PROPOSTA DE UMA POLITICA DE SEGURANÇA DA INFORMAÇÃO UM ESTUDO DE CASO APLICADO EM UMA ESCOLA DE IDIOMAS

Kamilla Preissler[1]
Marilei de Fátima Kovatli[2]

RESUMO

Ao longo do tempo a segurança da informação veio se tornando uma ferramenta necessária para as empresas, visto que a informação passou a se tornar um ativo de grande valor nas organizações. Percebendo essa importância, o tema deste artigo é abordar a aplicação de uma política de segurança da informação em uma escola de idiomas. Neste estudo de caso, escolheu-se como problema verificar qual é o impacto de um incidente na segurança das informações para a empresa. O objetivo geral deste estudo é elaborar uma política de segurança da informação baseada em boas práticas de TI. Este trabalho se justifica pelo fator da segurança da informação se tornar uma grande aliada das empresas, e para a escola de idiomas o estudo sobre o impacto de um incidente na área de segurança da informação possibilita elaborar um plano de ações corretivas e preventivas devido o reconhecimento da importância que a segurança da informação traz para ela. A metodologia para o estudo possui pesquisa teórica e teórica- empírica, com análise de dados qualitativos e quantitativos. Com este estudo foi possível identificar falhas de segurança da informação e propor possíveis soluções para as falhas identificadas.

Palavras-chave: Segurança da Informação – Política de Segurança da Informação – Impactos da falta de segurança

ABSTRACT

Over time, information security has become a necessary tool for companies, since information has become a valuable asset in organizations. Realizing this importance, the theme of this article is to address the application of an information security policy in a language school. In this case study, it was chosen as a problem to verify what is the impact of an incident on the security of the information for the company. The overall objective of this study is to develop an information security policy based on good IT practices. This work is justified by the fact that the information security becomes a great ally of the companies, and for the language school the study on the impact of an incident in the area of information security makes it possible to elaborate a plan of corrective and preventive actions due to the recognition of the importance that information security brings to it. The methodology for the study has theoretical and theoretical-empirical research, with qualitative and quantitative data analysis. With this study it was possible to identify information security flaws and propose possible solutions to the identified flaws.

[1] Acadêmica do Curso de Gestão em Tecnologia da Informação – 6º Semestre. Faculdades Integradas Machado de Assis. kamillapreissler@gmail.com
[2] Mestre em Ciência da Computação. Orientadora. Professora do Curso de Gestão da Tecnologia da Informação. Faculdades Integradas Machado de Assis. marilei_gti@fema.com.br

Keywords: Information Security - Information Security Policy - Impacts of lack of security

INTRODUÇÃO

A cada dia mais a segurança da informação vem se tornando uma ferramenta necessária para as empresas, visto que a informação passou a se tornar um ativo de grande valor nas organizações. Podemos entender como política de segurança da informação um método para ajudar a organização a alcançar a segurança da informação. Este trabalho apresenta uma proposta de política de segurança da informação um estudo de caso aplicado em uma escola de idiomas, que será aplicada no Instituto De Linguas Dewes E Diesel que atende como nome fantasia de HEY PEPPERS, localizada em Santa Rosa região Noroeste do Rio Grande do Sul, Brasil.

A organização apresenta uma forte cultura interna de compartilhamento de informações, que se não for feito com cuidado e segurança pode trazer problemas. Analisando a cultura da empresa, decidiu-se por criar uma política de segurança da informação baseada em boas práticas em TI.

O presente trabalho possui como objetivos específicos: Identificar quais políticas internas são adotadas pela empresa para entender o seu funcionamento; Verificar as falhas em relação a segurança para analisar os riscos desses incidentes sobre as operações da empresa; Definir critérios baseados nas boas práticas em TI, para elaboração da política de segurança da informação;

A segurança da informação vem se tornando cada vez mais relevante para empresas e usuários e como foi identificada uma carência na segurança da informação na empresa escolhida decidiu-se fazer sobre proposta de política de segurança da informação, pois muitos são os problemas que a falta da segurança pode trazer.

O estudo possui uma pesquisa teórica, utiliza livros e artigos, como teórica-empírica já que buscará dados dentro da empresa. Sobre os dados eles terão análise qualitativa de acordo com o que foi percebido na empresa e análise quantitativa já que será gerado gráficos sobre as pesquisas geradas.

Quanto aos fins da pesquisa eles serão exploratórios e descritivos pois irá explorar os dados dentro da empresa e sugerir melhorias para aumentar o grau de segurança da informação dentro da empresa. As interpretações de dados se darão

através de apoio bibliográfico, gráficos de interpretação, e métodos que sirvam de base comparativa.

No primeiro tópico é abordado o referencial teórico que inicia com a segurança da informação, seguindo com a governança em TI que se torna grande aliada com as boas práticas, a engenharia social e como funciona essa técnica que tira informações das pessoas e por último apresenta a política de segurança da informação juntamente com a ISO 27002 que trata sobre a gestão de segurança da informação.

No segundo tópico é apresentado a metodologia utilizada para o desenvolvimento da pesquisa, possui pesquisa tanto teórica quanto teórica empírica, com geração de dados de maneira direta e indireta, por meio de questionários e observação e a análise se deu pelo método hipotético dedutivo.

No terceiro tópico foi abordado o diagnóstico e análise dos dados, contando com o a análise do questionário com o gestor e os colaboradores assim como as falhas observadas e a proposta de melhorias.

1 REFERENCIAL TEÓRICO

O referencial teórico é um resumo sobre o que os autores dizem sobre o tema que será abordado no estudo. Para Furasté “trata-se da apresentação do embasamento teórico sobre o qual se fundamentará o Trabalho. São os pressupostos que darão suporte à abordagem do Trabalho” (FURASTÉ, 2010, p.154).

Este referencial teórico se divide em cinco partes que são: Segurança da Informação, Governança em TI e boas práticas em TI, Engenharia Social, Política de Segurança da Informação e ISSO 27002.

1.1 SEGURANÇA DA INFORMAÇÃO

A segurança da informação está ligada à proteção das informações na empresa, para proteger e assegurar que elas se mantenham disponíveis, integras e confiáveis. Para Fontes a segurança da informação existe para:

> “minimizar os riscos do negócio em relação a dependência do uso dos recursos de informação para funcionamento da organização. Sem a informação ou com a incorreta, o negócio pode ter perdas que comprometam o seu funcionamento e o retorno de investimento dos acionistas.” (FONTES, 2006, p.11).

A informação se tornou um ativo valioso para as organizações, pesquisas de mercado, desenvolvimento de novos produtos, informações de lucratividade, balancetes, informações de clientes e entre vários outros tipos de informação que podem ser classificados de acordo com a sua relevância e seu valor para a empresa precisam estar devidamente resguardados de pessoas que não devem possuir esta informação. Segundo LYRA, quando falamos em segurança da informação “estamos nos referindo a tomar ações para garantir a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações dentro das necessidades do cliente.” (LYRA, 2008, p.04).

