FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Rodolfo Francisco Souza dos Santos

Segurança da Informação

Proteção de dados em ambiente empresarial

Americana, SP.

2018

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Rodolfo Francisco Souza dos Santos

Segurança da Informação

Proteção de dados em ambiente empresarial

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Segurança da Informação, sob a orientação da Profa. Dra. Maria Cristina Aranda.

Área de concentração: Segurança da Informação.

Americana, SP.

2018

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

S238s SANTOS, Rodolfo Francisco Souza dos

Segurança da informação: proteção de dados em ambiente empresarial. / Rodolfo Francisco Souza dos Santos. – Americana, 2018.

48f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Profa. Dra. Maria Cristina Aranda

1 Segurança em sistemas de informação I. ARANDA, Maria Cristina II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Rodolfo Francisco Souza dos Santos

Segurança da Informação

Proteção de dados em ambiente empresarial

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 04 de Dezembro de 2018.

Banca Examinadora:

Maria Cristina Aranda (Presidente)
Doutora
FATEC Americana

José Martins Júnior (Membro)
Doutor
FATEC Americana

Eduardo Antonio Vicentini (Membro)
Mestre
FATEC Americana

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus, pela força e motivação para realização deste projeto, agradeço também a todos os professores que tive o prazer de conhecer na Fatec Americana e adquirir um pouco do conhecimento de cada um deles, em especial minha orientadora Profa. Dra. Maria Cristina Aranda.

Agradeço aos meus familiares pelo apoio e suporte nos momentos em que eu mesmo duvidei de minha capacidade, em especial minha futura esposa Vanessa Rocha Forti.

E por fim agradeço a todas as amizades que pude cultivar ao longo desta incrível jornada.

DEDICATÓRIA

Dedico este trabalho a meus pais, Francisco Brandão dos Santos e Euflosina Inês de Souza Brandão dos Santos, pois sem eles certamente não chegaria onde estou hoje e não me tornaria o ser humano que sou.

Dedico também a minha futura esposa Vanessa Rocha Forti, por acreditar em meu potencial e me dar apoio durante a jornada deste projeto.

Dedico ao meu filho Miguel Francisco Moreira dos Santos, mesmo que ainda jovem, espero que possa alçar voos ainda mais altos do que os meus.

Por ultimo dedico à instituição Fatec Americana, por tornar possível a realização do sonho de conquistar uma formação superior e por todas as historias e experiências conquistadas.

RESUMO

Nos dias atuais a grande preocupação em ambientes que utilizam a Internet, é a proteção *online* dos dados e os riscos a que estão expostos – dados pessoais ou dados bancários exigem uma atenção especial e proteção adequada. Empresas de pequeno e médio porte, por algumas vezes podem se descuidar da proteção que seria ideal, sem se atentar que os dados que circulam em suas redes, contendo informações sigilosas de clientes, fornecedores e da própria organização, que em mãos erradas podem gerar grande risco ao desenvolvimento estratégico, à continuidade dos negócios e prejuízos financeiros. Esta pesquisa buscou abordar a importância da segurança dos dados dentro de empresas, sendo *online* ou em ambiente de rede interna, onde muitas vezes não são utilizados os recursos disponíveis da forma mais adequada, o que pode gerar riscos e prejuízos. Foi exposta também a importância de preparação do fator humano na manipulação e segurança dos dados, sendo este passível de vulnerabilidade se não estiver devidamente instruído e orientado. Discutiram-se os métodos e tecnologias existentes para se realizar a segurança destes tipos de ambientes de modo geral e também a quais riscos devem ter atenção, atribuindo a um estudo de caso que abordou um cenário realista de como tudo isso pode ter ocorrido.

Palavras Chave: Segurança de informação, proteção de dados empresariais.

ABSTRACT

Nowadays the major concern in using the Internet is the online protection of data and the risks to which they are exposed - personal data or bank data require special attention and adequate protection. Small and mid-sized companies by can sometimes neglecting the protection that would be ideal, without heed to the data circulating on their networks containing sensitive information of your customers, suppliers and the Organization itself, which in the wrong hands can lead to great risk to strategic development, the business continuity and financial losses. This research sought to address the importance of data security in companies being online or in internal network environment, where they are often not used the resources available in the most appropriate way what can generate risks and losses. Was exposed to the importance of preparing the human factor in handling and security of data, this being subject to vulnerability if not properly instructed and guided. Also discussed the methods and existing technologies to perform the safety of these types of environments in general and also what risks should be attentive assigning a case study which addressed a realistic scenario of how it may have occurred.

Keywords: Information security, companies' data protection.

SUMÁRIO

LISTA DE FIGURAS E DE TABELAS

Figuras

Tabelas

1. INTRODUÇÃO

Nos dias atuais é comum ouvir e falar a respeito da tecnologia da informação devido seu grande crescimento ao decorrer dos últimos anos. O uso da Internet se tornou mais acessível através dos celulares *smartphones,* notebook e demais aparelhos portáteis que utilizam de uma rede móvel ou sinal de wi-fi para se conectar.

Junto a essa crescente utilização, houve um significativo aumento do fluxo de dados trafegados pelo mundo, e os riscos a que os usuários estão expostos também. A partir destes riscos existentes, se fez de grande necessidade adotar medidas preventivas e corretivas para proteção dos dados pessoais e para uma navegação na Internet mais segura, e para suprir esta necessidade surge a Segurança da Informação.

"A segurança da informação diz respeito à proteção de determinados dados, com a intenção de preservar seus respectivos valores para uma organização (empresa) ou um indivíduo." (KERDNA)[1], através desta afirmação é possível verificar a importância de adotar metodologias de segurança dentro do âmbito da informática, não somente para usuários comuns, mas também para empresas e organizações.

Uma empresa, mesmo sendo de pequeno ou médio porte, deve se alertar para os riscos a quê está exposta caso não disponibilize um sistema de gestão de segurança da informação (SGSI) e/ou uma boa política de segurança implementada em seus domínios, pois o comprometimento dos dados trafegados em sua rede pode gerar prejuízos financeiros e administrativos.

Além de um sistema e uma rede protegida, há a necessidade de uma boa orientação aos colaboradores da empresa, que serão os usuários a manipular os dados que trafegam pela rede da organização, de acordo com Filho (2018) "41% dos incidentes de segurança no Brasil têm origem nos próprios colaboradores da empresa, acima da média mundial que é de 35%. [...] somente 3% dos usuários são capazes de identificar um ataque de *phishing*", através dos números desta pesquisa é possível ter uma melhor noção da real importância nesta orientação aos funcionários.

[1] Disponível em < http://seguranca-da-informacao.info/ >. Acesso em: 10 Nov. 2018.

Justifica-se o desenvolvimento desta pesquisa a partir da importância e da necessidade de uma melhor proteção aos dados em ambientes empresariais.

O **problema** que se busca responder é: Quais os riscos que um ambiente empresarial está exposto e quais as metodologias e tecnologias disponíveis para proteção e como aplica-las de forma coerente e efetiva?

O **objetivo geral** é apresentar através de um estudo básico, o que é a segurança da informação, proteção de dados e os riscos e ameaças que um ambiente empresarial está exposto. Os **objetivos específicos** serão focados em expor as metodologias e recursos disponíveis dentro da segurança da informação para a proteção de dados, a preparação do fator humano através da conscientização dos riscos e ameaças que podem ocorrer dentro da empresa e na Internet em geral.

A **Metodologia** utilizada para este projeto será a de Pesquisa Bibliográfica do tipo Descritiva, sendo essa conceituada por Bertucci (2009) como aquela que “tem como objetivo primordial a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis”. E por fim será utilizada a técnica de Estudo de Caso que, segundo Bertucci (2009) é aquele que se “caracteriza como um tipo de pesquisa cujo objeto é uma unidade que se analisa profundamente e visa ao exame detalhado de um ambiente, de um simples sujeito ou de uma situação em particular”.

O trabalho foi estruturado em seis capítulos, sendo que o primeiro – esta Introdução - apresenta o tema da pesquisa; O capítulo segundo realizará um breve estudo e buscará conceituar os princípios básicos da Segurança da Informação; O capítulo terceiro abordará quais os riscos e ameaças existentes a que um ambiente empresarial possa estar exposto; O capítulo quarto buscará apresentar os tipos de controles e mecanismos existentes para a proteção de dados; No capítulo quinto será realizado um Estudo de Caso onde se buscará apresentar um ambiente real de uma empresa e sua rede de dados, de forma a aplicar os conceitos de proteção levantados durante a pesquisa; E o capítulo sexto trará as considerações finais, expondo os resultados obtidos pela pesquisa e pelo estudo de caso realizado.

2. SEGURANÇA DA INFORMAÇÃO

2.1. INFORMAÇÃO

Peixoto (2006) define informação como o ato ou o efeito de informar ou informar-se, um conjunto de conhecimentos sobre algo ou alguém, podendo ser transmitido e mantido através de um código e a informação "[...] representa a inteligência competitiva dos negócios e, é reconhecida como ativo crítico para a continuidade operacional da empresa.".

Setzer (2015) ainda define a Informação como "uma abstração informal que está na mente de alguém, representando algo significativo para essa pessoa." Sendo assim, ela é processada ou criada através de dados, e pode ser representada através deles.

