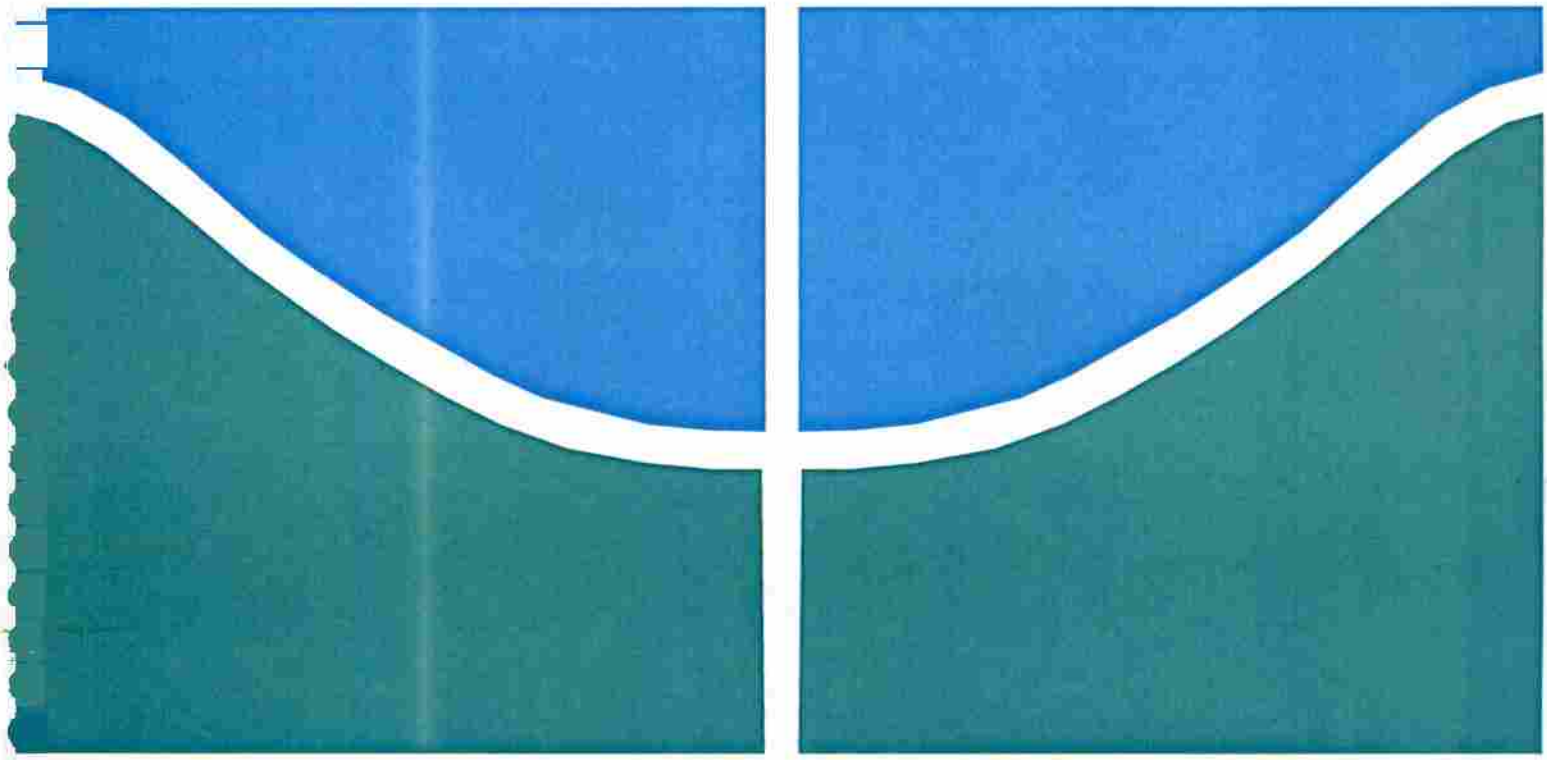


ESTUDO DE CASO: PROPOSTA PARA IMPLANTAÇÃO DE POLÍTICA DE SEGURANÇA EM EMPRESA DE PUBLICIDADE

EDILSON DA SILVA SANTOS

MONOGRAFIA
DE ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO DE CASO: PROPOSTA PARA IMPLANTAÇÃO DE POLÍTICA DE SEGURANÇA EM EMPRESA DE PUBLICIDADE

EDILSON DA SILVA SANTOS

ORIENTADOR: ALCYON FERREIRA DE SOUZA JUNIOR

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: UnBLabRedes.MFE.049/2017.

BRASÍLIA, DF: SETEMBRO/2017.

UNIVERSIDADE DE BRASÍLIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO DE CASO: PROPOSTA PARA IMPLANTAÇÃO DE POLÍTICA DE SEGURANÇA EM EMPRESA DE PUBLICIDADE

EDILSON DA SILVA SANTOS

MONOGRAFIA SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE PÓS GRADUADO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO.

APROVADO POR:

_____

ALCYON FERREIRA DE SOUZA JUNIOR
MESTRE, UNB/ENE (ORIENTADOR)

_____

ALEXANDRE PINHEIRO
MESTRE, UNB/ENE (EXAMINADOR INTERNO)

_____

RAFAEL TIMÓTEO DE SOUSA JÚNIOR
DOUTOR, UNB/ENE (EXAMINADOR INTERNO)

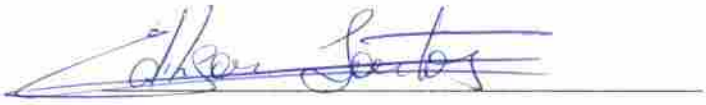
BRASÍLIA, DF, 11 DE SETEMBRO DE 2017.

CESSÃO DE DIREITOS

AUTOR: Edilson da Silva Santos

TITULO DA MONOGRAFIA: Estudo de Caso: Proposta para Implantação de Política de Segurança em Empresa de Publicidade.

GRAU / ANO: Pós Graduado / 2017



Edilson da Silva Santos
Quadra 306 Conj. 7 Casa 19 (Residencial Oeste)
São Sebastião / DF
CEP: 71.691-623
Tel. 55 – 61 – 99130-8630 / edilsonmk@gmail.com

AGRADECIMENTOS

Gostaria de agradecer primeiramente a Deus, pois acredito que tudo parte dele. Pela proteção, ajudar e por me guiar nessa longa jornada até aqui.

A toda minha família, em especial aos meus pais Felipe e Rosária pelo incentivo, apoio, educação e formação do meu caráter, pois tudo que sou é exemplo e inspiração neles.

A minha esposa, por estar sempre ao meu lado, me apoiando, dando força e me dar uma família maravilhosa.

A todos meus amigos, que compartilham momentos de descontração, inspiração, conhecimento e por estarem sempre ao meu lado.

A toda equipe do LabRedes pela convivência todo esse tempo, o conhecimento compartilhado e o apoio incondicional sempre.

Meus sinceros agradecimentos.

Dedico

Ao meu filho ***Ícaro****,*

que já me inspira a ser cada dia melhor e

um exemplo para ele,

assim como meu pai foi para mim.

RESUMO

ESTUDO DE CASO: PROPOSTA PARA IMPLANTAÇÃO DE POLÍTICA DE SEGURANÇA EM EMPRESA DE PUBLICIDADE.

Autor: Edilson da Silva Santos
Orientador: Professor Alcyon Ferreira de Souza Junior
Programa de Pós-graduação em Gestão de Segurança da Informação
Brasília, 11 de setembro de 2017.

Os avanços tecnológicos, a globalização, a Internet, trouxeram grandes melhorias e facilidades para a comunicação mundial, mas também demostraram fragilidades e o quanto estamos vulneráveis a ameaças que surgem diariamente. De olho nesse novo cenário, as organizações investem cada vez mais em tecnologias, capacitação, políticas de segurança e produtos que se enquadre na realidade dos seus negócios. Analisando essa nova realidade, a segurança da informação ganha destaque, sua importância não está apenas em ferramentas de detecção, proteção contra vírus e invasores, mas em medidas de prevenção, resposta, recuperação e principalmente a continuidade do negócio. Diariamente as organizações são expostas a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, sabotagem, espionagem, vandalismo, incêndio, inundações entre outros. Os danos podem ser causados por *hackers*, funcionários mal intensionados ou descontentes com a empresa, a cada dia surgem novas ferramentas que facilitam ataques como o de negação de serviço, que se tornam cada vez mais sofisticados e potentes, falha em algum protocolo de segurança ou a ausência dele, em fim, varias são as ameaças a que as empresas estão expostas. Pensando nisso, este estudo de caso é totalmente voltado a realidade da empresa. A implantação da Política de Segurança irá estabelecer regras para utilização de recursos computacionais, objetivando resguardar os interesses da instituição e a integridade dos seus ativos, seja ele hardware, software ou mesmo seu capital humano intelectual. Preservando sempre os pilares da integridade, confidencialidade e disponibilidade.

ABSTRACT

CASE STUDY: PROPOSAL FOR IMPLANTATION OF SECURITY IN ADVERTISING COMPANY.

Author: Edilson da Silva Santos
Supervisor: Professor Alcyon Ferreira de Souza Junior
Programa de Pós-graduação em Gestão de Segurança da Informação
Brasília, 11 de setembro de 2017.

Technological advances, globalization, the Internet have brought great improvements and facilities for global communication, but they have also shown weaknesses and how vulnerable we are to threats that arise daily. With this new scenario in mind, organizations are increasingly investing in technologies, training, security policies and products that fit into the reality of their business. Analyzing this new reality, information security is highlighted, its importance is not only in detection tools, protection against viruses and intruders, but in prevention, response, recovery and mainly business continuity. Organizations are exposed to a variety of threats to information security, including electronic fraud, sabotage, espionage, vandalism, fire, flood, and so on. The damage can be caused by hackers, employees who are poorly trained or dissatisfied with the company, new tools are emerging every day that facilitate attacks such as denial of service, which become increasingly sophisticated and powerful, fails in some security protocol or the absence of it, in short, several are the threats to which companies are exposed. Thinking about it, this case study is totally geared to the reality of the company. The implementation of the Security Policy will establish rules for the use of computing resources, aiming to safeguard the interests of the institution and the integrity of its assets, be it hardware, software or even its intellectual human capital. Preserving the pillars of integrity, confidentiality and availability.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ACRÔNIMOS

GRSI	Gestão de Riscos de Segurança da Informação
IDS	Sistema de Detecção de Intrusão
IPS	Sistema de Prevenção de Intrusão
IP	Internet Protocol
PSI	Política de Segurança da Informação
PDCA	Planejar, Fazer, Verificar e agir.
PCN	Plano de Continuidade do Negócio
SI	Segurança da Informação
TI	Tecnologia da Informação

1 - INTRODUÇÃO

O presente documento tem como escopo propor a implantação de uma Política de Segurança da Informação e Utilização de Recursos Computacionais que poderão ser adotadas pela empresa objeto de estudo, objetivando resguardar os interesses da instituição e oferecer serviços e recursos de tecnológicos preservando sempre os pilares da integridade, confidencialidade e disponibilidade.

