OS DESAFIOS CONTEMPORÂNEOS PARA IMPLANTAÇÃO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EM UMA ORGANIZAÇÃO DE MÉDIO PORTE

Daniel dos Santos[1]
Fernando Schmidt Gross [2]
Marilei de Fátima Kovatli[3]

RESUMO

Os avanços significativos da ciência possibilitaram a inserção de novos produtos eletrônicos e novas tecnologias lançadas para o uso domiciliar e empresarial. E esta evolução facilitou a comunicação e troca de informações no cenário mundial, entretanto, existem preocupações quanto a roubo e vazamento das informações armazenadas. Nesse contexto, a segurança da informação se tornou uma ferramenta de extrema importância no meio empresarial, visto que a informação passou a ser um ativo de grande valor para as organizações. Devido essa importância, o tema deste artigo é investigar os desafios contemporâneos para implantação de uma política de segurança da informação em uma empresa metalmecânica de médio porte. O objetivo principal do estudo é analisar os desafios enfrentados para a utilização de boas práticas de segurança da informação, a fim de elaborar uma política de segurança da informação. O artigo em questão justifica-se pelo fato da segurança da informação se tornar uma grande aliada nas organizações, pois sem uma política de segurança das informações a empresa estará vulneral a qualquer incidente, que trará grandes impactos e assim não terá como elaborar um plano de ações corretivas e preventivas. A metodologia empregada para o artigo, caracteriza-se como pesquisa teórica-empírica, com um estudo de caso, possuindo análises de dados qualitativos. Para o embasamento teórico, utilizou-se bibliografias dos seguintes autores: Dantas, Ferreira e Araújo, Fontes, Lyra e da norma ISO/IEC 27002:200. Como contribuição desse estudo está a elaboração de uma proposta para a política de segurança de informações, como solução para os problemas identificados, protegendo assim a empresa em relação as informações.

Palavras chave: Avanço – Tecnologias - Segurança da Informação – Política de Segurança.

[1] Acadêmico do Curso de Gestão da Tecnologia da Informação – 6º Semestre. Faculdades Integradas Machado de Assis. danisantos780278@gmail.com
[2] Acadêmico do Curso de Gestão da Tecnologia da Informação – 6º Semestre. Faculdades Integradas Machado de Assis. fernandoschmidtgross@gmail.com
[3] Mestre em Ciências da Computação. Orientadora. Professora do Curso de Gestão da Tecnologia da Informação. Faculdades Integradas Machado de Assis – marilei_gti@fema.com.br

ABSTRACT

Substantial advances in science have enabled the insertion of new electronic products and new technologies launched for household and business use. This evolution has facilitated communication and information exchange on the global scenario, however, there are concerns about the theft and leakage of stored information. In this context, information security has become an extremely important tool in the business environment, as information has become a valuable asset for organizations. Due to this importance, the subject of this paper is to investigate contemporary challenges for implementing an information security policy in a medium-sized metal-mechanic sector. The main objective of the study is to analyze the challenges facing the use of good information security practices in order to develop an information security policy. The article in question is justified by the fact that data security becomes a great ally in organizations, because without an data security policy the company will be vulneral to any incident, which will have major impacts and thus will not be able to elaborate a plan of action. corrective and preventive actions. The methodology used for the article is characterized as theoretical-empirical research, with a case study, with qualitative data analysis. As a contribution of this study is the elaboration of a proposal for the information safety policy, as a solution to the identified problems, thus protecting the company with regard to the information. For theoretical background, use the bibliographies of the following authors: Dantas, Ferreira and Araújo, Fontes, Lyra and ISO / IEC 27002: 200. As a contribution to this study, a proposal for information security policy is elaborated as a solution to problems. thus protecting a company from information.

Keywords: Advancement - Technologies - Information Security - Security Policy.

INTRODUÇÃO

Vivemos na era da informação, onde as tecnologias têm grandes avanços, possibilitando a criação de novos recursos e ferramentas tecnológicas. De modo geral os processos ficaram mais ágeis, facilitando assim, a troca de informações e a comunicação e nesse contexto, a informação pode ser considerada como o bem mais valioso de uma organização, em alguns casos a informação acaba se tornando uma vantagem competitiva para quem souber fazer o melhor uso.

As novas tecnologias possibilitaram a rápida troca de dados, e nesse contexto algumas pessoas buscam obter as informações que trafegam nas redes mundiais, tais como: senhas de bancos, e-mails, informações sigilosas de governos e empresas. Diante dessa realidade surgem dúvidas se realmente estas informações estão seguras, então surge a necessidade de implementar e seguir uma Política de

Segurança das Informações. Considerando este contexto o problema originário deste estudo está em verificar quais são os desafios para implantar uma Política de Segurança da Informação em uma organização.

Diante disso, o presente artigo tem por finalidade apresentar os principais desafios contemporâneos para a implantação de uma política de segurança da informação em uma organização de médio porte que está localizada em Boa Vista do Buricá – RS.

Este artigo tem como objetivo principal analisar os desafios enfrentados para a utilização de boas práticas de Segurança da Informação, a fim de entender as dificuldades enfrentadas para alteração ou a criação de novas práticas. Especificamente, buscou-se estudar os atributos básicos da segurança da informação; verificar junto à organização a existência de boas práticas em PSI; analisando as vulnerabilidades em relação a segurança das informações da organização; e por fim, elaborar uma proposta para implantar uma Política de Segurança da Informação, a partir das necessidades da organização.

Em relação a metodologia empregada para a elaboração deste artigo, quanto a natureza, a pesquisa caracterizam-se como teórico-empírica. Já em relação ao tratamento dos dados, a pesquisa caracteriza-se como qualitativa, por conta da análise do ambiente da organização e será feita por meio de questionários. Quanto aos fins, em razão dos objetivos traçados para este artigo a pesquisa será exploratória. Com relação aos procedimentos técnicos, o projeto caracteriza-se como pesquisa bibliográficas, feita em livros e será aplicada através de um estudo de caso. O artigo em questão justifica-se pelo fato da segurança da informação se tornar uma grande aliada nas organizações, pois sem uma política de segurança das informações a empresa estará vulneral a qualquer incidente, que trará grandes impactos e assim não terá como elaborar um plano de ações corretivas e preventivas.

Por meio do embasamento teórico, pode-se buscar conhecimento sobre o tema tratado e a partir da análise feita na organização, descobre-se as necessidades da empresa, a fim de solucionar o problema da pesquisa. Para o embasamento teórico, utilizou-se bibliografias dos seguintes autores: Dantas, Ferreira e Araújo, Fontes, Lyra e da norma ISO/IEC 27002:200.

O artigo estrutura-se com uma introdução apresentando seu tema, o problema que originou o estudo, o objetivo geral e a justificativa. Na sequência apresenta-se o

referencial teórico abordando a importância da segurança das informações para as empresas e como uma empresa do ramo metalmecânico pode aplicar uma Política de Segurança da Informação (SI). Logo após, descreve-se a metodologia utilizada na pesquisa, e a análise dos resultados obtidos, bem como, a proposta de uma política para a segurança das informações para a empresa. Por fim, segue a conclusão do estudo e as referências que nortearam o trabalho.

1 REFERENCIAL TEÓRICO

O referencial teórico é parte importante no desenvolvimento de um artigo, segundo Lakatos e Marconi, o referencial teórico diz respeito aos “[...] elementos de fundamentação teórica da pesquisa e, também, a definição dos conceitos empregados.” (LAKATOS; MARCONI, 2010, p. 207).

A respeito do artigo, fundamenta-se o construto teórico, por meio de quatro seções, onde tratarão do conteúdo pertinente a pesquisa. Na primeira seção, expõe-se os principais conceitos introdutórios sobre segurança da informação com o objetivo de situar o leitor.

Na segunda seção será apresentado um estudo pertinente aos desafios enfrentados para a criação de uma Política de Segurança da informação, demostrando as dificuldades ocorridas para o desenvolvimento. Outro ponto abordado durante está seção, será o usuário, como o responsável pelo cumprimento e execução da nova política criada e estabelecida.

Na terceira seção será apresentado o que é um Plano de Continuidade do negócio, mostrando os pontos a serem levados em conta na hora do planejamento em casos de acidentes. Também demonstrará as dificuldades enfrentadas no momento de elaborar o planejamento.

Já na quarta seção apresenta-se o embasamento teórico de uma Cultura Organizacional, mostrando suas finalidades e o impacto que uma mudança organizacional pode causar em uma organização.