Dado, de acordo com Setzer (2015) é:

> [...] uma sequência de símbolos quantificados ou quantificáveis. Portanto, um texto é um dado. De fato, as letras são símbolos quantificados, já que o alfabeto, sendo um conjunto finito, pode por si só constituir uma base numérica (...). Também são dados fotos, figuras, sons gravados e animação, pois todos podem ser quantificados a ponto de se ter eventualmente dificuldade de distinguir a sua reprodução, a partir da representação quantificada, com o original. É muito importante notar-se que, mesmo se incompreensível para o leitor, qualquer texto constitui um dado ou uma sequência de dados.

A relação entre esses dois conceitos e a tecnologia da informação reside no fato que o centro de qualquer negócio está em armazenar, interpretar e utilizar dados e informações oriundas desses dados para o sucesso e prosperidade. Entretanto, mesmo com a reconhecida importância desses dois ativos dentro de qualquer organização, estudos recentes mostram que as empresas não estão preparadas para garantir a segurança e privacidade de seus dados.

2.2. A SEGURANÇA DA INFORMAÇÃO

“Segurança tem início e termina nas pessoas.”. (FONSECA, 2009).

Sêmola (2003) define segurança da informação como “[...] uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

Já Silva Netto e Silveira (2007), definem a segurança da informação como: “[...] o processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade”.

A informação pode ser compreendida como qualquer conjunto de dados, que possuí valores seja para uma pessoa ou organização. Com os avanços tecnológicos e utilização de sistemas, essas informações ficam disponíveis e muitas vezes acessíveis, o que as deixam vulneráveis, comprometendo e ameaçando a integridade de ambas. (ABNT, 2005).

Nesse contexto, a segurança da informação se torna imprescindível, pois através dela que se garante a integridade dos dados, evitando o acesso não permitido e vazamento de informações sigilosas.

De acordo com Lima (2011), segurança da informação é definida como preservação da confidencialidade, da integridade e da disponibilidade da informação, adicionalmente, outras prioridades, como, autenticidade, responsabilidade e confiabilidade da informação.

Peixoto (2006) define como: “O termo segurança da informação pode ser designado como uma área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade”.

OS PILARES DA SEGURANÇA DA INFORMAÇÃO

Segundo Peixoto (2006) a segurança da informação é formada pelos seguintes pilares básicos, que podem ser definidos da seguinte maneira:

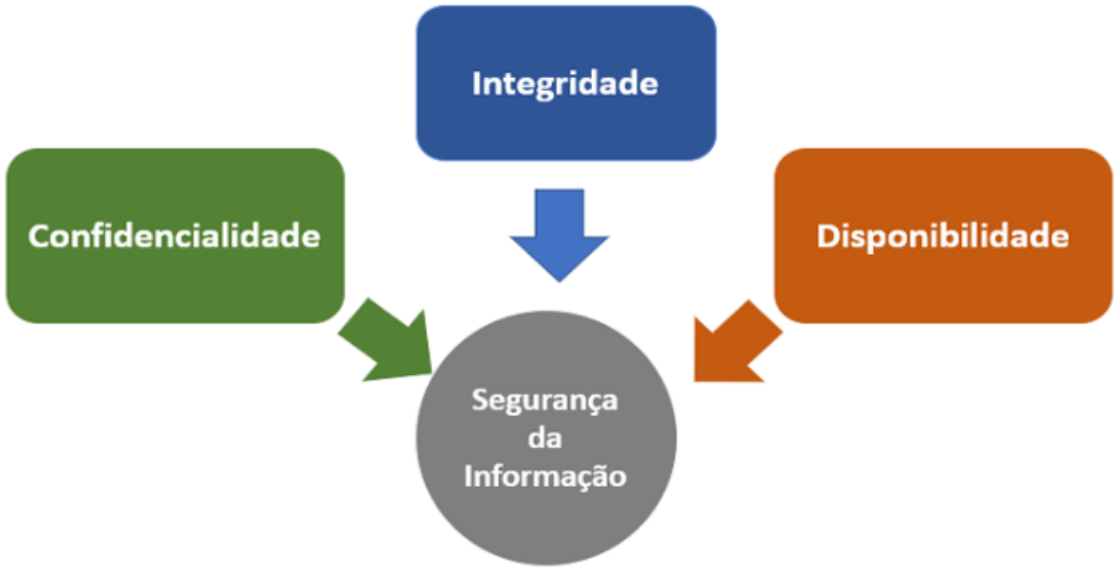
> **Confidencialidade**: é a garantia de que as informações transmitidas chegarão ao seu destino sem que se dissipem para outro lugar onde não deveria passar. Várias tecnologias como, por exemplo,

criptografia e autenticações podem ser usadas, desde que mantenham a integridade das informações;

Integridade: é a garantia de que as informações não sofreram nenhuma modificação durante o trajeto entre a pessoa que enviou e a pessoa que recebeu a informação, garantindo assim a sua real veracidade após chegarem ao destino;

Disponibilidade: De nada adianta possuir integridade e confidencialidade, se a informação nunca está disponível. Então, o grande desafio é manter essa estrutura de passagem de informações de forma confiável e integra sem que haja impossibilidade de captar as informações.

Figura 1: Princípios básicos da segurança da informação.



Fonte: Techtem[2]

É importante ressaltar, que além desses três principais atributos, aplicam-se na segurança da informação, o não repúdio, autenticidade e a privacidade. (STONEBURNER, 2001).

O não repúdio ou irretratabilidade pode ser definido como a junção de autenticidade com integridade, pois visa garantir a informação origem de forma que seja mantida e não comprometida em nenhum processo, se mantendo dessa forma, autêntica.

Segundo Stoneburner (2001), a segurança é obtida somente através da relação e correta implementação de quatro princípios da segurança, confidencialidade, integridade, disponibilidade e auditoria.

[2] Disponível em: <https://www.techtem.com.br/principios-basicos-da-seguranca-da-informacao>. Acesso em: 22 Ago. 2018.

A auditoria consiste em analisar de que forma os recursos computacionais estão sendo utilizados, quem esta usando, quando, e as alterações realizadas (GUIMARÃES, 2008).

Esses atributos são primordiais na segurança da informação, pois através deles que é orientado a análise, planejamento e implementação da segurança em um determinado conjunto de dados para um determinado usuário ou organização.

A informação pode se tornar vulnerável no ambiente de trabalho devido a muitos fatores como, por exemplo, o mau comportamento de usuários e até mesmo devido às falhas na estrutura estabelecida pela organização, entre muitos outros. Com isso é muito importante que seja estabelecido níveis de segurança na corporação e que a estrutura de segurança aplicada na mesma seja bem planejada, estabelecida e cumprida.

AS CAMADAS DE SEGURANÇA DA INFORMAÇÃO.

De acordo com Sêmola (2003) todos os tipos de tentativas de ataque que visam se aproveitar de brechas na segurança de uma empresa e são então exploradas, desde os ativos físicos e tecnológicos até os recursos humanos e a quebra de segurança, poderá se tornar uma possível ameaça.

Segundo Silva Netto e Silveira (2007), “as ameaças do mundo digital espelham as ameaças no mundo físico. Se o desfalque é uma ameaça, então o desfalque digital também é uma ameaça. Se os bancos físicos são roubados, então os bancos digitais serão roubados.”, com isso, pode-se entender o fato de que, os crimes que são cometidos no mundo físico, podem também ser cometidos no mundo digital, como por exemplo: fraude, exploração, trapaça, roubo, vandalismo, extorsão, etc.

Sêmola (2003), visando à gestão da segurança da informação, faz a classificação em três aspectos: físicos, tecnológicos e humanos, sendo que as empresas tem uma maior preocupação com os aspectos tecnológicos (computadores, redes, internet, vírus) e de quebra acabam dando menos importância para os aspectos físicos e humanos, que também têm uma alta relevância para a segurança da empresa quanto os tecnológicos.

2.3. NORMAS DE SEGURANÇA E REGULAMENTAÇÃO

Segundo Silva Netto e Silveira (2007), as normas servem para realizar a definição de critérios, princípios e regras, que visam padronizar e registrar as boas práticas, que irão funcionar como medidores para qualidades de serviços, produtos e processos. Os autores explicam de forma sintética:

> "Devido ao interesse internacional em uma norma de segurança da informação, em dezembro de 2000, foi publicada a norma internacional ISO 17799:2000. Em 2001, a Associação Brasileira de Normas Técnicas, (ABNT) publicou a versão brasileira que ficou com a denominação de NBR/ISO 17799 – Código de Prática para a Gestão da Segurança da Informação (OLIVA e OLIVEIRA, 2003). Em setembro de 2005, a norma foi revisada e publicada como NBR ISO/IEC 17799:2005. (ISO 17799, 2005). Segundo Holanda (2006), o comitê que trata da segurança da informação na ISO aprovou a criação de uma família de normas sobre gestão da segurança da informação, batizada pela série 27000, onde a então ISO/IEC 17799:2005 foi rebatizada por ISO IEC 27002:2005. A norma define 127 controles que compõem o escopo do Sistema de Gestão de Segurança da Informação (Information Security Management System – ISMS), agrupados em 11 seções de controles: Política de Segurança da Informação; Organização da Segurança da Informação; Gestão de Ativos; Segurança em Recursos Humanos; Segurança Física e do Ambiente; Gestão das Operações e Comunicações; Controle de Acesso; Aquisição, Desenvolvimento e Manutenção dos Sistemas de Informação; Gestão de Incidentes da Segurança da Informação; Gestão da Continuidade do Negócio e Conformidade." (SILVA NETTO; SILVEIRA, 2007).

