a Governança de TI abrange áreas mais amplas, como a execução de demandas presentes e futuras, tanto dos negócios (foco interno), quanto dos clientes (foco externo). E de acordo com o COBIT 5 (ISACA, 2012), a Gestão é responsável pelo planejamento, desenvolvimento, execução e monitoramento em conformidade com as diretrizes a fim de atingir os objetivos organizacionais. Já a governança define a direção por meio de priorizações e tomadas de decisão, monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos pela organização.

1.2 – Gestão de riscos de segurança da informação

Existe várias definições para definir o risco, no entanto, a norma ABNT ISO/IEC GUIA 73:2009[4], que o define como “efeito da incerteza nos objetos”. Um efeito é um desvio em relação ao esperado - positivo e/ou negativo. A incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

O risco é entendido como alguma coisa que cria possibilidades ou produz danos. No que se refere à segurança, os riscos são reconhecidos como circunstâncias que geram ou agregam a potencialidade de perdas e danos. É possivelmente calculado por meio da probabilidade de um evento acontecer e causar perdas (SAMPAIO, 2014).

Está seção mostrará os conceitos fundamentais para a Gestão de Riscos e apresentará a norma ABNT NBR ISO/IEC 27005:2011 – Tecnologia da informação – Técnicas de segurança - Gestão de riscos de segurança da informação.

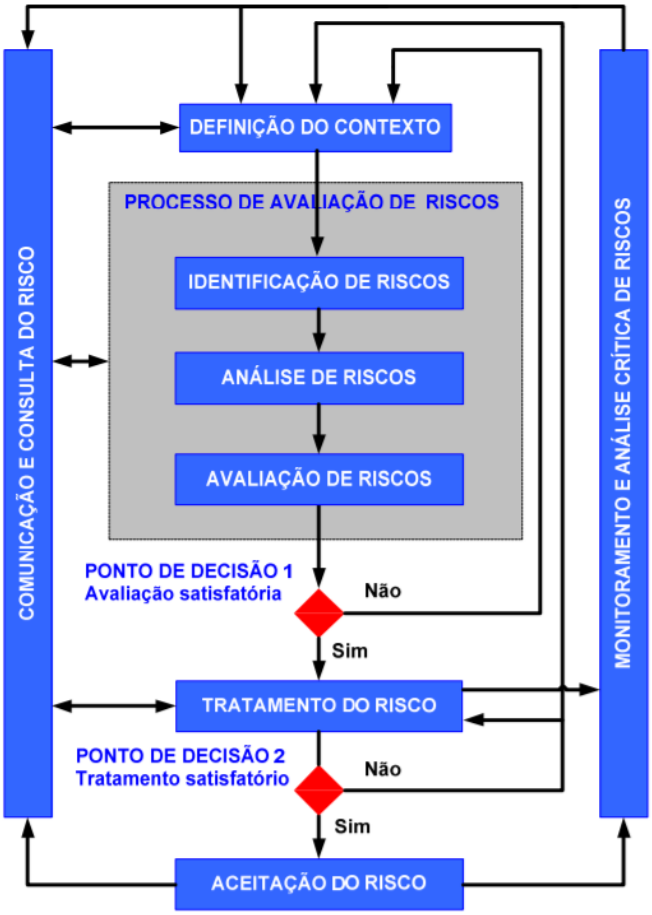
Esta norma que fornece orientações para o processo de gestão de riscos de segurança da informação, elaborada para facilitar a implementação da segurança da informação. Sua base está na abordagem de gestão de riscos – ISO/IEC 31000, que traz informações básicas, princípios e diretrizes para a implementação da gestão de riscos – podendo ser aplicada a todos os tipos de organizações, grandes, pequenas

[4] ABNT ISO/IEC GUIA 73:2009 – Gestão de riscos – Vocabulário – Recomendações para uso em normas

ou medias, desde que tenham a pretensão de gerir os riscos que poderiam comprometer a sua segurança da informação.

O processo de gestão de riscos de segurança da informação consiste na definição do contexto, processo de avaliação de riscos, tratamento do risco, aceitação do risco, comunicação e consulta do risco e monitoramento e análise crítica de riscos, como mostra a figura 1 (ABNT NBR ISO/IEC 27005, 2011).

Figura 1 – O processo de gestão de riscos da segurança da informação



Fonte: ABNT, 2011

Como mostra a Figura 1, o processo de gestão de riscos de segurança da informação pode ser iterativo para o processo de avaliação de riscos e/ou para as atividades de tratamento do risco. Um enfoque iterativo na execução do processo de avaliação de riscos torna possível aprofundar e detalhar a avaliação em cada repetição. A perspectiva iterativa permite minimizar o tempo e o esforço despendidos na identificação de controles e, ainda assim, assegura que riscos de alto impacto ou de alta probabilidade possam ser adequadamente avaliados.

Primeiramente, o contexto é estabelecido. Em seguida, executa-se um processo de avaliação de riscos. Se ele fornecer informações suficientes para que se determine de forma eficaz as ações necessárias para reduzir os riscos a um nível aceitável, então a tarefa está completa e o tratamento do risco pode suceder-se. Por outro lado, se as informações forem insuficientes, executa-se uma outra iteração do processo de avaliação de riscos, revisando-se o contexto (por exemplo: os critérios de avaliação de riscos, de aceitação do risco ou de impacto), possivelmente em partes limitadas do escopo (ver Figura 1, Ponto de Decisão 1).

A norma convém que a gestão de riscos de segurança da informação contribua para:

- Identificação de riscos;
- Processo de avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência;
- Comunicação e entendimento da probabilidade e das consequências destes riscos;
- Estabelecimento da ordem prioritária para tratamento do risco;
- Priorização das ações para reduzir a ocorrência dos riscos;
- Envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e mantidas informadas sobre a situação da gestão de riscos;
- Eficácia do monitoramento do tratamento do risco;
- Monitoramento e a análise crítica periódica dos riscos e do processo de gestão de riscos;
- Coleta de informações de forma a melhorar a abordagem da gestão de riscos;
- Treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los.

Em um SGSI, a definição do contexto, o processo de avaliação de riscos, o desenvolvimento do plano de tratamento do risco e a aceitação do risco fazem parte da fase "planejar". Na fase "executar" do SGSI, as ações e controles necessários para reduzir os riscos para um nível aceitável são implementados de acordo com o plano de tratamento do risco. Na fase “verificar” do SGSI, os gestores determinarão a necessidade de revisão da avaliação e tratamento do risco à luz dos incidentes e mudanças nas circunstâncias. Na fase “agir”, as ações necessárias são executadas, incluindo a reaplicação do processo de gestão de riscos de segurança da informação.

1.3– Gestão da segurança da informação

Diante da importância da informação para as organizações e da necessidade de proteger essas informações de qualquer forma do uso inadequado, então surge a gestão da segurança da informação, como forma de organizar e orientar os esforços da organização no sentido de evitar invasões, vazamentos e outras ocorrências que poderiam ser prejudiciais (CITTADIN, 2018).

Verifica-se que a gestão da segurança da informação não é apenas uma atividade, mas um processo permeado de cuidados, ações e medidas que envolvem cautela, atenção e uma busca para que os dados dos quais uma empresa disponibiliza não sejam utilizados de modo inadequado, colocando em risco os donos dessas informações (UNB, 2010).

É preciso que se desenvolva uma cultura que integre a gestão da segurança da informação nas atividades das empresas e órgãos públicos, considerando-se que a preocupação com o tema é real, as medidas criadas ainda são bastante incomuns, para conter o rápido crescimento dos ataques.

Enquanto não houver o entendimento de que a informação é patrimônio e, como tal, deve ser protegida, preconizada e resguardada da invasão de usuários não autorizados, já que esta pertence ao consumidor, que ofereceu esses dados e à empresa que recebeu os mesmos. Não deve haver intermediários, outras pessoas ou empresas que alcancem essas informações e delas façam uso de acordo com suas demandas particulares (CITTADIN, 2018).

Na maior parte dos casos em que a segurança não é tratada como prioridade, a razão está ligada à falta de conhecimento sobre a real ameaça de um ataque cibernético ou da falha de um sistema. É comum que o pequeno empresário acredite que a falha na segurança da informação esteja associada apenas às multinacionais (apesar da maior incidência), o que é um engano. Quando ela é negligenciada, pode custar muito caro, manchando a reputação do negócio (SANTANDER, 2019).

A gestão de segurança da informação envolve a definição e implantação de um Sistema de Gestão de Segurança da Informação (SGSI) que segue normas baseadas em padrões definidos pela ISO/IEC 27001:2013 e ISO/IEC 27002:2013. Na norma ISO/IEC 27001:2013, conforme a ABNT, são estabelecidos requisitos que possibilitam a definição, a implantação e a melhoria contínua de um sistema de

gestão de segurança da informação. Enquanto que na ISO/IEC 27002:2013 são definidas diretrizes que orientam a implantação destes requisitos.

Segundo Moura (2007) um SGSI é planejado para se certificar de que as seleções de controles de segurança sejam proporcionais e adequadas para proteger os ativos de informação e gerar confiança às partes interessadas. Um SGSI visa trazer parâmetros de resposta para alguns métodos que implementam, operam, monitoram, revisam, mantém e melhoram o sistema de gestão da segurança da informação. Pode-se definir um SGSI como uma equipe multidisciplinar que possui como principais objetivos estabelecer as políticas de segurança, ampliar o conhecimento envolvido e definir os seus responsáveis e as medidas a serem tomadas (ABNT ISO 27001, 2013).

1.4 – Segurança da informação

A segurança da informação evoluiu e saiu do nível técnico e restrito à área da TI, onde se preocupava em ter um sistema antivírus, um firewall bem configurado, para um nível de gestão, que além de pensar em tecnologia, precisa investir e desenvolver os processos, infraestrutura e pessoas.

A informação pode ser considerada o bem de maior valor para empresas privadas e públicas, assim como o recurso patrimonial mais crítico, pois quando adulterada, indisponível ou acessada por pessoas de mal intencionadas sem a devida autorização, ou por concorrentes, a imagem da instituição pode ser significativamente comprometida, assim como o andamento dos próprios processos institucionais. Ou seja, a continuidade de uma organização pode ser comprometida se não for dada a devida atenção à segurança de suas informações (BRASIL, 2014). Considera-se, então, que:

> Na sociedade da informação, ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes. Com isso, a segurança da informação tornou-se um ponto crucial para a sobrevivência das instituições. (BRASIL, 2007, p. 2).

A Segurança de Informação é definida na norma ISO/IEC 27000 (2009) como sendo a preservação da CID – Confidencialidade, Integridade e Disponibilidade–da informação. Partindo destes três pilares, procura-se garantir outras propriedades como o não-repúdio, a responsabilidade e a confiabilidade.