1.1 ATRIBUTOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO

Com o desenvolvimento tecnológico proporcionado através de pesquisas, os meios de comunicação tiveram um grande impacto positivo, aumentando a velocidade na troca de mensagens, onde se demorava dias para se enviar mensagens, agora necessitamos de frações de segundos. De acordo com Dantas, “o mundo moderno tem dedicado especial atenção à informação, devido à sua importância para a manutenção dos negócios e a realização de novos empreendimentos entre pessoas, empresas, povos, nações e blocos econômicos”. (DANTAS, 2011, p. 9)

> A informação é um ativo, que como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades. (NBR ISO/IEC 27002, 2005, p. X)

O conjunto de informações que compõe uma empresa, é de suma importância, uma vez que, detalha o funcionamento operacional e estratégico da organização, revelando a real importância em se manter o mais seguro possível, através destes dados, é possível descobrir a situação financeira, fornecedores e dados dos funcionários. Com o uso da internet dentro das organizações, reforça a ideia de se ter meios que possibilitem o controle dos utilitários utilizados para a realização efetiva da segurança da informação.

> Conhecer os conceitos sobre segurança da informação não significa necessariamente saber garantir essa segurança. Muitos têm experimentado esta sensação quando elaboram seus planos de segurança e acabam não atingindo os resultados desejados. (CAMPOS, 2007, p. 29)

Ao mesmo tempo em que a tecnologia sofreu grandes avanços, as técnicas de invasões evoluíram e a velocidade dos ataques aumentaram, mostrando que a segurança da informação, em determinados casos, não consegue acompanhar o avanço frenético, onde a falta de preparo por parte de seus usuários é o principal motivo, pois, acessam conteúdos que estão infectados com códigos maliciosos para o roubo de informação. No âmbito empresarial, os computadores utilizados para o trabalho, processam e armazenam a maioria das informações operacionais, deve-se

ter uma atenção maior, a proteção das informações requer tempo e dinheiro, além de profissionais capacitados para a elaboração de um projeto consistente para a prevenção de invasões.

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

Informação são dados organizados que conseguem transmitir um significado, não apenas palavras ou números vagamente soltos, neste sentido, é possível entender que a informação não engloba apenas os dados dos clientes, mas também dados da organização, seus produtos e serviços. De acordo com Perini, “informação é um conjunto de fatos organizados de modo a ter valor adicional, além de fatos propriamente ditos”. (PERINI, 2011, p. 3)

De acordo com Sêmola, "podemos definir segurança da informação como uma área de conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade" (SÊMOLA, 2014, p. 41). É notável que para existir uma boa segurança da informação no ambiente virtual, precisa-se de conhecimento técnico para realizar de forma correta e segura a proteção dos dados que necessitam ser compartilhados através de uma rede corporativa ou pública.

Para garantir a segurança da informação, foram criados três conceitos chaves, chamados de pilares da segurança da informação, sendo, confidencialidade, integridade e disponibilidade. Conforme 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. 4)

Confidencialidade: se caracteriza pela capacidade de sigilo da informação, autorizando o acesso a determinado grupo de pessoas, as informações que necessitam esta proteção são consideradas críticas e sua divulgação não autorizada causaria grande impacto negativo. Conforme Lyra, “capacidade de um sistema de permitir que alguns usuários acessem determinadas informações ao mesmo tempo em que impede que outros, não autorizados, a vejam”. (LYRA, 2008, p. 3)

Integridade: toda informação transmitida/armazenada deve possuir consistência e confiabilidade, quando transmitida para diferentes setores ou pessoas, deve ser compreendida pelo seu emissor e receptor. “Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados”. (BRASIL, 2012, p. 9)

Disponibilidade: a informação deve estar disponível quando necessária para consulta, quando os dados se encontram indisponíveis, paralisam atividades essenciais para o funcionamento da organização, gerando a cessão do lucro ou em situações extremas prejuízo. “A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário”. (NBR ISO/IEC 27002, 2005).

> Muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados. A identificação de controles a serem implantados requer um planejamento cuidadoso e uma atenção aos detalhes. A gestão da segurança da informação requer pelo menos a participação de todos os funcionários da organização. (NBR ISO/IEC 27002, 2005, p. X)

Seguindo está análise, deve se considerar que nenhum sistema está efetivamente seguro, uma vez que deve haver harmonia entre os meios técnicos e procedimentos apropriados para deste modo conseguir realizar a segurança da informação. A participação do usuário é um dos fatores vitais para concretizar a segurança, pois é ele quem estará em contato direto com os sistemas utilizados para as tarefas da área profissional.

1.2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

A informação que circula e é utilizada pela organização, é um bem que possui valor, portanto, deve ser protegida, cuidada e gerenciada. A tecnologia aliada aos negócios é grande influenciadora no seu crescimento, as tarefas diárias realizadas pelos funcionários tiveram grande queda no tempo necessário para a conclusão, além disso, possibilitou a redução de erros em atividades críticas. Para a proteção destes dados, surgiu a Política de Segurança da Informação (PSI), visando definir princípios para a proteção dos sistemas de informação.

A Política de Segurança da Informação (PSI), é constituída por um conjunto de regras e padrões, onde deve assegurar que os serviços e informações recebam a proteção devida a modo de garantir os três princípios básicos da informação, conforme citado no item 1.1. Entende-se, que a Política de Segurança da informação é um documento que engloba de modo geral a segurança das informações, apresenta dados e informações de uma organização, orientando e estabelecendo normas corporativas, de como os colaboradores devem lidar e fazer a proteção dos dados.

Portanto, uma Política de Segurança da Informação (PSI), pode ser entendida como um manual que reúne um conjunto de técnicas, ações e boas práticas da segurança da Informação, com o intuito de apresentar como deve ser o uso de forma adequada e segura dos dados de uma organização. Uma Política de Segurança da Informação (PSI), pode ser entendida como um código de conduta interno de uma organização, que visa a prevenção das responsabilidades legais de cada usuário e ainda estabelece o que é permitido ou o que é proibido de se fazer, como os profissionais devem agir diante a um incidente, por exemplo.

Conforme os autores Ferreira e Araújo, “A política de segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos dos usuários que fazem uso dos ativos de informação” (FERREIRA; ARAÚJO, 2008, p. 36).

Nesse contexto, pode-se dizer que o foco de uma Política de Segurança é manter os dados seguros, juntamente com os recursos tecnológicos da organização. Essa proteção é necessária, pois evita que as informações se percam, ou seja, roubadas e divulgadas por usuários mal-intencionados. Cuja suas ações visam prejudicar a organização.

> Uma das regras básicas para o sucesso de um processo de segurança de proteção da informação é tratar esse assunto através de uma abordagem profissional. Quanto mais seriedade, maiores as chances da organização obter sucesso na proteção da informação. Dessa forma, definições formais e explicitas são mais efetivas do que opiniões isoladas ou conceitos não formalizados. Definir os níveis de classificação da informação é uma boa prática. (FONTES, 2008, p. 191)

Para se obter sucesso na tentativa de proteger as informações armazenadas no sistema de arquivos da organização, deve-se tratar com seriedade e de maneira profissional, ao se ter claro o real objetivo de como proteger os ativos, se torna mais

fácil alcançar o objetivo esperado. A classificação das informações tem como propósito manter a confidencialidade de determinados arquivos, este é um aspecto a ser levado em conta no processo de segurança, dependendo do tipo de informação, esta não deve ser revelada a qualquer indivíduo, assim evitando conclusões precipitadas.

> As políticas da organização não devem admitir o uso dos recursos para a discriminação ou provocação em razão do sexo, raça, cor, religião, nacionalidade, idade, porte de deficiência física, condição de saúde, estado civil ou qualquer outra condição prevista em lei. Adicionalmente, em nenhuma hipótese, os colaboradores poderão utilizar meios tecnológicos para transmitir, receber ou armazenar qualquer informação que seja discriminatória, difamatória ou provocativa (material pornográfico, mensagens racistas, piadas, desenhos etc.). (FERREIRA; ARAÚJO, 2008, p. 87)

Um fator que ressalta a criação de uma política, é como os meios tecnológicos serão utilizados por parte dos funcionários, ao se obter acesso ao parque tecnológico da organização, é responsabilidade da organização evitar a disseminação de conteúdo cuja intenção é descumprir leis estabelecidas. A política deve ressaltar que o funcionário é responsável por usar os recursos computacionais cedidos com o intuito de aumentar a produtividade e contribuir para a imagem pública da empresa.

> As ações de segurança não podem ser apenas alguns procedimentos formais e escritos unicamente para mostrar aos executivos ou para evidenciar em uma auditoria. Devem ser uma filosofia de trabalho, de fato, algo sustentável e de cunho prático. Escrever algumas normas e pendurá-las nos murais, unicamente, não vai garantir a segurança da informação. (CAMPOS, 2007, p. 31).

O principal foco de uma Política de Segurança é manter os meios tecnológicos o mais seguro possível contra ações que visam prejudicar os equipamentos e o roubo de informações necessárias para o funcionamento rotineiro da organização. E por isso que se deve criar e implementar uma Política de Segurança das Informações, mas afinal, o que esse documento deve conter?