Conforme a NBR ISO/IEC 27002:2013:

> 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. Ela é alcançada a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Para isto, as Políticas de Segurança da Informação e Utilização de Recursos Computacionais, irão descrever as normas de utilização e as atividades que violam o bom uso dos serviços disponibilizados, as quais são consideradas proibidas.

Vivemos a era da informação, onde tudo é muito dinâmico e está facilmente acessível, ao passo de um click encontramos de tudo na Internet. O ciberespaço é um universo de oportunidades e os usuários mal intencionados já perceberam isso. Hoje encontramos facilmente ferramentas que facilitam invasões, ataques, fraudes, sabotagem, entre outros, e com isso, aumentam exponencialmente o número de ameaças, tornando as empresas despreparadas alvos fáceis. Com isso, fica claro a necessidade de funcionários cada vez mais capacitados e políticas claras que auxiliem no direcionamento e capacitação dos colaboradores e das organizações nessa nova realidade.

1.1 - MOTIVAÇÃO

Com os grandes avanços tecnológicos, a Segurança da Informação torna-se uma prioridade entre as organizações. A informação está entre seus ativos mais valiosos e necessita cuidado na sua obtenção, manuseio e descarte.

Pensando nisso, é imprescindível que uma empresa de grande porte nos dias atuais não possui uma Política adequada às novas técnologias e a suas regras de negócio. Este trabalho é totalmente voltado a realidade da empresa em questão, pois ainda não dispõe de tal ferramenta para criar normas internas, padronizar o trabalho e o uso de equipamentos de informática, para que com isso possa resguardar seus ativos e minimizar os riscos de perdas e danos.

A Política de Segurança tem que seguir a legislação, acompanhar as mudanças, atender e se adequar às necessidades da empresa e a novas tecnologias do mercado, sempre aberta a debates, observando relatório e estatísticas que possam mensurar e embasar essas mudanças.

1.2 - OBJETIVOS DO TRABALHO

O trabalho tem como escopo propor a implantação de uma Política de Segurança totalmente voltada ao ramo de negócio da organização, publicidade e propaganda e também estará de acordo com novas tecnologias, normas, regulamentos e a realidade atual do mercado, objetivando sempre resguardar os interesses da instituição e ao mesmo tempo oferecer os serviços, recursos com alta qualidade, desempenho e segurança.

Para obtenção do objetivo, a PSI será dividida em três etapas, que são:

a. Fazer uma revisão nas normas da família ISO 27000, e adequá-las a empresa.
b. Definir o cenário, seu ramo de negócio, processos e principais ativos para uma total adequação.
c. Definir o escopo do projeto e propor a implantar da PSI.

1.3 - METODOLOGIA DE PESQUISA

A metodologia de pesquisa proposta foi a busca por informações em livros, artigos e Políticas atuais de grandes empresas como forma de adquirir embasamento teórico e profundo conhecimento sobre o tema.

Em um segundo momento foi buscado o conhecimento das normas da família ISO 27000, para ter um maior conhecimento das leis pertinentes ao tema e ter uma noção dos processos que envolvem a criação de uma PSI, para cria-la já sobre estes pilares.

Por fim, em cima de um questionário respondido pelo departamento de TI, foi possível fazer um estudo de caso para conhecer a situação atual da empresa; seus ativos, trato com questões de segurança e discernimento entre os colaboradores para propor a implantação.

1.4 - CONTRIBUIÇÕES DO TRABALHO

Busca-se com este trabalho a implantação de uma PSI atualizada, voltada para o ramo de publicidade e propaganda, que atenda as normas e legislações e que padronizam o segmento.

Em um segundo momento almeja-se a mudança contínua na cultura da organização, inserindo aos poucos a segurança no dia a dia da empresa, buscando o uso consciente e responsável sobre cada ativo, gerenciando os riscos e padronizando os processos e procedimentos internos através da Política de Segurança.

O trabalho também contribuirá para criação de sistemas auxiliares de estatística e probabilidade de incidentes, para mensuração e melhoramento constante da PSI. Também contará com modelo de atualizações constantes o que facilitará a eficácia do processo.

1.5 - ORGANIZAÇÃO DO TRABALHO

Para um melhor entendimento deste trabalho, a sua organização é descrita a seguir.

O Capítulo 2 demostra o que é, e a relevância que tem para a empresa possuir uma Política de Segurança atual e nos moldes dos seus negócios. Demostra também os princípios da Segurança da informação e seus pilares segundo a ISO 27002.

O Capítulo 3 faz um estudo de algumas normas da família ISO 27000, tendo como foco as normas ISO/IEC 27002, 27001 e 27005, elencando pontos importantes das normas os quais são imprescindíveis para uma PSI, eficiente e eficaz para o uso da organização.

O Capítulo 4 é feito o estudo de caso, apresentando dados importantes sobre a rotina diária da empresa e definindo o escopo para implantação da PSI.

O Capítulo 5 é proposto a implantação da PSI, definindo de forma clara objetivos a serem alcançados, detalhando processos, implementando controles e definindo critérios para uso racional de cada ativo da organização.

O Capítulo 6 conclui fazendo uma explanação geral sobre o trabalho, apresentado tópicos relevantes sobre o cenário tecnológico atual e o engajamento das organizações nesse contexto.

2 – REVISÃO BIBLIOGRÁFICA E FUNDAMENTAÇÃO

A revisão bibliográfica é fundamentada no estudo das normas da família ISO 27000. Buscando o conhecimento teórico de normas e legislação, processos e procedimentos a fim de alcançar uma PSI eficiente e eficaz que realmente possa trazer a segurança necessária para o funcionamento diário da organização.

Este capítulo tem como foco demostrar a relevância que tem a empresa possui uma PSI voltada a sua área de atividade, respeitando normas e princípios legais e conhecer novos conceitos e tecnologias que comprovem sua real necessidade. Na seção 2.1 é apresentado o conceito de PSI. A seção 2.2 especifica, segundo os principais autores, os três tipos de PSI. Na seção 2.3 é demostrado a importância de uma empresa possuir uma PSI atualizada e adequada ao seu ramo de negócio. Na seção 2.4 é abordado os princípios basilares da segurança da informação. Na seção 2.4.1 é falado sobre o princípio da Confidencialidade. Na seção 2.4.2 é falado sobre o princípio da Integridade. Na seção 2.4.3 é falado sobre o princípio da Disponibilidade.

2.1 - Definição de Política de Segurança da Informação

É um documento de alto nível que representa o topo de uma pirâmide de outros documentos que fornecem informações em graus de detalhamento cada vez maiores sobre os padrões e procedimentos de segurança a serem aplicados aos dados e sistemas corporativos relativos à segurança.

Para Fontes (2006);

> É um documento que deve conter um conjunto de normas, métodos e procedimentos, os quais devem ser comunicados a todos os funcionários, bem como analisado e revisado criticamente, em intervalos regulares ou quando mudanças se fizerem necessárias. É o SGSI que vai garantir a viabilidade e o uso dos ativos somente por pessoas autorizadas e que realmente necessitam delas para realizar suas funções dentro da empresa.

Segundo o Cert.Br (2012), *"a política de segurança define os direitos e as responsabilidades de cada um em relação à segurança dos recursos computacionais que utiliza e as penalidades às quais está sujeito, caso não a cumpra"*.

É considerado como um importante mecanismo de segurança, tanto para as instituições como para os usuários, pois com ela é possível deixar claro o comportamento esperado de cada um. Dessa forma casos de mau comportamento ou descumprimento, que estejam previstos na política, podem ser tratados de forma adequada pelas partes envolvidas.

Dantas (2011), define como sendo: "*um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades para com a segurança da informação*".

2.2 - Tipos de Políticas

Existem três tipos de políticas: Regulatória, Consultiva e Informativa.

2.2.1 - Regulatória

Ferreira (2003), afirma que: "*políticas regulatórias são implementadas devido às necessidades legais que são importantes à organização. Normalmente são muito específicas para um tipo de atividade*".

Ela traz com riqueza de detalhes processos e procedimentos e a quem serão imputados ressaltando sua relevância.

2.2.2 - Consultiva

Ferreira (2003), sugere apenas que são: "*ações e métodos devam ser utilizados para realizar uma determinada tarefa. A ideia central é esclarecer as atividades cotidianas da empresa de maneira simples, direta e didática*".

2.2.3 - Informativa

Ferreira (2003), sugere que: *"essa política possui um caráter meramente informativo, nenhuma ação é desejada e o descumprimento não enseja risco ou punição"*.

2.3 – Por que Criar uma PSI

Segundo Nakamura & Geus (2003);

> na década de 70 e 80 o enfoque principal da segurança, nos negócios da organização, era o sigilo dos dados. Já nas décadas de 80 e 90, com o surgimento do ambiente de rede, a integridade era de suma importância, e a proteção era feita tendo em mente a informação e não os dados. A partir da década de 90 a informação tornou-se essencial para o negócio e com o crescimento das redes o enfoque passou a ser a disponibilidade, e a proteção passou a ser sobre o conhecimento.