São considerados os três pilares da informação (CID) a Confidencialidade, Integridade e a Disponibilidade da informação, juntos formam a base para que a segurança da informação tenha êxito. Para Fernando e Arujo (2008) os pontos críticos do êxito para a segurança da informação ultrapassam o CID e criam seis pilares:

- **Confidencialidade:** que somente pessoas autorizadas a determinada informação terão acesso à ela;
- **Integridade:** que os dados não sofrerão modificações não autorizadas, mantendo-se íntegros;
- **Disponibilidade:** que os usuários autorizados tenham sempre que necessitem a informação disponível;
- **Legalidade:** as informações precisam estar de acordo com as leis, regulamentos e contratos;
- **Auditabilidade:** registrar os usuários que fizeram acesso e uso da informação, para assim identificar quem realizou os acessos e o que fez com a informação.
- **Não Repúdio:** o usuário que alterou e acessou a informação não pode negar que o fez, pois existem mecanismos para comprovar isso.

Os três pilares adicionados ajudam a garantir que haverá meios de comprovar o usuário que fez a alteração e se esta não era devida lidar com o incidente e encontrar o verdadeiro agente causador da divergência.

Segundo Fontes (2006), toda a organização deseja continuar atuando, desenvolvendo as atividades durante um longo tempo, e isso só será possível com recursos de tecnologia, humanos, de conhecimento dos processos, do ambiente físico e da infraestrutura da organização.

Em se falando sobre segurança existem alguns conceitos que podem ser considerados básicos e essenciais dentre eles (SEMOLA, 2003):

- **Ameaças:** se aproveitam de vulnerabilidades e provocam perda dos três pilares da informação (CID), podem ser agentes ou condições e podem ser classificadas como: ameaças naturais (fenômenos da natureza), ameaças involuntárias (desconhecimento e falha) e ameaças voluntárias (propositais).
- **Vulnerabilidades:** são fragilidades presentes ou associadas a ativos (físicos ou lógicos) que se forem sondadas podem ser aproveitadas por ameaças e causarem dano a algum dos pilares da segurança da informação. As vulnerabilidades podem ser físicas, lógicas, naturais ou humanas.
- **Riscos:** são probabilidades de ameaças aproveitarem as ameaças e provocarem dano aos pilares de segurança da informação gerando impactos para a organização.
- **Incidente:** é um evento consequente a ação de uma ameaça que explorou uma vulnerabilidade, ocasionando impactos negativos na organização.

Estes conceitos podem causar alto impacto na empresa, este impacto pode possuir deferentes alcances dependendo do incidente gerado e deve ser analisado individualmente. Os impactos podem ir desde lentidão nos processos e rede a empresa à parada total das atividades e perda de informações importantes para o seu funcionamento.

1.2 GOVERNANÇA EM TI E BOAS PRÁTICAS EM TI

A governança de TI é um conjunto de processos, que visa alinhar a TI com o objetivo da organização, dando suporte e alinhando suas estratégias. De acordo Fernandes e Abreu:

> [...] a governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização. (FERNANDES; ABREU, 2012 p.12)

A Governança em TI de responsabilidade dos diretores e da alta direção da empresa, ela da suporte pra organização. De acordo com o site da ISACA:

> Governança de TI integra e institucionaliza boas práticas para garantir que a TI da empresa suporta os objetivos de negócio. A governança de TI possibilita

> que a empresa tenha toda a vantagem de suas informações, maximizando os benefícios, capitalizando em oportunidades e ganhando vantagens competitivas.

Algo que vem muito ligado com a Governança em TI são as boas práticas em TI. Podemos definir as boas práticas como um conjunto de instruções que o usuário pode utilizar para aproveitar o máximo dos recursos em TI.

Um exemplo de framework que aplica boas práticas é o CobiT (Control Objectives for Relsted Tecnhology), um modelo de estrutura de controle voltado para a governança e gestão em tecnologia da informação. Segundo Ferreira “sua estrutura de controles possui padrões aceitos mundialmente como os melhores praticados para o estabelecimento de controles e padrões de segurança da área de Tecnologia da Informação das empresas dos mais variados segmentos do negócio. ”(FERREIRA, 2008, p.57).

Para Fernandes e Abreu:

> [...] a estrutura do CobiT integra e institucionaliza boas práticas de planejamento e organização, aquisição e implementação, entrega e suporte, e monitoramento e avaliação de desempenho de TI. A Governança de TI, quando implantada de forma integrada, permite que a empresa gerencie de forma eficiente seus investimentos em recursos tecnológicos e suas informações, transformando-as em maximização de benefícios, oportunidades de negócio e vantagem competitiva no mercado. (FERNANDES; ABREU; 2012 p. 213).

O Framework Val IT assim como o Cobit, é um modelo de Governança de TI. O Val IT tem foco na demonstração do retorno que a TI oferece para a empresa. Os objetivos do Val IT são:

> - Auxiliar a gerência para assegurar que as organizações obtenham o máximo de retorno dos investimentos em TI para suporte ao negócio, a um custo razoável e com um nível de risco conhecido e aceitável de TI.
> - Prover diretrizes, processos e práticas de apoio para subsidiar a Diretoria e a gestão executiva no entendimento e no desempenho dos seus respectivos papéis, em relação aos investimentos de TI. (FERNANDES; ABREU; 2012, p.228)

O Framework Val IT ajuda a identificar o retorno do investimento que a empresa tem com a tecnologia da informação, quem teve está a frente da iniciativa é o IT Governence Institute (ITGL) que desenvolve novas metodologias e utiliza algumas já existentes para construir o framework.

De acordo com o ITGL o framework Val IT é

> “uma estrutura de organização abrangente e pragmática que permite a criação de valor comercial a partir de investimentos habilitados para TI. Projetado para alinhar e complementar a COBIT, a Val IT integra um conjunto de princípios, processos, práticas e diretrizes de apoio práticos e comprovados que ajudam os conselhos, equipes de gerenciamento executivo e outros líderes empresariais a otimizar a realização do valor dos investimentos em TI.” (ITGL, 2008, p.13)

De acordo com o site da ISACA:

> “Especificamente, a Val IT centra-se nos processos de decisão de investimento relacionados à TI (estamos fazendo as coisas certas?) E a realização de benefícios com eles (estamos recebendo os benefícios?). COBIT concentra-se mais nos processos de execução de TI (estamos fazendo-os de maneira correta? E estamos fazendo isso bem?).”.

O Val IT e o Cobit se completam e juntos conseguem trazer uma visão mais ampla e completa de o que está sendo feito e como estão sendo feitos os processos dentro da organização de maneira que dão um bom suporte para os gestores.

1.3 ENGENHARIA SOCIAL

A engenharia social consiste na arte de influenciar pessoas e tirar informações sigilosas e valiosas de empresas a partir delas. Para Junior ela consiste em “técnicas utilizadas por pessoas com o objetivo de obter acesso e informações importantes e/ou sigilosas em organizações ou sistemas por meio da ilusão ou exploração da confiança das pessoas. ” (JUNIOR, 2006, p.01).