Para Ferreira e Araújo, a elaboração de uma política de Segurança da Informação deve ressaltar as normas e procedimentos de segurança da informação e ainda deve ser:

> a) Simples;
> b) Compreensíveis (escritas de maneira clara e concisa);
> c) Homologadas e assinadas pela Alta Administração;
> d) Estruturadas de forma a permitir a sua implementação por fases;
> e) Alinhadas com as estratégias de negócio da empresa, padrões e procedimentos já existentes;
> f) Orientadas aos riscos (qualquer medida de proteção das informações deve direcionar para os riscos da empresa);
> g) Flexíveis (moldáveis aos novos requerimentos de tecnologia e negócio);
> h) Protetores dos ativos de informação, priorizando os de maior valor e de maior importância;
> i) Positivas e não apenas concentradas em ações proibitivas ou punitivas." (FERREIRA; ARAÚJO, 2008, p. 37 e 38).

Nesse sentido, a elaboração do documento si de uma Política de Segurança Informação, é uma etapa de extrema importância, que exige um certo grau de delicadeza, pelo fato de que esse documento deve interligar os princípios e normas de segurança da Informação, alinhada aos objetivos e estratégias do negócio. Esse documento ainda deve ser escrito de forma simples e o mais claro possível para evitar as interpretações erradas dos usuários.

O primeiro aspecto da linha de segurança que terá de ser implementado é a utilização de senhas, onde devem ser seguras e não apenas sequencias numéricas previsíveis, ou o próprio nome, cabe a Política de Segurança determinar o padrão a ser seguido para a criação de uma senha válida e que se julgue segura. De acordo com Ferreira, "a política deve ressaltar que determinados recursos tecnológicos da empresa podem ser acessados apenas mediante o fornecimento de uma senha válida, ou seja, as senhas são utilizadas para prevenir acessos não autorizados à informação e não conferem ao colaborador nenhum direito de privacidade." (FERREIRA; ARAÚJO, 2008, p. 88).

Seguindo o contexto, outro tópico que deve ser abordado em uma Política de Segurança da informação, é em relação ao controle de acesso. Esse controle deve ser restrito e as informações devem ser acessadas por aqueles que necessitam das informações para desempenhar as suas atividades profissionais na empresa, ou seja, cada usuário deve acessar o que lhe foi autorizado através da hierarquia, sendo assim o usuário só terá acesso apenas as informações que pertencem ao seu nível de hierárquico. Para garantir a confidencialidade a proteção, pode ser feita através de requerimento de acesso, demanda pelo gestor. Conforme Fontes, "a liberação do acesso da informação para os usuários será autorizada pelo gestor, que levará em

conta a confidencialidade da informação e a necessidade de acesso do usuário.” (FONTES, 2008, p. 249).

Partindo deste pressuposto, além de escrever a nova política de segurança, é de suma importância a divulgação para os usuários da rede, explicando os conceitos criados com o propósito de proteger as informações da rede corporativa, assim sendo, proporcionando treinamento para os colaboradores. O número de tentativas em contornar a segurança rígida de uma rede é grande, deve-se criar um equilíbrio entre confiança e segurança.

> O comprometimento do usuário é uma atitude fundamental para o sucesso da proteção da informação. Podemos ter o melhor controle de acesso lógico, porém será de pouca valia se é comum na organização o usuário emprestar sua senha para outro ou ausentar-se do local onde está o seu computador e o mesmo não possui uma proteção de tela. Pouco adianta ter um excelente sistema de cópias de segurança se o usuário não coloca seus dados pessoais na área destinada para tal. (FONTES, 2008, p. 123)

Para determinar o sucesso de uma nova política, é fundamental conseguir o comprometimento do usuário, conscientizando-o sobre os riscos ocorridos caso não haja uma vontade do coletivo para realizar a segurança dos ativos de uma organização. A solução para integrar as pessoas necessita de ações gradativas com o principal propósito de fortalecer a cultura da segurança da informação, esta cultura não deve ficar limitada a organizações, é um trabalho onde o resultado positivo é garantido, entretanto, não é imediato e requer planejamento. [...] deve ser clara o suficiente para ser bem compreendida pelo leitor em foco, aplicável e de fácil aceitação. A complexidade e extensão exageradas da PSI pode levar ao fracasso de sua implementação. (BRASIL, 2012, p. 12)

Dessa maneira, acerca dos aspectos que envolvem a política de segurança das informações, entende-se que para ser efetivo o documento deve ser simples e claro, contendo orientações que englobam de modo geral a tecnologia da informação (TI), voltada a segurança das informações, alinhada diretamente aos objetivos e estratégias da empresa. É preciso ressaltar, que não basta apenas a criação da política, se não for repassada e ensinada aos colaboradores, mostrando a importância das informações e porque devem ser protegidas.

1.3 PLANO DE CONTINUIDADE (PCN)

As operações da organização, sempre irão estar vulneráveis a uma vasta gama de riscos e impactos que podem ser ocasionados por desastres naturais (terremotos, inundações, furacão, entre outros), ou por incidentes (falhas no sistema, queda de energia, entre outros). Estes eventos podem ocasionar a paralisação das atividades operacionais, caso não haja algum plano para a reestruturação dos processos.

Para realizar o entendimento, deve-se considerar o risco operacional como o conceito macro, que envolve todo o assunto, para Fontes, “qualquer evento que potencialmente pode impedir a organização de atingir seus objetivos (operacionais) é uma ameaça”, ainda para Fontes, “O risco (operacional) é a possibilidade dessa ameaça se transformar em realidade” (FONTES, 2008, p. 74).

> 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. (BRASIL, 2012, p. 32)

Nenhuma organização está de fato livre de qualquer ameaça, o plano de continuidade (PCN) tem então como objetivo, restaurar o mais rápido possível os serviços afetados por algum problema, seja de caráter técnico ou ambiental, no cenário atual, tempo é dinheiro, deste modo, ficar com as atividades operacionais congeladas por problemas, gera a perda de renda. No cenário atual, é indiscutível a dependência tecnológica para a realização das atividades operacionais de uma organização, o plano de continuidade visa amenizar problemas ocorridos.

> A abrangência do plano depende da definição do cenário dos recursos, do escopo organizacional e das ameaças consideradas. Um dos erros mais comuns é tentarmos elaborar da primeira vez um plano que considere todas as situações. Comece pelas situações de maior risco e maior impacto. Elabore o plano, treine as pessoas e permita que a organização aprenda a gerenciar riscos, enfrentar crise e garantir a continuidade do negócio. (FONTES, 2008, p. 76)

O plano de continuidade deve ser criado especificamente para a organização, ou seja, não é recomendado copiar o PCN de outras instituições, uma vez que, foi

planejado para determinados recursos, onde estes podem não fazer parte dos equipamentos pertencentes da empresa, tornando o PCN inutilizável. Os recursos que têm maior risco e impacto, são os principais a receberem um planejamento de continuidade, sem eles, pode acabar paralisando todas as atividades por tempo indeterminado, é imprescindível os colaboradores saberem os passos básicos para o reestabelecimento do serviço afetado.

Para validar o plano de continuidade, é preciso manter pelo menos dois aspectos: a disponibilidade e a integridade, porque de nada adianta conseguir manter uma informação se ela estiver corrompida ou durante a interrupção do serviço ou ela gerar resultados contestáveis. Conforme Brasil, “o objetivo do Plano de Continuidade do Negócio é manter a integridade e a disponibilidade dos dados da instituição, bem como a disponibilidade dos serviços quando da ocorrência de situações fortuitas que comprometam o bom andamento dos negócios.” (BRASIL, 2012, p. 33)

Para a garantia que o Plano de Continuidade atenda o seu propósito inicial, de reestabelecer os processos afetados, é primordial que haja uma simulação de casos reais, colocando a prova a real efetividade descrita no plano, entretanto, é importante que estes testes sejam periódicos com a intenção de procurar falhas, aperfeiçoando cada vez mais o plano. Conforme Ferreira e Araújo, “[...] deve-se detalhar que o Plano de Contingência e/ou Continuidade seja revisado e testado periodicamente de forma a garantir o seu funcionamento em caso de necessidade.” (FERREIRA; ARAÚJO, 2008, p. 111)

Conforme a organização vai sofrendo um maior crescimento e desenvolvimento no setor de tecnologia, surge a necessidade de revisão do Plano de Continuidade, várias situações podem fazer surgir a demanda de atualizações, pode ser por novas exigências na legislação, aquisição de novos equipamentos, contratação de novos funcionários, entre outros. Para Brasil, “mudanças que tenham ocorrido e que não estejam contempladas no Plano de Continuidade do Negócio devem gerar atualizações. Quando novos requisitos forem identificados, os procedimentos de emergência relacionados devem ser ajustados de forma apropriada.” (BRASIL, 2012, p. 36)

Todas as informações que trafegam dentro de uma organização, passam pelos servidores e estações de trabalho, deve-se haver um método para criação de uma cópia de segurança, para a restauração em casos de problemas nos equipamentos

ou desastres que impossibilitem a recuperação, assim diminuindo os riscos que afetam diretamente a continuidade do negócio. Conforme Ferreira e Araújo, “para manter as informações disponíveis é necessário, além dos recursos de hardware, possuir procedimentos de *backup* e *restore d*as informações. Estes por sua vez devem ser capazes de orientar as ações de realização e recuperação das informações.” (FERREIRA; ARAÚJO, 2008, p. 112)

> A preparação para a continuidade do negócio quando a ocorrência de um desastre ou de outra situação de indisponibilidade de recursos demonstra como como a organização leva verdadeiramente a sério este assunto. Após os acontecimentos de 11 de setembro de 2001 muitas empresas voltaram a entender que tão importante como ter cópias de segurança é ter pessoas e infraestrutura para retornar à realização das atividades de negócio. (FONTES, 2008, p. 81)

Após acontecer desastres que impossibilitem o prosseguimento normal das atividades diárias, deve-se executar o Plano de Continuidade, além de evitar falhas na utilização dos sistemas de informações, demonstra que há um comprometimento por parte da empresa para a continuação dos seus sistemas produtivos. Não se recomenda guardar as cópias de segurança no local onde está toda a infraestrutura, deve-se procurar um meio de distanciá-la das instalações físicas, criando a hipótese de que a estrutura desabe, todas as informações armazenadas nos servidores serão perdidas assim como as cópias, havendo este distanciamento é possível recuperar todos os arquivos prejudicados no desastre.