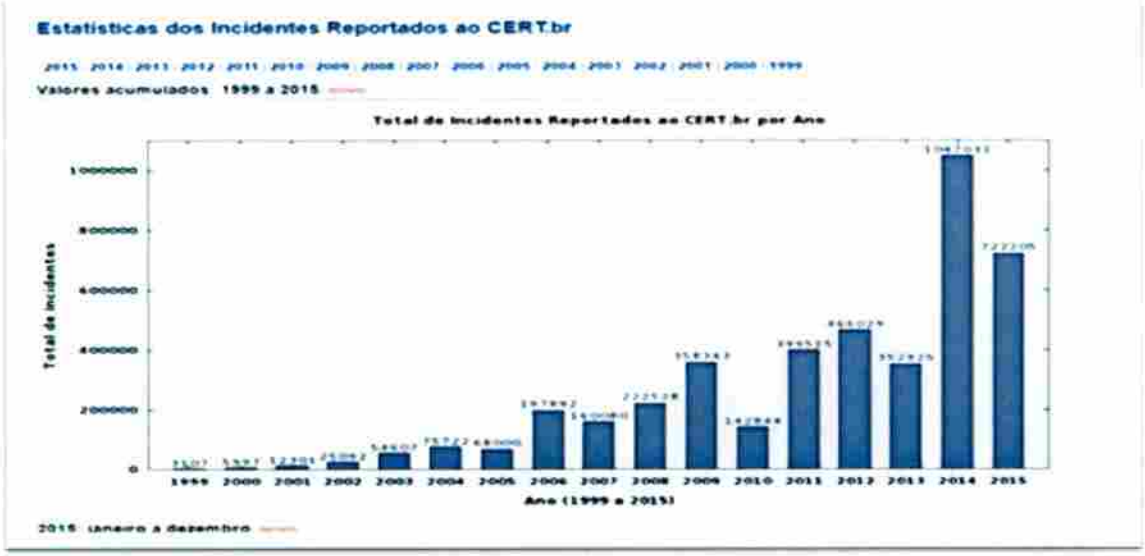
O bem mais importante que as empresas possuem, sem dúvida, são as informações gerenciais, sendo muito importantes para a tomada de decisões. Com o crescimento da internet e o uso de dispositivos móveis nas empresas é inevitável à ocorrência de problemas de segurança, é preciso muito planejamento e muito trabalho da equipe de TI para lidar com tudo isso. É importante criar normas, regras rígidas e principalmente treinar toda a equipe interna e externa.

Estudos publicados pelo site support net workerik (2013), revelam que:

> A maioria dos incidentes relacionados à segurança são ocasionados no ambiente interno, sendo que atualmente a grande parte dos recursos são investidos no ambiente externo (medidas de proteção, firewall, IDS, IPS, etc). A equipe interna pode ser um grande problema, se não for bem treinada. É preciso mostrar como é fundamental a proteção das informações gerenciais, tanto para a organização quanto para o profissional. É através de uma política de segurança bem elaborada que podemos minimizar problemas e conscientizar os usuários.

Na pesquisa a seguir, é possível identificar o crescimento no número de incidentes reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), contudo não podemos precisar de fato os números, pois muitos incidentes não são reportados.

Figura 1 - Estatística de Incidentes

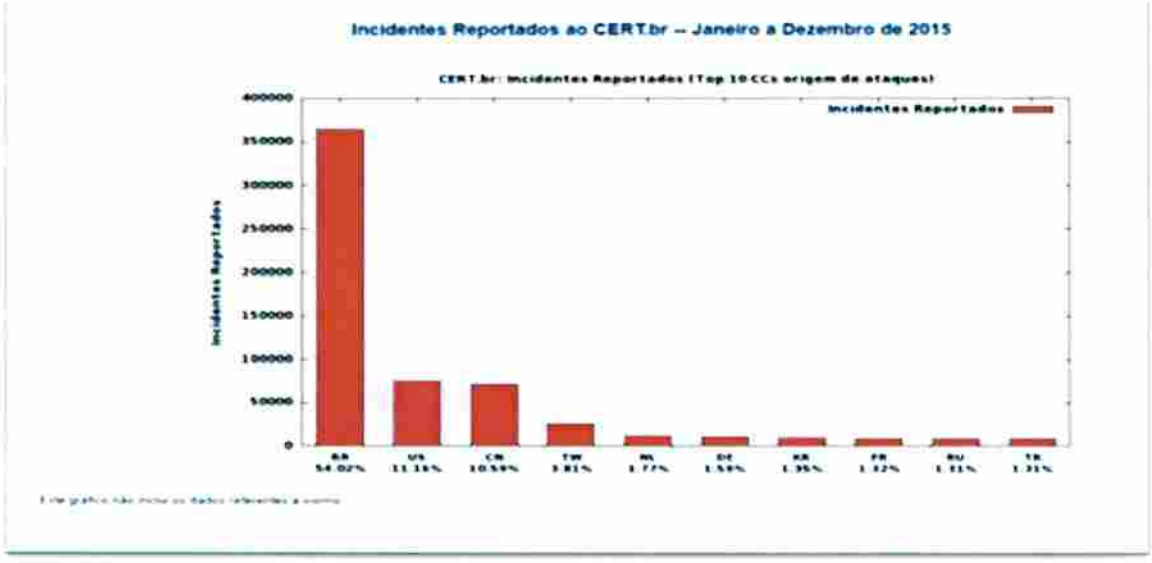


Fonte: www.cert.br

A Figura 1 apresenta informações de ataques, invasões, relatos de incidentes e de roubo de informações na internet, reportado anualmente de 1999 a 2015, com isso é possível ver o aumento assombroso no número de incidentes. A questão da segurança passa a ser vista com olhos mais atentos pelas organizações, porque agora estamos falando de danos incalculáveis em alguns casos irreversíveis.

O estudo demostrado na figura abaixo coloca o Brasil como recordista no top 10, quando se busca a origem dos ataques.

Figura 2 - Incidentes Reportados (Top 10 – Origem de ataques).



Fonte: www.cert.br

Na Figura 2, podemos observar que quando se fala em origem de ataques temos o Brasil em destaque com números exorbitantes de janeiro a dezembro de 2015.

Com isso é possível notar a urgência em adotar medidas de segurança que proteja seus ativos. As organizações necessitam de um maior controle na utilização de seus recursos, maior capacitação e controle por parte dos seus gestores.

2.4 - Princípios da Segurança da Informação

Segundo ABNT NBR 17799:2005;

> a Segurança da Informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de softwares e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e os requisitos de segurança de uma organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

Para (DIAS, 2000, p. 42);

> quando se pensa em segurança, a primeira ideia que nos vem à mente é a proteção das informações, não importando onde estas informações estejam armazenadas. Um computador ou sistema computacional é considerado seguro se houver uma garantia de que é capaz de atuar exatamente como o esperado. Porém a segurança não é apenas isto. A expectativa de todo usuário é que as informações armazenadas hoje em seu computador, lá permaneçam, mesmo depois de algumas semanas, sem que pessoas não autorizadas tenham tido qualquer acesso a seu conteúdo.

Baseando-se na norma NBR ISO 27002 os princípios da Segurança da Informação se mantem sobre três pilares, que são Confidencialidade, Integridade e Disponibilidade.

2.4.1 - Confidencialidade (RFC 2828)

A propriedade que a informação não esteja disponível ou divulgada a indivíduos, entidades ou processos não autorizados, isto é, a informação não deve nem ficar acessível, nem ser divulgada para um usuário, uma entidade, um processo, ou a qualquer entidade não autorizado ao sistema.

2.4.2 - Integridade (RFC 2828)

A propriedade que os dados não foram alterados, destruídos, ou foram perdidos de forma não autorizada ou acidental.

2.4.3 - Disponibilidade (RFC 2828)

Estabelece que um sistema ou um recurso do sistema deve ser acessível e utilizável sob demanda por uma entidade autorizada do sistema, de acordo com as especificações de desempenho para o sistema, isto significa que um sistema é considerado disponível se ele fornece serviços de acordo com o projeto do sistema sempre que os usuários solicitem.

Equivale à propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada.

2.5 – Níveis da PSI

Para o bom entendimento é disseminação do conhecimento entre todos os colaboradores da empresa é necessário que a PSI seja descrita de forma clara e objetiva com as devidas responsabilidades e imputações em caso de descumprimento.

A PSI deve ser aprovada pelos Diretores e Executivos e logo em seguida publicada de forma clara para ter uma total aceitação na empresa e uma maior adesão entre os funcionários. Não pode haver qualquer dúvida entre os usuários. Todos os colaboradores da organização incluindo aqueles que são terceirizados e prestadores de serviço, deverão receber um treinamento adequado para que se adequem às mudanças.

A PSI pode ser dividida entre vários níveis para uma maior compreensão. Entre os executivos temos um nível mais genérico, estratégico, já em nível do usuário temos uma

Segundo a NBR ISO/IEC 27002, "*ao longo da história a experiência tem mostrado alguns fatores tidos como primordiais para o sucesso na criação e implementação de uma PSI na organização*".

São eles:

- Política de segurança da informação, objetivos e atividades, que reflitam os objetivos do negócio;
- Uma abordagem e uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional;
- comprometimento e apoio visível de todos os níveis gerenciais;
- um bom entendimento dos requisitos de segurança da informação, da análise e ou avaliação de riscos e da gestão de risco;
- divulgação eficiente da segurança da informação para todos os gerentes, funcionários e outras partes envolvidas para se alcançar a conscientização;
- distribuição de diretrizes e normas sobre a política de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas;
- provisão de recursos financeiros para as atividades da gestão de segurança da informação;
- provisão de conscientização, treinamento e educação adequados;
- estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação;
- implementação de um sistema de medição, que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria.

Sendo assim, é necessário um estudo de viabilidades sobre cada item descrito acima, tendo em vista que é fator decisivo para o sucesso ou fraco da Política de Segurança.

2.7 – Síntese do Capítulo

Neste capítulo foi possível demostrar o que é uma Política de Segurança da Informação ressaltando sua importância, como está classificada para alcançar um maior engajamento em todos os níveis da organização, do estratégico ao operacional.

Também foi demonstrada a evolução tecnológica que vivemos, e como o trato com as informações gerenciais mudaram nas últimas décadas, passando a tê-la como o bem mais precioso, demonstrou principalmente, o cenário de grandes ameaças tecnológicas e grandes oportunidades, onde um *cracker* com pouco conhecimento pode causar um grande estrago ou um simples funcionário descontente pode parar todo o negócio da organização.

Cracker; *perito em informática que usa seus conhecimentos para violar sistemas ou redes de computadores.*

3 – ESTUDO DE ALGUMAS NORMAS DA FAMÍLIA ISO 27000

A norma ISO 27000 é um padrão internacional que versa sobre as boas práticas da Gestão da Segurança da Informação, que levam empresas ao nível máximo de excelência internacional em Segurança da Informação.

Faz-se mister um profundo conhecimento dessas normas para uma melhor adequação da empresa, com procedimentos, boas práticas e Políticas de Segurança adequadas ao seu ramo de negócio. Necessário também para quem almeja certificação.

3.1 - Norma ABNT NBR ISO/IEC 27002:2013

A norma ISO/IEC 27002 é um código de boas práticas para a gestão de segurança da informação. Esta norma pode ser vista como o início, para quem pretende desenvolver diretrizes, princípios gerais, controles e metas aceitas no processo de gestão da segurança da informação.