De acordo com as normas da ABNT (2005), são abordados requisitos de gestão da segurança para que seja adotada na empresa, entre elas estão a ISO 27001 e 27002, certificação para a organização e para o profissional respectivamente. O ideal é que as duas sejam solicitadas e utilizadas em conjunto em uma organização, empresa se manterá capacitada e atendendo as normas, e com profissionais capacitados para manter a organização e política de segurança.

- **ISO 27001**

Norma internacional que define os requisitos para Sistemas de Gestão de Segurança da Informação (SGSI). Auxilia a empresa a aplicar um sistema de segurança da informação que permita reduzir os riscos de segurança e adequar os atributos da norma para a empresa construir assim um sistema seguro e com uma política definida em relação à proteção de dados e a rede no geral. Pode-se listar então, alguns benefícios da norma, como:

- ✓ Diminuir o risco de responsabilidade pela não implementação ou determinação de políticas e procedimentos;
- ✓ Identificar e corrigir pontos fracos;
- ✓ Direcionamento de responsabilidade pela segurança da informação;
- ✓ Oferece maior confiança aos parceiros comerciais, partes interessadas, e clientes;
- ✓ Maior conscientização sobre Segurança da Informação;
- ✓ Combinar recursos com outros Sistemas de Gestão;
- ✓ Métodos e mecanismos para verificar sucesso do sistema.

Sendo assim, esses benefícios apresentados a partir da estrutura da norma:

- ✓ Introdução;
- ✓ Objetivo;
- ✓ Referência normativa;
- ✓ Termos e Definições;
- ✓ Sistema de Gestão da Segurança da Informação (SGSI);
- ✓ Responsabilidade da direção;
- ✓ Auditorias internas;
- ✓ Análise crítica;
- ✓ Melhoria do Sistema de Gestão da Segurança da Informação.

A certificação ISO 27001 é apenas empresarial, podendo ser certificada somente a organização e não profissionais, para isso a empresa é submetida à regulamentação das normas e auditada para receber o certificado.

- **ISO 27002**

É recomendável que a ISO 27001 seja utilizada em conjunto com a ISO 27002, pois é um conjunto de práticas com um conjunto completo de controles que auxiliam aplicação e utilização de um Sistema de Gestão da Segurança da Informação, facilitando atingir objetivos especificados pela norma ISO 27001.

A ISO 27002 é um conjunto de controles baseados nas melhores práticas para a segurança da informação. Ela não deve ser utilizada em auditorias, mas simplesmente servir como um guia.

Ao contrário da ISO 27001, a certificação para a ISO 27002 pode ser realizada somente por profissionais.

Silva Netto e Silveira (2007) apresentam, conforme a Tabela 1, as seções da norma divididas nas três camadas da segurança da informação:

Tabela 1: Camadas x Seções da segurança da informação.

CAMADA	SEÇÃO	OBJETIVOS
Física	Gestão das operações e comunicações.	Garantir a operação segura e correta dos recursos de processamento da informação.
	Segurança física e do ambiente.	Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização; impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.
	Controle de acesso.	Controlar acesso à informação; assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação; prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação; prevenir acesso não autorizado aos serviços da rede.
	Gestão de incidentes de segurança da informação.	Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes da segurança da informação.
Lógica	Aquisição, desenvolvimento e manutenção de Sistemas de Informação.	Garantir que segurança é parte integrante de sistemas de informação; prevenir a ocorrência de erros, perdas, modificação não autorizada ou mal uso de informações em aplicações; proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos; Garantir a segurança de arquivos de sistema; manter a segurança de sistemas aplicativos e da informação.
Humana	Organizando a segurança da informação.	Gerenciar a segurança de informação dentro da organização; manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas.
	Gestão de Ativos.	Alcançar e manter a proteção adequada

		dos ativos da organização; assegurar que a informação receba um nível adequado de proteção.
	Segurança em recursos humanos.	Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis e reduzir o risco de roubos, fraudes ou mau uso de recursos.
	Gestão da continuidade do negócio.	Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil se for o caso.
	Conformidade.	Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.
	Política de segurança da informação.	Prover 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.

Fonte: Adaptado de Silva Netto e Silveira (2007).

A ISO/IEC 27002:2005 possui diversas seções onde suas características se encaixam dentro das três camadas de segurança da informação (física, lógica e humana). Buscou-se classificar neste trabalho a seção pela camada que melhor apresentasse a maioria dos controles de cada uma delas.

3. RISCOS E AMEAÇAS NO AMBIENTE EMPRESARIAL

Em todos os tipos de negócios existem riscos e ameaças, e com a tecnologia da informação não seria diferente; conforme a tecnologia se aprimora e avança. Praticamente tudo hoje é feito *online* e dados são armazenados em computadores e dispositivos móveis, tais como *tablets* ou celulares, ou ainda em nuvem, tendência que domina o mercado atualmente. Proteger dados pessoais requer mais cuidado e atenção por parte dos usuários, cuidados estes que muitas vezes não são observados por colaboradores de empresas.

Em Segurança da Informação, são inúmeros os riscos e ameaças possíveis, busca-se então nesta pesquisa dividi-los entre riscos físicos e lógicos.

3.1. RISCOS FÍSICOS

FATOR HUMANO

Segundo Alves (2010) um dos maiores problemas na segurança da informação é o ser humano e sua ignorância.

De acordo com Pinto (2014), em um estudo realizado pela Cisco em 2014, foi possível verificar que toda a região da Europa, Ásia e Rússia estavam em risco por que as empresas se preocupam mais com os riscos externos a elas (ataques cibernéticos) do que com as ameaças internas. Ainda segundo este estudo, o comportamento dos colaboradores é também um fator crítico à segurança dos dados, pois é uma brecha causada pela condescendência ou pelo desconhecimento; os colaboradores creem que os mecanismos de segurança protegem totalmente suas atividades *online*.

O que arremete a afirmativa de Alves (2010) “Práticas que permitem o acesso não autorizado a dados, lugares, objetos e entre outros, fragiliza qualquer esquema de segurança da informação, uma vez que as pessoas acabam tendo acesso a informações indevidas, colocando em risco a segurança da informação.”, o autor completa sua visão concluindo que “a questão comportamental pode afetar significativamente as demais medidas de segurança, por mais modernas que elas sejam.”.

Assi (2011) reforça a ideia de que os colaboradores são a vulnerabilidade final, vulnerabilidade esta que é explorada pelos *hackers* ou *crackers*. *E-mails* fraudulentos, uma propaganda enganosa que seja clicada por acidente, já abrirá uma porta na rede da empresa para acesso indevido. Em seu artigo ele exemplifica a ameaça exposta:

> "Um exemplo disso ocorreu em março na RSA, a divisão de segurança da EMC Corp, companhia americana de armazenamento de dados cujos equipamentos e serviços são usados por milhares de outras empresas. Um *hacker* enviou *e-mails* para dois pequenos grupos de funcionários que pareciam bastante inocentes, incluindo uma planilha intitulada "plano de recrutamento 2011". A mensagem foi tão convincente que um empregado recuperou a mensagem da pasta de "lixo eletrônico" e, em seguida, abriu o anexo. Ao fazê-lo, introduziu um vírus na rede da RSA, que acabou por dar aos *hackers* acesso a dados confidenciais da empresa, e permitiu que mais tarde os ataques contra clientes da RSA acontecessem.".

De acordo com estudo publicado por Gonçalves (2003), os *hackers* e *crackers*, são classes de especialistas em informática que invadem um sistema alheio de forma ilegal, a fim de obter vantagens financeiras ou realizar fraudes através das informações acessadas. A CERT.BR (2017) faz o alerta de que, um dos tipos de ataques mais usados por esses indivíduos é a utilização do *ransomware,* um tipo de *malware* que ao infectar arquivos, ele os criptografam e sequestram estes dados, para posteriormente solicitar um resgate financeiro ao proprietário legal das informações para que somente desta forma possam ser devolvidas.

ACESSO NÃO AUTORIZADO

Esta é uma conhecida forma de realizar furto ou a corrupção de dados: o acesso deliberado, sem controle ou supervisão adequada à *datacenters* e/ou sala de servidores, por exemplo, pode comprometer toda a estrutura de dados, rede e sistemas de uma empresa. É necessário que se tenha um controle especial das pessoas que acessam determinados locais, que possam gerar risco de prejuízo para empresa com o vazamento de informações ou o uso mal intencionado delas.