1.4 CULTURA ORGANIZACIONAL

A cultura organizacional diz muito sobre uma empresa, pois sem ela a organização estará perdida sem crenças e valores para seguir e lhe orientar. Com base nisso, todas as empresas possuem uma cultura organizacional, independente do seu tamanho ou segmento atuante, no entanto, essa cultura pode ser formalizada ou não. Por mais que a cultura não esteja formalmente instituída, a empresa não deixa de ter sua própria personalidade, com os seus próprios costumes e métodos, podendo ser conservadora ou inovadora. De acordo com os autores Lacombe e Heilborn, a cultura organizacional pode ser conceituada como: “conjunto de crenças, costumes,

sistema de valores, normas de comportamento e forma de fazer negócios, que são peculiares a cada empresa [...]" (LACOMBE e HEILBORN, 2008, p. 356).

Através da cultura organizacional presente, é possível traçar com mais facilidade os objetivos desejados a serem atingidos, pois já existe um modelo que rege o comportamento dos colaboradores, tornando viável os planejamentos realizados. A cultura existente é utilizada também para a tomada de decisões, em razão que, já possuem comportamentos pré-estabelecidos e que torna possível prever determinadas ações que irão acontecer, sendo assim, uma ferramenta de grande valia para a gestão de uma organização. Assim como os autores Wagner e Hollenbeck apontam que:

> "[...] a cultura organizacional funciona como um tipo de cola social que ajuda a reforçar comportamentos persistentes e coordenados no trabalho. Ao fazer isso, a cultura de uma organização pode melhorar seu desempenho e servir como valiosa fonte de vantagem competitiva." (WAGNER e HOLLENBECK, 2012, p. 442).

Sendo assim, a cultura organizacional é a base de toda organização e está ligada diretamente à rotina da empresa, a sua estrutura de negócio e serve como guia que orienta o comportamento e a mentalidade dos funcionários. Por isso é importante que haja um relacionamento mútuo e recíproco de ambas as partes, (empresa - colaboradores e vice-versa), pelo fato de que para a criação da cultura precisa-se da ajuda e colaboração de todos, primeiramente deve-se considerar a missão, visão e valores da empresa, sem deixar de lado a percepção do funcionário e na fase final, quando a cultura estiver pronta e formalizada, ela deve ser ensinada aos funcionários de forma simples e clara, podendo ser através de campanhas e palestras, ou até mesmo através de documentos e banners. No entanto, para Lacombe e Heilborn, "As organizações podem ensinar sua cultura por meio de documentos escritos, nos quais ela estará explicitada, ou por meio de reuniões, seminários e palestras para empregados." (LACOMBE e HEILBORN, 2008, p. 358).

Já os funcionários desde a parte operária até a direção, podem criar subculturas dentro das áreas funcionais que atuam, são diversos pontos de vistas e percepções diferentes que ao comparar com outras, cria-se um conflito, através de uma média conseguem entrar em um consenso e evitar conflitos interpessoais. É importante esta subcultura, os trabalhadores conseguem chegar a um consenso de

seus principais ideais que consideram corretos e aceitar os dos companheiros de trabalho, evitando um conflito por diferenças de ponto de vista e valores que acreditam serem corretos. Conforme Robbins, “As subculturas tendem a se desenvolver para refletir problemas, situações ou experiencias comuns a alguns membros; podem ser definidas por designações de departamentos e por separação geográfica.” (ROBBINS, 2009, p. 227).

A cultura organizacional pode ser mudada, mas acaba gerando problemas com a adaptação dos funcionários, pois deve-se criar condições necessárias para que possa surgir novas crenças e valores, primeiro tem de conhecer a própria cultura presente para depois mudá-la e conseguir progredir. Segundo Wagner e Hollenbeck “[..] sempre que os gestores tentam acionar alguma mudança, podem esperar resistência, porque as pessoas tendem a resistir àquilo que percebem como ameaça à maneira estabelecida de fazer as coisas. Quanto mais intensa a mudança, mais intensa tende a ser a resistência resultante.” (WAGNER e HOLLENBECK, 2012, p. 452).

Quando a cultura de uma empresa se torna um diferencial competitivo, passa a ser valorizada pelos seus funcionários e principalmente pelos clientes**.** Com tudo, o que faz destacar-se e ter um diferencial competitivo perante os concorrentes é o sistema de valores da empresa, pois será através deles que a organização terá sua “identidade”, sua filosofia própria, bem como a maneira que trabalha e como alcança suas metas e objetivos.

2 METODOLOGIA

A metodologia engloba os métodos e meios utilizados para o desenvolvimento do mesmo, é através da metodologia que é determinado o escopo do estudo, assim como, para Lakatos e Marconi, “A especificação da metodologia da pesquisa é a que abrange maior número de itens, pois responde, a um só tempo, às questões como?, com quê?, onde?, quanto? [...].” (LAKATOS; MARCONI, 2010, p. 204).

Para a melhor compreensão, essa parte do estudo está dividida em três tópicos, que possibilita analisar da melhor forma as informações como: categorização da pesquisa, geração de dados e análise e interpretação dos dados.

2.1 CATEGORIZAÇÃO DA PESQUISA

Quanto à metodologia empregada para a realização deste estudo, a pesquisa caracteriza-se como teórico-empírica, com pesquisas bibliográficas e coleta de dados. Já em relação ao tratamento dos dados, a pesquisa caracteriza-se qualitativa, por conta da análise do ambiente da organização por meio de um questionário aberto, aplicado ao gestor.

Quanto aos fins, em razão dos objetivos traçados a pesquisa é categorizada como exploratória, por meio das informações coletas sobre segurança da informação da empresa.

Com relação aos procedimentos técnicos, caracteriza-se como pesquisa bibliográfica e um estudo de caso. Por meio dos embasamentos teóricos, pode-se buscar conhecimento sobre o tema tratado e a partir da análise feita na organização, pode-se compreender a situação da empresa.

2.2 DADOS GERADOS

Quanto a coleta de dados foi realizado através de duas formas: a documental direta, que se deu por meio de aplicação de um questionário aberto ao gestor e aos colaboradores, com o intuito de conhecer sobre a organização, buscando levantar dados sobre a segurança dos seus dados e se a mesma possui uma política de segurança da informação.

Já a segunda forma, refere-se a coleta de dados documental indireta, por meio de pesquisas bibliográficas em livros. A partir da coleta de dados, pode-se interpretar os objetivos do trabalho.

2.3 ANÁLISE E INTERPRETAÇÃO DOS DADOS

Neste artigo foi utilizado o método de estudo de caso no qual visou conhecer os desafios para implantar uma política de segurança das informações. Dessa forma os dados coletados foram analisados e comparados ao embasamento teórico para ser possível elaborar uma proposta que atenda a necessidade da empresa objeto de estudo.

3 ANÁLISE DOS RESULTADOS

O artigo em questão busca apresentar os principais desafios contemporâneos para a implantação de uma política de segurança da informação em uma organização de médio porte que está localizada em Boa Vista do Buricá – RS. Diante disso, a análise dos dados coletados na empresa, foi feito por meio de dois questionários, um especial para o gestor e outro para os colaboradores.

O primeiro questionário foi voltado especialmente para o gestor da empresa, contou com perguntas básicas sobre segurança das informações, política de segurança e controle de acesso. O intuito principal dessas perguntas era para levantar informações da empresa em relação a segurança das suas informações, se a mesma se preocupa e segue alguma política e se existe ou já teve algum problema relacionado a perca e roubo de dados.

Já o segundo questionário foi aplicado aos colaboradores, com o intuito de descobrir quais são as percepções em relação a segurança das informações, se isso na opinião deles é importante. E também buscou-se descobrir como é a utilização da comunicação (como o uso das redes sociais, *e-mail*) no ambiente corporativo e se os computadores possuem senhas e se possuem algum tipo de gerenciamento.