É importante ressaltar que ela não tem força de lei, apenas trás critérios e boas práticas para melhor prover a segurança de várias formas na organização.

Quanto a organização, está norma contém 14 seções de controles de segurança da informação, 35 objetivos de controles e 114 controles. Os objetivos dos controles definem o que deve ser alcançado.

A norma ISO/IEC 27002 traz a descrição dos controles como sendo:

1 – **Política de segurança da informação:** Promove a orientação e apoio a direção da organização para a segurança da informação, observando dispostos legais, regulamentos relevantes para organização.

É importante que a PSI esteja de acordo com a estratégia do negócio e de acordo com regulamentos, legislação e contratos vigentes, observando sempre o cenário atual da TI.

A PSI deve ser analisada criticamente em intervalos planejados ou quando ocorrerem mudanças significativas, para garantir sua adequação, eficácia e continuidade.

2 - **Organização da segurança da informação:** Estabelece a estrutura do gerenciamento para iniciar a implementação de controle sobre os ativos.

Estabelecendo responsabilidades de forma clara e em conformidade com a PSI da organização.

3 - **Segurança em recursos humanos:** Assegurar que cada funcionário ou colaborador entenda sua responsabilidade e esteja à altura dela. É necessária a verificação do histórico profissional, mas sempre de acordo com a ética, regulamentos e leis relevantes. A verificação deve ser feita de acordo com a legislação em vigor e observando a intimidade da pessoa no que tange a sua privacidade.

4 – **Gestão de ativos:** A organização deve manter um inventário atualizado de ativos, com a definição do respectivo responsável e mantida uma documentação com sua importância o seu ciclo de vida.

5 – **Controle de acesso:** Deve ser estabelecido uma política de controle de acesso, baseado em requisitos da segurança da informação e dos negócios.

6 – **Controle criptográfico:** Implementar uma política para o uso de controles criptográficos para a proteção da informação, garantindo assim, o uso efetivo e adequado da criptografia a fim de proteger os princípios da confidencialidade, autenticidade e a integridade da informação.

7 – **Segurança física e do ambiente:** Definir o perímetro de segurança para proteger as instalações de processamento da informação, prevenindo o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações críticas ou sensíveis da organização.

8 – **Segurança nas operações:** Garantir a operação segura dos recursos de processamentos da informação. Documentando procedimentos e disponibilizando a todos os usuários que necessitem deles.

9 – **Segurança nas comunicações:** Garantir a proteção das informações em redes e dos recursos de processamento da informação que os apoiam.

10 – **Aquisição, desenvolvimento e manutenção de sistemas:** Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas.

11 – **Relacionamento na cadeia de suprimento:** Garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores, criando uma política com procedimentos e implementando controles para mitigar os riscos associado ao acesso.

12 – **Gestão de incidentes de segurança da informação:** Assegurar um efetivo gerenciamento para os incidentes de segurança da informação,

incluindo a comunicação sobre fragilidades e eventos de segurança. Atribuir responsabilidades e criar procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

13 – **Aspectos da segurança da informação na gestão da continuidade do negócio:** Assegurar a continuidade da segurança da informação em situações adversas, determinando requisitos para segurança da informação e continuidade do negócio. É necessária a implementação do planejamento da continuidade do negócio e da recuperação de desastre.

14 – **Conformidade:** Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança.

Embora o conteúdo da PSI possa variar de acordo com o tipo de instituição, ela deverá buscar abranger os controles relacionados acima. Os controles devem ser adequados e revisados periodicamente para uma melhor adequação a realidade do negócio da organização.

3.2 - Norma ABNT NBR ISO/IEC 27001:2006

A Norma ISO/IEC 27001 *(Information Technology – Information Security Management Systems - Requirements)* é o padrão internacional para a gestão da Segurança da Informação e em conjunto com a Norma ABNT ISO/IEC 27002:20013 (Código de Boas Práticas da Gestão de Segurança da Informação) constituem a principal referência, atualmente, para quem procura tratar a questão da segurança da informação de maneira eficiente e com eficácia.

Através da norma em comento é possível implementar um SGSI de forma rápida e eficiente, pois ela define através do modelo PDCA *(Plan-Do-Check-Act ou Planejar-Fazer-Verificar-Agir)* é um método de gestão que se caracteriza por um ciclo de ações que se repete continuamente de forma a incorporar alterações no ambiente.

Segundo a ISO/IEC 27001, as fases Plan-Do ou Planejar e Fazer, estão relacionados às seguintes ações: *"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, implementar e operar a política, controles, processos e procedimentos do SGSI."*

Nestas duas primeiras etapas deverão ser definidos limites para implantação do SGSI, também deverá definir o escopo do projeto com definição objetiva de ativos, responsáveis, vulnerabilidades e possíveis ameaças, implementando ainda procedimentos e controles para mitigar os riscos.

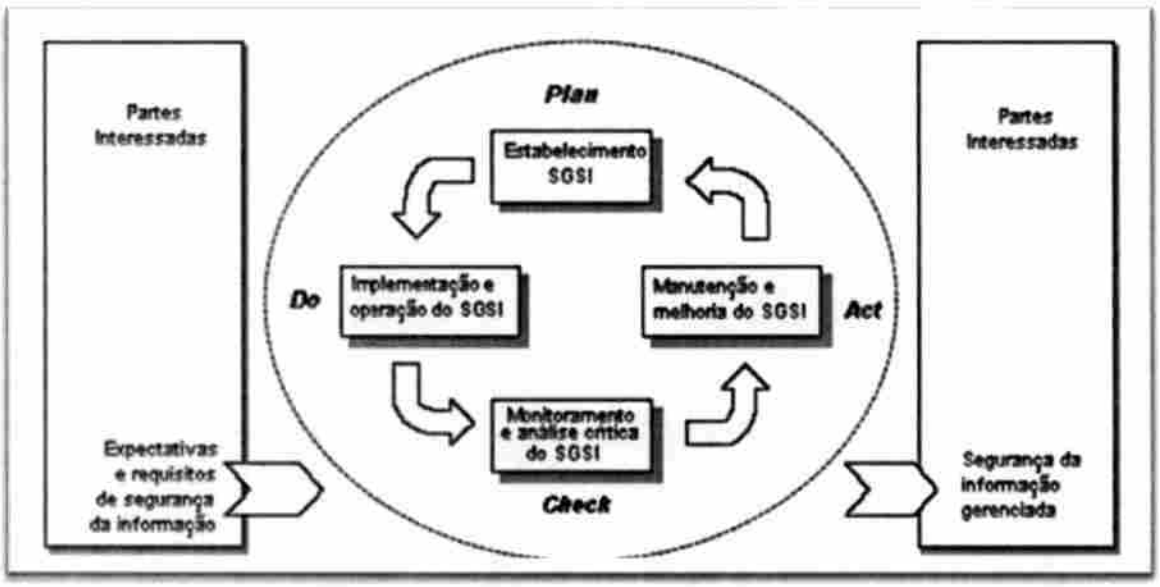
Conforme descrito na ISO/IEC 27001, às últimas etapas do ciclo PDCA correspondem à parte de auditoria e a ações relacionadas a elas são:

> Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência pratica do SGSI e apresentar os resultados para a análise crítica pela direção; 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.

Às fases (Check-Ack) estão relacionadas à verificação de que as medidas de segurança especificadas estão sendo aplicadas, às soluções de segurança utilizadas e à melhoria contínua do conjunto de segurança, além das auditorias periódicas de cada componente do sistema.

A figura a seguir demostra fielmente as ações pertinentes a cada etapa do processo.

Figura 4 - Modelo PDCA aplicado aos processos de SGSI



Fonte: Norma ABNT ISO/IEC 27001:2006

3.3 - Norma ABNT NBR ISO/IEC 27005:2008

Esta norma internacional fornece diretrizes para o processo de gestão de riscos de segurança da informação nas organizações. Vale ressaltar que ela traz requisito e é baseada na ISO 27001, portanto trata de forma global a questão do risco cabendo a cada empresa definir questões como contexto, escopo do projeto e adequá-la conforme sua necessidade, pois várias são as metodologias utilizadas.

Segundo a ISO 27005; *"riscos de segurança da informação são as possibilidades de uma ameaça explorar vulnerabilidades dos ativos, comprometendo a confidencialidade, integridade e disponibilidade das informações de uma organização"*.

A análise e avaliação dos riscos deverão ser revisadas em períodos de tempo determinados, ou toda vez que seja necessária, ou ocorra fato que mereça atenção.

3.3.1 – Visão Geral do Processo de Gestão de Risco de SI

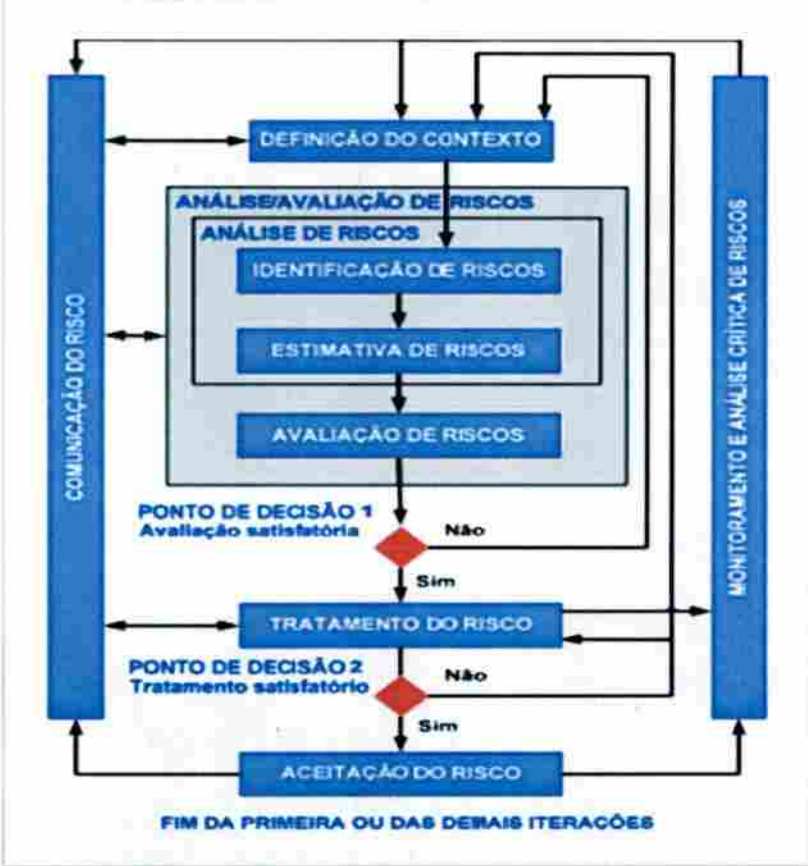
A norma trata o processo de gestão de riscos definindo vários contextos e analisando-os separadamente por seções:

A (seção 7) trata do contexto, (seção 8) análise/avaliação de riscos, (seção 9) tratamento do risco, (seção 10) comunicação do risco, (seção 11) monitoramento e (seção 12) análise crítica de riscos.