Mas infelizmente, não basta somente ter uma portaria e identificação física; também é necessário que todo o pessoal esteja sintonizado com os princípios da Segurança da Informação, conforme Campos (2007):

> "Apesar de todos os cuidados em se definir os perímetros de segurança, essa ação não produzira resultados positivos se os colaboradores não estiverem sintonizados com a cultura de segurança da informação. Essa cultura deve estar pulverizada em toda a organização e especialmente consolidada dentro das áreas críticas de segurança. A informação pertinente ao trabalho dentro dessas áreas deve estar restrita a própria área e somente durante a execução das atividades em que ela se torna necessária. Essas atividades sempre deverão ser realizadas sob supervisão para garantir a segurança. Quando houver atividade, essas áreas devem permanecer fechadas de forma validável, como, por exemplo, através do uso de lacres de segurança, e supervisionadas regularmente."

De certa forma, este tópico também engloba a questão do comportamento dos colaboradores.

3.2. RISCOS LÓGICOS

Os riscos lógicos estão diretamente ligados à parte de *software* do ambiente de TI, e é possível destacar alguns que dentro de um ambiente empresarial podem se tornar os principais riscos à segurança da informação:

SENHAS

De acordo com o CERT.BR (2017) pode-se definir que:

> "Uma senha, ou *password*, serve para autenticar uma conta, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. É um dos principais mecanismos de autenticação usados na Internet devido, principalmente, a simplicidade que possui."

As senhas representam um problema quando são fracas; como há uma grande necessidade (em número e em urgência) de criar novas senhas, principalmente para uso de aplicações dentro das empresas, muitos preferem a criação de senhas fracas ou fáceis de lembrar, o que deixa o sistema vulnerável a ataques. Ainda segundo o instituto, uma senha fraca possibilita invasores a:

> "[...] acessar a sua conta de correio eletrônico e ler seus e-mails, enviar mensagens de *spam* e/ou contendo *phishing* e códigos maliciosos, acessar o seu computador e obter informações sensíveis nele armazenadas, como senhas e números de cartões de crédito; utilizar o seu computador para esconder a real identidade desta pessoa (o invasor) e, então, desferir ataques contra computadores de terceiros [...]" (CERT.BR, 2017).

Uma forma de evitar que sejam criadas senhas fracas, a empresa pode determinar uma série de regras que devem ser observadas e seguidas, do contrário, a senha não será aceita.

VÍRUS, *PENDRIVES* E ATAQUES VIRTUAIS.

Intimamente ligado com os dispositivos externos/móveis (tais como *pendrive*, CD, DVD, cartão de memória, HD externo), os vírus ou *malwares* têm crescido e com isso, os ataques às redes corporativas também. Um estudo realizado pela Kaspersky Lab (2013) mostra que 91% das organizações sofrem algum tipo de ataque cibernético em um período de 12 meses, e este é um número alarmante.

Grande parte dos ataques se deve às vulnerabilidades expostas acima, mas também ao uso crescente de dispositivos de armazenamento móveis, e ao aumento dos números de vírus existentes que infectam esses tipos de dispositivos. Ainda segundo este estudo, a maioria dos ataques visava o furto de informações e também foram identificados ataques contra colaboradores; abaixo, segue um resumo dos objetivos identificados ao longo do ano de 2013 pela Kaspersky Lab (2013):

> "Grupos de criminosos virtuais terceirizados realizaram operações que, em geral, visavam roubar informações. Outros ataques foram baseados em sabotagem – o uso de programas maliciosos para limpar dados ou bloquear operações de infraestrutura. Alguns cavalos de Tróia especiais foram capazes de roubar dinheiro por meio de sistemas de bancos *online*. Os criminosos virtuais também conseguiram comprometer *sites* corporativos e redirecionar seus visitantes para recursos maliciosos, prejudicando a reputação da empresa. Prejuízos financeiros foram causados por ataques DDoS, que podem desativar os recursos da *web* voltados para o público de uma empresa por vários dias. Os clientes começam a procurar companhias mais confiáveis, o que resulta em perdas financeiras de longo prazo."

Pinto (2014) informa que através de uma pesquisa realizada pela TIC Microempresas no Brasil, foi possível verificar em um período de três anos aumentarem de 39% para 48% o número de microempresas que sofreram ataques por vírus.

Teixeira (2018) alerta para outro número preocupante revelado por pesquisa realizada pela Kaspersky, informando que por ano a taxa de ataques por *malwares* no Brasil cresce em 60%. A pesquisa também revelou os crimes que ocorreram com mais frequência no Brasil no ano de 2017:

> “53% dos crimes envolviam ter aparelhos infectados por vírus ou outras ameaças de segurança. 34% envolviam senhas de contas *on-line* descobertas. 34% fizeram compras *on-line* que eram na verdade golpes. 32% clicaram em *e-mails* fraudulentos, ou enviaram informações sigilosas em resposta a *e-mails* fraudulentos.” (KASPERSKY, 2017).

Grandes empresas, devido ao maior poder aquisitivo, podem dispor de um setor específico para os cuidados de segurança da informação e utilizar *softwares* de licença paga, que em sua maioria fornece melhores recursos para defesa do sistema. Já em pequenas empresas isso pode não ocorrer com tamanha frequência, além de algumas sequer contar com *softwares* gratuitos, devido à falta de conhecimento e despreparo no assunto.

4. CONTROLES E MECANISMOS DE SEGURANÇA

De acordo com as normas da ISO/IEC 27002 (2005), os mecanismos e controles de acesso buscam através de sua aplicação executar os princípios de maior importância na Segurança da Informação, utilizando metodologias de defesa e proteção para o ambiente de dados.

Segundo Rainer e Cegielski (2015) os **controles de acesso físico** buscam proteger e evitar o acesso indesejado de indivíduos não autorizados aos locais onde se encontram os computadores ou equipamentos de maior importância dentro da empresa. Dentre os controles físicos existentes, os que mais se destacam são: paredes, portas, trancas, sistemas de alarmes, câmeras de vigilância, crachá com foto para identificação, leitores biométricos (impressão digital, voz, íris), guardas de segurança.

A Telium Networks (2016) diz que "Os **controles de acesso lógicos** são qualquer tipo de aplicação ou equipamento que usa a tecnologia para impedir que pessoas acessem documentos, dados ou qualquer tipo de informação sem a autorização adequada.". Os mecanismos dentro deste controle utilizam-se em sua maioria de *softwares* e/ou sistemas para a proteção ou combate aos riscos que os dados possam estar expostos, os mais comuns são antivírus, *firewall* e as senhas.

4.1. AUTENTICAÇÃO

"Autenticação determina a identidade da pessoa pedindo acesso." (RAINER; CEGIELSKI, 2015), ou seja, é o processo onde se confirma que a pessoa que está tentando acessar o local ou sistema é realmente ela mesma. No acesso físico o processo de autenticação pode ser realizado através de crachás de uso pessoal com foto e/ou chip de segurança que irá destravar uma tranca ou catraca, leitores biométricos que contam com uma tecnologia mais avançada onde é praticamente impossível se passar por outra pessoa na tentativa de um acesso ilegal.

Para o acesso lógico o processo de autenticação mais conhecido é a senha. As senhas são vinculadas a um usuário, e para que haja uma maior segurança e confiabilidade dos dados manipulados, ela deve pertencer a uma única pessoa.

"A senha é o recurso mais utilizado em função da facilidade de construção, [...] e do bom nível de segurança que se pode alcançar." (FONTES, 2017). As senhas devem ser de caráter pessoal e intransferível, e na criação de uma senha os

usuários precisam ser orientados a levar em consideração a utilização de técnicas que dificultam a sua quebra ou descoberta, como por exemplo: uso de letras maiúsculas e minúsculas, caracteres alfanuméricos e símbolos/caracteres especiais, tendo uma extensão mínima de 10 caracteres. Não são recomendadas senhas que utilizem informações vinculadas à vida pessoal do usuário, como por exemplo: datas especiais para a pessoa, nome do animal de estimação, apelidos, nome de um integrante da família, pois a probabilidade de que a senha possa ser quebrada ou descoberta por alguém mal intencionado e que conheça um pouco sobre a vida do usuário, pode aumentar significativamente.

Além das senhas, com o crescimento da necessidade de uma maior segurança no ambiente de dados, outro recurso muito utilizado são as assinaturas digitais e certificados digitais, que, segundo Menke (2003) “servem para agregar os valores confiança e segurança às comunicações e negócios veiculados em ambiente virtual, especialmente na Internet.”, sendo assim as assinaturas digitais utilizam técnicas de criptografia assimétricas e os certificados digitais utilizam técnicas de criptografia simétricas.

4.2. CRIPTOGRAFIA

A Strong Security (2018) conceitua a criptografia como “um conjunto de técnicas desenvolvidas com o objetivo de proteger a informação”. A criptografia de dados dentro de uma rede empresarial irá buscar proteger as informações sigilosas caso algum invasor acesse o sistema indevidamente, evitando que as informações obtidas possam ser lidas diretamente e utilizadas para prejudicar a empresa.