3.1 APRESENTAÇÃO DA ORGANIZAÇÃO

A organização situa-se na área industrial do município de Boa Vista do Buricá - RS, atuando no ramo metalmecânico, desenvolvendo projetos e fabricando produtos para grandes empresas nacionais e multinacionais em todo país e para o exterior. A empresa é especializada em manufatura seriada de produtos, na produção de embalagens metálicas, e no desenvolvimento de projetos.

A organização em questão a ser analisada foi fundada em 1998, e no início sua linha de produção era somente de implementos agrícolas. No ano de 2005 iniciou um processo de mudança no ramo de negócios, passou a reformar e fabricar embalagens metálicas. A mudança teve grande sucesso, pois o segmento estava crescendo exponencialmente e acabou tornando-se sua principal linha de produção, tanto é que a empresa está até hoje fabricando embalagens metálicas, racks, containers metálicos, bancadas, carros de movimentação e diversos dispositivos.

Atualmente a organização conta com cerca de 45 funcionários divididos nos diversos setores da produção, escritório e engenharia. A empresa tem à disposição em suas instalações um data center(servidor) contendo o seu sistema de ERP (*Enterprise Resource Planning*) voltado para ao ramo metalmecânico e para o desenvolvimento dos projetos a engenharia trabalha com o software “Creo” que realiza projetos 3D.

3.2 ANÁLISE DA COLETA DE DADOS COM O GESTOR

No mês de setembro de 2019, foi elaborado e aplicado um questionário para o Gestor de Tecnologia da Informação da empresa, a fim de entender o atual modo operante da organização, com o intuito de observar as vulnerabilidades e sugestões de melhorias, aumentando a segurança das informações. A primeira pergunta realizada foi se já possuíam uma Política de Segurança da Informação (PSI), o gestor afirmou que não possuem, sem uma normativa para padronizar determinados aspectos na área da Tecnologia da Informação, em relação ao modo de usar e um padrão mínimo de segurança por meio de senhas. Em outra pergunta realizada, a empresa está interessada em elaborar e implementar uma Política de Segurança da Informação, para maximizar os meios de proteções.

A empresa conta com um gerenciamento parcial de acessos, onde este controle é feito através de senhas, tanto no sistema como no computador em que o funcionário utiliza, ainda neste sentido, quando questionado se havia um padrão pré-estabelecido para a geração de uma senha, afirmou que não. De acordo com Lyra “[...] o usuário que não mantiver a confidencialidade da senha, não evitar o registro da mesma em papéis que não estão guardados em locais seguros, não utilizar senhas de qualidade ou ainda que compartilhe senhas individuais, compromete a segurança da informação.” (LYRA, 2015, p. 47)

Esta pode ser uma vulnerabilidade grande em relação a segurança do sistema, pois qualquer senha inserida será aceita, e assim o invasor através de combinações simples pode obter o acesso e roubar todos os dados da empresa.

Quando questionado sobre a empresa ter um Plano de Continuidade do Negócio (PCN), verificou-se que não possuem um em casos de desastres naturais ou falhas de hardware, deste modo, caso venha acontecer algum sinistro no

departamento de informática ou nos demais, não terão um roteiro a seguir para a restauração parcial ou completa dos serviços, gerando perdas financeiras. Um PCN tem como finalidade, elaborar um roteiro para reestabelecer serviços interrompidos de maneira rápida e eficaz, para Fontes “qualquer evento que potencialmente pode impedir a organização de atingir seus objetivos (operacionais) é uma ameaça”, seguindo esta analogia, qualquer ato que possa interromper as atividades operacionais deve-se ter uma atenção para a correção imediata do problema surgido.

Também em relação a questão sobre um procedimento de Backup dos dados, o gestor informou que existe backup, sendo que atualmente ele é feito de forma diária. Anteriormente esse procedimento era realizado semanalmente, onde acabou por gerar perda de informações e projetos realizados. O Backup diário fornece maior segurança, pois caso ocorra algum problema no sistema responsável por armazenar as informações, o intervalo de tempo entre uma cópia e outra é muito menor, consequentemente a perda de dados também. Conforme Lyra “As atividades que contemplam a contingência são as mais realizadas pelas organizações. A grande maioria das organizações realiza procedimentos de contingência visando garantir que não ocorra perda de informações caso algum desastre ocorra.” (LYRA, 2015, p. 129).

Sobre a questão de vazamento de dados da organização, a resposta obtida foi que até o presente momento não houve nenhuma situação. O Gestor salientou que se preocupa em manter de forma segura todos os dados da empresa e não houve até o momento vazamento de informações onde o funcionário seja responsável. Por mais que não tenha acontecido um vazamento, segundo Brasil “Quando detectada uma violação, é preciso averiguar as causas, consequências e circunstâncias em que ocorreu.” (BRASIL, 2012, p. 14). Pois existem vulnerabilidades, que por mais simples que sejam, podem acarretar grandes perdas financeiras e materiais, pois o sistema pode ser manipulado para induzir ao erro.

3.3 ANÁLISE DOS DADOS COLETADOS COM OS COLABORADORES

No mês de outubro de 2019 foi realizado um questionário para os funcionários. Foi desenvolvido utilizando a ferramenta Forms, onde o Google disponibiliza para o uso e criação de perguntas estruturadas, onde também gera gráficos com as repostas assinaladas, o questionário ficou disponível por cinco (5) dias, e nove (9)

colaboradores responderam, em especialmente os que utilizam computadores para realizar as tarefas diárias.

O questionário foi dividido em três seções, sendo elas: segurança, senhas, computadores e ambiente. No início das perguntas foi abordado o tema segurança da informação, se na percepção deles existe métodos que visam proteger os dados da organização.

Na primeira seção, quando questionados em relação a segurança, as respostas foram positivas, revelando que eles reconhecem que está sendo feita a segurança dos dados que trafegam na intranet da empresa, também reconhecem que é fundamental e necessário realizar a proteção das informações. Para finalizar a primeira seção, quando indagado se possuem o conhecimento de vulnerabilidades física, natural ou em relação aos softwares utilizados, na Ilustração 1, 33,3% afirmaram que há vulnerabilidades físicas onde o servidor está localizado, não havendo um controle de acesso.

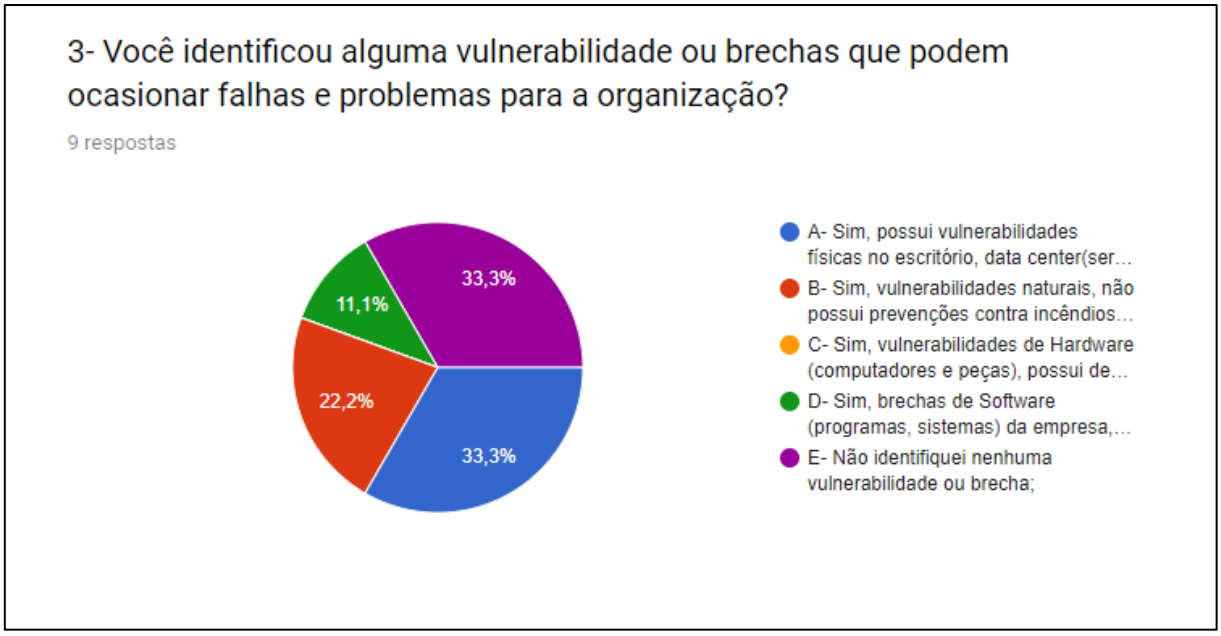

Ilustração 01: Vulnerabilidades e brechas identificadas na empresa pelos funcionários
Fonte: Produção do pesquisador

Falhas físicas onde o servidor fica localizado, aliado a uma falta de controle de acesso, é um grande risco, pois fica desprotegido, onde qualquer pessoa consegue ter acesso, e utilizando-se de meios tecnológicos pode instalar códigos maliciosos para a obtenção de informação. A falha física se não for corrigida pode acabar por

destruir o servidor, e caso não possua um sistema de backup na nuvem, acarretando a perda de todas as informações armazenadas de forma local. Assim como Dantas aponta que:

> As vulnerabilidades físicas dizem respeito aos ambientes em que estão sendo processadas ou gerenciadas as informações. Podem ser: instalações inadequadas; ausência de recursos para combate a incêndio; [...]portas destrancadas; acesso desprotegido às salas de computador; sistema deficiente de combate a incêndio; edifícios mal projetados e mal construídos[...]. (DANTAS, 2011, p. 9)

A segunda seção do questionário, contém quatro perguntas em relação a senhas, com o objetivo de saber como é o padrão utilizado pelos funcionários, se utilizam em ambos os sistemas a mesma senha, questão de compartilhamento e quantidade de caracteres.