Segundo a norma em comento; *"as atividades do processo se iniciam com a atividade de definição do contexto, seguidas de análise/avaliação de riscos, tratamento do risco, aceitação do risco, comunicação do risco, por final monitoramento e análise crítica do risco"*.

A figura abaixo ilustra as atividades do processo de GRSI.

Figura 5 – Visão Geral do Processo de Gestão de Riscos de SI



Fonte: ABNT ISO 27005:2008

3.3.2 – Definição do Contexto

Por se tratar da primeira fase do processo deve ser muito bem definido e está umbilicalmente ligado ao escopo, assim sendo poderá afetar todo o processo.

Aqui é onde recebe as primeiras informações relevantes sobre a organização para iniciar o processo de gestão do risco de SI.

Tem como saída o escopo e os limites do processo de gestão de riscos de SI.

3.3.3 – Avaliação de Riscos de SI

A ISO 27005 recomenda que essa etapa seja desenvolvida levando em conta alguns aspectos da organização, como:

O valor estratégico do processo que trata as informações de negócio.

A criticidade dos ativos de informação envolvidos.

Requisitos legais e regulatórios, bem como as obrigações contratuais.

Importância do ponto de vista operacional e dos negócios, da disponibilidade, da confidencialidade e da integridade.

Expectativas e percepções das partes interessadas e consequências negativas para o valor de mercado (em especial, no que se refere aos fatores intangíveis desse valor), a imagem e a reputação.

3.3.4 – Tratamento do Risco de SI

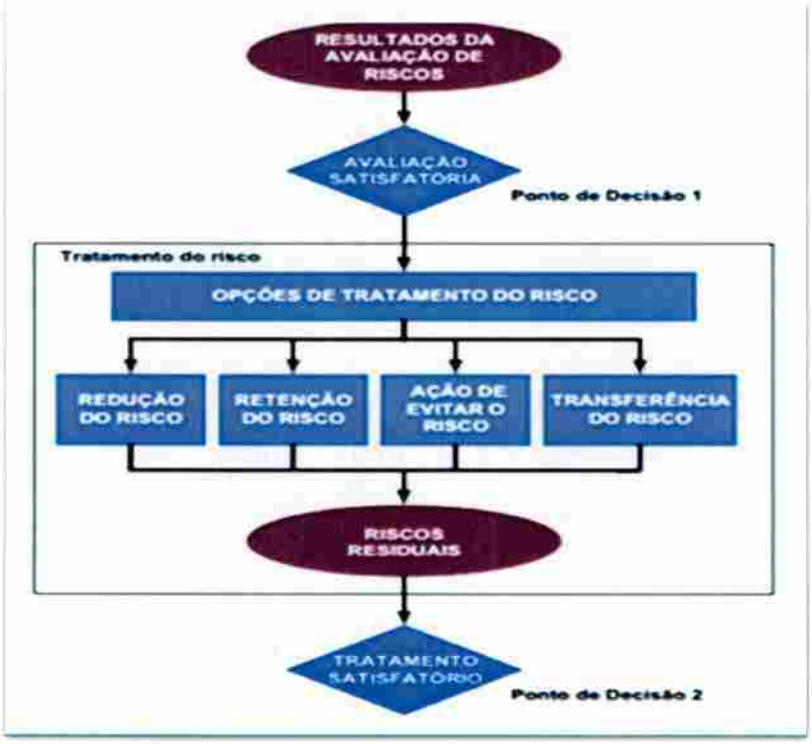
Aqui a norma elenca de forma ordenada e por prioridade (de acordo com os critérios de avaliação de riscos), associados aos cenários de incidentes que os provocam.

As ações relativas a essa seção são: reduzir, reter, evitar ou transferir os riscos de forma a definir conhecer o plano de tratamento do risco.

Está etapa condiciona à aceitação a decisão tomada pelos gestores.

A figura a seguir detalha cada etapa do processo.

Figura 5 – Descrição das Atividades de Tratamento do Risco em GRSI



Fonte: ABNT ISO 27005:2008

3.3.5 – A aceitação do Risco de Segurança da Informação

É o plano de tratamento do risco residual sujeito a decisão e aceitação formal dos por parte dos gestores da organização.

A norma estabelece que a decisão de aceitar os riscos seja formalmente registrada, juntamente com a responsabilidade pela decisão.

Estabelece ainda a elaboração de uma lista com os riscos aceitos assim como a justificativa para os que não satisfaçam.

3.3.6 – Comunicação do Risco de SI

Nesta etapa temos como entrar toda a informação sobre riscos obtida através das atividades de gestão de riscos.

A norma recomenda que as informações sobre os riscos sejam compartilhadas com todos os interessados e quem for responsável pela tomada de decisão.

É recomendável que a organização desenvolva planos de comunicação dos riscos tanto para as operações rotineiras como também para situação emergencial. Por tanto a comunicação deve ser contínua.

3.3.7 – Monitoramento e Análise Crítica de Riscos de SI

Segundo a ISO 27005:

> Essa é última atividade do processo de GRSI convém que todos os riscos e seus fatores (isto é, valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidades de ocorrência) sejam monitorados e analisados criticamente, a fim de se identificar, o mais rapidamente possível, eventuais mudanças no contexto da organização e de se manter uma visão geral dos riscos.

Os riscos não são estáticos. As ameaças, vulnerabilidades, probabilidades ou consequências podem mudar rapidamente, portanto deve estar sobre constante monitoramento é necessário tentar prever e prevenir tais mudanças, de modo que o impacto seja o menor possível para a organização.

É um processo que deve estar sobre atenção constante, sendo analisado e melhorado constantemente.

3.3.8 – Síntese do Capítulo

Muitos são os obstáculos quando se pensa em implementar uma PSI na organização, o estudo das normas da família ISO 27000 busca facilitar o entendimento, pois conhecendo melhor os processos que envolvem os conceitos de gestão e o tratamento dos riscos, assim como os controles relacionados a Segurança da Informação fica mais fácil visualiza-los no dia a dia.

O sucesso na implementação vai depender de uma adequação dos controles as exigências da organização, assim como o total engajamento pela Direção no sentido de qualificar os profissionais envolvidos e demostrar sua importância, pois estudos apontam que a maioria dos incidentes partem de agentes internos o que reafirma a posição estratégica do gestor nesse processo.

4 – ESTUDO DE CASO

Este capítulo fará um estudo visando definir o escopo do projeto em cima dos ativos relevantes a serem protegidos, para isso elaborou um questionário que foi respondido pelo departamento de TI da organização o que possibilitou delimitar o campo de atuação e principais tópicos a serem abordados pela Política de Segurança.

4.1 – Conhecendo a Organização

A empresa foi fundada em 1967, desde a sua criação tenta revolucionar o mercado publicidade e propaganda com ações inovadoras, comunicações integradas e diferenciadas. A proposta é ter o cliente em primeiro lugar e não há objetivo que não possa ser alcançado.

Atualmente está entre as 20 maiores agências de publicidade do Brasil. Conta com a matriz no Rio de Janeiro e filiais nas principais capitais do Brasil, possui mais de 600 colaboradores.

4.1.1 - Missão

Ser uma empresa de excelência no ramo publicitário e estar entre as 10 maiores agências 100% brasileiras, até 2018.

4.1.2 - Visão

Ser reconhecida como agência modelo, por entregar soluções inovadoras, utilizar processos eficientes alcançando sempre o melhor resultado para o cliente.

Figura 6 - Organograma Geral da Organização

Fonte: Departamento de TI da empresa.

4.2 – Estrutura de Informática

Atualmente o departamento de informática está dividido em três áreas distintas, conforme demostra a figura a seguir:

Figura 7 - Organograma do Departamento de TI da empresa

Fonte: Departamento de TI da Empresa

Conforme ilustra a figura 8, a divisão das responsabilidades é dividida da seguinte forma:

- **Redes e Telecomunicações:** É responsável pela criação e monitoramento no ambiente de redes, telecomunicações e internet da empresa. Também criar perfis dos usuários (login, senha), no AD, e-mail, rede e backup. Instalação e manutenção dos servidores, controle de tráfico de rede e

internet, equipamentos de telecomunicações e telefonia controle dos dados dos usuários.

- **Sistemas**: Cuida de novos projetos de softwares relevantes para a empresa, faz o suporte, otimização de sistemas existentes, cuida da administração dos Bancos de Dados (específicos para bom andamento da empresa). Suporte ao usuário, no quesito sistemas e treinamentos.
- **Suporte:** Serviço de Help Desk, instalação, manutenção, suporte ao usuário e reparos em laboratório.

4.3 – Relevância da Política de Segurança da Informação

Atualmente a organização não dispõe de uma PSI nos moldes do seu ramo de negócio e que atenda a realidade do mercado. A ausência, de uma PSI inviabiliza alguns procedimentos e torna ineficaz medidas simples de segurança.

Devido a isso, pequenos procedimentos não são implementados na empresa, tornando-a vulnerável em vários aspectos, como:

- Não há monitoração nas áreas da empresa por CFTV, o que dificulta uma possível identificação a um invasor.
- Não é necessário o uso de crachá nas áreas internas da empresa.
- Não há uma restrição maior a entrada no Centro de Processamento de Dados, onde ficam os servidores, firewall, proxy área mais sensível da empresa.
- O Storage (disco com todo backup da empresa) fica no CPD.
- Não existe isolamento acústico ou sala cofre.
- Faltam equipamentos e um plano de contingência.

De forma exemplificativa, esses foram alguns pontos falhos encontrados na estrutura organizacional da empresa e um ponto motivador para criação da PSI.

4.4 – Definindo o Escopo do Projeto

Em cima de um questionário respondido pela equipe de TI, foi possível identificar ativos relevantes e como é a rotina diária no trato com questões essenciais como:

- Acesso físico;
- Backup;
- Segurança;
- Treinamento e se a empresa já possui uma PSI.

Com essas informações foi possível definir o escopo em cima dos processos relevantes e os ativos responsáveis pelo bom andamento dos serviços diários da organização.