Concerino (2005, p. 155), define os três pilares básicos da segurança da informação:

a) **Confidencialidade**: refere-se ao sigilo de informações. Busca assegurar que a informação será acessível somente às pessoas devidamente autorizadas. Quando alguma informação é vista ou copiada por alguém que não possui autorização para fazê-lo, este aspecto da segurança não está sendo observado;

b) **Integridade**: refere-se à impossibilidade de alteração de informações na rede. Visa salvaguardar os dados e as informações, garantindo, assim, a veracidade e autenticidade da informação, bem como os seus métodos de processamento. A perda da integridade se dá quando, inexistindo a devida segurança, ocorre a modificação de um tópico importante, que pode ser alterado pelos mais surpreendentes motivos, até mesmo intencionalmente;

c) **Disponibilidade**: busca assegurar que dados, informações e sistemas estarão devidamente disponíveis sempre que solicitados. A ausência de disponibilidade ocorre quando a informação é deletada ou se torna inacessível ao usuário autorizado a consultá-la.

Segundo Lyra (2008, p.4), pode-se citar mais alguns aspectos complementares para garantia da segurança da informação:

- **Autenticação**: “Garantir que um usuário é de fato quem alega ser”.
- **Não repúdio**: “Capacidade do sistema de provar que um usuário executou uma determinada ação”.
- **Legalidade**: “Garantir que o sistema esteja aderente à legislação”.
- **Privacidade**: “Capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações”.
- **Auditoria**: “Capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque”.

A ABNT ISO/IEC 27002 (2005, p. ix) diz que a segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. Sêmola (2014) argumenta que segurança da informação é uma área de conhecimento dedicada a proteger ativos de informação contra acessos não autorizados, alterações indevidas ou indisponibilidade. Donner e

Oliveira (2008) conceituam segurança da informação como o processo de proteção das informações de ameaças para assegurar sua integridade, disponibilidade e confidencialidade. Muito já foi feito no sentido de aprimorar a segurança da informação, apesar de não ser possível erradicar completamente o risco de seu uso indevido, como observam Silva e Stein (2007, p.48).

A segurança da informação é obtida por meio de um conjunto de práticas e atividades como a definição/elaboração de processos, políticas de segurança da informação (PSI), procedimentos, treinamento de profissionais, uso de ferramentas de monitoramento e controle, dentre outros pontos.

Como princípio, a segurança tem a finalidade de proteger aquilo que tem valor para organização, que são seus ativos. De acordo com a ISO/IEC 27001:2013, um ativo é “qualquer coisa que tenha valor para organização”. Portanto, podem existir diversos tipos de ativos incluindo a própria informação (contratos e acordos, documentações de sistema, bases de dados, manuais de usuário, trilhas de auditoria, planos de continuidade, etc), pessoas e suas qualificações/experiências, ativos de software (sistemas, aplicativos, ferramentas, etc), ativos físicos (mídias removíveis, equipamentos computacionais, equipamentos de comunicação, etc), serviços (iluminação, eletricidade, refrigeração, etc) e aqueles que são intangíveis como é o caso da reputação da organização. (ABNT NBR ISO/IEC 27002:2013).

Figura 2 - Ativos de informação

Fonte: Lyra, 2008 – Adaptado.

Um dos fatores fundamentais de sucesso para a garantia da segurança da informação é a correta identificação, controle e constante atualização dos diferentes tipos de ativos.

Como princípio básico, é recomendado que todo ativo seja identificado e documentado pela organização. E para cada um deles deve-se estabelecer um

proprietário responsável que lidará com a manutenção dos controles que podem ser enviados a outros profissionais, porém, sempre sob a responsabilidade do proprietário.

Em face da responsabilidade dos ativos, deve-se realizar a sua correta classificação com base na importância, criticidade, sensibilidade e seu valor para o negócio. Como resultado, será possível definir os níveis adequados de proteção. (ABNT NBR ISO/IEC 27002:2013)

Desta forma, Garantir a segurança da informação exige a proteção dos ativos contra a perda, furto, alteração, divulgação ou destruição indevida. Toda organização precisa adquirir uma visão sistêmica das suas necessidades de segurança dos recursos a serem protegidos e das ameaças a que estão sujeitas. Enfim, utilizando um conjunto de controles que permite conhecer e gerir riscos, orientar as ações de continuidade do negócio, níveis de responsabilidade e conformidade com diretrizes, legislação e acordos contratuais como recomenda a norma ISO para segurança da informação.

1.5 – ABNT NBR ISO/IEC 27001:2013

A norma ABNT NBR ISO/IEC 27001 é uma norma internacional emitida pela *International Organization for Standardization* (ISO) e descreve como gerenciar a segurança da informação em organizações. A versão mais recente desta norma foi publicada em 2013.

A ISO 27001 pode ser implementada em qualquer tipo de organização, com ou sem fins lucrativos, pública ou privada, pequena ou grande. É escrito e revisado por grandes especialistas e fornece a metodologia para implementar a gestão da segurança da informação na organização. Também permite que uma organização seja certificada, isto significa que uma entidade independente confirma que a segurança da informação foi implementada naquela organização em conformidade com a ISO/IEC 27001.

O objetivo central da ISO 27001 é proteger a confidencialidade, integridade e disponibilidade da informação em uma organização. Isso é feito investigando quais são os possíveis problemas que podem afetar as informações e definindo o que precisa ser feito para evitar que esses problemas ocorram como mitigação ou tratamento do risco.

Isso significa que a filosofia principal do padrão ISO 27001 é baseada na gestão de riscos que se baseia em descobrir onde estão os riscos e então, tratá-los.

Uma vez que a implementação irá requerer a gestão de múltiplas políticas, procedimentos, pessoas, ativos, etc., a ISO 27001 descreve como encaixar todos esses elementos de forma coerente no sistema de gestão de segurança da informação (SGSI).

A ISO/IEC 27001 em suas versões anteriores, utilizava o modelo PDCA (*Plan-Do-Check-Act*) para estruturar o SGSI como mostra a figura 3. Apesar da versão atual, a ISO/IEC 27001:2013, não sugerir e explicitar na introdução o uso do ciclo PDCA, ele ainda pode ser aplicado. Ele é tão importante que o Anexo SL[5] requer que todas as normas ISO estruturem suas cláusulas principais em torno do ciclo PDCA conforme figura 4. As etapas do ciclo PDCA são definidas como:

***Plan* (estabelecer o SGSI):** Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.

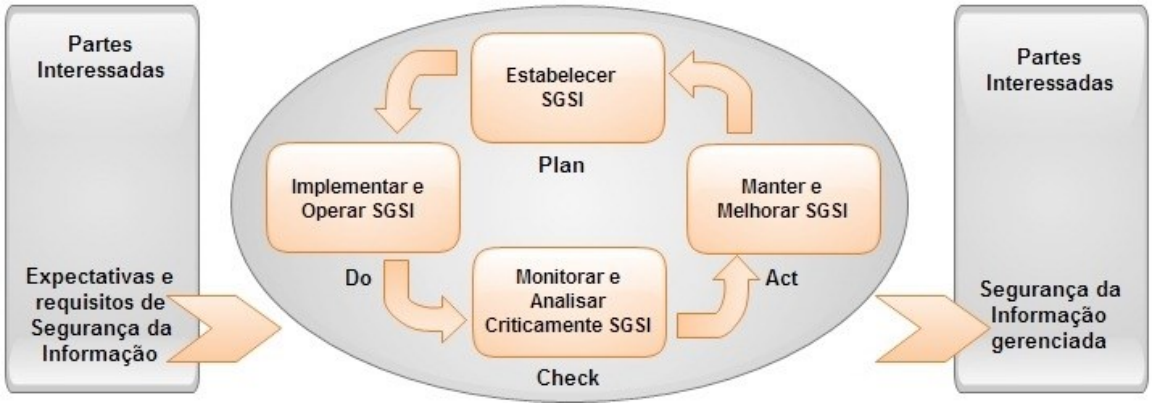
***Do* (implementar e operar o SGSI):** Implementar e operar a política, controles, processos e procedimentos do SGSI.

***Check* (monitorar e analisar criticamente o SGSI):** Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.

***Act* (manter e melhorar o SGSI):** Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

[5]Anexo responsável pela estruturação dos capítulos da norma, definindo e denominando a “Estrutura de alto nível – HSL”. Escopo, Referências normativas, Termos e definições, Contexto da organização, Liderança, Planejamento, Suporte, Operação, Avaliação de Desempenho, Melhorias.

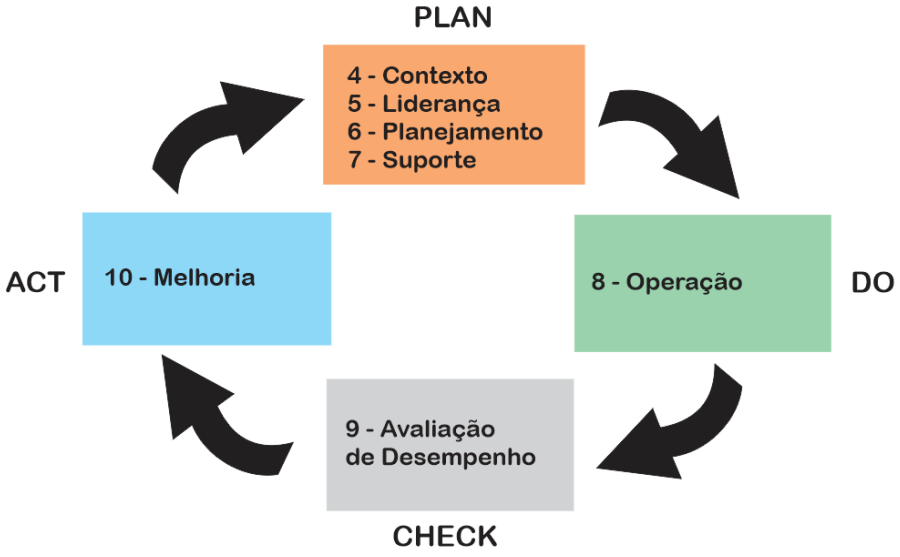
Figura 3 - Ciclo PDCA aplicado aos processos de um SGSI



Fonte: ABNT, 2006, p. VI.

A norma ISO 27001 provê e apresenta requisitos para que uma organização possa estruturar seu SGSI. A norma funciona como um guia para implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI. Ela incorpora um processo de escalonamento de risco e valorização de ativos, orientando quanto à análise e identificação de riscos e a implantação de controle para minimizá-los. A norma permite que as organizações possam certificar suas práticas de gestão de segurança da informação (MANOEL, 2014, p.90). Com a alta direção comprometida e o treinamento eficaz dos colaboradores, é possível reduzir o número de ameaças que exploram eventuais vulnerabilidades.

Figura 4 – Ciclo PDCA, distribuição das diretivas do Anexo SL para a ISO/IEC 27001:2013.



Fonte: Adaptado da internet

A norma está estruturada em seções na qual, cada seção possui uma série de controles que podem ser implementados, que vai depender do tamanho e necessidade de cada empresa. Além disso, é constituída, em sua versão atual, de 14 seções de controles de segurança da informação, 35 objetivos de controles e 114 controles que podem ser implementados (ABNT NBR ISO/IEC 27001, 2013). As 14 seções apontadas na norma são (ABNT NBR ISO/IEC 27001, 2013):

a) Política de Segurança da Informação;
b) Organizando a Segurança da informação;
c) Segurança em Recursos Humanos;
d) Gestão de ativos;
e) Controle de Acesso;
f) Criptografia;
g) Segurança Física e do Ambiente;
h) Segurança nas operações;
i) Segurança nas Comunicações;
j) Aquisição, Desenvolvimento e Manutenção de Sistemas;
k) Relacionamento na cadeia de suprimento;
l) Gestão de incidentes de segurança da informação;
m) Aspectos da segurança da informação na gestão da continuidade do negócio;
n) Conformidade.