De acordo com a CERT.br (2017) as técnicas de criptografia mais conhecidas atualmente utilizam o mecanismo de chaves criptográficas, que utilizam uma chave de codificação através de um algoritmo para transformar o texto dos dados originais em uma informação sem sentido enquanto trafegam na rede, e somente o receptor que tem a chave correta irá conseguir decodificar os dados e acessar as informações originais. Essas chaves podem ser divididas entre Chaves Simétricas e Chaves Assimétricas, onde cada uma utiliza um método de criptografia diferente:

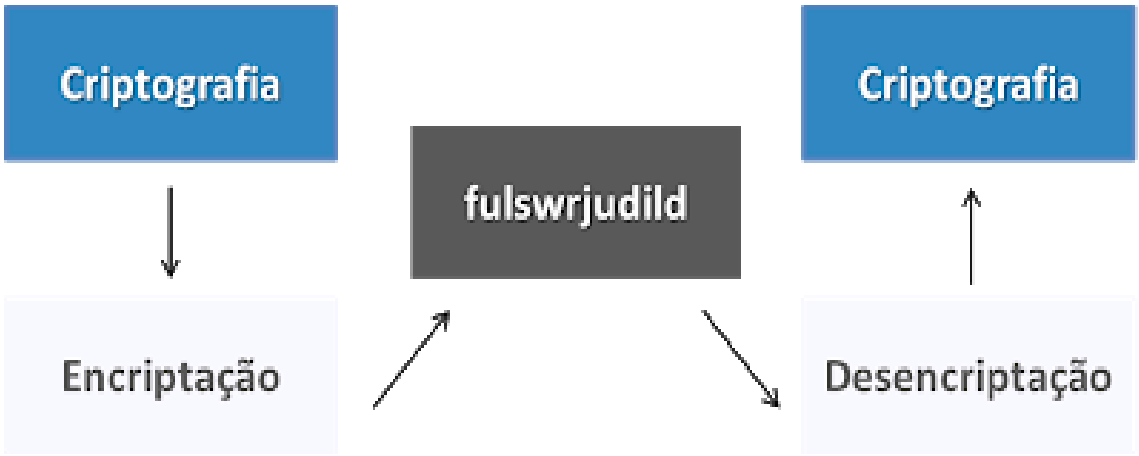
> **Criptografia de chave simétrica:** também chamada de criptografia de chave secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados. Casos

> nos quais a informação é codificada e decodificada por uma mesma pessoa não há necessidade de compartilhamento da chave secreta. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave). Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA.
> **Criptografia de chaves assimétricas:** também conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não-repúdio. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um smartcard ou um token. Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ECC e Diffie-Hellman. (CERT.BR, 2017).

A técnica de criptografia poderá ser utilizada para a proteção dos dados trafegados na rede interna da empresa e também no acesso à Internet, não sendo obrigatório escolher apenas um método a ser utilizado, eles podem trabalhar em conjunto dentro de um sistema.

Veja a contextualização da criptografia na imagem apresentada na Figura 2:

Figura 2: Contexto Básico da Criptografia



Disponível em: <https://sites.google.com/site/kryptosgraphein/visaogeral>. Acesso em 24 Out. 2018

4.3. FIREWALL

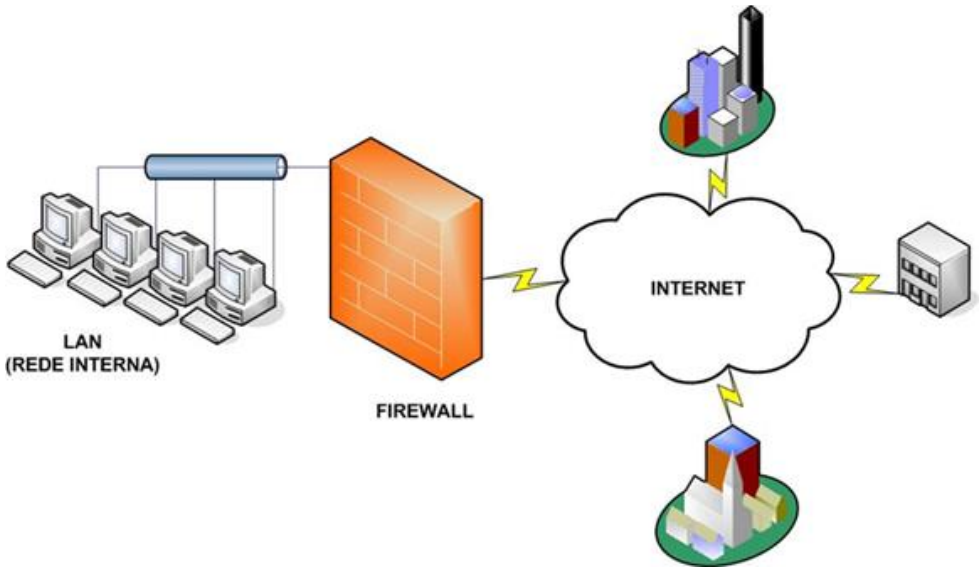
A Cisco (2018) define *firewall* como um dispositivo de segurança que tem a funcionalidade de monitorar o tráfego de dados dentro de uma rede, verificando as informações que entram e saem dessa rede e através de um conjunto de regras

configuráveis ele irá decidir quais tipos de dados serão permitidos ou bloqueados de trafegarem dentro da rede.

Servindo como um tipo de “barreira”, o *firewall* tem como uma de suas finalidades proteger a rede de dados interna contra acessos não autorizados ou intrusão de códigos maliciosos (*malware*) vindos pela Internet e também pode ser configurado para evitar a vazão de dados da rede interna para a Internet. Um sistema *firewall* pode ser um software instalado na rede, um hardware (roteadores físicos) ou a combinação de ambos.

Existe disponível no mercado um tipo de *firewall* que já vem integrado junto ao sistema operacional instalado no computador, que é o caso do Microsoft Windows, porém existem *softwares* que podem ser instalados e configurados à parte, podendo ser gratuitos ou pagos. É possível também encontrar um sistema *firewall* integrado junto a *softwares* antivírus, fazendo com que ambos trabalhem em conjunto em um único programa, O conceito básico de funcionamento do *firewall* pode ser visto na Figura 3:

Figura 3: Conceito de *Firewall*



Fonte: Gestaodeti[3]

[3] Disponível em: < http://www.gestaodeti.net/balanceamento-de-links-de-internet-e-firewall/>. Acesso em 27 Out. 2018

4.4. ANTIMALWARES E FILTRO ANTI-SPAM

Os *malwares* ou códigos maliciosos são programas desenvolvidos e projetados para causar danos ou executar ações maliciosas em um sistema de computador. (CERT.BR, 2017). Dentre os diversos tipos de *malwares* existentes, os mais conhecidos são: vírus, *spyware*, cavalo de Tróia (*trojan*) e *worm*.

Para a detecção e proteção contra esses tipos de *malwares* existem os *softwares* ***antimalwares****,* popularmente conhecidos como: antivírus e *antispyware.* A Microsoft (2012) define um *software* antivírus como "um programa de computador que detecta, evita e atua na neutralização ou remoção de programas mal-intencionados, como vírus e *worms."*

Os antivírus modernos estão englobando as funcionalidades que outros programas faziam separadamente na proteção contra vários tipos de *malwares*, e não apenas vírus, fazendo com que seja possível monitorar os computadores e a rede com apenas um *software.* A rede também deve ser monitorada, pois um vírus de computador tem a capacidade de se espalhar pela rede e infectar outras máquinas, podendo causar grande prejuízo dentro de uma rede corporativa se não tiver a tratativa correta.

"*Spam* é o termo usado para referir-se aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas.". (ANTISPAM.BR, 2018).

Em sua origem os *spams* eram utilizados para espalhar propagadas via *e-mails,* porém com o passar do tempo ele passou a ser usado também para a aplicação de golpes, estelionato e também disseminação de *malwares,* fazendo uso da inocência dos usuários que, ao abrirem um destes *e-mails* acabavam clicando no conteúdo e por descuido acabavam "abrindo as portas" de seu computador para indivíduos mal intencionados. (CERT.BR, 2017).

Para auxiliar as pessoas e buscar reduzir este problema, os servidores de *webmail* e programas usados para leitura de *e-mails,* passaram a utilizar o mecanismo chamado **filtro anti-spam**.

De acordo com a CERT.br (2017) o filtro anti-spam possibilita que o usuário possa configurar através de listas, os *e-mails* que ele deseja receber ou não, ou marcar os destinatários como confiável ou não, e conforme as alterações realizadas

o filtro automaticamente vai se aplicando às mensagens semelhantes, quase como se o filtro “aprendesse” a diagnosticar e separar o que é um e-*mail spam*.

4.5. *BACKUPS* E LOGS

De acordo com Jesus e Schimiguel (2018) “*backup* é uma apólice de seguro contra a perda de dados”, ele consiste em realizar uma ou mais cópias dos arquivos de dados do sistema e armazená-los em um local e/ou mídia alternativos, assim, caso haja a perda, danificação, sequestro ou infecção por vírus no servidor principal, estes dados podem ser restaurados do servidor secundário, pois a empresa necessita de suas informações para poder dar continuidade nos negócios. As organizações têm a possibilidade de programar sistemas de *backups* automáticos, que podem ser programados dentro de uma rotina diária, para garantir a conformidade dos dados da empresa no seu dia a dia.

Segundo a CERT.br (2017) “*Log* é o registro de atividade gerado por programas e serviços de um computador. Ele pode ficar armazenado em arquivos, na memória do computador ou em bases de dados.”. Os *logs* terão a funcionalidade de, no caso de necessitar descobrir um acesso ou atividade realizada, ao consultá-lo, será possível identificar o autor e quando este acesso foi feito. Será possível saber se foi um acesso interno na empresa, ou um acesso forçado externamente, realizado de forma ilegal.