Já para a CertBr o termo engenharia social é utilizado para “os métodos de obtenção de informações importantes do usuário, através de sua ingenuidade ou da confiança. Quem está mal-intencionado geralmente utiliza telefone, e-mails ou salas de bate-papo para obter as informações que necessita. ” (CertBr, 2000, p.05).

A pessoa que realiza a engenharia social é conhecida como engenheiro social, este por sua vez pode realizar a engenharia sem nem ao menos ter visto pessoalmente a pessoa que sofrerá a engenharia, como por exemplo em uma ligação telefônica.

Para Souza o engenheiro social “não é um profissional da engenharia social, mas sim uma pessoa que possui conhecimento em diversas áreas, visto que não é uma faculdade, e sim um agrupamento de técnicas. ” (SOUZA, 2016, p.04).

Várias são as técnicas que podem ser utilizadas pelo engenheiro social para retirar as informações, ele sempre busca conseguir a confiança das pessoas seja por meio de assuntos em comum ou comentários sobre sua aparência.

1.4 POLITICA DE SEGURANÇA DA INFORMAÇÃO

A política de segurança da informação é um documento que abrange vários métodos, normas e procedimentos para gerar e melhorar a gestão da segurança da informação que se aplica para todos os usuários que utilizam as informações da organização. Para Netto e Silveira ela possui o objetivo de “promover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. ” (NETTO, SILVEIRA, 2007, p.25).

Uma política de segurança é dever da organização de informar os colaboradores de sua existência e obrigação de cara usuário cumprir com as diretrizes que nela estão estabelecidos. Para Fontes

> “a segurança e proteção da informação é uma responsabilidade continua de cada usuário da organização em relação às informações que acessa e gerencia. Todos os usuários devem utilizar a informação da organização, de acordo com as determinações da Política de Segurança e Proteção da Informação.” (FONTES, 2008, p.252).

Normas como a ISSO/IEC 27002 e 27001, assim como as boas práticas em ti, CobiT, ITIL, Governança de Segurança e Gestão de riscos ajudam na criação de uma boa política de segurança da Informação.

Na política leva-se em consideração não somente a parte lógica da segurança, mas também a parte física da organização e as pessoas. Para Lyra as “pessoas são os elementos centrais de um sistema de segurança da informação. Os incidentes de segurança sempre envolvem pessoas [...].” (LYRA, 2008, p.19), os usuários são elos fracos em se tratando de segurança da informação pois ao contrário das maquinas eles possuem o lado humano e frequentemente a vontade de ajudar ao próximo.

De acordo com Ferreira e Araújo para a política de segurança:

> “deve-se utilizar uma visão metódica, criteriosa e técnica em seu desenvolvimento e elaboração, de forma que possam ser sugeridas alterações na configuração de equipamentos, na escolha de tecnologia, na definição de responsabilidades e, por fim, na elaboração das politicas com o perfil da empresa e dos negócios que ela pratica.” (FERREIRA, ARAUJO, 2008, p.36).

As empresas possuem diferenças umas das outras, seja por cultura organizacional, ramo, equipamentos utilizados, tipo de informações que usam que acabam por causar diferenças na política de informação, por isso elas devem ser feitas com foco especifico em cada empresa.

Semola (2003) fala sobre a gestão da segurança da informação e aborda sobre os desafios encontrados sobre como realizar essa gestão, no planejamento da segurança diz:

> "Elaborar uma Política de Segurança da Informação sólida, considerando com extrema particularização e detalhamento as características de cada processo do negócio, perímetro e infraestrutura, materializando-a através de Diretrizes, Normas, Procedimentos e Instruções que irão oficializar o posicionamento da empresa ao redor do tema e, ainda, apontar as melhores práticas para o manuseio, armazenamento, transporte e descarte de informações na faixa de risco apontada como ideal." (SEMOLA, 2003, p. 34).

A política de segurança deve ser feita rigorosamente e de maneira que entenda os processos e a maneira como a empresa funciona para assim evitar gaps onde a segurança deixe de estar presente. É importante ressaltar que essa política de segurança da informação deve ser de conhecimento de todos os colaboradores da empresa, além de ser redigida de maneira clara para que todos a entendam.

1.4.1 ISO/IEC 27002

A ISO/IEC 27002 é sobre o Código de prática para a gestão da segurança da informação. O objetivo da norma é estabelecer diretrizes e princípios gerais para iniciar, manter e melhorar a gestão de segurança da informação de uma empresa, a norma provê diretrizes e metas para serem implementados nas empresas. (ABNT IS/IEC 27002, 2005).

Para Fontes a norma NBR ISO/IEC

> "tem como objetivo fornecer recomendações básicas e mínimas para a gestão de segurança da informação nas diversas organizações. Na medida em que várias organizações seguem esta norma, tem início a criação de uma base comum para a pratica da segurança da informação." (FONTES, 2008, p.223).

A norma é um ótimo guia para as organizações que desejam implantar um processo de segurança da informação efetivo, porém somente a utilização desta norma não torna a empresa a salvo e completamente segura.

Fernandes e Abreu afirmam que:

> [...] os benefícios da segurança da informação estão na prevenção de perdas financeira que a organização pode ter, no caso de ocorrência de incidentes de segurança da informação. A organização pode abalar a sua imagem ou sofrer ações na justiça pelas perdas que seus sistemas possam causar aos seus clientes. (FERNANDES; ABREU, 2012 p.425)

Cabe a todos os interessados na continuidade da organização não ignorar e esperar até que aconteça algum incidente na organização para perceber a importância de garantir a proteção dos ativos da informação na empresa. Entretanto isso só será possível através do uso da segurança da informação juntamente com uma política de segurança alinhada com o negócio e com o treinamento dos funcionários.

A Norma possui onze sessões que vão da letra A à K (ABNT NBR ISO 2702, 2005), sendo elas:

A- Política de segurança da informação: deve haver o documento que regulamente a política, sendo ele objetivo, explicativo sobre as políticas, princípios e normas que estão inclusas, que deixe claro as definições de responsabilidade e referencias que apoiem a política de segurança além de fazer um controle sobre a política e as diretrizes para implementação.

B- Organizando a segurança da informação: conta com foco na organização interna para gerenciar a segurança da informação dentro da organização, estabelecer uma estrutura de gerenciamento para iniciar e controlar a implantação da segurança da informação e também conta com foco nas partes externas, possui o objetivo de manter o processamento da informação e a informação da organização que são gerenciados, comunicados, processados ou acessados por partes externas em segurança.

C- Gestão de ativos: possui com foco nos ativos onde deve haver um inventário com todos os ativos e que eles sejam atribuídos para responsáveis, que sejam identificados e controlados e possui também foco na classificação da informação e visa assegurar que ela recebe um nível adequado de proteção. A informação deve ser classificada para indicar o nível de segurança que será adequado em cada informação.