Conforme a ABNT NBR ISO/IEC 27001 (2013) os requisitos definidos nesta norma são genéricos e é pretendido que sejam aplicáveis a todas as organizações, independentemente de tipo, tamanho e natureza. Qualquer exclusão de algum de seus controles precisa ser criteriosa e justificada e a aceitação de que os riscos associados, inerentes à retirada, foram aceitos pelas pessoas responsáveis e precisa ser fornecida. Desta forma, isso facilita a implementação e auditoria nas organizações.

1.6 – ABNT NBR ISO/IEC 27002:2013

A versão atual ABNT NBR ISO/IEC 27002:2013, nomeada como: Tecnologia da Informação – Técnicas de Segurança – Código de Prática para controles de segurança da informação contempla a mesma divisão da ISO/IEC 27001, com 14

seções de controles de segurança da informação, 35 objetivos de controles e 114 controles que podem ser implementados, sendo um detalhamento da implementação. Tais normas, ISO/IEC 27001 e 27002, são tidas como uns dos principais documentos de referência para elaboração de um SGSI.

Desta forma, esta norma dispõe dos controles para implementação de um SGSI baseado na ABNT NBR ISO/IEC 27001 e recomenda a existência de políticas de segurança da informação, na qual "convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas interessadas" (ABNT NBR ISO/IEC 27002, 2013, item 5.1.1).

A norma ABNT NBR ISO/IEC 27002, tem por objetivo sugerir boas práticas de gestão de segurança da informação para as organizações, por meio da seleção, implementação e gerenciamento de controles baseados nos ambientes organizacionais (ABNT NBR ISO/IEC 27002, 2013).

1.7 – Análise do cenário atual

Atualmente, a gestão de segurança da informação é uma prática cada dia mais necessária em empresas de todos os portes e em todos os segmentos de atuação. Desta forma, é uma preocupação tão importante quanto enfrentar os desafios de inovação frente às necessidades de seu negócio.

Com a mesma velocidade com que a tecnologia avança – seja em questões como nuvem, big data, *IoT* e outras inovações, cresce também a chamada “indústria *hacker*”, além dos desafios relacionados à confiabilidade, disponibilidade e integridade dos dados presente no dia a dia operacional.

O primeiro semestre de 2017 foi marcado pela ocorrência massiva e a nível global de casos de *ransomwares*[6], um tipo de *malware* que cifra os arquivos do computador de um usuário e libera somente mediante pagamento de resgate. Em junho, houve os ataques do *WannaCry* (ou *Wannacryptor*) e *NotPetya*, e meses depois do *BadRabbit*, com imensa repercussão pública, operações de negócios interrompidas no mundo todo e, consequentemente, grandes prejuízos (RNP, 2017).

[6] ***Ransomware*** código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário.

No Brasil, foram registrados casos de infecção por alguns desses *ransomwares* em alguns órgãos do serviço público e também em instituições conectadas à rede de ensino e pesquisa (RNP, 2017).

Dados da *KaperskyLab* informa que dentro de todos os novos arquivos maliciosos detectados em 2018, o número de *backdoors*[7] aumentou 44%, enquanto o volume de *ransomware* cresceu 43%. Um terço (30%) dos computadores se deparou com pelo menos uma ciberameaça em 2018. Estes resultados mostram que *malware*, especialmente *backdoors* e *ransomware*, continuam sendo um perigo significativo para os usuários de computadores.

E no primeiro trimestre de 2019, o Brasil foi o país que teve a maior parcela dos usuários atacados por golpes de *phishing* (22%, em comparação com 19% no 1º trimestre de 2018) e, em seguida, vêm Austrália (17%) e Espanha (17%). O aumento se deve a spams sofisticados oferecendo falsas ofertas de emprego que supostamente vinham de recrutadores de grandes corporações.

1.8 – A política de segurança da instituição

O Instituto Nacional do Seguro Social – INSS foi criado em 27 de junho de 1990, por meio do Decreto n° 99.350, a partir da fusão do Instituto de Administração Financeira da Previdência e Assistência Social – IAPAS com o Instituto Nacional de Previdência Social – INPS, como autarquia vinculada ao Ministério da Previdência e Assistência Social – MPAS.

O INSS é uma instituição com aproximadamente 45.000 colaboradores distribuídos em 1.800 unidades. Regimentalmente, a Coordenação-Geral de Tecnologia da Informação – CGTI é a área responsável por coordenar a tecnologia da informação e comunicação em toda a instituição.

A Gerência Executiva Garanhuns tem na sua estrutura 11 seções e abrange 18 Agências da Previdência Social – APS, um quadro de 267 colaboradores, onde 178 são servidores e 89 estagiários.

A Política de Segurança da Informação na organização teve início após a Portaria Conjunta MPS/INSS/DATAPREV Nº01, de 05 de novembro de 2008, publicada no Diário Oficial da União em 06 de novembro do mesmo ano, assim

[7]***Backdoor*** é um software malicioso muito utilizado para dar acesso remoto não autorizado ao invasor. Uma maneira não documentada de acessar um programa, um serviço on-line ou um sistema de computador inteiro. Um programador que cria um programa de ameaça, escreve também um código para uma porta dos fundos.

estabelecendo a Política de Segurança da Informação no âmbito do Ministério da Previdência Social – MPS, do Instituto Nacional do Seguro Social – INSS e da Empresa de Tecnologia e Informações da Previdência Social – Dataprev.

Essa portaria também criou o Comitê de Segurança da Informação e Comunicações – CSIC, um órgão formado por representantes das três casas (MPS, INSS e DATAPREV), responsável pela orientação estratégica das ações relativas à segurança da informação a serem implementadas no âmbito do MPS e de suas entidades vinculadas. Em 09 de abril de 2009, a Portaria Conjunta MPS/INSS/DATAPREV Nº01, publicada no Diário Oficial da União em 14 de abril de 2009, alterou a nomenclatura e as atribuições do Comitê, que passou a ser denominado de Comitê de Segurança e Tecnologia da Informação e Comunicações da Previdência Social – CSTIC/PS.

No ano de 2010 foi criado o Guia de Segurança da Informação e Comunicações, com base na Portaria Conjunta MPS/INSS/DATAPREV Nº01 de 09 de abril de 2009, dando conhecimento resumido aos seus colaboradores, de suas funções e atribuições para a segurança da informação na instituição, em relação a senhas, vírus, e-mail, sites e proteção ao acesso físico e lógico.

Em 2011, a Portaria N° 947/PRES/INSS, de 29 de setembro, criou o Comitê de Segurança e Tecnologia da Informação e Comunicações para o INSS – CSTIC/INSS, tendo atribuições de propor políticas, diretrizes, normas, padrões, metodologias, planos, programas e projetos de Segurança, Tecnologia da Informação e Comunicações no âmbito do INSS, em consonância com o CSTIC/PS.

A criação de uma política específica para o INSS foi no ano de 2013, com a Resolução Nº 323/PRES/INSS, de 22 de julho, que instituiu a Política de Segurança da Informação e Comunicações do Instituto Nacional do Seguro Social – POSIC/INSS. Esta resolução tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação e Comunicações, especificamente para o INSS, para orientação quanto ao uso adequado da informação de sua propriedade, em complemento e em consonância com o estabelecido na Política de Segurança da Informação e Comunicações da Previdência Social, estabelecida pela Portaria Conjunta MPS/INSS/DATAPREV nº 1, de 5 de novembro de2008.

Elaborada a partir das principais leis, decretos e normas, define os princípios da segurança da informação, penalidades, competências e responsabilidades, diretrizes gerais e específicas como: tratamento da informação, tratamento de

incidente de rede, gestão de risco, gestão de continuidade, auditoria e conformidade, controles de acesso, uso de e-mail e acesso à internet e gestão de mudanças. Sendo prevista a revisão da mesma e de todos os atos normativos decorrentes, sempre que necessário, não excedendo o período máximo de três anos.

Atualmente, a política em vigor é a Resolução Nº 672 /PRES/INSS, de 27 de dezembro de 2018 que tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação e Comunicações com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade.

Esta resolução foi elaborada com base nos seguintes normativos:

I - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;
II - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;
III - Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011;
IV - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;
V - Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
VI - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;
VII - Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;
VIII - Normas Complementares nº 1 a 21/IN01/DSIC/GSIPR;
IX - NBR ISO/IEC 27002:2013, que instituiu o código de melhores práticas para a Gestão de Segurança da Informação; e
X - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

E princípios:

1. preservação da imagem do Instituto e de seus agentes públicos;
2. salvaguarda das informações do cidadão;
3. estabelecimento de ações de segurança orientadas pela gestão de riscos;
4. continuidade dos serviços aos cidadãos assegurada;
5. alinhamento com a missão institucional e seu planejamento estratégico; e
6. respeito à natureza e finalidade de cada área do Instituto.

Estes definem as seguintes diretrizes: tratamento de informação, tratamento de incidentes de rede, gestão de continuidade, controle de acesso, correio eletrônico, acesso à internet, gestão de mudanças de TIC, educação e conscientização, auditoria e conformidade e as penalidades.

O Gestor de Segurança da Informação e Comunicações fica responsável em promover a cultura de segurança da informação e comunicações, acompanhar as investigações e avaliações dos danos decorrentes de quebras de segurança, propor os recursos necessários à implementação das ações de Segurança da Informação e Comunicações, coordenar o Comitê de Segurança da Informação e Comunicações – CSIC-INSS e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR-INSS, além de detalhar as diretrizes por meio de normas e procedimentos e acompanhar sua implementação.

2 – Percurso metodológico

Com a finalidade de atingir aos objetivos propostos, este trabalho utilizou a pesquisa descritiva e a pesquisa bibliográfica, de natureza qualitativa com a utilização de questionários e observação sistemática.

A pesquisa foi do tipo descritiva, pois segundo Marconi (2005) procura observar, registrar, analisar, classificar e interpretar os fatos ou fenômenos (variáveis), sem que o pesquisador interfira neles ou os manipule, além de envolver o uso de técnicas padronizadas de coleta de dados tais como questionário e observação sistemática e será realizada no INSS/GEXGAR – Instituto Nacional do Seguro Social/Gerência Executiva Garanhuns.

A pesquisa qualitativa foi utilizada por proporcionar uma compreensão do objeto de estudo por meio do contato direto do pesquisador com o campo de estudo que, segundo Prodanov e Freitas (2013), na abordagem qualitativa, a pesquisa tem o ambiente como fonte direta dos dados na qual o pesquisador mantém contato direto com o ambiente e o objeto de estudo em questão. Em suma, o pesquisador direciona-se ao campo para investigar como estava sendo executado a gestão de segurança da informação.

Como fonte da pesquisa bibliográfica foi utilizada as normas ABNT NBR ISO/IEC 27001, ABNT NBR ISO/IEC 27002 e as normas da organização e também foram consultados os temas voltados para a segurança de informação em organizações disponíveis em artigos, dissertações e periódicos.