4.6. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Segundo Laudon (2005) “um objetivo chave da Política de Segurança da Informação é assegurar a proteção da integridade da informação armazenada”, a Política de Segurança da Informação (PSI) “[...] estabelece regras e normas de conduta que diminuirão a probabilidade da ocorrência de incidentes que provoquem, por exemplo, a indisponibilidade, furto ou perda de informações [...]” (SILVA, 2013); é um documento geralmente pautado em uma norma técnica, como a NBR ISO/ 27001:2005, de gestão de Segurança da Informação, que contém práticas para iniciar, programar, manter e melhorar a gestão de segurança da informação em uma organização.

Dentro das políticas de segurança, serão definidos os controles e mecanismos de segurança utilizados dentro da empresa, e de que forma eles serão abordados e como deverão ser cumpridos.

De acordo com estudo realizado pela Cisco (2014 *apud* PINTO, 2014), foi possível verificar que as políticas de segurança não são tão enfáticas como deveriam; enquanto 59% dos colaboradores desconfiam que exista uma política de segurança, outros 23% não sabem ao certo se ela existe ou não.

Este estudo mostra a importância de uma política de segurança bem construída e da capacitação dos funcionários em conhecê-la e cumpri-la de forma que se mantenha um ambiente de dados mais seguro dentro da empresa.

5. ESTUDO DE CASO

A Empresa fictícia HDC Service, provê serviços de manutenções, reparos e utilidades domésticas, situada na cidade de Americana, disponibilizando seus serviços também para as cidades de regiões vizinhas.

A HDC Service surgiu da ideia de negócio entre associados onde cada um teria um papel nos trabalhos disponibilizados (elétrica, hidráulica, informática, reparos e manutenções gerais), e sendo contratados alguns funcionários para funções internas da empresa. Por se tratar de uma pequena empresa em seu início, foi instalado um servidor para recepção de um *link* dedicado de acesso à Internet para compartilhamento em rede entre os setores.

Sem a presença de um sistema gerenciador para os negócios, partes das documentações são feitas em planilhas Excel e outras em arquivos de papel e fichado em pastas.

Com a crescente demanda e aumento dos serviços prestados pela empresa, foi decidido entre os associados a expansão dos negócios, com a contratação de novos colaboradores e implantação de um novo sistema de gerenciamento de dados.

Até aqui já é possível diagnosticar os grandes riscos que a empresa já está se submetendo, como perda, vazamento ou roubo de informações e dados, uma vez que não há uma estrutura sólida de política de segurança da informação, sendo esse um aspecto de alta importância para o funcionamento adequado da mesma, podendo acarretar em prejuízo financeiro, perda de clientes e até mesmo danos legais à empresa.

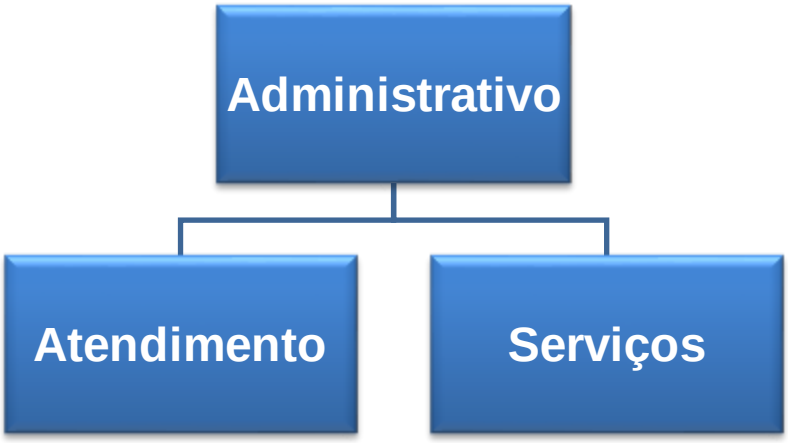
Para auxiliar nesta transição de expansão dos negócios, foi contratada uma empresa especializada de consultoria de TI e Sistemas de Informação.

5.1. CENÁRIO INICIAL

A HDC Service não possui uma política de segurança da informação, com isso algumas falhas podem ser levantadas, como por exemplo, a falta de um *firewall* em sua conexão à Internet, o uso de um antivírus gratuito com poucas funções e ausência de regras de acesso de acordo com cada setor.

A empresa conta com um quadro de doze funcionários divididos em apenas três setores (conforme figura 4), sendo eles: administrativo, atendimento e serviços. A infraestrutura conta com um servidor utilizando Microsoft Windows Server 2003 e mais 10 estações de trabalho, que utilizam sistema operacional Microsoft Windows Seven.

Figura 4: Organograma da empresa HDC Service



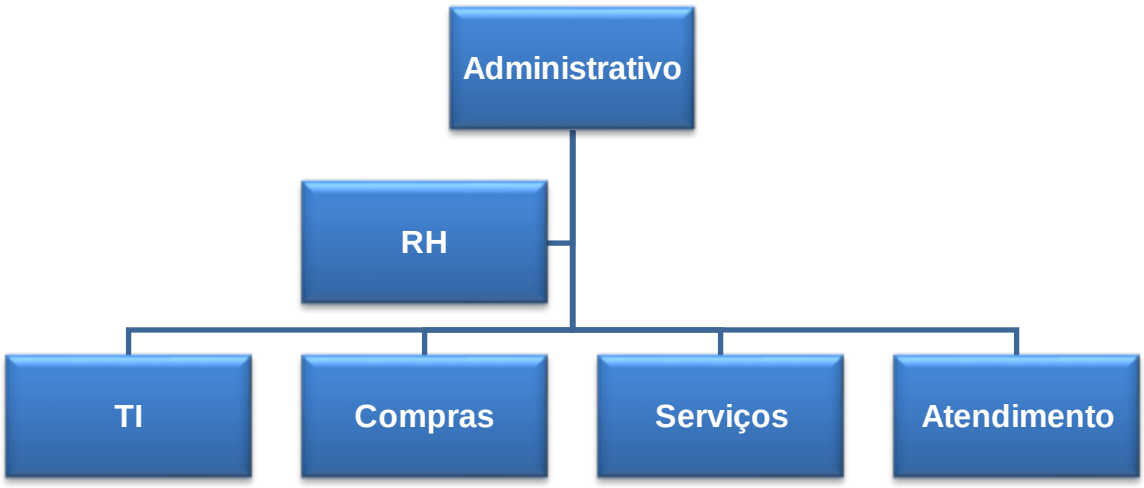
Fonte: Elaborado pelo Autor.

Todas as estações de trabalho possuem acesso a Internet via *Proxy*, porém o mesmo não tem uma configuração e manutenção apropriada, não sendo monitorados nem restringidos os acessos a qualquer tipo de *web sites*. Por este motivo a empresa teve seu número de manutenções corretivas nas máquinas aumentados em 65%, devido a vírus, *spams* e falhas causadas por fator humano, se tornando um dos fatores mais preocupantes.

5.2. ESTRUTURAÇÃO ORGANIZACIONAL

Diante do cenário inicial foi realizado um estudo pela empresa HDC Service junto à empresa contratada para auxiliar nas mudanças a serem realizadas e após uma reunião foi decidido à reformulação do organograma, diante do crescimento no número de funcionários e para uma melhor organização da empresa. O novo organograma da empresa está apresentado na Figura 5:

Figura 5: Novo Organograma da empresa fictícia HDC Service



Fonte: Elaborado pelo Autor.

Com essa nova estrutura o setor Administrativo continuará a ser responsável por toda a empresa, porém com auxílio do RH e com menos atividades sob sua responsabilidade devido à criação do setor de Compras e criação do setor de TI. Além do novo organograma, ficou decidido o uso de um sistema único de gerenciamento de dados, a atualização de equipamentos em nível de *hardware* e *software*, implantação de uma política de segurança que será desenvolvida pela empresa contratada junto ao Setor Administrativo e responsável de cada uma das demais áreas da empresa, para que seja atendida a necessidade de todos, e por ultimo será aplicado treinamento específico para todos os colaboradores da empresa, onde será possível adquirir novos conhecimentos sobre as atualizações realizadas na organização, aprendizagem de uso do novo sistema, e técnicas de proteção e prevenção de perda de dados.

5.3. POLITICAS DE SEGURANÇA

Após a implantação da nova política de segurança, fica sob a **responsabilidade** do setor de TI o acompanhamento, atualização e execução desta política.

Os cumprimentos das normas e regras definidas cabem a todos os funcionários, inclusive do setor administrativo, visando garantir a integridade, confidencialidade e a disponibilidade das informações, estrutura e recursos da empresa.

A **análise de risco** terá como foco a identificação, avaliação e correção dos riscos e fatores presentes na empresa, sendo possível através deste estudo uma visão do impacto antes que o mesmo ocorra. Aplicando esse processo, será possível estabelecer prioridades de ação, qual o impacto do risco e o investimento necessário para correção pontual ou prevenção futura, visando evitar quedas de desempenho e interrupção dos serviços e recursos essenciais da empresa.

Cada setor possui seus processos internos e individuais, cada qual com um nível de criticidade e deverão ser criteriosamente levantados. Após ser feita a analise de risco, esses **processos** devem ser cautelosamente avaliados e estabelecidos.