Quando indagados sobre a utilização da senha, todos os funcionários afirmaram que utilizam senhas diferentes nos sistemas da empresa, e 66,7% não compartilharam a senha com algum colega de trabalho, o ponto positivo é o fato de utilizarem senhas diferentes, aumentando ainda mais a segurança contra invasores, um ponto negativo é que 33,3% compartilharam a senha ou ainda utilizam a mesma. Em relação a qualidade da senha, 44,4% usam caracteres alfanumérico e letras minúsculas e maiúsculas, este padrão é o correto a seguir, sistemas que tentam invadir sistemas possuem bancos de dados com milhares de senhas salvas, e vão tentando acessar e eliminando as senhas que não estão corretas, este padrão alfanumérico protege de maneira melhor e eficaz. Conforme Moraes “Após prover a identidade ao sistema, o usuário deve fornecer uma senha, frase secreta, certificado, PIN ou algo que ele possua para garantir sua autenticidade.” (MORAES, 2010, p.29)

A terceira seção englobou como é feita a utilização dos computadores fornecidos pela empresa e o ambiente. Quando questionados, ao se ausentar-se da sala se hibernavam o aparelho, conforme a Ilustração 2 55,6% realizam este procedimento e 33,3% nunca. O correto é sempre hibernar o computador, nem todos os funcionários possuem o mesmo nível de permissão para a visualização de determinado conteúdo, ao se ausentar da sala, qualquer indivíduo terá livre acesso a todo e qualquer tipo de dados pertencentes aquele usuário.

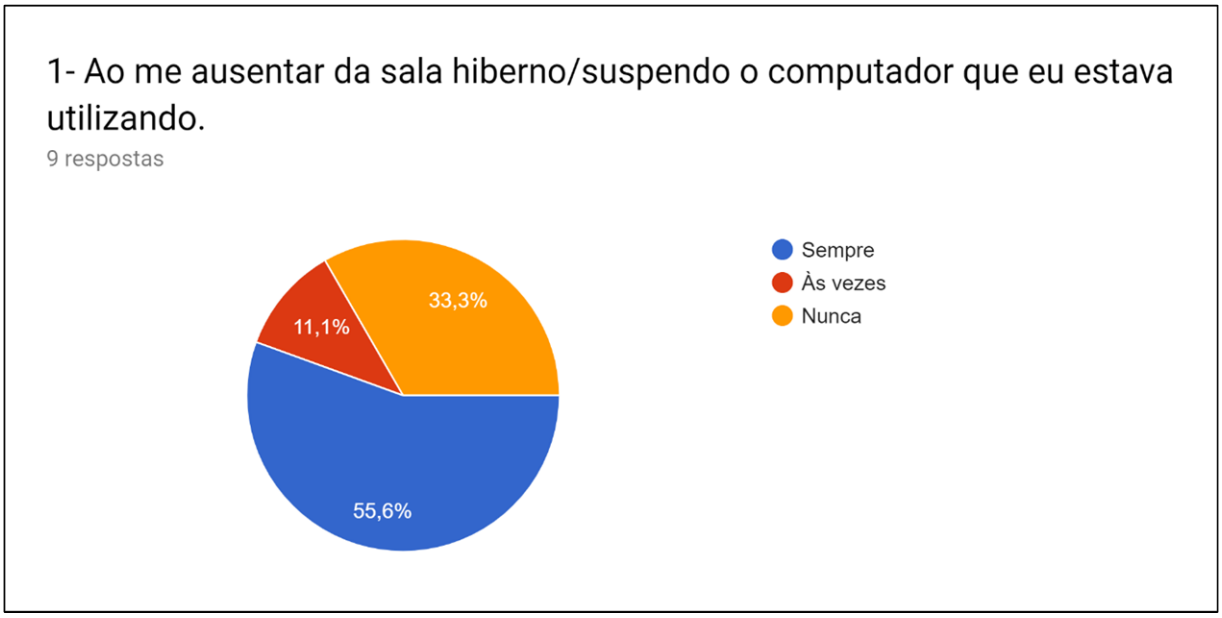

Ilustração 02: Colocar o computador no modo hibernar/suspender
Fonte: Produção do pesquisador

Outro ponto questionado, foi se utilizam as redes sociais no ambiente de trabalho, onde 88,9% responderam que as vezes fazem o uso, ainda, 55,6% realizam o download de arquivos, programas ou músicas através da rede da organização. Em relação ao recebimento de e-mails, apenas 22,2% conferem o formato de arquivo anexado antes de realizar o download do arquivo, e 33,3% responderam que repassam informação dos processos ou funcionários através do telefone.

O uso das redes sociais, somado aos downloads executados durante o expediente, acarreta a lentidão da rede, pois sempre haverá um grande fluxo de dados supérfluos, que não condizem com a operação diária da empresa. Um ponto que expõe a empresa a grandes riscos, são os downloads dos e-mails sem verificar o formato do arquivo, alguns códigos maliciosos são possíveis identificar apenas visualizando o formato. Segundo Moraes “Tornou-se uma prática comum por muitos funcionários o uso indevido da internet para baixar arquivos de vídeo e softwares piratas, como comentado. Esse comportamento tem como consequência, em muitos casos, mais de 70% do tráfego de dados de rede não relacionado com os negócios” (MORAES, 2010, p. 23). Essas condutas inadequadas em uma organização podem trazer muitos problemas, o que necessita uma atenção especial em relação aos usuários da rede corporativa.

3.4 PONTOS E FALHAS OBSERVADOS

As observações feitas da empresa sobre o seu funcionamento, processos e funcionários, foram realizadas por meio de dois questionários, um para o gestor e outro para os funcionários que tem acesso ao computador. Levando em conta o tema e os objetivos propostos, o ponto que mais chamou a atenção é que a organização não conta e nem segue uma política de segurança da informação, e isso pode ser considerado uma vulnerabilidade muito grave, pois com o porte da empresa e quantidade atual dos funcionários que tem acesso as informações da mesma, se faz necessário a implementação de uma política que vise proteger as suas informações.

Atualmente a empresa não possui um controle e gerenciamento de acesso adequado, pois é feito de forma parcial, o que acaba gerando vulnerabilidades e brechas para invasores. É importante ressaltar que a ausência de um gerenciamento de acesso eficaz, coloca em risco toda a segurança da empresa, abrindo espaço as ameaças tanto externas como internas

Por meio do questionário aplicado aos colaboradores observou-se que a organização possui diversas vulnerabilidades físicas e naturais. Mas é importante que a organização não tenha nenhum tipo de vulnerabilidade, pois cada uma delas podem trazer grandes problemas e perdas para a empresa.

Sendo assim, uma vulnerabilidade física, é um ponto fraco presente nas instalações e na infraestrutura tecnológica, o mais ocorrido são as salas onde o servidor se encontra, sem nenhum tipo de controle de acesso e permitindo a entrada e saída de qualquer pessoa, ou ainda, um layout mal estruturado tendo como problemas a má alocação dos equipamentos no ambiente de trabalho. Existem vulnerabilidades naturais (terremoto, furacão, enchente, raios) e estas não podem ser controladas, entretanto, pode-se criar meios com o objetivo de reduzir o impacto e o restabelecimento dos serviços prestados de forma mais rápida e organizada.

Durante a observação, percebeu-se uma grave falha em relação as senhas, não existe nenhum tipo de padrão mínimo aceitável durante a criação, não tem uma quantidade mínima de caracteres que se deve utilizar, fazendo com que, a invasão do sistema possa se tornar mais fácil para o invasor, pois são consideravelmente fáceis de se descobrir, ainda no que tange a criação de senhas, percebeu-se que não é obrigatório o uso de caracteres especiais (números, maiúsculo, minúsculo). Outra

questão, é o compartilhamento de senhas de acesso que ocorrem entre os funcionários, que acabam por saber a senha dos companheiros da organização, e deste modo agravando ainda mais a situação relacionada ao acesso não autorizado a determinado conteúdo.