D- Segurança em Recursos Humanos: conta com o antes da contratação, que é para garantir que os colaboradores, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis afim de reduzir o mau uso

de recurso, risco de roubo, furto e fraude. Sobre durante a contratação, onde os funcionários, fornecedores e terceiros devem ser conhecedores das ameaças e preocupações relativas à segurança da informação e estarem preparados para apoiar a política de segurança da informação. A parte dos recursos humanos trata sobre o encerramento ou mudança da contratação, onde deve assegurar que as pessoas envolvidas deixem a organização ou mudem de trabalho de maneira ordenada.

E- Segurança Física e do Ambiente: conta com áreas seguras, que é direcionada ao espaço físico e instalações onde deseja prevenir o acesso não autorizado as instalações e informações da organização, criação de perímetros protegidos criando áreas seguras e com a segurança de equipamentos, onde deve-se proteger os equipamentos contra as ameaças físicas e do ambiente, danos, perdas, furtos.

F- Gestão das Operações e Comunicações: tem foco no processamento da informação de maneira correta e segura, gerenciar os serviços terceirizados, o planejamento e aceitação dos sistemas, com foco em minimizar os riscos e falhas nos sistemas, proteção contra códigos maliciosos e códigos móveis, cópias de segurança, o gerenciamento da segurança de redes, o manuseio de mídias, a manter a troca de informações seguras assim como os softwares internos, garantir a segurança de serviços de comercio eletrônico e manter sua utilização segura e também possui foco no monitoramento, afim de detectar atividades que não são autorizadas no processamento da informação.

G- Controle de Acesso: se preocupa com os requisitos de negócio para o controle de acesso, gerenciamento de acesso do usuário, as responsabilidades dos usuários, o controle de acesso à rede prevenindo o acesso não autorizado a rede, o controle de acesso ao sistema operacional, controle de acesso à aplicação e à informação, a computação móvel e trabalho.

H- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação: conta com os requisitos de segurança de sistemas de informação, processamento correto das aplicações, controles por meios criptográficos, a segurança dos arquivos do sistema, a segurança em processos de desenvolvimento e de suporte, gestão de vulnerabilidades técnicas conhecidas.

I- Gestão de Incidentes de Segurança da Informação: conta com notificação de fragilidades e eventos de segurança da informação relacionados com

sistemas de informação, gestão de incidentes de segurança da informação e melhorias tornando- o mais plausível.

J- Gestão de Continuidade do Negócio: conta com os aspectos da gestão da continuidade do negócio relativo à segurança da informação, para proteger de falhas ou desastres significativos em processos chaves a fim de evitar a paralização do negócio.

K- Conformidade: conta com a conformidade com os requisitos legais, a conformidade com as normas e políticas de segurança da informação, conformidade técnica, maximização da eficiência de auditorias de sistemas de informação.

As onze sessões não estão organizadas por ordem de importância, dependendo da organização é que ocorrerá a ordem de importância por isso há a necessidade de fazer uma análise interna dos processos e de como a empresa se estrutura para assim se definir a partir das diretrizes a melhor maneira de implantar uma política de segurança efetiva.

2 METODOLOGIA

A metodologia é a descrição de como foi realizada a pesquisa, técnicas e métodos. Através da metodologia é proposta a categorização, coleta, análise e interpretação dos dados e apresentação da empresa, onde se busca abranger os objetivos propostos no projeto em desenvolvimento.

2.1 CATEGORIZAÇÃO DA PESQUISA

O estudo possui uma pesquisa tanto teórica pois utilizou-se livros, artigos e sites que abordam o assunto, como teórica-empírica que buscou coletar dados por meio de questionários com gestores e funcionários e também realizou-se a observação dos processos e estrutura da empresa. Sobre os dados coletados foi realizado uma análise qualitativa de acordo com o que foi percebido na empresa por meio da observação e análise quantitativa já que os dados da pesquisa objetiva foram quantificados para uma análise mais clara sobre o funcionamento da segurança. A pesquisa é bibliográfica e também considerada um estudo de caso pois usa dados da empresa e busca elaborar uma proposta com melhorias.

Quanto aos fins da pesquisa eles são exploratórios e descritivos pois exploram os dados dentro da empresa e sugerem melhorias para aumentar o grau de segurança da informação dentro da empresa.

2.2 GERAÇÃO DE DADOS

Para a geração de dados foram utilizadas coleta indireta de dados com busca em pesquisas bibliográficas por meio de livros, artigos, cartilhas de segurança e conteúdo online disponibilizado por instituições com foco em tecnologia e segurança da informação.

Além da coleta indireta também se utilizou a coleta direta de dados dentro da empresa onde foram utilizados três questionários, dois aplicados ao gestor da empresa totalizando quinze (15) perguntas, e outro aplicado aos funcionários que totalizou vinte e duas (22) perguntas. Os questionários foram elaborados na ferramenta do Google Docs, e respondidos online os Formulários do Google foram disponibilizados com questões objetivas e descritivas para todos os colaboradores, ainda para o gestor houve reuniões para dúvidas sobre algum processo.

Foi também realizada uma visita a organização para ver e entender melhor sobre seus procedimentos do dia a dia, equipamentos utilizados, estrutura de rede e além disso também houve uma reunião com o colaborador responsável pela parte de TI da organização onde foram esclarecidas dúvidas a respeito dos programas e a maneira como os professores utilizam os computadores disponíveis.

2.3 ANÁLISE E INTERPRETAÇÃO DOS DADOS

Após a coleta de dados é necessário fazer o processo de análise e interpretação dos mesmos. Eles devem ser analisados para obter exatidão e integridade, pois dados incorretos podem prejudicar o estudo.

Para Gil o mais importante no processo de análise é “a sensibilidade teórica, ou seja, a habilidade para reconhecer que é importante nos dados e atribuir-lhes sentido. Essa sensibilidade deriva tanto da literatura técnica quanto da experiência profissional.” (GIL, 2010, p.145)

A análise e interpretação de dados se deu pelo método hipotético-dedutivo, assim como pelo método de abordagem utilizou-se o método estatístico, que tem

como base o questionário como principal fonte de informação para ser analisado e quantificado possibilitando gerar informações relevantes para este estudo.

3 DIAGNÓSTICO E ANÁLISE

O diagnóstico e análise da empresa apresentam a descrição e análises sobre os dados coletados na empresa, através de entrevistas e questionários

No primeiro momento houve uma entrevista com o Gestor da empresa sobre o nivelamento de informações, como são os processos que necessitam da TI. Ficou claro a maneira aberta de como ocorre a comunicação interna e de como os colaboradores são livres para se expressar e contribuir com ideias assim como para fazer pesquisas internas sem qualquer tipo de restrição, se transcorreu sobre os processos e softwares utilizados dentro da empresa e como eles se interligavam além de exaltar a necessidade focar na parte da segurança.