O escopo do projeto foi definido em cima dos ativos descritos no Centro de Processamento de Dados (CPD), por se tratar de uma área de risco, onde guardar os equipamentos responsáveis pelas atividades vitais da empresa.

A definição foi baseada na ISO 27001 onde descreve *"cabe à organização definir o escopo e os limites do SGSI nos termos das características do negócio, da organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo"*.

4.5 – Ativos

Conforme descrito no capítulo anterior e com base na ISO 27002:2013; *"é qualquer coisa que tenha valor para a organização e que precisa ser protegido, mas para isso devem ser identificados e classificados de tal forma que o inventário possa ser estruturado e mantido posteriormente. O documento também deve definir o responsável pelo ativo e o tipo de uso permitido"*,

Deve ser feito um levantamento dos ativos demostrando a importância para a organização e o dano causado por uma eventual perda.

Os ativos podem ser divididos da seguinte forma:

- Ativos (informação): como qualquer outro é essencial para os negócios da organização e consequentemente necessita ser protegido. A informação pode estar em diversas locais, tais como; banco de dados, documentação de sistemas, planos de continuidade, material de treinamento, arquivadas, etc.

Seja qual for à forma de apresentação ou meio de transporte, compartilhamento ou armazenamento, é necessária proteção adequada.

- Ativos (software): sistemas de forma geral, aplicativos, utilitários, sistemas operacionais, ferramentas de desenvolvimento.
- Ativos (físicos ou hardware): é a parte palpável da organização, como seus computadores, servidores, roteadores, switches, mídias magnéticas, telefonia e todos os equipamentos físicos da organização.
- Ativos (Serviços): computação e serviços de comunicação, utilidades gerais, como eletricidade, ar-condicionado.
- Ativos (Pessoas): aqui entra o capital intelectual humano, conhecimentos, experiências.
- Ativos (Intangíveis): reputação, marca, confiabilidade e imagem da organização.

4.6 – Gestão de Ativos

A tabela a segui descreve os ativos fundamentais para o funcionamento diário da organização.

Nº	Nome do Ativo	Qtd	Descrição	Critério / Impácto
01	Servidor do Sistema (Publi)	01	Controla todos os serviços da empresa.	Alto
02	Servidor do Sistema (VBS)	01	Interligado ao (Publi).	Alto
03	Servidor do Sistema (IBOPE)	01	Dados de mídia e estatística	Médio
04	Servidor do Banco de Dados (Oracle)	01	Banco de dados do sistema (Publi)	Alto
05	Servidor de Domínio e acesso a rede (Active Directory)	01	Gerencia o acesso a rede da empresa.	Alto
06	Servir de Arquivos	01	Gerencia os arquivos da empresa.	Alto

07	Firewall	01	Controla todo o tráfico de acesso a internet	Alto
08	Servidor de rede (intranet)	01	Mantem a intranet online	Médio
09	Servidor responsável por toda telefonia da empresa	01	Gerencia toda a telefonia da empresa.	Alto
10	Nobreak	01	Mantem os servidores em caso de queda ou falta de energia.	Médio

Tabela 1 - Ativos Relevantes para Empresa

4.7 – Critério de Impacto

Critério	Valor do Ativo	Consequência para organização
Alto	Ativo de grande valia e difícil recuperação.	Paralisa todos os processos essenciais para o serviço da organização.
Médio	Ativo de médio valor e médio tempo de recuperação.	Perda da eficiência em alguns processos.
Baixo	Ativo de baixo valor.	Mínimo dano ao negócio.

Tabela 2 - Critério de Impacto

Analisando as tabelas 1 e 2, é possível perceber que no CPD ficam os servidores responsáveis pelos sistemas de grande valia para empresa, responsável por processos essenciais no dia a dia e sua paralização ou perda causaria danos incalculáveis para a organização.

Para a obtenção de um nível aceitável de segurança no ambiente computacional e preservar os ativos corporativos de modo a garantir os princípios da integridade, confidencialidade e disponibilidade das informações institucionais, é imprescindível a implantação de uma PSI, com objetivo de identificar e adotar soluções que minimizem os riscos e evitem prejuízos, não só em relação às questões que envolvem tecnologia, mas também de ordem financeira e de imagem institucional.

Com a implantação da PSI será possível identificar, monitorar e gerenciar os riscos, além de permitir que se faça no âmbito da intranet, a segmentação da sua rede local em sub-redes, de modo a prover um maior nível de segurança, selecionando ambientes críticos e autorizando usuários determinados.

4.8 – Síntese do Capítulo

Nesse capítulo foi possível conhecer a empresa como um todo, tendo uma visão micro e macro dos processos que envolvem suas rotinas, conhecemos a estrutura de TI e seus principais ativos, podendo assim definir o escopo do projeto.

Foi possível perceber que no CPD é onde se reúnem os principais recursos computacionais, entre eles os servidores que executam os serviços essenciais da organização. Com base na gestão de riscos levando em conta o critério de impacto para o organização foi criada a proposta para implantação da PSI.

5 – PROPOSTA PARA A IMPLANTAÇÃO DA PSI

A proposta de criação da Política de Segurança a seguir foi elaborada com base no estudo das normas:

ISO 27002, ISO 27001 e ISO 27005, conforme estudo no capítulo 3.

Para maiores informações acerca das necessidades, abrangências, rotinas e como está estruturado o departamento de informática da empresa, foi elaborado um questionário e respondido junto ao departamento de TI.

Segundo Dantas (2011);

> O nosso sistema de informações é constituído por um conjunto de elementos ou componentes inter-relacionados, que coletam, manipulam e disseminam os dados e a informação para as nossas atividades de negócios. Ele é composto de *hardware, software,* banco de dados, telecomunicações, pessoas e procedimentos, que formam a infraestrutura tecnológica da nossa organização. Hoje, esses sistemas são essenciais e críticos para o sucesso das atividades de negócios da nossa organização.

É com foco nesse contexto que a PSI foi adotada, em cima de conceitos modernos alinhado com padrão internacional das normas ISO, para que funcionários, clientes, fornecedores, colaboradores e acionistas possam desempenhar seus papéis certos de que o fazem em um ambiente seguro.

5.1 – Objetivo Geral da PSI

A Política de Segurança da Informação tem como escopo prover a orientação e apoio a direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentos.

A PSI aplica-se de modo geral a todos os colaboradores, incluindo prestadores de serviços, também poderá se estender a trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento, ou acesso a informações pertencentes à organização. O objetivo é resguardar sempre os interesses da instituição e oferecer os serviços e recursos com alta qualidade, desempenho e segurança.

A meta é mudar a cultura corporativa dos colaboradores, incluindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade da informação entre as necessidades diárias do negócio.

5.2 – Classificando a Informação

O Supervisor ou Diretor de cada departamento ficará responsável por estabelecer critérios relativos ao nível de confidencialidade da informação tratadas naquele setor (relatórios, documentos, mídias), entre outros, de acordo a numeração abaixo:

1) Pública
2) Interna
3) Confidencial
4) Restrita

Conceitos:

Informação Pública: É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.

Informação Interna: É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

Informação Confidencial: É toda informação que pode ser acessada por usuários da organização e por parceiros. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

Informação Restrita: É toda a informação que pode ser acessada somente por usuários da organização explicitamente indicando pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos aos negócios e/ou comprometer a estratégia de negócio da organização.

Todo Supervisor ou Diretor deve orientar seus subordinados a não circularem informações, documentos, mídias consideradas confidenciais ou restritas, como também não deixar relatórios nas mesas ou impressoras, de forma que pessoas estranhas ao setor possam visualizá-las.

5.3 – Política de Segurança para Recursos Computacionais

A PSI para ativos computacionais abortará necessariamente itens relacionados à segurança da informação, como a utilização dos recursos de rede, criação de conta, senha, e-mail e acesso a intranet, assim como o uso sustentável de impressoras e papel.

Representa uma violação a essa política qualquer ato que:

- Exponha a companhia a uma perda monetária ou que de qualquer forma comprometa a segurança dos dados ou informação, ou ainda que danifique qualquer equipamento.
- Envolva ou exponha dados confidenciais, direitos autorais, patentes, negociações ou qualquer tipo de dados da corporação.
- Envolva qualquer tipo de ato ilícito, que venha violar legislação ou regulamento interno.
- De qualquer modo exponha a organização trazendo prejuízo financeiro ou a imagem.

5.3.1 – Política para o Uso dos Recursos de Rede

- Ao ser admitido na empresa o Diretor do departamento deverá enviar um e-mail passando os dados pessoais e solicitando o acesso a rede interna, assim como pasta para armazenamento de arquivos.
- Ao sair do seu local de trabalho, tenha a certeza de que fechou os programas em uso, e efetuou o *logout/logoff* da rede ou bloqueio do computador através de senha, evitando assim, o uso por pessoas não autorizadas.
- Fica proibido o armazenamento de arquivos desnecessários ou inúteis na rede, evitando assim, sobrecarga no servidor.
- A equipe de TI fica autorizada a fazer buscas na rede e apagar arquivos desnecessários, garantindo assim seu bom desempenho.
- É vedado o acesso, armazenamento, ou distribuição de qualquer material de cunho pornográfico ou racista. Devendo o responsável ser responsabilizado diretamente pelo descumprimento.

- Também fica proibido o armazenamento e instalação de jogos de qualquer natureza na rede.
- O uso de equipamentos particulares como computador, laptop, celulares, entre outros, acessará a internet por wi-fi, mas não acessará a rede da empresa ou contará com auxílio. O departamento de TI não se responsabiliza por possíveis danos decorrentes de falha humana ou mau uso do equipamento.

5.3.2 – Política para Criação de Contas

Todo funcionário ao entrar na empresa terá uma conta que o proporcionará acesso à rede e recursos computacionais. O diretor do departamento fará a solicitação via e-mail descrevendo o cargo e funções e o acesso aos sistemas necessários para suas atividades.

Após a criação funcionário terá uma pasta no servidor para armazenamento dos arquivos de trabalho, a pasta terá o backup feito diariamente.

Em caso de desligamento o Diretor do departamento informará imediatamente o departamento de TI, que providenciará o backup dos arquivos de trabalho e a remoção da conta.

5.3.3 – Política para Criação de Senhas

É importante ressaltar que a senha é secreta, pessoal e intransferível, e deverá ser mantida em total sigilo.

Senhas são o meio mais comum de validação da identidade do usuário para obtenção de acesso a um sistema ou serviço, todos os sistemas da empresa serão acessados por senhas, o cadastro é feito pelo departamento de TI.