Para alcançar aos objetivos foi utilizada a observação sistemática, que conforme Gil (2008), na observação sistemática o pesquisador, antes da coleta de dados, elabora um plano específico para a organização e o registro das informações que implica em estabelecer, antecipadamente, as categorias necessárias à análise da situação. Ou seja, será feito previamente um planejamento dos pontos que serão observados no campo de pesquisa.

Foi determinado um período para observação no local, fazendo um levantamento de informações, possíveis problemas e comportamentos dos servidores, para então elaborar o questionário, e realizar a coleta de dados. Para a coleta de dados foi realizado um levantamento de dados a partir de questionário (Anexo I) aos servidores para identificar informações e problemas sobre a segurança na organização. Assim, foi utilizado um formulário do *Google Forms*, enviado via e-

mail, a todos os servidores, do INSS/GEXGAR, contendo 27 perguntas para ser respondida no período de 01 a 15 de junho de 2019. Onde 77 servidores receberam e 41 deles responderam, assim partindo dessas respostas realizar a análise e a proposta.

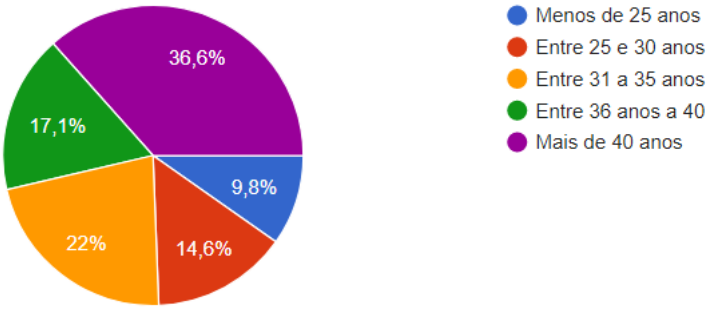
Desta forma, a partir da análise dos dados e os estudos realizados sob a literatura foi possível concretizar os objetivos propostos sobre a pesquisa e propor algumas soluções e considerações sobre o problema apresentado. Então, mediante a análise dos dados se construiu as interpretações necessárias para entender como está a segurança da informação e, a partir disso, propor o SGSI para a organização.

3 – Apresentação e integração dos dados

Aqui serão apresentadas as análises dos dados coletados por meio do questionário, Anexo I, aplicado na INSS/GEXGAR, na qual obteve 41 respostas de um total de 77.

As três primeiras perguntas foram em relação ao perfil do servidor, com a média de idade, média de tempo de serviço na instituição e quanto tempo em média utiliza o computador. As respostas se encontra nos gráficos abaixo.

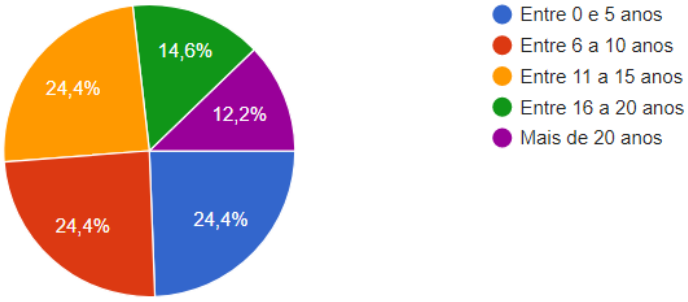
Gráfico 1 – Idade dos servidores



Fonte: Elaboração própria

Conforme observado no gráfico 1, tem-se que 53,7% dos servidores está acima dos 36 anos de idade. E como pode ser observar no gráfico 2, eles possuem mais de 6 anos de tempo de serviço.

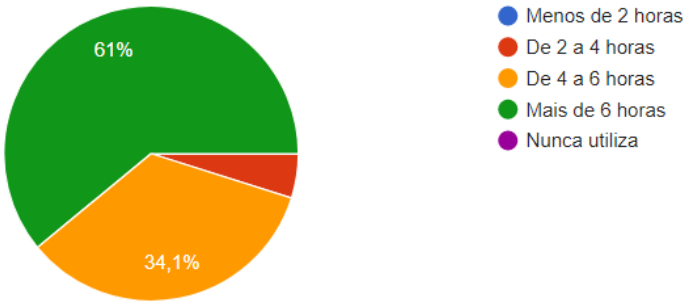
Gráfico 2 –Tempo de serviço na instituição



Fonte: Elaboração própria

Em relação ao tempo médio de utilização do computador durante o expediente, conforme pode ser observado no gráfico 3, tem-se que 61% disseram que trabalham mais de 6 horas diárias.

Gráfico 3 –Tempo médio de utilização do computador

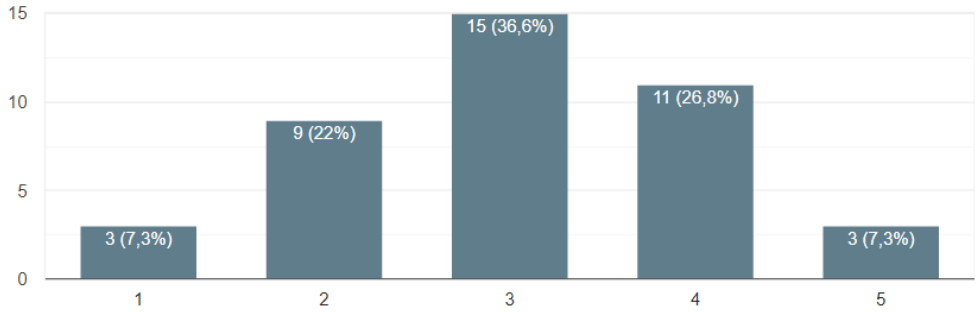


Fonte: Elaboração própria

As próximas perguntas são relacionadas aos conhecimentos sobre a política de segurança da informação e informações necessárias para a análise da segurança na instituição.

Desta forma, em relação ao conhecimento dos servidores sobre a política de segurança da informação na instituição, considerando a escala de 0 (desconhece totalmente) a 5 (conhece totalmente), sendo a nota 3 considerada como neutra, o gráfico 4, mostra que 34,1% dos que responderam tem conhecimento sobre a política de segurança da instituição. Ou seja, 65,9% não tem conhecimento.

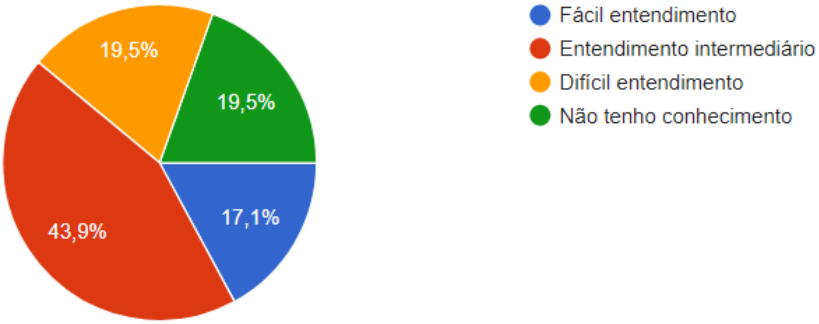
Gráfico 4 –Conhecimento da política de segurança da informação na instituição



Fonte: Elaboração própria

Foi questionado aos que tinham conhecimento sobre a política, como eles classificavam o entendimento, 43,9% classificou como intermediário, 19,5% como difícil, 19,5% não tem conhecimento e 17,1% como fácil, como mostra o gráfico 5.

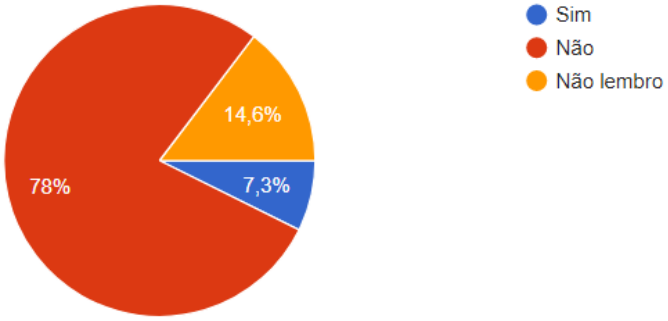
Gráfico 5 - Entendimento da política de segurança na instituição



Fonte: Elaboração própria

Em relação a recebimento algum treinamento sobre segurança da informação, 78% disseram que não, conforme o gráfico 6.

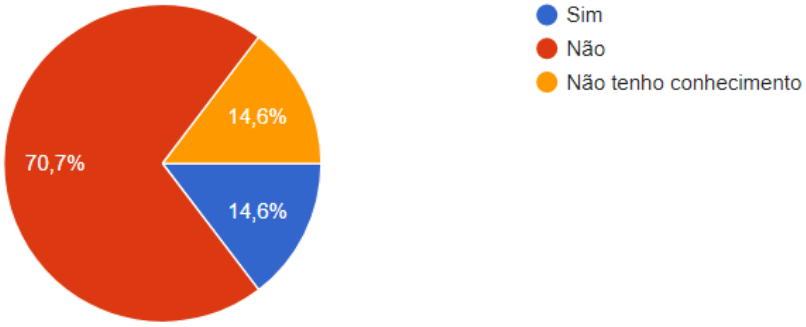
Gráfico 6 – Treinamento sobre segurança da informação



Fonte: Elaboração própria

Questionados se todo usuário antes de iniciar suas atividades profissionais na instituição recebe orientações em relação à segurança da informação e toma conhecimento dos regulamentos existentes, 70,7% informaram que não receberam orientações e nem tiveram conhecimento dos regulamentos existentes e apenas 14,6% que sim e os outros 14,6% não tem conhecimento, como mostra o gráfico 7.

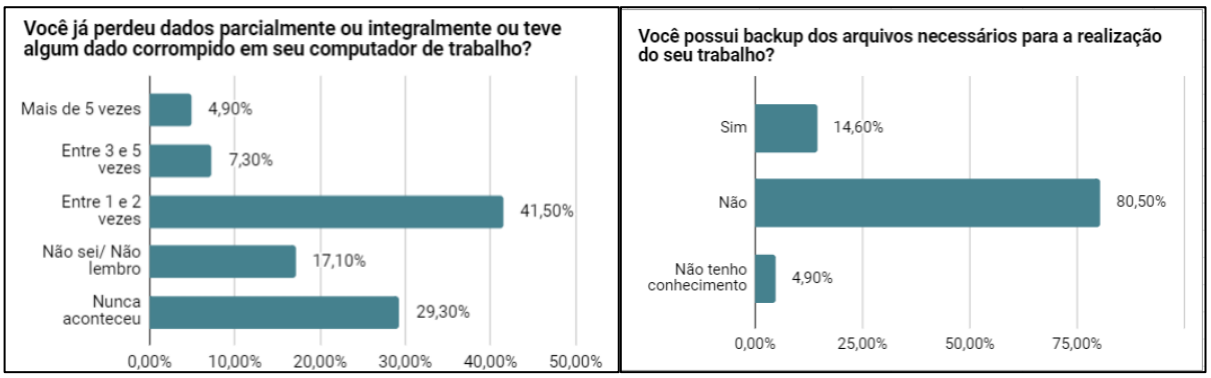
Gráfico 7 – Recebimento de orientações e regulamentos existentes



Fonte: Elaboração própria

Em relação a integridade e backup dos dados, foi perguntado se já perderam de dados parcialmente ou integralmente ou tiveram algum dado corrompido em seu computador do trabalho, com 53,7% ocorreu ao menos uma vez, mas quando perguntado se os mesmos possuem backup de arquivos necessários para realização do trabalho, 80,5% disseram que não tinha, apenas 14,6% fazem backup dos arquivos. A gráfico 8 nos mostra esse resultado.