O primeiro questionário contou com perguntas básicas sobre nome da empresa, as diversas maneiras que utilizam para a comunicação (com uso de redes sociais, *e-mail*, conversas, reuniões, mural...), a utilização de computadores próprios dos colaboradores para realização de tarefas é algo livre e normal, que os computadores disponibilizados para sala de aula não possuem senhas, as documentações de rede estão desatualizadas e que existe um funcionário com foco pedagógico na TI que é quem auxilia a empresa quando existe algum problema relacionado na área porem o seu foco não é em serviços de TI.

O segundo questionário serviu para tirar as dúvidas restantes sobre a empresa, como quantidade de professores até o momento, sobre a inexistência de uma política de download e contou com um comentário sobre a lentidão na rede que causa atraso nos processos, o uso de um streaming para a música ambiente e a não ocorrência de danos a informação com relação a segurança.

3.1 QUESTIONÁRIO DOS COLABORADORES

O questionário aplicado aos funcionários ficou disponível por 25 dias e foi disponibilizado para eles pelo gestor da empresa e pelo responsável da TI.

A primeira parte do questionário aplicado aos funcionários tratava sobre segurança e como os funcionários sabiam ou entendiam sobre sua importância,

segurança da informação na empresa e sobre política de segurança. Todos os colaboradores que responderam afirmaram que a segurança da informação é importante e a maioria diz que há segurança na empresa e não identificaram alguma vulnerabilidade nela. Não possuem muito entendimento sobre o que é uma política de segurança da informação, as poucas respostas que traziam um entendimento mostravam que a política seria ligada somente a divulgação de informações da empresa.

A seção de senhas contou com perguntas básicas referentes as senhas que os colaboradores usam na empresa. No gráfico ao lado (Ilustração 1), fica claro que mais da metade dos colaboradores (66,7%) utilizam uma senha diferente para cada sistema e ao *e-mail* utilizado e isso é algo positivo já que o ideal é que cada *login* possua uma senha distinta das demais utilizadas pelo usuário pois em casos de tentativas de invasão e hackers de senhas bem sucedidas eles possuirão somente um acesso em comparação aos demais e as informações que alcançarão e conseguirão realizar as alterações será muito menor.

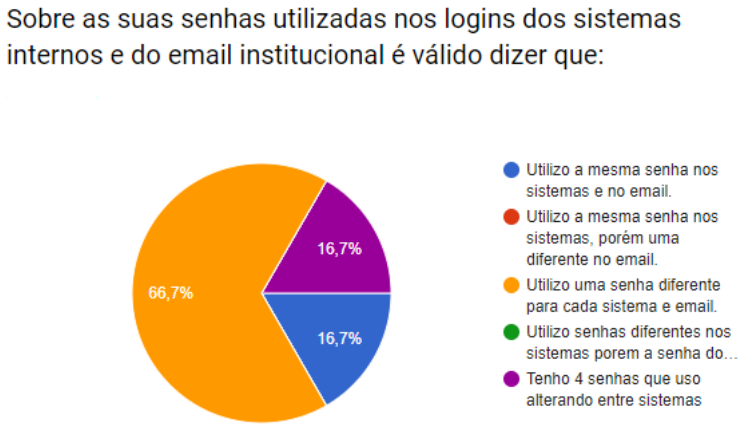

Ilustração 01: Utilização de senhas em sistemas e *e-mails*
Fonte: Gráfico gerado pelo Formulário do Google

A segunda pergunta da sessão de senhas contou com o compartilhamento, 33,3% dos colaboradores que responderam a pergunta compartilham a senha com outro colega de trabalho e somente 66,7% possuem sua senha confidencial. Um grande problema do compartilhamento das senhas é que caso ocorra qualquer alteração com determinado *login,* a pessoa responsável por ele é que será a responsável pela alteração e as modificações que podem estar causando problemas e atrasos nos processos da empresa.

A terceira pergunta possuía foco na qualidade das senhas, 50% dos colaboradores que responderam possuem somente senha com caracteres numéricos e 33,3% possuem somente caracteres alfabéticos, 16,7% possuem caracteres alfabéticos minúsculos e numéricos, 16,7% caracteres maiúsculos e minúsculos e numéricos e 16,7% possuem caracteres maiúsculos e minúsculos, numéricos e especiais. Uma senha que contenha somente caracteres numéricos ou somente alfabéticos são senhas com uma possibilidade muito maior de serem descobertas por pessoas mal intencionadas, facilita ao invasor no método de força bruta onde se testam diferentes padrões de senhas já utilizados e novas combinações para descobrir a senha do usuário e se a senha conter dados básicos como o nome, data de nascimento ou time do “coração” as possibilidades são ainda maiores. Técnicas de uso de um dicionário direcionado a determinada pessoa, alimentado com informações dela, assim como troca de vogais por números “parecidos” como o “e” pelo “3” também são levados em consideração pelos hackers.

Além disso, a quantidade de caracteres também é um fator que influencia, no caso da empresa 66,7% das pessoas que responderam a o questionário possuem de 5 à 8 caracteres e 33,3% de 9 à 12 caracteres, mais da metade possui senhas com poucos caracteres e se considerar a pergunta anterior sobre qualidade se percebe que há muito a melhorar com uma coisa tão simples como a senha.

A última sessão do questionário contou com perguntas sobre os computadores e o ambiente, ficou claro que os colaboradores ficam na maioria das vezes divididos entre as ações que realizam no ambiente de trabalho como 50% dos que responderam nunca passam informações dos funcionários por telefone ou passam qualquer informação por e-mail que não seja coorporativo, assim como esta mesma quantidade utiliza o e-mail pessoal no trabalho.

A maior parte dos colaboradores não possuem o hábito de hibernar ou suspender as maquinas que estão utilizando ao se ausentar da sala, realizam downloads de anexos dos e-mails sem verificar em qual formato se encontram, além da realização de downloads de diversos formatos.

Esta última sessão possuiu um foco voltado as ações dos colaboradores, muitas dessas ações descritas acima são vulnerabilidades que estão presentes e podem ser exploradas por pessoas mal intencionadas e assim virarem incidentes trazendo impactos negativos para a empresa. As vulnerabilidades permitem desde acesso não autorizado que pode trazer modificações indevidas gerando transtorno e

perda de informações relevantes para a empresa, assim como malwares que podem causar desde lentidão, perda da parte lógica até mesmo roubo de informações relevantes para a empresa.

3.2 PONTOS E FALHAS OBSERVADOS

As observações dos espaços da empresa assim como sobre o seu funcionamento, contaram com horários e dias distintos possibilitando a análise com diferentes volumes de pessoas circulando no local. Os funcionários foram observados sem saberem, como se fosse somente mais um dia normal de trabalho e somente no dia final da observação foram abordados sobre duvidas de processos.