Informações e Cuidados:

A primeira senha será informada pela equipe de TI, a qual deverá ser imediatamente modificada. A próxima alteração será no prazo de 45 (quarenta e cinco) dias. Por motivos de segurança, é recomendável que não se utilize senhas fáceis ou que possa ser facilmente identificadas durante a digitação.

A senha terá no mínimo 8 (oito) caracteres, incluindo letras, números e caracteres especiais.

As 3 (três) últimas senhas não serão aceitas.

Evite colocar seu nome ou sobre nome, assim como o de pessoas próximas, como; pais, vizinhos, amigos, parentes, namorado etc.

Em caso de esquecimento a equipe de TI gerará uma nova senha a qual será mudada no primeiro acesso não é possível descobrir a anterior.

Todo ato praticado com uso de senha pessoal é de inteira responsabilidade do funcionário ou colaborador.

5.3.4 – Política para Utilização de E-mail

O e-mail é fornecido pela empresa a todos os funcionários e colaboradores, é uma ferramenta essencial para a comunicação interna e externa da organização. As mensagens devem ser escritas de forma clara, concisa, profissional, de forma que não comprometa a imagem da instituição e sempre respeitando a legislação e os princípios éticos e morais da organização.

O uso do correio eletrônico é pessoal e cada usuário responsável pelo seu, de forma que fica proibido o envio de e-mail que:

- Contenham expressões difamatórias ou linguagem ofensiva que fuja ao que a instituição prega.
- Traga qualquer prejuízo para a organização, ou seja, desnecessária ou inútil.
- Contenha qualquer tipo de material racista ou pornográfico ou que possa denegrir a imagem da organização.
- Possa prejudicar outro funcionário ou colaborador.
- Ou que de qualquer forma seja incompatível com a política e o caráter profissional da empresa.

Cuidados:

- Ao receber e-mail de estranhos com arquivos executáveis (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança, solicite sempre auxílio da equipe de TI.

- Quando receber e-mail com link ou anexo suspeito de pessoa desconhecida, não click ou abra, contate imediatamente o departamento de TI.

É obrigatória a manutenção da caixa de e-mail, evitando o acúmulo de e-mails e arquivos inúteis, podendo solicitar auxílio da equipe de suporte para isso.

5.3.5 – Política para Uso do Ambiente Web

Todas as estações de trabalho tem conexão ativa com a internet, lembrando que é uma ferramenta essencial para o desempenho das atividades rotineiras da empresa, no entanto alguns cuidados devem ser adotados para seu uso.

A navegação somente será feita a sites permitidos.

As informações relativas ao cotidiano, estrutura e negócios da empresa são confidenciais, não podendo ser divulgadas de forma alguma no ambiente web.

Toda a navegação será monitorada pelo departamento de TI da empresa, inclusive com geração de relatório mensal de navegação "*log*" (arquivo que demonstra detalhes da navegação), como: usuário, ip, sites acessados e tempo de conexão.

Navegação será feita obrigatoriamente pelos navegadores *Chrome, Mozilla, Internet Explorer,* ou outro homologado e autorizado pelo departamento de TI.

Não será permitida a utilização de softwares do tipo *peer-to-peer* (P2P), tais como Kazaa, Morpheus, utorrent e afins.

É proibida a navegação em sites de cunho pornográfico, racista ou que pregue de qualquer forma a homofobia, assim como jogos e rádios on-line terão seu acesso bloqueado.

A utilização de recursos de mensagens instantâneas deverá ser solicitada pelo Diretor do departamento e homologada pelo departamento de TI.

O download e instalação de softwares relacionados diretamente ao ramo de atividade da empresa serão feitos pela equipe de TI.

Todo upload dentro da rede empresa será monitorado e deverá ser autorizado pelo Diretor do departamento e equipe de TI.

A internet pode ser utilizada de forma recreativa, mas responsável, somente nos horários de almoço e após o expediente.

5.3.6 – Política para Utilização das Estações de Trabalho (Desktop)

Cada funcionário ao ser admitido na empresa receberá uma estação de trabalho em seu nome, com IP fixo e códigos internos que facilitam a sua identificação na rede da empresa.

O usuário fica responsável por toda atividade feita na sua estação de trabalho, devendo por tanto, mantê-la bloqueada sempre que não estiver usando ou ausente.

Toda instalação de software ou hardware, assim como a desinstalação e suporte será feita pela equipe de TI.

Fica proibido o armazenamento de músicas, filmes, fotos ou softwares sem os devidos direitos autorais. A empresa só trabalha com softwares originais, licenciados e homologados.

A empresa não fará backup das estações de trabalho e não se responsabilizará por eventuais perdas ou danos, por tanto, todos os dados relativos à empresa devem ser armazenados na rede, onde é feito backup diariamente.

5.3.7 – Política para Uso de Laptops, Celulares e Computadores Pessoais

Os usuários que tiverem direito ao uso de computadores pessoais (laptop, notebook, celulares), ou qualquer outro equipamento computacional, de propriedade da organização, devem estar cientes de que:

- Os recursos de Tecnologia da Informação, disponibilizados para usuários, têm como objetivo a realização de atividades profissionais.
- A propriedade do recurso computacional de uso individual é de responsabilidade do próprio usuário.
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
- O usuário não deve alterar a configuração do equipamento recebido, devendo acionar o departamento de TI para qualquer alteração de hardware ou software.

Fora do Trabalho:

- Mantenha o equipamento sempre com você ou em segurança;

- Atenção redobrada em hotéis, aeroportos, aviões, táxis e afins.
- Quando transportar o equipamento em automóvel utilize sempre o porta malas ou lugar não visível.
- Atenção ao transportar o equipamento na rua.

Em caso de furto:

- Registre a ocorrência na delegacia mais próxima.
- Comunique imediatamente seu superior imediato e o departamento de TI.
- Envie uma cópia da ocorrência para o departamento de TI.

5.3.8 – Política para Elaboração de Backup

Todos os dados da empresa deverão ser protegidos através de rotinas sistemáticas de backup. Cópias de segurança dos sistemas integrados e servidores de rede e arquivos são de responsabilidade do departamento de TI e deverão ser feitas diariamente.

Ao final de cada mês também deverá ser feita uma cópia de segurança com o fechamento mensal e arquivos do servidor, os quais deverão ser salvos no STORAGE, localizado fora empresa.

O conjunto de backup armazenado externamente deverá sofrer rodízio semanal com um dos conjuntos de backup ativo. A validação de backup mensal deverá ser feita pela equipe de informática, devendo ser acompanhado pelo responsável da área de TI.

5.3.9 – Política para Utilização de Impressoras

A empresa contará com um servidor de impressão, o qual escalona por ordem de chegada toda impressão enviada, com isso é possível monitorar e cancelar possíveis impressões indesejadas.

Antes de imprimir, verifique na impressora se o que foi solicitado já está impresso ou se realmente é necessária impressão.

Se a impressão deu errada e o papel pode ser reaproveitado, utilize-o na sua próxima impressão, senão, utilize como rascunho ou em último caso descarte-o.

É proibido o acúmulo de folhas com impressões erradas na mesa das impressoras.

Ao enviar a impressão é possível ver o status dos suprimentos de tonner e papel, ao perceber o fim avise a equipe de suporte.

Problemas técnicos devem ser relatados imediatamente a equipe de suporte.

Por ser mais onerosa a impressão colorida deve ser evitada, devendo ser utilizada apenas quando o documento estiver revisado e for a versão final do trabalho.

5.4 – Política de Segurança para Acesso Física a Empresa

Nesta seção trataremos do acesso não autorizado, com intuito de evitar perdas, danos, interferências aos negócios da organização. Pensando em como resguardar os ativos, incluindo regras, procedimentos de segurança física, mantendo assim o perímetro seguro de pessoas não autorizadas.

No que tange o acesso físico da empresa, atualmente é feito uma simples identificação para os visitantes e um cartão magnético para os funcionários do prédio, o que seria facilmente burlado com um pouco de engenharia social. Pensando nisso e para resguardar a organização de possíveis sabotagens, acessos indevidos e até mesmo contra desastres naturais foi pensado em alguns controles visando à proteção a pontos críticos da empresa.

5.4.1 – Controlando o acesso

Toda empresa tem um departamento ou setor que merecem uma maior atenção, são áreas que acumulam documentos ou equipamentos de grande valia para organização e que se algo acontecesse traria grande prejuízo. Esses locais precisam de um maior controle e que só pessoais autorizadas e de relevância para o departamento tenho acesso a ele. Como é o caso do Centro de Processamento de Dados – CPD, onde ficam os servidores responsáveis pelos serviços essenciais da empresa.

Convém que estas áreas sejam protegidas por controles de entrada apropriados para assegurar que apenas pessoas autorizadas tenham acesso liberado. Instalações desenvolvidas para fins especiais que abrigam equipamentos importantes exige maior proteção que o nível normalmente oferecido nas outras áreas.

O acesso ao (CPD) contara com identificador biométrico e somente os funcionário do setor poderão ter acesso, ao transitar ali, os funcionário deverão estar identificados com chacha, garantindo assim um maior controle e segurança no ambiente.

A sala do (CPD), por abrigar equipamentos vitais da empresa, devem ser monitoradas diariamente verificando questões relacionadas a temperatura, humidade e ventilação das instalações, pois devem estar de acordo com especificações técnicos dos seus fabricantes.

Outros departamentos da empresa também merecem um maior cuidado por tratar com informações confidenciais como é o caso do departamento financeiro, RH, Criação, Atendimento.

A perda ou extravio de crachás com respectivo cartão de acesso deve ser comunicado imediatamente para devido bloqueio e providências.

5.4.2 – Política de Mesa e Tela Limpa

A política de mesa limpa consiste no uso racional de material de trabalho e o não acúmulo de objetos sobre a mesa, evitando assim, a exposição de documentos confidenciais a pessoas que transitem no setor.

Os departamentos devem ser mantidos limpos, sem o acúmulo de papéis, caixas ou qualquer tipo de material que dificulte a passagem no setor.

A tela limpa trata das informações que o usuário esta utilizando na sua área de trabalho de forma que não exponha e feche sempre ao terminar o trabalho, evitando assim a disseminação das informações por pessoa que não estejam autorizadas.

Sempre que o computador não estiver sendo usado mantenha-o bloqueado, nunca com documentos abertos.

Agendas, livros manuais ou qualquer material que contenha informações confidenciais sobre a empresa ou informações particulares devem sempre ser guardados em local fechado, com acesso restrito.