É necessário realizar o levantamento de todos os requisitos, bem como as informações confidenciais e importantes pertinentes a cada setor, que devem ser criteriosamente manipuladas para evitar ao máximo a exposição indevida e/ou vazamento (risco lógico, dados) e também os riscos que podem ser gerados pelo fator humano, conforme tabela 2:

Tabela 2: Setores x Riscos

Setor	Riscos Lógicos / Dados	Risco Humano
Administrativo	Processos jurídicos, dados confidenciais da empresa, ativos empresarias.	Digitação, Vírus, Internet.
RH	Informações pessoais de funcionários, folha de pagamento.	Digitação, Vírus, Internet.
TI	Processos de segurança, senhas, sistemas integrados.	Internet, Vírus, Acessos Ilegais.
Compras	Dados confidenciais da empresa, orçamentos, dados bancários.	Digitação, Vírus, Internet.
Atendimento	Dados empresariais, dados confidenciais de clientes.	Digitação, Vírus, Internet.
Serviços	Nota fiscal, dados confidenciais de clientes.	Digitação, Vírus, Internet.

Fonte: Elaborado pelo Autor.

A **classificação de dados** ou informações é de alta importância, pois a partir desta, são apontados os pontos que devem ser priorizados e quais tipos de controles deverão ser adotados. Conforme dito anteriormente, cada setor possui informações internas e restritas, porém, há também as informações que são relacionadas entre dois ou mais setores para o andamento do negócio, sendo assim cada tipo de informação deverá ter um tipo de proteção adequado a ela.

As **senhas** serão de caráter pessoal e intransferível, visando à integridade do trabalho desenvolvido por cada colaborador. Uma senha segura deverá ser adotada de acordo com as políticas do sistema, devendo conter no mínimo oito dígitos, sendo ao menos uma letra maiúscula, uma letra minúscula, um caracter alfanumérico e um símbolo.

Essas senhas terão um prazo de validade estabelecido, devendo ser alteradas ao fim deste e não podendo ser igual ou semelhante às ultimas três senhas registradas.

Serão elaboradas e estabelecidas normas de **acesso à Internet e *e-mail* corporativo**, além de regras que poderão ser previamente programadas via sistema. Todos os acessos e *e-mails* encaminhados/recebidos ficarão armazenados em *logs* nos servidores destinados e serão avaliados periodicamente para evitar o uso incorreto ou indevido das ferramentas.

Os colaboradores deverão evitar *downloads* indevidos e/ou desnecessários, de acordo com as políticas de segurança da informação e aprendizagens obtidas no treinamento realizado, que consiste e orienta em fazer o uso somente das ferramentas homologadas e disponibilizadas pela empresa.

Acessos a *sites* impróprios também serão desativados via sistema, com bloqueio por categorias e palavras-chave, como: jogos/*games*, esportes, pornografia, mídias sociais, entretenimento, entre outros que serão definidos pela gerência.

Os **acessos físicos e lógicos** serão determinados de acordo com cada setor, seus colaboradores terão uma identificação física única via crachá e a identificação lógica via usuário e senha de rede.

Serão traçados os perfis lógicos de cada setor e disponibilizados locais de rede para salvar e trocar informações pertinentes a cada um. Usuários com perfil mais

alto, no caso do Administrativo e Gerência, terão acessos ilimitados a toda à rede da empresa. Mas, serão instruídos para tal e responsabilizados por atividades ilegais.

Fisicamente alguns locais não poderão ser de comum acesso, devido aos riscos possíveis. Como por exemplo, o setor de TI onde somente equipe capacitada e treinada terá acesso, bem como toda e qualquer visita, mesmo da gerência, deverá ser acompanhada por um responsável do setor devido à alta criticidade do local que armazenará os servidores e *backups* da empresa. O controle de acesso será realizado por porta com fechadura que necessitará de uma senha para abertura, onde cada colaborador pertencente ao setor de TI terá uma senha própria para que a identificação de acesso seja individual.

Ficará totalmente proibido o **uso de mídias externas e dispositivos móveis**, como, *pendrive*, celular, CD/DVD, HD externo, para usuários comuns em suas estações de trabalho, para que não haja o risco de infecção das máquinas por vírus ou *malweres* trazidos de fora da empresa, que possa gerar algum tipo de brecha na rede ou sistema. Somente a equipe de TI com aval da gerência poderão utilizar estes tipos de dispositivos quando necessário. A monitoração por *logs* também irá auxiliar no caso de algum colaborador por descuido ou má fé realizar o uso de algum destes, podendo descobrir via *login* registrado nas atividades quem foi o infrator de tal ação.

Todos os funcionários, sem exceção, passarão por rigoroso **treinamento específico**, visando o melhor entendimento e uso das políticas de segurança adotadas, para que todos possam compreender e desenvolver suas atividades dentro do esperado pela organização, no uso correto de suas estações de trabalho e na manipulação de informações e dados da empresa.

Periodicamente serão elaborados e disponibilizados novos treinamentos *on-line* em que os colaboradores terão acesso via sistema, para se atualizarem e aprenderem as novas metodologias e políticas elaboradas conforme necessidades e/ou mudanças organizacionais. Essas mudanças poderão ocorrer, caso seja julgado necessário pelo setor administrativo em conjunto com a gerência de cada setor, em reuniões que serão realizadas a cada seis meses para a revisão e atualização da política de segurança.

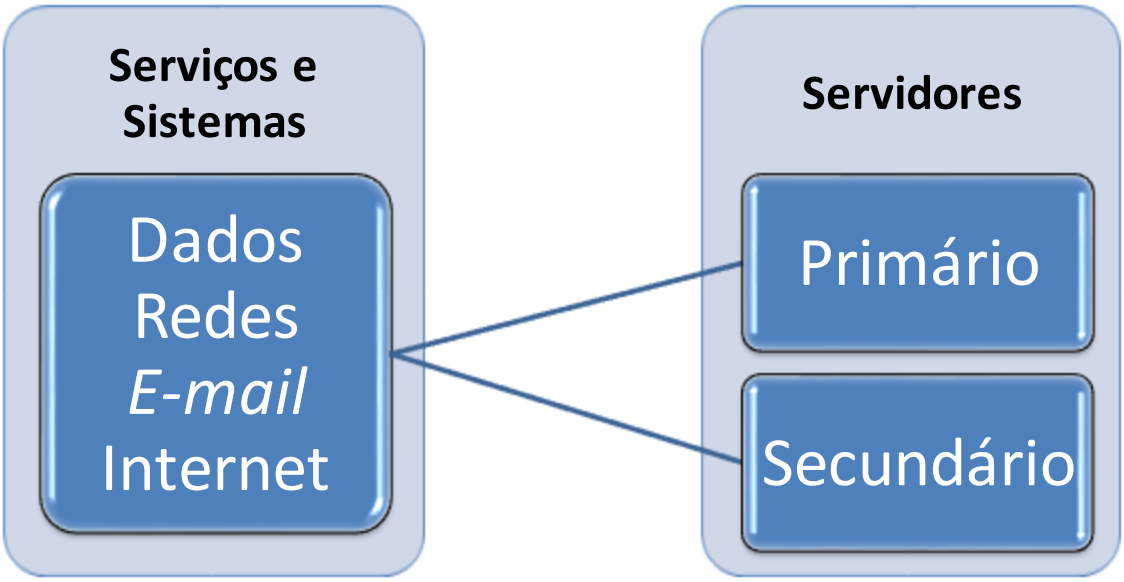
5.4. PLANO DE CONTINGÊNCIA

O plano de contingência visa à necessidade em manter a empresa funcionando, os dados e serviços disponíveis em tempo integral, driblando qualquer adversidade ou fatalidade que possa ocorrer no ambiente físico ou lógico.

Para isso é elaborado um “plano B” ou redundância para que não tenha impacto direto ou significativo nos negócios da empresa.

Dessa forma o sistema foi projetado para trabalhar utilizando a estratégia de trabalho em *high-availability clusters*[4] *(*cluster de alta disponibilidade) trabalhando com dois servidores simultaneamente. Os sistemas e serviços essenciais da empresa serão espelhados simultaneamente do servidor principal, para um segundo servidor, onde, caso haja algum tipo de falha no servidor primário, o servidor secundário assume todos os serviços sistêmicos necessários, garantindo a integridade, confidencialidade e bom funcionamento dos dados da organização.

Figura 6: Plano de Contingência- Espelhamento e Redundância Sistêmica.



Fonte: Elaborado pelo Autor.

O setor de TI será o responsável pela manutenção dos computadores da empresa. As **manutenções corretivas** serão as de caráter emergencial, como por exemplo: troca de periféricos (*mouse,* teclado, memória, monitor, HD), formatação

[4] Disponível em: < https://www.hardware.com.br/dicas/clusters-alta-disponibilidade.html > Acesso em: 01 out, 2018.

de sistema operacional, limpeza lógica de disco. Tais manutenções deverão ser solicitadas via sistema, sendo aberto um chamado para que a equipe de TI retire o equipamento da estação de trabalho e seja levado para correção da falha. Cada equipamento terá uma identificação individual, para que seja possível realizar o controle de ativos, equipamentos danificados ou que necessitam de reparo.