Foi observado que os funcionários da secretária e do atendimento permanecem conectados, com seus logins, nas maquinas ao se ausentarem o computador permanece livre e desbloqueado para qualquer pessoa mal-intencionada. As portas e paredes da secretaria assim como a da sala de reuniões são de vidro, o que facilita enxergar se há alguma pessoa que não deveria estar ali, porém foi observado que em mais de um momento no andar de baixo da empresa, que conta com a sala da secretária e a parte do atendimento, não havia nenhum funcionário no local ou perto e que o acesso ficou livre para alunos e outras pessoas que poderiam entrar.

A sala de reuniões não conta com tomadas suficientes para comportar a quantidade de equipamentos, que gerou aglomeração de réguas e T's (adaptadores de tomada), que se encontram abaixo de uma estação de trabalho, podendo ocorrer derramamento de líquidos e gerando curtos ou até mesmo bater no local gerando mal contato.

As salas de aula permanecem abertas e vazias após as aulas, os computadores não possuem senhas ficam acessíveis a qualquer pessoa que entrar. Alguns computadores das salas de aula possuem uma *tag* com um e-mail e a senha para acessar este e-mail, assim como os *Chromebooks* usados em sala de aula por alunos. Um possível impacto que isso causaria na organização é transtorno, já que há possibilidade de alterações na maquina, instalações de programas indesejados, malwares, bloqueio de computador por senha não autorizada.

A rede de internet não conta com cabeamento estruturado, não possui otimização e planejamento de rede havendo cascateamentos, há muitos roteadores

espalhados pela empresa que possui uma área grande, porem quantidade não trouxe qualidade na rede que não possui nenhum proxy firewall ou otimização interna. A empresa possui somente um link de internet, que é instável e fica fora de funcionamento frequentemente, e como não possui nenhum servidor interno depende de desta rede para acessar os servidores e arquivos compartilhados na nuvem. A empresa é altamente dependente da rede para seu funcionamento, sem a internet ela acaba por parar seus processos.

A empresa não conta com inventários de equipamentos, documentações de software por computador, licenciamento de softwares e nem todos os computadores possuem um antivírus, na maioria dos casos possui somente o Windows defender ativo. Não existe nenhuma política interna sobre como utilizar os computadores, downloads ou uso de internet de maneira geral, tudo é baseado no prévio conhecimento do usuário. Isso faz com que a empresa não possua controle dos seus equipamentos e softwares, em casos de auditoria isso atrasa o processo além de gerar multa por falta de documentação.

3.3 PROPOSTA DE MELHORIAS

A proposta de melhorias começa com a adoção de uma política de segurança da informação, que ajudará a resolver grande parte das falhas encontradas e trabalhará o usuário que é um ponto importante a se levar em consideração, tanto pelo fato de ser considerado o elo mais fraco em segurança assim como pela cultura organizacional que é aberta.

Para a adoção dessa política, seria interessante realizar uma reunião para proporcionar um treinamento aos funcionários sobre a segurança e as técnicas de engenharia social, assim como para tirar dúvidas sobre a política e os processos envolvidas para que ela seja efetiva e determinar um prazo de três meses depois dessa reunião para que todas as diretrizes da política de segurança da informação sejam cumpridas.

É necessária uma nova estruturação sobre os computadores das salas de aula implantando o padrão de senha apresentado na política de segurança da informação, porem neste caso a senha será disponibilizada aos professores sempre que necessitem utilizar a sala de aula, havendo documentação de horários sobre cada um que utilize os computadores para casa houver algum problema relacionado haverá os

arquivos de logs e câmeras para encontrar a pessoa responsável sobre o problema causado.

A *tag* com os e-mails com as respectivas senhas dos computadores dos professores disponibilizados nas salas de aula devem ser retirados e estes serão disponibilizados somente aos professores. Porem internamento deveria ser feito um levantamento da utilização destes e-mails saber se são realmente necessários, uma vez que os professores já possuam e-mail próprios com os materiais salvos em nuvem, assim como os e-mails disponibilizados aos alunos para o uso dos Chromebook.

Depois dessa parte estruturada é indispensável a criação de um inventário de TI, onde devem constar todos os equipamentos disponíveis na organização assim como a documentação dos softwares existentes em cada uma das maquinas e seus licenciamentos. O ideal é que somente o responsável de TI tenha acesso de administrador nas maquinas, para evitar softwares piratas instalados, vírus e para que a documentação esteja sempre atualizada. No momento em que apenas uma pessoa possui a permissão de instalar softwares, recai sobre ela a responsabilidade da legalização dos mesmos em caso de auditorias.

É fundamental o uso de antivírus em todas as maquinas da organização, a política de segurança expressa que os usuários devem fazer uso do antivírus e verificar os dispositivos que são conectados nos computadores. Somente o uso do Windows defender não é suficiente, softwares como o Bitdefender e o Kaspersky são conhecidos por terem um bom resultado, ambos são antivírus pagos que possuem versões free que podem ser utilizadas nos computadores, entretanto é recomendável que se faça um orçamento e se pague o software que para a empresa traga maior custo benefício.

No que se refere a rede da organização, se sugere uma reestruturação completa, com definição de somente três redes internas sendo elas uma para o administrativo, professores e outra para os alunos. Assim como definir políticas de downloads e distribuição de banda por endereço Ip através de uma *RouterBoard.*

CONCLUSÃO

A política de segurança da informação está diretamente ligada a todos com colaboradores da empresa, não importando o nível de hierarquia. Ela não está

somente ligada aos dados que a empresa possui, mas sim a todos os processos e ações que acontecem na empresa pois toda ação causa uma reação e a política de segurança é um documento que ajuda a diminuir os impactos das reações e fornecendo diretrizes para serem estabelecidas.

O presente trabalho atingiu o objetivo de elaborar uma política de segurança baseada em boas práticas de TI, assim como possui um foco mais voltado para o usuário como também atendeu os objetivos específicos de avaliar as políticas internas da empresa para entender seu funcionamento como também definir os critérios baseados em boas práticas em TI para a elaboração da política de segurança.

O trabalho identificou diversas falhas e problemas na empresa, alguns deles podendo trazer um alto impacto nos processos e funcionamento e o que foi identificado não é algo que a empresa reconhecia como problemas a serem corrigidos.

De uma maneira geral, o trabalho apresenta diferentes falhas que podem ser observadas no dia a dia de qualquer empresa, essas falhas são pontos que podem e devem ser analisados e corrigidos. O documento que é a política de segurança da informação é uma base que pode ajudar qualquer empresa a manter a segurança da informação na empresa.

REFERÊNCIAS

ABNT. NBR ISSO/IEC 27002. **Tecnologia da Informação –** Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2005.

CertBr. **Cartilha de segurança da Informação.** 2000. Disponivel em <https://www.cert.br/>. Acessado em 16/06/2017.

FERREIRA, Fernando Nicolau Freitas. ARAUJO, Márcio Tadeu de. **Política de Segurança da Informação –** Guia prático para Elaboração e Implementação. 2ª. ed. Editora Ciência Moderna. Rio de Janeiro, 2008.

FERNANDES, Aguinaldo Aragon. ABREU, Vladimir Ferraz de. **Implantado a Governança de TI:** estratégia à gestão dos processos e serviços. 3. ed. Brasport. Rio de Janeiro, 2012.