Chaves de gavetas, armários, de portas dos departamentos devem ser guardadas em lugar adequado, com acesso restrito aos responsáveis.

5.4.3 – Plano de Contingência e Continuidade do Negócio

Segundo o manual de boas práticas de SI (TCU, 2012), plano de continuidade do negócio;

> *"Consiste num conjunto de estratégias e procedimentos que devem ser adotados quando a instituição ou uma área depara-se com problemas que comprometem o andamento normal dos processos e a consequente prestação dos serviços. Essas estratégias e procedimentos deverão minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade. O PCN é um conjunto de medidas que combinam ações preventivas e de recuperação".*

A existência de um plano de contingência visa facilitar a continuidade das operações da empresa em caso de problemas. O plano de contingência é um documento onde estão definidas as responsabilidades e a organização para atender a uma emergência, contendo informações detalhadas sobre procedimentos a serem adotados.

Para Dantas (2011), *"as medidas de continuidade devem incluir as ações de respostas imediatas ao evento, as ações para garantir a performance mínima para a continuidade das atividades, assim como as ações de recuperação e restauração do status quo anterior à materialização do evento, devendo constar do documento denominado"*: **Plano de Continuidade de Negócios (PCN).**

Deverá ser adotado na elaboração do PCN:

- Os procedimentos de emergência devem ser feitos de modo a recuperar as condições de Trabalho dentro de prazos que garantem o menor impacto ao negócio;
- Todos os procedimentos deverão ser documentados;
- Deverá ter treinamento constante para os responsáveis (operadores / executores) dos procedimentos, afim de atualização dos mesmos;
- Os procedimentos deverão ser testados e melhorados.

A Diretoria Executiva, Financeira e de TI, deverão se comprometem a reservar um fundo de emergência para elaboração de um Plano de Contingência e Continuidade do Negócio em 6 (seis) meses. O documento cobrirá obrigatoriamente os ativos descritos no capítulo anterior, os quais estão responsáveis pelos serviços e processos essenciais da organização; cobrirá também as melhorias no acesso físico, cobrindo os fatos descritos e a previsão de catástrofes naturais.

5.5 – Termo de Compromisso

Todos os funcionários, estagiário e colaboradores deverão assinar o termo de compromisso da empresa, como forma de ciência dos seus direitos, deveres e obrigações, assim como o conhecimento de atos que implicam em possíveis sanções disciplinares.

5.6 – Da Violação a PSI

Todo ato de possível descumprimento ou violação deve ser reportado para o departamento de TI, que analisará e fará um relatório mensal demostrando as causas, se geraram danos e proposta de melhorias para conter futuras falhas. Ao demostrar a lesividade do ato também informará se é fruto de negligência, imprudência ou imperícia do usuário.

Segundo o manual de boas práticas em Segurança da Informação (TCU, 2012);

"A própria Política de Segurança de Informações deve prever os procedimentos a serem adotados para cada caso de violação, de acordo com a severidade, a amplitude e o tipo de infrator que a perpetra. A punição pode ser desde uma simples advertência verbal ou escrita até uma ação judicial".

Fica estabelecido que todo colaborador passará por um treinamento para conhecimento e conscientização da política de segurança. O programa de treinamento deve fazer parte da rotina de inicialização de novos funcionários e um ciclo de reciclagem periódica deve ser criado para que ninguém possa alegar o desconhecimento.

5.6.1 – Das Penalidades

O descumprimento a Política de Segurança implicará em falta e estará passível das seguintes sanções:

- Advertência escrita;
- Suspensão;

- Rescisão dos vínculos trabalhistas e outras sanções disciplinares, assim como a responsabilização civil e criminal pelo dano causado quando for o caso.

Fica estabelecido que não há uma progressividade como requisito para configurar a rescisão do contrato de trabalho, podendo a Diretoria de forma discricionária aplicar a pena que entender cabível diante da gravidade da falta.

5.7 – Proposta para Atualizações da PSI

Conforme prescrito na ISO 27001; *"fica estabelecido que a Política de Segurança da Informação não é estática devendo passar por constantes estudos, avaliações e melhorias, para mantê-la atualizada com as novas tendências e acontecimentos em segurança da informação"*.

O intervalo para atualização será definido pelo departamento de TI, quando acharem convenientes ou surgirem fatos relevantes, mas convém que não exceda o período de 1 (um) ano.

O departamento de TI contará com auditoria externa com a finalidade de fazer uma revisão nos processos da política levando em conta as atividades da organização que será abrangida pela política. O objetivo da auditoria é avaliar se a organização está operando dentro dos padrões estabelecidos pela PSI.

O departamento de TI elaborará um relatório mensal detalhando os incidentes e violações a PSI, de forma que sirva como base para elaboração da proposta de melhorias e propositura do ciclo de treinamento de colaboradores o qual não ultrapassará 6 (seis) meses.

5.8 – Aprovação da PSI

É necessária que a PSI seja aprovada e assinada pelos Dirigentes da organização, de forma que os colaboradores percebem a importante de inseri-la no seu dia a dia. A assinatura demostrará o total engajamento da equipe na intenção de coloca-la na cultura corporativa da empresa, junta aos valores de visão e missão do negócio. Com a proposta de um serviço equânime e uma cultura de segurança em todos os processos da empresa.

5.9 – Procedimentos para Divulgação da PSI

Convém que a Política de Segurança da Informação seja inserida no cotidiano da organização de forma que seja amplamente divulgada e conhecida por todos os colaboradores.

Para isso contará com:

- Campanhas internas de conscientização;
- Palestras periódicas;
- Treinamento na implantação e atualizações a cada 6 meses.
- Criação de uma cartilha informativa;
- Divulgação na intranet;

Após ampla divulgação da PSI entre os colaboradores ninguém poderá mais alegar o desconhecimento.

A PSI entra em vigor a partir da assinatura dos Dirigentes da organização.

6 – CONCLUSÃO

O trabalho proposto foi elaborado baseando-se em Políticas de Segurança relacionadas ao ramo de atividade da empresa, objeto de estudo. Buscou conhecimento no estudo das normas da família ISO 27000, que são referências para esse tipo de projeto e ainda fez uma análise no cenário mundial em busca de novas tecnologias e ameaças às organizações. Com isso, foi possível perceber que a informação é o bem mais precioso das organizações, e por isso está sobre risco constante devendo ser protegida em todas as suas formas.

O objetivo será alcançado à medida que o conhecimento da norma for disseminado na organização, o conceito de segurança for incorporado no dia a dia da empresa e todos comunguem desses princípios. O usuário precisa saber que faz parte do processo como um todo e suas condutas influenciam diretamente no sucesso da organização por isso os princípios precisam ser revistos e a cultura aos poucos modificada.

Durante o estudo foi possível perceber que as organizações que possuem uma PSI alinhada ao seu ramo de negócio, com posições bem definidas, políticas claras e com engajamento de todos os colaboradores conseguem sobressair melhor às ameaças.

É importante ressaltar que o trabalho não acaba com a implantação, é necessário o treinamento, conscientização, dos funcionários, estagiários e colaboradores de forma geral. A ideia do guia é que seja implantado de modo a colaborar com a segurança e melhorias no ambiente de trabalho, mas sempre aberto a possíveis mudanças.

Por fim, a Política de Segurança da Informação não é estática, devendo ser revista e melhorada constantemente, pois a cada dia surgem novas ameaças e novas tecnologias e as empresas precisam estar atentas a essas mudanças.

REFERÊNCIAS BIBLIOGRÁFICAS

Associação Brasileira de Normas Técnicas - **ABNT NBR ISO/IEC 27002:2013. (2013)**. - Código de Prática para Controles de Segurança da Informação.

Associação Brasileira de Normas Técnicas - **ABNT NBR ISO/IEC 27001:2006. (2006).** - Sistema de Gestão de Segurança da Informação.

Associação Brasileira de Normas Técnicas - **ABNT NBR ISO/IEC 27005:2008. (2008).** – Gestão de riscos de Segurança da Informação.

Associação Brasileira de Normas Técnicas - **ABNT NBR 17799:2005** - Tecnologia da Informação: Código de práticas para a gestão da Segurança da Informação.

ANALISTA TI *Politica de Segurança da Informação;* [on line]. Disponível em: <https://analistati.com/politica-de-seguranca-da-informacao-como-fazer/>
Acessado em 11 abr. 2017.

CERT, *Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil,* [on line]. Disponível em:< https://www.cert.br/stats/incidentes/>. Acessado em 11 abr. 2017.

CERT, *Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil,* [on line] **Cartilha de Segurança para Internet 2017.** Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acessado em 12 mai. 2017.

Dantas, Marcus Leal – **Segurança da Informação**: Uma abordagem focada em gestão de riscos. / Marcus Leal Dantas. - Olinda: Livro Rápido, 2011.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Axcel Books. Rio de Janeiro, 2000.

FERREIRA, Fernando Nicolau Freitas – **Segurança da Informação** – Rio de Janeiro:

Editora Ciência Moderna LTDA., 2003

FONTES, Edison Luiz. **Segurança da Informação**: O usuário faz a diferença. 1ª edição. São Paulo: Saraiva, 2006.

HENRIQUE, Carlos – **Política de Segurança da Informação.** Disponível em: <https://pt.slideshare.net/CarlosHenrique372/aula-3-poltica-de-segurana-da-informao-psi> Acessado em 15 mai. 2017.

Livro Verde – **Segurança Cibernética no Brasil.** / Raphael Mandarino Junior e Claudia Canongia (Organizadores) – Brasília – DF, 2010.

Lei Nº 12.527, de 18 de novembro de 2011, Regula o Acesso a Informação.

NAKAMURA, Emilio Tissato, GEUS, Paulo Lício. **Segurança de redes:** em ambientes cooperativos. 2. ed. São Paulo: Futura, 2003.

Manual de boas práticas TCU. **Boas Práticas em Segurança da Informação TCU**. 4ª edição. Brasília, 2012.

Política de Segurança. Disponível em: < https://supportnetworkerik.wordpress.com/page/6/ > Acessado em 28 ago. 2017.

RFC 2828 Internet Security Glossary – IETF [on line] Disponível em: <https://www.ietf.org/rfc/rfc2828.txt>
Acessado em 18 abr. 2017.

Segurança Cibernética. Disponível em: < https://go.oracle.com/> acessado em 27 ago. 2017.

Sobre a Artplan. Disponível em: <http://www.artplan.com.br> acessado em 12 jul. 2017.

WADLOW, Tomas A. **Segurança de Redes:** Projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus, 2000. Tradução: Fabio Freitas da Silva