Foi constatado ainda, que no momento que o funcionário se ausenta da sala, não realiza o procedimento de bloqueio de tela, acarretando o livre acesso por qualquer um presente na organização, ocasionando o rapto de informações ou situações constrangedoras para o proprietário do login.

No que tange a utilização dos computadores no ambiente de trabalho, bem como o acesso à internet, não existe nenhuma política interna regulamentando o uso correto, possibilitando o acesso a qualquer tipo de rede social e e-mail, outro fator prejudicial ao tráfego da intranet, é a possibilidade de realizar downloads de qualquer arquivo. Além de prejudicar o desempenho da rede interna, expõe de forma gravíssima a empresa a obter programas piratas contendo códigos maliciosos, onde acabam prejudicando ou roubando a base de dados.

Devido a empresa não possuir uma Política de Segurança da Informação, não existe qualquer tipo de treinamento ou instrução para a utilização dos equipamentos tecnológicos, deixando para o funcionário utilizar os meios fornecidos pela organização do modo que desejar. A falha presente aqui, é a falta de controle por parte da empregadora, por não possuir nenhum método ativo para realizar a verificação do que está sendo feito em cada usuário registrado no sistema.

3.5 PROPOSTA DE MELHORIAS

Como já apontado no item acima, a organização não segue uma PSI, sendo assim, a proposta de melhorias começa com a criação e a implementação de uma política de segurança da informação, que certamente irá resolver grande parte das falhas e problemas encontrados, fazendo com que o usuário seja o ponto chave, pois é considerado o elo mais fraco quando se fala em segurança das informações.

Para a implementação desta política, seria necessário realizar uma palestra/conversação para proporcionar um melhor entendimento para os colaboradores e em sequência um treinamento sobre o que é segurança das informações, quais são as principais vulnerabilidades e como cada funcionário deve

se portar em relação aos dados da empresa. Dessa forma poderá ser esclarecido as dúvidas sobre a política e os processos que a envolvem, tornando assim uma solução efetiva. Ainda é importante determinar um prazo de implementação entre a direção e os colaboradores para que todas as diretrizes da PSI sejam cumpridas.

Se faz necessário um melhor controle e gerenciamento de acesso aos computadores e softwares disponível na organização, fazendo com que cada colaborador tenha o seu login com senha para a máquina, sistema e e-mail, é claro que para a criação das senhas haja padrão mínimo de pelo menos 9 caracteres e ainda exija uma senha com caractere alfanumérico com caracteres especiais incluindo letras minúsculas e maiúsculas e o ideal ainda é que seja estabelecido um prazo de 6 meses para a troca da senha, ou seja, em alguns dias antes de fechar o prazo o usuários receberá uma mensagem de notificação para lembra-lo que dentro 2 ou 3 dias sua senha expedira e terá que criar uma nova.

É importante ressaltar aos colaboradores, que cada um deve saber dos seus atos e se responsabilizar por qualquer informação vazada da empresa, pois os procedimentos internos de uma organização é de interesse somente dela, sendo assim, cada um deve apresentar uma conduta ética, evitando passar informações internas para familiares e terceiros, caso contrário poderá haver advertências suspensão de três dias ou em casos mais extremos no desligamento do colaborador da empresa.

No que se refere a utilização da rede(internet) da organização, se sugere uma reestruturação completa, começando com a definição das políticas de downloads, proibindo downloads de arquivos (fotos, músicas e jogos) que sejam para uso e benefício próprio. Outro fato que deve ser controlado é o acesso as redes sociais, deve-se restringir o acesso durante expediente e se necessário pode ser feito uma distribuição de banda por endereço “IP”.

Um dos pontos que necessita de uma atenção especial é as vulnerabilidades independente do seu tipo, pois uma vulnerabilidade nada mais é que uma fraqueza ou falha de um processo ou procedimento e que se for explorada permite ao “atacante” acesso a instalações, sistemas e as informações de uma empresa, é claro que o resultado será catastrófico, podendo até levar uma empresa a falência. Nesse sentido, é essencial que a política apresente um tópico/item em suas diretrizes voltada

inteiramente para as vulnerabilidades, orientando a organização a eliminar as mesmas o mais rápido possível.

CONCLUSÃO

Uma Política de Segurança tem o objetivo de manter os meios tecnológicos o mais seguro possível contra ações que podem danificar os equipamentos e o roubo de informações que podem impactar os processos rotineiros de uma organização.

O problema desta pesquisa foi de investigar os desafios contemporâneos para implementação de uma política de segurança da informação de uma metalmecânica de Boa Vista do Buricá. Para isso desenvolveu-se um estudo, que através das análises, foi possível identificar quais eram as necessidades da organização e assim atingir o objetivo geral e elaborar uma política de segurança da informação para a empresa.

Pode-se concluir através do estudo que uma política de segurança da informação envolve diversos aspectos, bem como: informações, dados e todos os processos, ações que acontecem na empresa e sem deixar de lado os colaboradores, que podem ser considerado o aspecto chave, pois são eles que realizam todas as tarefas da empresa e são eles que lidam diretamente com a informação. É importante ressaltar que para se ter um ambiente seguro a implementação da Política de Segurança da Informação é apenas um “passo” inicial e para que ela seja efetiva deve-se ter o comprometimento de todos os colaboradores.

O trabalho identificou diversas falhas e problemas na empresa bem como as fragilidades em seu gerenciamento de acesso, não possuindo um padrão para a criação das senhas, facilitando assim o acesso de invasores. Observou-se que as vulnerabilidades observadas pelos funcionários podem colocar em risco toda a segurança da empresa, pois acabam abrindo espaço para ameaças que podem trazer alto impacto nos processos e funcionamento da organização. Dessa forma o estudo elaborou uma proposta de uma PSI para atender as necessidades da empresa, possibilitando uma medida preventiva para futuros problemas em relação a segurança das informações que circulam na empresa. Conclui-se com este trabalho que o documento que engloba a política de segurança da informação é a base para manter o ativo da informação seguro.

REFERÊNCIAS

ABNT, Associação Brasileira de Normas Técnicas. **NBR ISO 27002:2005:** Tecnologia da informação – Técnicas de Segurança – Código da prática para a gestão da segurança da informação. 2. ed. ABNT, 2005.

BRASIL, Tribunal de Contas da União. **Boas práticas em segurança da informação.** 4. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

CAMPOS, André. **Sistema de Segurança da Informação.** 2. ed. Florianópolis: Visual Books, 2007.

DANTAS, Marcus Leal. **Segurança da informação:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

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

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

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de Segurança da informação:** Guia prático para Elaboração e Implementação. 2. ed. Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.

LACOMBE, Francisco José Masset; HEILBORN, Gilberto Luiz José. **Administração: princípios e tendências.** 2ª Ed. rev. Atualizada. São Paulo: Editora Saraiva, 2008.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de Metodologia Científica**. 7. ed. São Paulo: Atlas, 2010.

LYRA, Mauricio Rocha. **Segurança e auditoria em Sistemas de Informação.** Rio de Janeiro: Editoria Ciência Moderna Ltda, 2008.

LYRA, Mauricio Rocha. **Governança da Segurança da Informação**. Brasília: Edição do autor, 2015.

MORAES, Alexandre Fernandes de. **Segurança em redes: fundamentos.** São Paulo: Érica, 2010.

PERINI, Luis Cláudio. **Administração de sistemas de informação.** São Paulo: Pearson Prentice Hall, 2011.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** uma Visão Executiva. 2 ed. São Paulo: Elsevier, 2014.

ROBBINS, Stephen Paul. **Fundamentos do comportamento organizacional**. Tradução Reynaldo Marcondes. – São Paulo: Pearson Prentice Hall, 2009.

WAGNER, John A. III; HOLLENBECK, John R. **Comportamento organizacional:** criando vantagem competitiva. Tradução Silvio Floreal Antunha. – São Paulo: Saraiva, 2012.

APÊNDICES

APÊNDICE A – Política de Segurança da Informação

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1 ASPECTOS GERAIS

Este documento descreve a Política de Segurança da Informação de uma metalmecânica de médio porte, de Boa Vista do Buricá.

A política define as diretrizes necessárias para garantir a segurança dos bens e serviços que englobam a tecnologia da informação adquiridos, disponibilizados da empresa, a fim de garantir a integridade, confiabilidade, disponibilidade das informações e dos processos internos da organização.

1.1 OBJETIVOS

O objetivo primário dessa política é assegurar a proteção das atividades relacionadas à tecnologia da informação da empresa, visando a criação e o estabelecimento de padrões de segurança da informação.

Outro objetivo é em relação a consciência dos usuários sobre as suas responsabilidades para com a empresa. Alerta-los sobre suas responsabilidades, visando a confiabilidade e sigilo das informações da empresa e ensiná-los o comportamento ético e correto.

1.2 RESPONSABILIDADES

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.