Gráfico 8 – Integridade e backup dos dados



Fonte: Elaboração própria

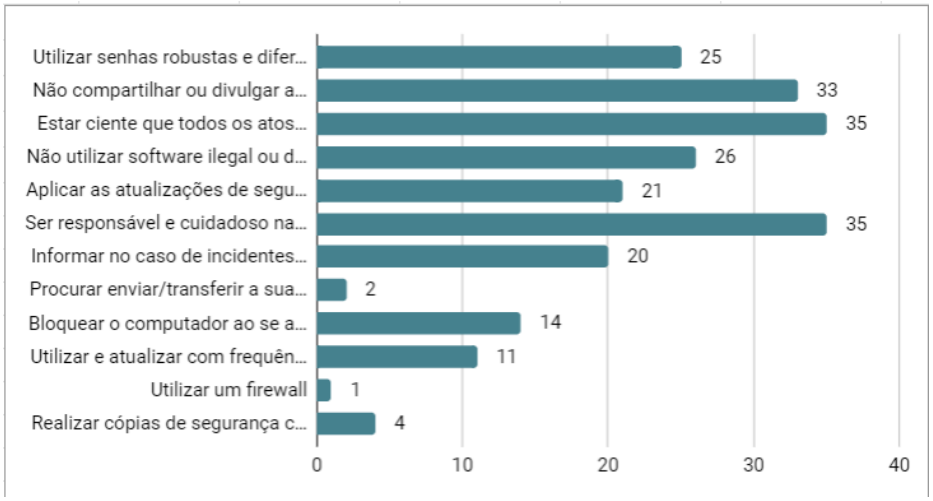
Em relação as medidas adotadas pelos servidores em seu posto de trabalho para a segurança da informação. Foram colocadas 12 opções, podendo ser escolhida mais de uma, que são elas:

- Utilizar senhas robustas e diferentes em cada aplicação;
- Não compartilhar ou divulgar as suas senhas com os outros;
- Estar ciente que todos os atos praticados têm consequências;
- Não utilizar software ilegal ou de compartilhamento de arquivos (Ex: torrent);
- Aplicar as atualizações de segurança recomendadas;
- Ser responsável e cuidadoso na utilização da Internet e do correio eletrônico;
- Informar no caso de incidentes com vírus, roubos ou perdas de informação;
- Procurar enviar/transferir a sua informação de forma encriptada;
- Bloquear o computador ao se ausentar;
- Utilizar e atualizar com frequência os programas antivírus e *antispyware*;

- Utilizar um firewall;
- Realizar cópias de segurança com regularidade.

No gráfico 9, tem-se os resultados na mesma ordem da lista acima.

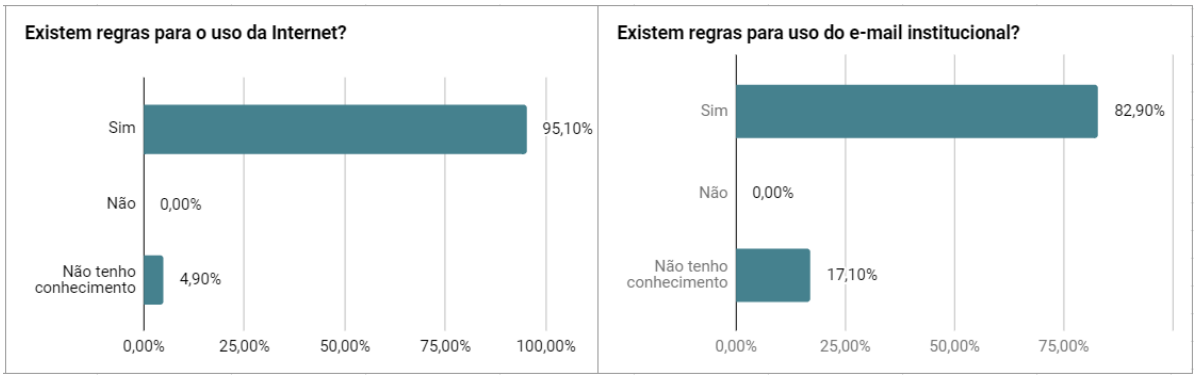
Gráfico 9 – Medidas de segurança utilizadas no posto de trabalho



Fonte: Elaboração própria

O resultado das perguntas sobre regras de uso da internet e e-mail, foram 95,1% e 82,9% disseram que sim, e 4,9% e 17,1% disseram não ter conhecimento, respectivamente, como mostrado no gráfico 10.

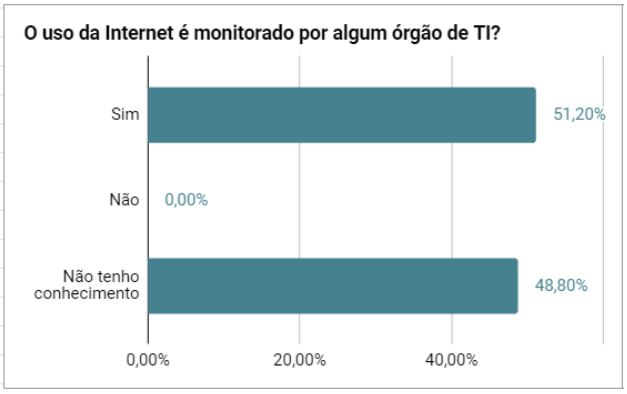
Gráfico 10 – Regras de uso da internet e e-mail



Fonte: Elaboração própria

Em relação ao monitoramento da internet, tem-se que 51,2% dos servidores dizem que existe um monitoramento de algum órgão de TI, os outros 48,8% disseram que não tem conhecimento de monitoramento, conforme o gráfico 11.

Gráfico 11 – Monitoramento da internet

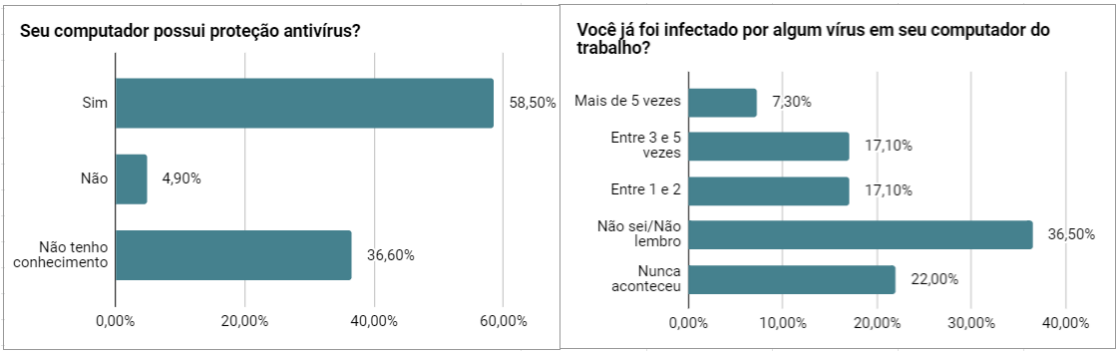


Fonte: Elaboração própria

Em relação a antivírus e *spywares,* foi perguntado se o computador possuía proteção antivírus, se já tiveram seu computador de trabalho infectado alguma vez por vírus, e se era executado o antivírus em mídias removíveis.

Os resultados para a primeira pergunta, 58,5% disseram que possuíam proteção antivírus e 36,6% não tem conhecimento se em seus computadores tem antivírus. Na segunda pergunta, 41,5% já foram infectados com vírus ao menos uma vez, e 36,5% não sabem ou não lembram ter sido infectados, conforme a gráfico 12.

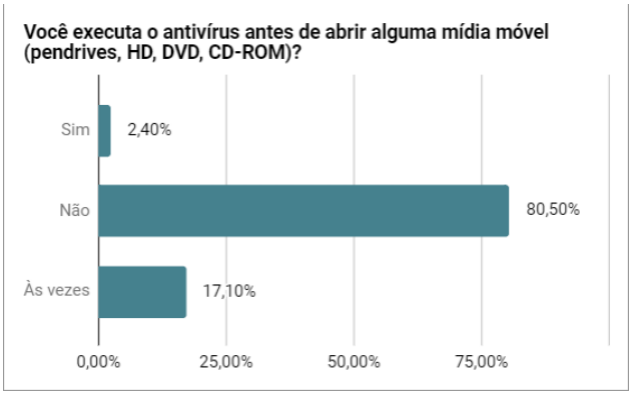
Gráfico 12 – Computadores com antivírus e infectados com vírus



Fonte: Elaboração própria

E na terceira pergunta, 80,5% dos servidores disse que não executa o antivírus nas mídias removíveis ao abrir, como mostra o gráfico 13.

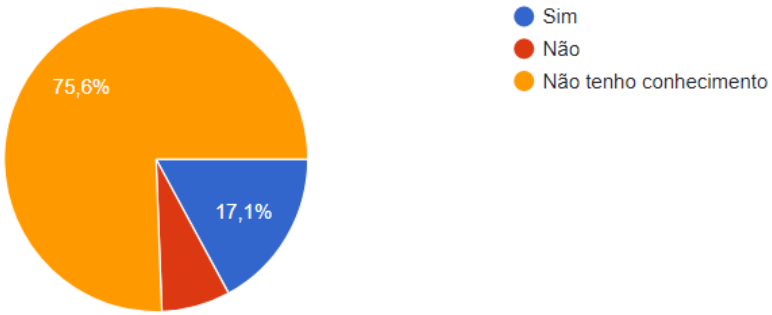
Gráfico 13 – Verificação em mídias removíveis



Fonte: Elaboração própria

Seguindo com as perguntas, em relação da existência de algum procedimento para informar um incidente de segurança da informação, 75,6% dos que responderam disseram que não tem conhecimento de tal procedimento, como mostra o gráfico 14.

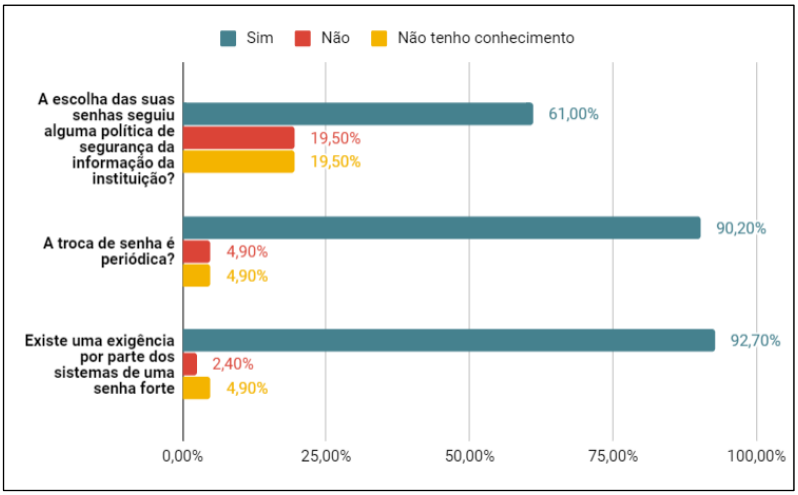
Gráfico 14 – Existência de procedimento para informar incidente de segurança da informação



Fonte: Elaboração própria

Em relação se a criação de senhas segue a política de segurança da informação da instituição, se a troca da senha periódica e se existe exigência de criação de senhas fortes. Para a primeira pergunta 61% disseram que sim e 19,5% disseram que não tinha conhecimento. Na segunda pergunta 90,2% disseram que a troca de senha é periódica. E na terceira pergunta 92,7% afirmaram que os sistemas utilizados exigem a criação de uma senha forte. Os resultados estão expostos do gráfico 15.