FONTES, Edison Luiz Gonçalves. **Praticando a segurança da informação.** Brasport. Rio de Janeiro, 2008.

FONTES, Eduardo. **Segurança da informação:** o usuário faz a diferença. Saraiva. São Paulo, 2006.

FURASTÉ, Pedro Augusto. **Normas Técnicas para o Trabalho Científico**. 15 ed. Editora do Autor. Porto Alegre, 2010.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 5. ed. Atlas. São Paulo, 2010

ISACA. **COBIT 5 e o Valor Agregado da Governança da TI Corporativa.** Disponível em <http://www.isaca.org/COBIT/focus/Pages/cobit-5-and-the-added-value-of-governance-of-enterprise-it-portuguese.aspx>. Acessado em 29/05/2017

ISACA. **Val IT FAQs.** Disponível em < http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT-FAQ.aspx#reg2>. Acessado em 05/11/2017.

ITGI, IT Governence Institute. **Governance od IT Investments. The Val IT Framework 2.0 Extract.** 2008**.** Disponível em < https://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Documents/Val-IT-Framework-2.0-Extract-Jul-2008.pdf>. Acessado em 05/11/2017.

JUNIOR, Guilherme. **Entendendo o que é engenharia social.** 2006. Disponível em <https://www.vivaolinux.com.br/artigo/Entendendo-o-que-e-Engenharia-Social>. Acessado em 16/06/2017.

LYRA, Mauricio Rocha. **Segurança e Auditoria em Sistemas de Informação.** 1. Ed. Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

NETTO, Abener da Silva. SILVEIRA, Marco Antonio Pinheiro da. **Gestão Da Segurança Da Informação:** fatores que influenciam sua adoção em pequenas e médias empresas. JISTEM: Journal of Information Systems and Technology Management, 2007 Disponível em <http://www.redalyc.org/html/2032/203219581007/>. Acessado em 24/06/2017

SEMOLA, Marcos. **Gestão da segurança da informação:** visão executiva da segurança da informação. Rio de Janeiro. Elsevier, 2003.

SOUSA, Natan Lima Ferreira Fernandes De. **Engenharia social na segurança da informação.** Instituto Federal De Educação, Ciência E Tecnologia Do Triângulo Mineiro. Paracatu. 2016.

APÊNDICES

APÊNDICE A – Questionários aplicados na empresa

QUESTIONÁRIO APLICADO AO GESTOR:

1 - Razão Social
2 - Nome Fantasia
3 - Como é realizada a comunicação interna?
4 - A organização conta com quantos computadores?
5 - Os computadores (salas de aula) possuem senhas? Se sim, elas distintas?
6 - Os professores/colaboradores hibernam ou suspendem os computadores ao se ausentar da sala?
7 - Possui uma estrutura de rede mapeada? (Possui alguma documentação)
8 - A estrutura de rede conta com cabeamento estruturado? Conta com rede wireless?
9 - A estrutura de rede conta com algum bloqueio a sites?
10 - Existem profissionais específicos da área de TI trabalhando na empresa ou somente um serviço terceirizado?
11 - Atualmente há quantos professores no Hey Peppers?
12 - Como funciona a política de download? Existe alguma ou é livre? (Inclui músicas e vídeos usados em sala de aula, além de anexos em e-mail)
13 - Quando fui na escola, notei que havia música tocando, existe o uso de um streaming de música ou é feito download delas?
14 - Já ocorreu algum problema na empresa em relação a segurança da informação que gerou problemas? (Virus que apagou arquivos, arquivos que desapareceram ou foram modificados sem saber quem o fez)
15 - Há alguma informação relevante que você acredite que eu deva saber? Ou mesmo uma que você não julgue realmente relevante?

QUESTIONÁRIO APLICADO AOS FUNCIONÁRIOS:

SEGURANÇA:

1 - Você considera a segurança da informação algo importante para a organização? Por que?
2 - Na sua opinião, percebe-se que há segurança da informação na empresa?
3 - O que você entende por política de segurança da informação?
4 - Você utiliza computador próprio ou da empresa?
5 - Há algum riso, vulnerabilidade ou brechas que você identifica na organização que podem ocasionar falhas e problemas?

SENHAS:

1 - Sobre as suas senhas utilizadas nos logins dos sistemas internos e do e-mail institucional é válido dizer que:
A - Utilizo a mesma senha nos sistemas e no e-mail.
B - Utilizo a mesma senha nos sistemas, porém uma diferente no e-mail.
C - Utilizo uma senha diferente para cada sistema e e-mail.

D - Utilizo senhas diferentes nos sistemas porem a senha do e-mail se repete em um deles
E - Outros

2- Sobre a(s) sua senha dos sistemas, no quesito de compartilhamento, é correto afirmar que:
A - Somente eu possuo acesso a minha senha.
B - Eu e um colega de trabalho possuimos a senha.
C - A minha senha é algo público que compartilho com quem pedir.
D - Já passei minha senha para algum colega acessar o sistema, mas o mesmo não se encontra mais na organização
E – Outros

3- Sobre a senha, com foco em qualidade de senha, é correto afirmar que:
A - Possui somente caractere numérico. Ex: 12345
B - Possui caractere alfabético somente com letras minusculas. Ex: abcd
C - Possui caractere alfabético somente com letras maiúsculas. Ex: ABCD
D - Possui caractere alfabético com letras minúsculas e maiúsculas. Ex: abCD
E - Possui caractere alfanumérico somente com letras minúsculas. Ex: ab12
F - Possui caractere alfanumérico somente com letras maiúsculas. Ex: CD34
G - Possui caractere alfanumérico com letras minúsculas e maiúsculas. Ex: ABcd12
H - Possui caractere alfanumérico e especiais somente com letras minúsculas. Ex: ab12#
I - Possui caractere alfanumérico e especiais somente com letras maiúsculas. Ex: AB12#
J - Possui caractere alfanumérico e especiais com letras minúsculas e maiúsculas. Ex: ABcd12@

4- Sobre a quantidade de caracteres existentes na sua senha é correto afirmar:
A - 0 a 4 caracteres
B - 5 a 8 caracteres
C - 9 a 12 caracteres
D - mais de 12 caracteres

COMPUTADORES E AMBIENTE:

As opções de resposta para estas afirmações são: Nunca, Algumas vezes, Não concordo nem discordo, Quase sempre e Sempre.
1 - Ao me ausentar da sala hiberno/suspendo o computador que eu estava utilizando.
2 - Desligo a tela do computador ao me ausentar da sala.
3 - Nunca deixo um cliente sozinho na sala com o computador desbloqueado.
4 - Faço as atualizações dos programas sempre que janelas flutuantes aparecem.
5 - Faço downloads de arquivos (musicas, fotos, programas, etc.) nos computadores.
6 - Se possuo tempo livre costumo jogar jogos online.
7 - Ao receber e-mails com anexo, sempre faço download deles sem antes conferir o formato que se encontram.
8 - Utilizo minhas redes sociais (pessoais) no ambiente de trabalho.
9 - Há necessidade de utilizar o computador para realizar as tarefas do dia a dia.