1.2.1 RESPONSABILIDADES DA EMPRESA:

A empresa é responsável por garantir que a política de segurança da informação (PSI) será aplicada e será passada/ensinada para todos os funcionários. É responsabilidade da empresa ter arquivado o termo de responsabilidade e conhecimento da política de segurança assinado pelos colaboradores.

- Cada departamento é responsável pelos os seus dados, devem garantir que estarão seguros sob seu controle e deveram ser guardados em sigilo.
- Estabelecer punições, quando houver descumprimento da política. As punições devem ser clara e devem ser divulgadas para todos os funcionários.
- Definir e manter procedimentos de contingência para os recursos sob sua responsabilidade.

1.2.2 RESPOSABILIDADES DOS USUÁRIOS

- Respeitar e cumprir as determinações da política de segurança

Todos os usuários devem respeitar as regras estabelecidas pela política de segurança. O usuário deve estar ciente que o não cumprimento da mesma, deixara sujeito a punições.

- Manter a salvaguarda os recursos sob sua responsabilidade

Todos os usuários até mesmo o presidente, são responsáveis pela classificação das informações sob sua utilização, zelando assim a manutenção de sua confidencialidade, integridade e disponibilidade.

Cada usuário deve comprometer-se com aquilo que tem acesso, deve manter segura a informação de que lhe é disponibilizada e somente poderá repassá-las para as pessoas que devem ter acesso a essa informação. Garantido que a disseminação desta informação seja apenas a quem necessita.

- Acessar somente os recursos disponíveis a sua Hierarquia

Se um usuário eventualmente tem acesso a uma informação que não pertence ao seu nível hierárquico, não deve alterá-la, copiá-la e nem a repassar mesmo que o responsável por tal autorize, pois todos estamos sujeitos a cometer erros e alterar informações sigilosas sem a intenção.

1.3 NÃO CUMPRIMENTO DA POLÍTICA DE SEGURANÇA

A organização tem o direito tanto administrativo como jurídico de punir os colaboradores que não cumprirem a PSI da empresa. Sendo assim, o não cumprimento da política irá gerar advertência para o funcionário, dependendo da gravidade da ocorrência, pode ocasionar em uma suspensão de três dias ou em casos mais extremos no desligamento do colaborado. Considera-se uma Falta Grave:

- Repassar qualquer informação que de exclusividade da organização, para familiares e terceiros;
- Manipulação de quaisquer tipos de documentos eletrônicos, desviando as informações para um uso próprio ou de terceiros;
- Envolvimento de quaisquer tipos de ataques ao sistema de informação da organização. Não importando o grau de funcionalidade do ataque;
- Obter indevidamente acessos a recursos de qualquer natureza, que não seja de responsabilidade do usuário;
- Instalação de software ou hardware que não seja solicitado e do conhecimento do gestor;

1.4 REVISÕES E ATUALIZAÇÕES DA POLÍTICA

Conforme for surgindo as necessidades de utilização de novos softwares, novos serviços ou até mesmo o surgimento de novas formas de burlar a segurança da empresa, ou sempre que houver algo que gere dúvidas em relação a política de segurança vigente.

É importante manter a PSI sempre atualizada, por isso a revisão deve ser realizada sempre que se fizer necessário, pois suas diretrizes estão ligadas diretamente a segurança dos usuários, dos sistemas e serviços de informação da empresa. Quando houver sugestões de revisão da parte dos usuários, estas devem

ser avaliadas e analisadas pelos responsáveis da política de segurança da informação.

1.5 DIVULGAÇÃO DA POLÍTICA

A divulgação da PSI é obrigação inteiramente da organização e deve ser passada para todos os seus funcionários. Essa divulgação pode ser feita através de uma palestra/conversação e ainda podem ser publicadas cópias nos murais de cada setor.

A divulgação da política deve ser feita de maneira clara e objetiva, para que todos possam compreendê-las.

Todo o novo colaborador assim como os já existentes, devem ler a política e assinar um termo de responsabilidade e de conhecimento da política da empresa a fim de evitar alegações de desconhecimento.

Todas as alterações feita na política de segurança devem ser comunicadas com antecedência de um mês aos usuários para que haja um período de adaptação. Evitando assim, transtornos com os usuários, por isso é importante que a organização antes de lhes impor novas regras é preciso demonstrar-lhes o porquê destas regras, pois muitos não se conformam com aquilo que lhes foi imposto. As alterações podem ser também divulgadas nas conversas e reuniões que ocorrem na organização.

Toda a nova alteração irá gerar um novo termo de responsabilidade e de conhecimento que deverá ser assinado pelos usuários.

2 POLÍTICA DE SENHAS

A senha funciona como uma assinatura digital, identificando o usuário e autorizando serviços conforme a hierarquia. E por isso o usuário não pode repassar sua senha para seus colegas.

- É de responsabilidade do usuário manter sua senha em sigilo, sendo estritamente proibido compartilhá-la para qualquer pessoa.
- Para a criação das senhas, será implementado um padrão mínimo de pelo menos 9 (nove) caracteres e ainda exija uma senha alfanumérica com caracteres especiais incluindo letras minúsculas e maiúsculas;
- Não serão mais permitidas senhas que contenha datas de aniversários, número de telefone, número de documentos ou sequências numéricas ou alfabéticas (abc, 123, qwert, etc.);
- O prazo estabelecido para a troca da senha será 6 meses, alguns dias antes de fechar o prazo o usuário será notificado para lembrá-lo que deverá trocar a senha;
- A senhas do e-mail corporativo e do sistema devem ser distintas;

3 ACESSO Á INTERNET

Inclui-se nesta Política também o uso do tempo e conteúdo acessado pelos usuários, que em horário de expediente devem ser somente em função do trabalho. Sendo assim, não será permitido o uso para fins particulares, deixando claro que esse item é válido durante todo o tempo de permanência do usuário na empresa.

3.1 - Correio Eletrônico (E-MAIL):

- Propriedade: O sistema de correio eletrônico(e-mail) e todas as mensagens que trafegam por ele, incluindo as copias back-up, são consideradas de propriedade da organização.
- Utilização: O sistema de correio eletrônico(e-mail), deve ser utilizado apenas para fins e interesse da empresa.
- Individualização dos Usuários: Todos os usuários da organização devem possuir uma única conta individual no sistema de correio eletrônico(e-mail), a mesma ainda deve ser protegida por senha, e devem ser autenticados quando acessada.

3.1.2 - Restrições:

- Proibido repassar e-mails que contenha informações da organização, brincadeiras, promoções ou até mesmo spam.
- Proibido abrir anexos de natureza desconhecidas, exemplo: .bat, .exe, .src e .com, exceto se tenha sido solicitado pelo gestor.
- Proibido abrir links desconhecidos.
- Proibido o uso do e-mail corporativo para fins pessoais.

3.2 Utilização das Redes Sociais:

- É permitido aos usuários "navegar" na Internet, no entanto, essa "navegação" deve ser para fins coorporativo, tudo que for de interesse pessoal do usuário deve ser acessado ao fim do seu expediente. Bem como jogos, Faceboobk, WhatsApp e demais atividades pessoais também devem ser realizadas fora do horário de trabalho do usuário.

3.3 - Tráfego de Informações:

- Todo e qualquer arquivo ou software obtido por download originado fora da rede, deve-se primeiramente a autorização do gestor e logo após submetido a verificação de vírus antes de ser aberto e executado, mesmo que a origem da fonte seja de natureza "conhecida" da empresa.
- Toda e qualquer informação obtida via Internet deve ser considerada suspeita até ser confirmada sua fonte de informação.

3.4 - Proteção da Informação:

- Toda e qualquer informação considerada sigilosa da empresa não pode ser enviada ou recebida via Internet sem estar devidamente protegida por métodos criptográficos.

4 POLÍTICA DE USO DA ESTAÇÃO DE TRABALHO

- Sempre que se ausentar da sala bloqueie/hiberne seu computador.
- Proibido a instalação de softwares piratas, proibido também downloads de músicas, vídeos, programas entre outros tipos de arquivo, sem a autorização do gestor de TI.
- Não execute arquivos desconhecidos.
- Sempre que for necessário a utilização uma mídia removível, é preciso de uma autorização do gestor e mesma deve passar por uma verificação do antivírus.
- Não utilize o computador de colegas.

5 POLÍTICA SOCIAL

- Não diga sua senha a outros funcionários.
- Evite comentar sobre informações de outros funcionários, como faltas, atrasos ou qualquer informação (processos e problemas) internos da empresa à familiares e terceiros.
- Não faça login em máquinas de terceiros que podem estar logadas na rede da empresa.
- Não aceite ajuda de qualquer outra pessoa, aceite ajuda técnica apenas de colaboradores previamente qualificados.
- Proibido o utilizar a internet para acessar conteúdos impróprios.

Apêndice B – 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 organização. Assumo a responsabilidade de manter a segurança da informação e seguir as diretrizes da política de segurança.

Me comprometo em 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 casos mais extremos o desligamento da empresa.

Boa Vista do Buricá, ____ de _____ de _____.

_____

Assinatura do colaborador