Gráfico 15 – Senhas

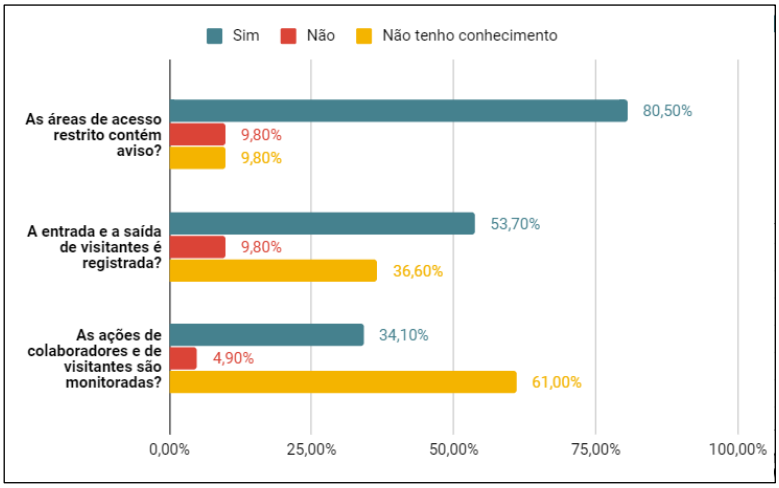


Fonte: Elaboração própria

Dando continuidade, foram feitas perguntas em relação a segurança no ambiente em relação a aviso em salas de acesso restrito, registro de entrada e saída de visitantes e monitoramento de ações de colaboradores e visitantes.

Os resultados, conforme a gráfico 16, tem-se que para a primeira pergunta, 80,5% disseram que as áreas com acesso restrito contêm avisos. Na segunda,53,7% disseram que os visitantes eram registrados para entrada e saída, e 36,6% disseram que não tinham conhecimento sobre os registros dos visitantes. A terceira sobre o monitoramento de ações dos colaboradores e visitantes, 61% disseram que não tem conhecimento sobre o monitoramento, e apenas 34,1% disseram que sim.

Gráfico 16 –Segurança do ambiente, salas, registro de visitantes e monitoramento de colaboradores e visitantes

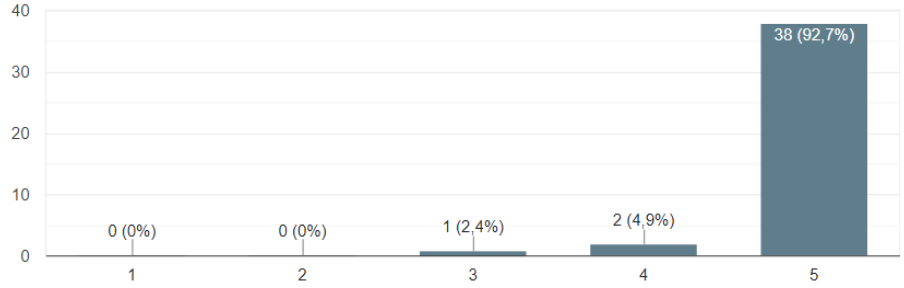


Fonte: Elaboração própria

Por fim, a duas últimas perguntas, uma para saber a opinião do grau de importância da segurança da informação e a outra uma questão opcional, para fazer um comentário sobre a segurança da informação na instituição.

Em uma escala de 0 (sem importância) a 5 (muito importante), foi perguntado qual o nível de importância que considera a segurança da informação. 92,7% das respostas consideram a segurança da informação muito importante, gráfico 17.

Gráfico 17 – Nível considerado de importância da segurança da informação



Fonte: Elaboração própria

Dos 8 comentários recebidos sobre a segurança da informação na instituição, percebe-se comentários diversificados, uns falando da importância para instituição, divulgação da política de segurança, treinamento para os servidores, dentre outras. A tabela 1 traz os comentários recebidos.

Tabela 1 – Comentários sobre a segurança da informação na instituição

A Segurança da Informação é muito importante para instituições como a que trabalho, por sermos responsáveis por dados de várias pessoas.
Na minha opinião, é importante temos conhecimento amplo sobre o assunto, para maior segurança quanto a acessos de arquivos ou mensagens indevidas.
Precisa ser amplamente divulgada, inclusive com treinamento para servidores.
Todo usuário antes de iniciar suas atividades profissionais na instituição DEVE receber orientações em relação à segurança da informação e tomar conhecimento dos regulamentos existentes (Pergunta nº 8).
De forma geral, muito fraca.
Algumas perguntas não foram respondidas com segurança por falta de conhecimento.
Imprescindível ao bom andamento e execução eficiente do trabalho.
Se existe, falta divulgação.
Não tenho conhecimento da política de segurança
Falta divulgação e torná-lo simples. Ouvi falar sobre, procurei e achei, é muito extenso. Deve-se deixá-lo com simples entendimento para que todos compreendam e apliquem na instituição.

Fonte: Elaboração própria

Foi observado por meio da análise das respostas do questionário, uma amostra atual da segurança da informação na instituição. Embora alguns que responderam expressem certo grau de conhecimento e consciência sobre a necessidade de boas práticas de segurança da informação, demonstra-se a necessidade de ajustes, de maior conscientização e alinhamento de ações que venham atender às demandas.

3.1 – Detalhamento da análise e proposta do SGSI

No item anterior ficou evidente que os servidores não têm conhecimento sobre a política de segurança da informação, pois 65,9% responderam desconhecer. Desta forma é preciso que mudar está cultura na organização, pois é fundamental que esse conhecimento esteja explícito para se ter uma melhor segurança das informações dentro da organização. Visto que aqueles que conhecem, 43,9% e 19,5% classificou a compreensão da política como intermediária e difícil, respectivamente, então é necessário elaborar uma política de segurança da informação que seja de fácil compreensão para todos os colaboradores, assim ter eficácia da segurança na instituição.

Em face aos resultados sobre o recebimento de treinamento, 78% dos servidores responderam que não receberam e 14,6% não lembram. E os resultados obtidos sobre recebimento de orientações e regulamentos existentes em que 70,7% responderam que não. Então, tendo em vista esses problemas, para solucionar é necessário que os servidores ao iniciarem o trabalho na instituição, receberem treinamentos e orientações sobre a segurança da informação, e para aqueles servidores mais antigos informar fazer com que eles tenham conhecimento da política existente, e no decorrer do tempo realizar capacitações a cada atualização da política de segurança da informação.

A análise dos resultados sobre integridade e backup dos dados, para 53,7% teve ao menos uma vez dados perdidos parcialmente ou integralmente ou corrompidos, e diante disso, 80,5% não realiza backups dos dados. Em atenção os valores obtidos nestas questões, podemos considerar que os servidores não comportamentos e atitudes aceitáveis a realização de backup dos dados, tendo em vista que um pouco mais de 50% já perdeu dados pelo menos uma vez, pretende-se deixá-los conscientes da importância de realizar o backup dos dados com

regularidade, assim criando a cultura para que a porcentagem se inverta, evitando problemas posteriores de perca de dados.

Os resultados para as 12 medidas de segurança adotadas no posto de trabalho, observa-se que apenas 6 medidas que tiveram mais de 50% das respostas que são: ser responsável cuidadoso na utilização da Internet e do correio eletrônico (85,3%), estar ciente que todos os atos praticados têm consequências (85,3%), não compartilhar ou divulgar as suas senhas com os outros (80,5%), não utilizar software ilegal ou de compartilhamento de arquivos (63,4%), utilizar senhas robustas e diferentes em cada aplicação (60,9%) e aplicar as atualizações de segurança recomendadas (51,2%). Assim, mesmo sendo essenciais vê-se que muitos servidores não adotam coisas simples como: informar no caso de incidentes com vírus, roubos ou perdas de informação (48,8%), bloquear o computador ao se ausentar (34,14%), utilizar e atualizar o software antivírus (26,82%), realizar cópias de segurança com regularidade (9,75%), enviar/transferir a sua informação de forma encriptida (4,87%) e utilizar um firewall (2,43%). Desta forma é necessário estabelecer regras para informar o quão importante é cada ponto desse para segurança da informação.

Sobre a existência de regras de uso da internet e e-mail institucional, temos que 95,1% e 82,9% afirmaram que sim, respectivamente. A análise desses resultados mostra que os servidores estão cientes das regras para utilizar a internet e o e-mail institucional. Desta forma, pretende-se expor essas regras para atingir todos, assim deixá-los cientes sobre o uso da internet na instituição e do e-mail institucional.

Os resultados da pergunta sobre a existência de algum órgão de TI que monitora a internet, 51,2% responderam que sim e 48,8% responderam que não tem conhecimento. A análise desses resultados mostra que deve-se divulgar mais a existência desse órgão, para então os servidores terem consciência do uso da internet na instituição.

Em face dos resultados obtidos dos servidores de que 58,5% possuem em seu computador antivírus instalado e 36,6% não tem conhecimento se tem antivírus instalado. E que 41,5% já foram infectados com vírus pelo menos uma vez e 36,5% não sabem ou não lembram se já foram infectados. E que 80,5% não executam o antivírus antes de abrir alguma mídia removível. Analisando esses resultados nota-se que é necessário informar a importância do programa antivírus para a segurança

da informação, de mantê-lo atualizado, de fazer verificações no sistema e ao conectar mídias removíveis. E assim desta forma, contribuir com uma melhor segurança da informação. Os resultados mostram que 75,6% disseram que não tem conhecimento da existência de um procedimento para informar um incidente de segurança da informação. Desta forma, é necessário criar um órgão local para que os servidores informem sobre os incidentes, para que as providências sejam tomadas o mais rápido possível.

Como se pode observar pelos resultados obtidos sobre a questão da senha pessoal, vê-se que 61% disseram que a criação da senha segue uma política da informação, 90,2% disseram que a troca de senha é periódica e 92,7% disseram que os sistemas exigem a criação de uma senha forte. Diante desses resultados os servidores apresentam comportamento e atitudes positivas em relação a criação e a troca de senha, apesar de 49% não saber que a escolha da senha segue uma política, os sistemas utilizados determinam essa política.