10 - Verifico as unidades removíveis ao conecta-las no computador (utilizando anti-vírus).
11 - Utilizo meu *e-mail* pessoal no ambiente de trabalho.
12 - Passo informações sobre os colaboradores, processos ou o funcionamento por telefone.
13 - Passo informações sobre os colaboradores, processos ou o funcionamento da empresa por e-mail (que não tenha domínio @heyperppers).

APÊNDICE B – Política de Segurança da Informação

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:

1 ASPECTOS GERAIS

Este documento descreve a Política de Segurança da Informação da empresa Hey Peppers.
A política define diretrizes, procedimentos e condutas que devem ser cumpridos afim de garantir a integridade, confiabilidade e disponibilidade da informação e dos processos interno dentro da empresa.

1.1 OBJETIVOS

O principal objetivo desta política de segurança é garantir a segurança da informação, dos processos e atividades relacionadas à tecnologia da informação na empresa Hey Peppers.
O outro objetivo se dá a necessidade de ampliar o conhecimento dos usuários sobre a importância da segurança da informação, de como cada um possui responsabilidades para que a empresa se mantenha segura.

1.2 RESPONSABILIDADES

É de responsabilidade do gestor da empresa informar e disponibilizar a política de segurança da informação para todos os colaboradores da empresa.
É de responsabilidade de todos da organização respeitar e cumprir a política de segurança assim como comunicar qualquer violação da política para o gestor da empresa.
É responsabilidade da empresa ter arquivado o termo de responsabilidade e conhecimento da política de segurança assinado pelos colaboradores.

1.3 ATUALIZAÇÃO DA POLÍTICA

Sempre que houver necessidade pela troca de legislação, surgimento de novas formas de ludibriar a segurança da empresa ou ocorrer algo não previsto que gere dúvidas sobre a política de segurança vigente.
Quando houver sugestões de revisão ou melhoria da política de segurança por parte dos usuários, estas devem ser avaliadas e analisadas pelos responsáveis da política de segurança da informação.

1.4 DIVULGAÇÃO DA POLÍTICA

É de responsabilidade do gestor divulgar para todos os colaboradores a política de segurança. A divulgação será feita a partir da fixação de uma cópia no mural interno e através de um e-mail informativo.
A divulgação da política deve ser feita de maneira clara e objetiva, para que não deixe duvidas e deve estar disponível para todos os usuários.
Todo o novo colaborador assim como os já existentes, devem ler a política e assinar um termo de responsabilidade e de conhecimento da política de segurança da informação da empresa para assim evitar argumentos de desconhecimento da mesma.
Todas as alterações da política de segurança devem ser comunicadas com antecedência de um mês aos usuários para que haja um período de adaptação. As alterações podem ser também divulgadas nas conversas semanais que ocorrem na organização.
Toda a nova alteração irá gerar um novo termo de responsabilidade e de conhecimento que deverá ser assinado pelos usuários.

1.5 O NÃO CUMPRIMENTO DA POLÍTICA DE SEGURANÇA

O não cumprimento da política irá gerar advertência para o funcionário, podendo ocasionar em suspensão ou desligamento do colaborador de acordo com a gravidade da ocorrência.

2 POLÍTICA DE SENHAS

- É de responsabilidade do usuário manter sua senha em sigilo, sendo estritamente proibido compartilha-la para qualquer pessoa.
- As senhas devem possuir no mínimo 8 (oito) caracteres, sendo eles: minúsculos, maiúsculos e numerais.
- Não são permitidos como senha datas de aniversários de pessoas próximas, número de telefone, número de documentos, sequências numéricas ou alfabéticas (abc, 123, qwert, etc.), trocar o “a” por 4 ou “i” por 1 e assim sucessivamente, ou qualquer outra sequência ou lógica que crie padrões simples.
- O tempo de troca de senha será de 90 dias, mas se achar que sua senha não é mais segura o usuário poderá alterar em um período menor de tempo a troca.
- A senhas do e-mail corporativo e do sistema devem ser distintas.
- Tudo o que for executado com o login e senha do usuário será de total responsabilidade dele.

3 POLÍTICAS DE UTILIZAÇÃO DO *E-MAIL*

- Somente solicitar e transmitir informações internas requisitadas pelo e para o e-mail corporativo.
- Não enviar e repassar e-mails de corrente, desaparecimentos, brincadeiras, promoções, etc.
- Não abra anexos com extensões desconhecidas, .bat, .exe, .src e .com se não tiver total certeza de ter solicitado o arquivo.
- Não abra links desconhecidos se não tiver certeza de ter solicitado o e-mail.
- Não use o e-mail corporativo para fins pessoais.

4 POLÍTICA DE USO DA ESTAÇÃO DE TRABALHO

- Sempre que se ausentar da sala bloqueie a estação de trabalho.
- Não instale softwares sem ter autorização do responsável de TI.
- Proibido a instalação de softwares piratas, sem a licença.
- Não efetue downloads de músicas, vídeos, programas entre outros tipos de arquivo, peça auxilio para o responsável do TI que tomará os devidos cuidados no momento do download.
- Não execute arquivos desconhecidos.
- Sempre que utilizar uma mídia removível verifique a mesma com o antivírus.
- Utilize a estação de trabalho destinada a sua função.

5 POLÍTICA SOCIAL

- Não diga sua senha para ninguém. O responsável da TI não irá solicitar sua senha.
- Não fale sobre a política de segurança da empresa com terceiros ou fora da empresa.
- Não fale sobre processos e problemas internos com terceiros ou fora da empresa.
- Evite comentar sobre informações dos colaboradores, como férias, faltas, atrasos, localização ou qualquer informação interna da empresa à terceiros.
- Não faça login ou digite sua senha em maquinas de terceiros que podem estar logadas na rede da empresa.
- Somente aceite ajuda técnica de colaboradores previamente apresentados e identificados. Não aceite ajuda de qualquer outra pessoa.
- Proibido o uso da internet para acessar conteúdos impróprios.

Apêndice C – Termo de responsabilidade da política de segurança da informação

TERMO DE RESPONSABILIDADE

Eu _____, portador do RG: _____, da função: _____ _____, declaro que li e estou ciente das diretrizes, procedimentos e condutas apresentadas na Política de Segurança da Informação da escola Hey Peppers, INSTITUTO DE LINGUAS DEWES E DIESEL. Assumo a responsabilidade de manter a segurança da informação e seguir as diretrizes da política de segurança.

Me comprometo a não divulgar informações internas da empresa para terceiros. Estou ciente que o não cumprimento da Política de Segurança da Informação pode resultar em advertências e em piores casos desligamento da empresa.

Santa Rosa, Brasil, ____ de _____ de _____.

_____

Assinatura do colaborador