Os resultados obtidos sobre a segurança do ambiente, observa-se que 80,5% disseram que as áreas restritas contêm aviso. Para o registro de entrada e saída de visitantes, 46,4% disseram que não ou não sabem. E para a existência de monitoramento de ações de colaboradores, 61% disseram não ter conhecimento. Em face desses resultados para deixar o ambiente seguro, é necessário a utilização de crachá para todos colaboradores, colocar avisos em todas as áreas restritas, registrar todos os visitantes e se possível acompanhá-los ao destino e ter monitoramento eletrônico, para então não comprometer a segurança da informação com acesso de pessoas não autorizadas a locais restritos da instituição.

Diante do exposto tem-se que 97,6% dos servidores consideram a segurança da informação importante. Com isso, afirma há uma preocupação por parte dos servidores com a segurança da informação, então pretende-se elaborar uma proposta de um SGSI, que seja exposto e de entendimento de todos os colaboradores, para assim alcançar os objetivos previstos.

Em face aos problemas apresentados acima, a proposta do SGSI para o INSS/GEXGAR tem a finalidade de adotar um planejamento, onde pretende-se criar uma comissão constituída pelos seguintes integrantes:

- Comitê Estratégico de TIC - CETI
- Coordenação-Geral de Tecnologia da Informação – CGTI

- Comitê de Segurança e Tecnologia da Informação e Comunicações da Previdência Social – CSTIC/PS
- Gestor de Segurança da Informação e Comunicações
- Coordenador de TIC Regional
- Coordenação de TIC do INSS/GEXGAR

Realização de diversas reuniões e atividades com esta comissão, por fim definindo os seguintes planejamento previsto:

1. Treinamento sobre ABNT NBR ISO/IEC 27001 e 27002 para os envolvidos no planejamento e implantação do SGSI;
2. Criação do escopo e política do SGSI;
3. Identificação dos ativos nos setores relacionados ao escopo;
4. Identificação dos riscos relacionados ao escopo;
5. Realização das análises de riscos;
6. Classificação da informação;
7. Criação da declaração de aplicabilidade;
8. Criação de novos e documentação dos controles existentes através de procedimentos, políticas e manuais;
9. Criação dos indicadores;
10. Realização das reuniões de analises críticas e auditorias internas;
11. e Conscientização para todos os envolvidos no SGSI da entidade.

Com o planejamento definido, então estabelecer um período para a execução das atividades pré-estabelecidas.

1) **Escopo e política do SGSI:**A coordenação de TIC do INSS/GEXGAR, definirá o escopo e a política em consonância com os órgãos superiores a ele.
    a. Escopo: ter por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação e Comunicações, especificamente para o INSS/GEXGAR, para orientação quanto ao uso adequado da informação de sua propriedade, em complemento e em consonância com o estabelecido na Política de Segurança da Informação existentes;
    b. Política: a política de segurança da informação vai buscar a proteção contra vários tipos de ameaças para garantir a continuidade do negócio, reduzir riscos, visando preservar a

disponibilidade, integridade, confidencialidade, autenticidade e salvaguarda das informações geradas, processadas e armazenadas no âmbito do Instituto e ampliar as oportunidades de melhoria no Sistema de Gestão de Segurança da Informação;

c. Estabelecer a política de segurança da informação do INSS/GEXGAR, abrangendo servidores, ocupantes de cargo comissionado ou em comissão, prestadores de serviço e estagiários e partes interessadas no SGSI, afim de atender os seguintes itens: confidencialidade, integridade, disponibilidade.

2) **Identificação de ativos:** realizar reuniões e entrevistas nos setores para a identificação de ativos e atividades relacionadas ao escopo do SGSI. O resultado deve ser registrado e categorizado.
3) **Identificação de riscos:** realizar reuniões com servidores, chefes e coordenações de setores envolvidos no escopo, no qual serão identificados e registrados.
4) **Análise de riscos:** utilizando os riscos identificados na atividade anterior, será realizada uma análise que resultará em uma planilha contendo:
    a. Nome;
    b. Descrição;
    c. Probabilidade;
    d. Impacto;
    e. Ações (tratamento).
5) **Classificação da informação:** classificar por nível de confidencialidade, rótulos de identificação, critérios de classificação, restrição de acesso, devido transporte e descarte.
6) **Declaração de aplicabilidade:** criar uma planilha para gerenciar a declaração de aplicabilidade do SGSI. Informado quais das seções e controles estão sendo utilizados, se é aplicável, qual objetivo e como ocorre o controle deste item, através de políticas, procedimento, manuais, registros, entre outros.
7) **Documentação do SGSI:** criar documentos para controle do SGSI.
8) **Indicadores:** para monitorar e medir o desempenho dos objetivos e metas do SGSI.

9) **Reuniões de análises críticas e auditorias internas:** determinar um período de tempo para ocorrer as análises críticas e auditorias internas, discutindo as seguintes informações:
    a. Ações de acompanhamento das reuniões e auditorias anteriores;
    b. Análise do SGSI;
    c. Desempenho relacionado à eficácia do SGSI;
    d. Resultado de avaliações de riscos e situação dos planos de tratamento de riscos;
    e. Alterações em questões internas e externas que possam afetar o SGSI;
    f. Identificação de sugestões para melhorias;
10) **Conscientização do SGSI:** garantir que os colaboradores executem as atividades do trabalho em conformidade da política de segurança da informação do instituto, dando contribuições para a eficácia do SGSI.

Com a adoção desta proposta os colaboradores irão ter:

- O conhecimento sobre a política de segurança da informação da instituição, em uma linguagem simples, clara e objetiva;
- Receber treinamento para saber a importância e a necessidade ter a segurança da informação forte e eficaz, assim vê que coisas simples, como bloquear o computador ao se ausentar, é de extrema importância para manter a segurança;
- Realizar backup dos dados periodicamente;
- Instalar e atualizar o antivírus em todos computadores da instituição;
- Executar varredura do antivírus no sistema, em mídias removíveis;
- Melhor conscientização dos servidores no que se refere à utilização e criação de senhas de acesso à sistemas, rede e internet**;**
- Ter o conhecimento dos órgãos superiores estão no monitoramento do uso da internet, na criação de regras do e-mail institucional e da internet;
- Ter um setor responsável local para informar em casos de incidentes na segurança da informação;

- Toda área restrita terá que ter aviso, os colaboradores terão que usar crachá de identificação;
- Visitantes serão registrados na entrada e saída, se possível acompanhado por alguém da instituição;
- Ampliar o monitoramento eletrônico para acompanhar as ações de colaboradores e visitantes.

Considerações finais

A realização deste trabalho proporcionou um maior conhecimento em relação as normas e procedimentos abordados nas ABNT NBR ISO/IEC 27001:2013 e 27002:2013 em conformidade com proposta de criação de um SGSI.

No período de análise no INSS/GEXGAR, verificou-se que o normal funcionamento da instituição está cada vez mais dependente dos seus sistemas de informação, o que intensifica a necessidade de maximizar a segurança dos mesmos.

Percebeu-se que existe uma preocupação com a segurança da informação na instituição, inclusive por contar com uma política de segurança definida, embora ainda não exista um bom mecanismo para divulgação e conscientização desta política. Por se tratar de uma instituição federal prestadora de serviços previdenciários, a informação é considerada como elemento crítico, então se faz necessário que todos os colaboradores tenham conhecimento da política de segurança da informação da instituição, contudo se faz necessário uma melhor prática para solução deste problema, mesmo diante de toda a complexidade.

Diante dos resultados expostos, verificou-se que em sua maioria os servidores não conhecem a política de segurança da informação da instituição. Então é possível inferir que o comportamento dos servidores, em relação a segurança da informação, está diretamente ligado a falta de conhecimento da política da instituição, isso faz com que algumas atitudes erradas sejam tomadas.

Com isso, constatou-se que é de extrema importância para o INSS/GEXGAR a política de segurança da informação, pois define regras que devem ser seguidas facilitando o trabalho realizado. Ela está totalmente ligada aos objetivos da instituição, todos os colaboradores têm que ter acesso a ela, e será revisada em um período determinado, para seja feito ajustes para a melhoria contínua.

A proposta apresentada pretende-se diminuir a incidência das inúmeras ameaças à segurança da informação, bem como criar uma cultura organizacional de segurança. Com a implementação da proposta do SGSI prevê-se que o INSS/GEXGAR obtenha:

- Um aumento da consciência interna referente à segurança da informação;
- Uma otimização de planos e processos de gestão da informação, através da padronização de processos;

- Definição das responsabilidades pelos ativos;
- O comprometimento com a aplicação da política;

Por meio do desenvolvimento do SGSI destina-se a melhorar e cobrir suas deficiências, a fim de proteger seu ativo mais importante é a informação, espera-se atenda os três pilares da segurança da informação, confidencialidade, integridade e disponibilidade. Sendo necessário sensibilizar o grupo de trabalho da instituição com treinamentos, capacitações, palestras de formação, a fim de conhecer os processos de gerenciamento de informações e seus ativos de computação. A informação se torna a cada dia mais importante para as organizações, portanto, fica cada vez mais indiscutível a importância da sua proteção. A falta de conhecimento geralmente leva as pessoas a cometerem condutas inadequadas. Esta política de segurança pode também ser utilizada como um auxílio na antecipação do risco e na garantia de continuidade do serviço.

Espera-se desse trabalho bons resultados com a implementação do SGSI, através dos resultados obtidos do questionário, nota-se que, muitos mesmo sem conhecer a políticas de segurança da instituição, tratam a segurança como algo muito importante para realização do trabalho diário.

Para trabalhos futuros, também podem ser definidos no sentido de se buscar compreender de que forma a instituição pode conseguir a sua modernização, diante do cenário atual. Sugere-se a replicação deste trabalho, para buscar sanar limitações que esta pesquisa possa ter tido ao longo de sua execução. Validar os mecanismos através de mais estudos de caso, avaliando a aplicabilidade dos mecanismos identificados ou mesmo novos mecanismos de segurança da informação. Então, posteriormente com os resultados positivos após a implementação do SGSI, espera-se implantá-los em outras Gerências Executivas do INSS.

Referências Bibliográficas

ABNT NBR ISO/IEC 27001. **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisito**. Rio de Janeiro: ABNT, 2013.

ABNT NBR ISO/IEC 27002. **Tecnologia da Informação: Código de Prática para a Gestão da Segurança da Informação**. Rio de Janeiro: ABNT, 2013.

ABNT NBR ISO/IEC 27005. **Tecnologia da Informação - Técnicas de segurança - Gestão de riscos de segurança da informação.** Rio de Janeiro: ABNT, 2011.

BATISTA, I. D. S.; da Silva, C. A.; da Silva, R. G. **Governança da tecnologia da informação na atualidade: A importância da adoção de modelos de melhores práticas nas organizações**. In: II World Congress on Systems Engineering and Information Technology. **Anais**[...] Vigo – Espanha 2015.

BRASIL. Superior Tribunal de Justiça. Secretaria de Controle Interno. Coordenadoria de Auditoria de Tecnologia da Informação. **Cartilha de Segurança da Informação**. Brasília, [2014]. Disponível em: https://ww2.stj.jus.br/publicacaoinstitucional//index.php/Cartseginf/issue/archive. Acesso em: 01 nov. 2018

CITTADIN, J. O. B. **Gestão da Segurança da Informação: Desafios E Perspectivas**. Universidade Federal de Santa Catarina. Campus Araranguá. Santa Catarina. 2018.

CONCERINO, A. J. **Internet e segurança são compatíveis?** In: LUCCA, N.; SIMÃO FILHO, A. (Coord.). Direito & Internet: aspectos jurídicos relevantes. 2. ed. São Paulo: Quartier Latin, 2005. cap. 4.

COSTA, I. et al. **Qualidade em tecnologia da informação**. São Paulo: Atlas, 2013.FERNANDES, A. A.; ABREU, V. F. DE. **Implantando a Governança de TI da**

Estratégia à Gestão dos Processos e Serviços. 4a ed. Rio de Janeiro: Brasport Livros e Multimídia Ltda, 2014.

DONNER, M. L.; OLIVEIRA, L. R. Análise de Satisfação com a Segurança no Uso de Internet Banking em Relação aos Atuais Recursos Disponíveis no Canal Eletrônico. In: XXXII Encontro da ANPAD, EnANPAD 2008, Rio de Janeiro. **Anais**[...] ANPAD, 2008.

FERNANDES, A. A.; ABREU, V. F. **Implantando a governança de TI**. 3 ed. Rio de Janeiro: Brasport, 2012.

GIL, A, C. **Como elaborar projetos de pesquisa**. São Paulo: Editora Atlas, 2002.

ISACA. **COBIT 5: Governança e Gestão de TI da Organização**. 2012.

ITGI, I. **Board briefing on IT governance.** 2 ed. Illinois, EUA. IT Governance Institute. 2003. Disponível em: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx. 2003. Acesso em 10 de nov. 2018.

KASPERSKY. **Kaspersky detecta 350 mil novos vírus por dia em 2018**. Disponível em: https://www.kaspersky.com.br/blog/kaspersky-detecta-novos-virus-dia-2018/11143/. Acesso em: 06 de fev. 2019.

LORENS, E. M. **Aspectos normativos da segurança da informação: um modelo de cadeia de regulamentação**. 2007. Dissertação (Mestrado em Ciência da Informação) — Departamento de Ciência da Informação, Universidade de Brasília, Brasília.

LYRA, M. R. **Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro: Ciência Moderna, 2008.

MALLMANN, A. C. W. et al. **Análise do nível de maturidade da governança de TI da empresa Breithaupt**. Faculdade Senac Jaraguá do Sul, Jaraguá do Sul, Santa Catarina. 2018.

MANOEL, S. S. **Governança de Segurança da Informação - Como criar oportunidades para seu negócio**. Editora Brasport, Rio de Janeiro, 2014.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 5. ed.-São Paulo: Atlas, 2003.

MOURA, H. P.; ANDRADE, J. N. **Implantando a Gestão de Serviços de TI: Uma abordagem horizontal baseada no catálogo de serviços de TI**. Recife, 2007. Disponível em: http://www.lbd.dcc.ufmg.br/colecoes/sbsi/2008/0016.pdf. Acesso em: 20 fev. 2019.

NIMER, F. **Segurança da Informação em Ambientes Distribuídos**. Developers Magazine, vol. 24, pág. 22-24, 1998

PETERSON, R. **Crafting information technology governance**: Information Systems Management, v. 21, n. 4, p. 7–22, 2004.

PRODANOV, C. C.; FREITAS, E. C. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2 ed. Novo Hamburgo: Feevale, 2013.

RNP. **Relatório Anual de Incidentes de Segurança na Rede Brasileira de Ensino e Pesquisa**. Brasília: CAIS. 2017. Disponível em: https://www.rnp.br/sites/default/files/12_rnp_ra_cais_2017.pdf. Acesso em: 20de maio 2019.

ROCHA, P. C. C. **Segurança da informação: uma questão não apenas tecnológica**. Instituto de Ciências Exatas, Universidade de Brasília, Brasília, 2008.SAMPAIO, D. R. L. **Um estudo sobre riscos de segurança da informação no campus da UFC em Quixadá com base na norma ISO/IEC 27005**. Universidade Federal do Ceará, Campus Quixadá, Quixadá, 2014.

SANTANDER. **Os 4 erros mais comuns de segurança da informação**. 29 de janeiro de 2019. Disponível em:

https://www.santandernegocioseempresas.com.br/detalhe-noticia/seguranca-da-informacao.html. Acesso em 03 de março de 2019.

SÊMOLA, M. **Gestão da segurança da informação: uma visão executiva**. - 2. ed. Rio de Janeiro: Elsevier, 2014.

SILVA, C. A. **Gestão da segurança da informação: um olhar a partir da Ciência da Informação**. Campinas, São Paulo. 2009.

SILVA, D. R. P.; STEIN, L. M. **Segurança da Informação: uma reflexão sobre o componente humano**. Rio de Janeiro: Ciências & Cognição. v.10, p.46-53, mar. 2007.

TAROUCO, H. H.; GRAEML, A. R. **Governança de tecnologia da informação: um panorama da adoção de modelos de melhores práticas por empresas brasileiras usuárias**. Revista de Administração, v. 46, n. 1, p. 7-18, 2011.

UNB – Universidade Brasília. **Gestão da segurança da informação e comunicações: volume 1**. Jorge Henrique Cabral Fernandes, organizador. Brasília: Faculdade de Ciência da Informação, c2010

WEILL, P.; ROSS, J. W. **Governança de TI: Tecnologia da Informação**. São Paulo: Makron Books, 2006.

ANEXO I

Questionário - Segurança da Informação

Pesquisa realizada para a realização do Trabalho de Conclusão de Curso (TCC) do aluno Samir Josué Laranjeira Soares, no curso de Ciência da Computação, na Universidade Federal Rural de Pernambuco - Unidade Acadêmica Garanhuns.

Você está convidado(a) a responder este questionário anônimo, que faz parte da coleta de dados da pesquisa sobre a Gestão da Segurança da Informação, sob responsabilidade do pesquisador Samir Josué Laranjeira Soares.

Caso você concorde em participar da pesquisa, leia com atenção os seguintes pontos: a) você pode deixar de participar da pesquisa e não precisa apresentar justificativas para isso; b) sua identidade será mantida em sigilo; c) caso você queira, poderá ser informado(a) de todos os resultados obtidos com a pesquisa, independentemente do fato de mudar seu consentimento em participar da pesquisa.

*Obrigatório

Perfil

1 - Qual a sua Idade? *

- ◯ Menos de 25 anos
- ◯ Entre 25 e 30 anos
- ◯ Entre 31 a 35 anos
- ◯ Entre 36 anos a 40
- ◯ Mais de 40 anos

2 - A quanto tempo está na Instituição? *

- ◯ Entre 0 e 5 anos
- ◯ Entre 6 a 10 anos
- ◯ Entre 11 a 15 anos
- ◯ Entre 16 a 20 anos
- ◯ Mais de 20 anos

3 - Quantas horas em média por dia você utiliza o computador para realizar suas tarefas? *

- ◯ Menos de 2 horas
- ◯ De 2 a 4 horas
- ◯ De 4 a 6 horas
- ◯ Mais de 6 horas
- ◯ Nunca utiliza

Políticas de segurança da informação

4 - Em uma escala de 1 a 5, como você conhece as políticas de segurança da informação existentes na instituição? *

	1	2	3	4	5	
Desconheço totalmente	◯	◯	◯	◯	◯	Conheço totalmente

5 - Se você tem algum conhecimento sobre a política de segurança da informação da instituição, como você classifica a compreensão? *

- ◯ Fácil entendimento
- ◯ Entendimento intermediário
- ◯ Difícil entendimento
- ◯ Não tenho conhecimento

6 - Você já recebeu algum treinamento sobre segurança da informação? *

- ◯ Sim
- ◯ Não
- ◯ Não lembro

7 - Qual o nível de importância a respeito da segurança da informação, você considera?*

	1	2	3	4	5	
Sem importância	◯	◯	◯	◯	◯	Muita importância

8 - Todo usuário antes de iniciar suas atividades profissionais na instituição recebe orientações em relação à segurança da informação e toma conhecimento dos regulamentos existentes? *

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

9 - Na sua opinião, os usuários da instituição conhecem regulamentos de segurança de informação existentes? *

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

10 - A escolha das suas senhas seguiu alguma política de segurança da informação da instituição? *

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

11 - A troca de senha é periódica? *

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

12 - Existe uma exigência por parte dos sistemas de uma senha forte*? *

*Senhas contendo letras, números e caracteres especiais. E sem conter informações pessoais (data de nascimento, nome, telefone e etc.).

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

13 - Quais são as medidas de segurança que você adota no seu posto de trabalho? *

Marque todas que se aplicam.

- ☐ Aplicar as atualizações de segurança recomendadas
- ☐ Utilizar e atualizar com frequência os programas antivírus e antispyware
- ☐ Realizar cópias de segurança com regularidade
- ☐ Utilizar senhas robustas e diferentes em cada aplicação
- ☐ Procurar enviar/transferir a sua informação de forma encriptada
- ☐ Não compartilhar ou divulgar as suas senhas com os outros
- ☐ Ser responsável e cuidadoso na utilização da Internet e do correio eletrônico
- ☐ Estar ciente que todos os atos praticados têm consequências
- ☐ Informar no caso de incidentes com vírus, roubos ou perdas de informação
- ☐ Utilizar um firewall
- ☐ Bloquear o computador ao se ausentar
- ☐ Não utilizar software ilegal ou de compartilhamento de arquivos (Ex: torrent)

14 - Você possui backup dos arquivos necessários para a realização do seu trabalho? *

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

15 - Você já perdeu de dados parcialmente ou integralmente ou teve algum dado corrompido em seu computador do trabalho? *

- ◯ Mais de 5 vezes
- ◯ Entre 3 e 5 vezes
- ◯ Entre 1 e 2 vezes
- ◯ Não sei/ Não lembro
- ◯ Nunca aconteceu

16 - Existem regras para o uso da Internet? *

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

17 - O uso da Internet é monitorado por algum órgão de TI? *

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

18 - Existem regras para uso do e-mail institucional? *

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

19 - Seu computador possui proteção antivírus? *

- ◯ Sim
- ◯ Não
- ◯ Não sei

20 - Você já foi infectado por algum vírus em seu computador do trabalho? *

- ◯ Mais de 5 vezes
- ◯ Entre 3 e 5 vezes
- ◯ Entre 1 e 2 vezes
- ◯ Não sei/ Não lembro
- ◯ Nunca aconteceu

21 - Você executa o antivírus antes de executar algum arquivo presente em alguma mídia removíveis (pendrives, HD, DVD, CD-ROM)? *

- ◯ Sim
- ◯ Não
- ◯ Às vezes
- ◯ Nunca

22 - Existe algum procedimento para informar sobre um incidente de segurança da informação? *

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

23 - As áreas de acesso restrito contêm aviso? *

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

24 - A entrada e a saída de visitantes é registrada? *

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

25 - As ações de colaboradores e de visitantes são monitoradas? *

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

26 - Como você julga o nível de importância do seu trabalho para a instituição?

	1	2	3	4	5	
Sem importância	◯	◯	◯	◯	◯	Muita importância

27 - Adicione seu comentário, sobre a segurança da informação na instituição.

*Opcional

_____