As **manutenções preventivas** serão divididas em duas categorias, as sistêmicas, sendo essa as atualizações de sistema operacional, antivírus e sistema de banco de dados, que ocorrerão diariamente sem impacto ao desenvolvimento das funções do colaborador. E as pontuais, que serão informadas previamente sobre sua execução, devido à necessidade de interrupção temporária da estação de trabalho, porém sem a remoção do equipamento da estação de trabalho, a principal atividade neste caso será a atualização de *softwares* de uso específico de um setor, onde a equipe de TI não tem o controle das atualizações, que são distribuídas pelos seus fabricantes e não ocorrem de forma automática em algumas ocasiões.

Devido à alta criticidade e importância em manter todos os dados e informações da empresa, os **sistemas de *backups*** rodarão em tempo real.

Serão realizadas as cópias de segurança do servidor principal e redundante, como forma de garantia de que todas as informações sejam salvas. E para uma maior segurança, assim como os servidores do sistema principal da empresa, o servidor de *backup* também trabalhará com espelhamento, havendo duas cópias disponíveis em dispositivos distintos, onde caso haja problema e/ou risco de perda em um deles, haverá um de reserva.

Para a **segurança do trabalho**, serão instalados na empresa, extintores de incêndio, hidrantes, sistemas de alarme e sistema para evacuação de pessoas de acordo com as exigências impostas pelos órgãos reguladores.

Semestralmente será realizada vistoria por um engenheiro de segurança do trabalho, para que sejam verificados os equipamentos e sistemas de emergência, atualização do mapa de risco que contem as posições dos extintores e hidrantes e saídas de emergência e treinamento de colaboradores para a atualização da equipe de brigada de incêndio.

No caso de não cumprimento das políticas de segurança estabelecidas, os colaboradores estarão sujeitos a **penalidades**, que serão impostas de acordo com o nível da infração ou descumprimento de regra cometido, sujeitando o funcionário a

advertências, suspensões ou até mesmo desligamento. Cada caso será analisado pela gerência cautelosamente para que não haja injustiças ou punições indevidas.

Na tabela 3 a seguir, seguem alguns exemplos de Infrações x Nível da Infração:

Tabela 3: Infrações x Nível de Penalidades

Infrações (Exemplos)	Nível da Infração
Vazamento de dados empresariais	Gravíssimo
Acesso físico não autorizado	Médio / Grave
Uso indevido ou Mau uso do *e-mail* corporativo	Médio / Grave
Uso indevido da Internet	Médio / Baixo

Fonte: Elaborado pelo Autor.

A **vigência das políticas de segurança** será estabelecida a partir de uma data determinada pela administração, sendo esta data decidida somente após todo o quadro de funcionários terem passado por treinamento e estando aptos a seguir as novas normas e regras.

Os colaboradores serão notificados sobre o início da vigência através do e-mail corporativo, murais de avisos da empresa e também pelos gestores responsáveis por cada setor.

Será realizada uma reunião geral da empresa, para que todos os colaboradores fiquem cientes das mudanças que ocorrerão, bem como o reforço dos direitos e deveres de cada um a partir do momento que passará a ser executada a política de segurança.

Para a formalização da nova política de segurança entre a empresa e os funcionários, será criado um **termo de compromisso,** onde todos se comprometerão a cumprir e agir de acordo com as normas estabelecidas e tomarão ciência de que estarão passíveis de punições caso não seguidas, conforme Apêndice.

Após seis meses do inicio da vigência da política de segurança e da capacitação dos colaboradores, a empresa se submeterá a um processo de **certificação** com intuito de adquirir a ISO 27001, mostrando estar apta e eficaz em desenvolver e atuar de acordo com as normas exigidas pelo órgão regulamentador, que é à base do desenvolvimento da política da empresa, mostrando assim ser uma empresa melhor qualificada dentro do mercado de trabalho.

6. CONSIDERAÇÕES FINAIS

A segurança da informação propõe soluções para a proteção de dados, tanto de usuários domésticos, quanto de organizações e empresas. Ferramentas como antivírus, *antispyware*, *firewall*, são algumas dessas soluções que foram desenvolvidas e são melhoradas continuamente, buscando a melhor proteção possível aos seus usuários, contra fatores maliciosos existentes na Internet e em redes de computadores, tais como, infecção e perda de dados por serem corrompidos por agentes maliciosos ou mal intencionados. Diante da crescente demanda de usuários que prezam pela comodidade em realizar suas atividades de forma ágil através da Internet, pagando contas, acessando e-mail, arquivos em nuvem, é extremamente importante que, não só o usuário busque se proteger como também as instituições que fornecem o serviço não deixe de investir em segurança, para elas e para seus "clientes", visando mitigar os riscos a que ambos estão expostos e buscando assim evitar prejuízos.

Através da coleta e análise de dados, é possível observar que a segurança da informação é um item de alta importância para ambientes empresariais, independente do tamanho da organização, pois a proteção dos dados aos possíveis riscos existentes irá permitir um melhor desenvolvimento das atividades da empresa. No entanto, mesmo diante dessa importância, estudos expõem que empresas de diversas localidades do mundo não dão a atenção necessária para os riscos a que estão submetidas, não utilizando os recursos básicos ou então utilizando de forma inadequada, sem atualizar ou configurar corretamente suas ferramentas para que se tenha uma segurança de suas redes e seus dados.

Além disso, é de extrema importância que, não somente os ambitos físicos e lógicos estejam de acordo dentro das organizações, o fator humano pode ser colocado como o de maior relevância, pois serão os funcionários e prestadores de serviços que irão realizar a manipulação dos computadores e sistemas. Em diversas ocasiões os colaboradores não tem o conhecimento sobre uma política de segurança, e muitos acreditam ser um dever somente da empresa em prestar atenção nesse quesito. Pesquisas revelaram que o comportamento de empregados no momento em que usam a Internet, em sua maioria para atividades fora do contexto do trabalho, como por exemplo, compras ou acesso a e-mail pessoal, se

torna um fator de risco maior do que se não houvesse um sistema de segurança, pois o uso mal orientado, em diversas ocasiões acaba abrindo brechas no sistema, possibilitando a ação de agentes maliciosos como *hackers* e/ou *crackes*, infecção por vírus e sucessivamente o comprometimento e até perda dos dados.

No estudo de caso realizado neste projeto foi possível visualizar a importância de se ter uma política de segurança aplicada dentro de um ambiente empresarial, mesmo ainda sendo uma empresa de pequeno porte, e que posteriormente veio a ter uma crescente em suas demandas, como no caso da HDC Service. Foi possível verificar que além dos danos aos computadores, gerando diversas manutenções, há também a perda de informações importantes para o negócio da empresa por não haver uma organização sistêmica adequada, acarretando em possíveis prejuízos financeiros para a companhia.

Após o desenvolvimento e aplicação da política de segurança, junto ao ganho de conhecimento dos colaboradores através de treinamento e somado a criação de uma equipe de TI aplicada à gestão sistêmica, notou-se uma crescente e significativa melhora nos prejuízos, redução na manutenção corretiva de *hardware* e *software,* e melhor desenvolvimento dos funcionários em suas atividades no local de trabalho. Sendo assim, os resultados atingidos através destes estudos foram de grande satisfação, mas com o alerta de que a política de segurança tem que ser analisada, avaliada e atualizada periodicamente para se estabelecer uma segurança dos dados e da rede empresarial.

De forma a dar continuidade nesta pesquisa, sugere-se os possíveis assuntos a serem abordados: Metodologias e Aplicações de Segurança da Informação em Ambientes Empresariais, que buscaria expor de forma loquaz as possíveis formas das empresas protegerem seu ambiente de dados, Estudo das Normas NBR/ISO 27001 e 27002, buscando aprofundar o conhecimento das normas e de suas aplicações, Comportamento Humano e Engenharia Social no Ambiente Corporativo, explorando as diversidades do comportamento de funcionários se transformando em potenciais vítimas e também o estudo do comportamento dos agentes que realizam os ataques de formal mal intencionada.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Cássio Bastos. **Segurança da informação vs. Engenharia social** – como se proteger para não ser mais uma vítima. Disponível em: < http://www.administradores.com.br/_assets/modules/academicos/academico_3641.pdf >. Acesso em: 28 Ago. 2018.

ASSI, Marcos. **Você é o maior risco de segurança da empresa.** Disponível em: < http://www.marcosassi.com.br/voce-e-o-maior-risco-de-seguranca-da-empresa > Acesso em: 29 Ago. 2018.

BERTUCCI, J.L.O. **Metodologia básica para elaboração de TCC**. São Paulo: Ed. Atlas S.A., 2009.

CAMPOS, A. **Sistema de segurança da informação**. 2. ed. Florianópolis: Visual Books, 2007.

CEGIELSKI, C., RAINER, R.K**., Introdução a sistemas de informação:** apoiando e transformando negócios na era da mobilidade, 2015. Disponível em: <https://books.google.com/books?id=Bq84DwAAQBAJ>. Acesso em: 22 Out. 2018

CERT.BR - **Cartilha CERT.BR**, 2017. Disponível em < http://cartilha.cert.br >. Acesso em: 04 Set. 2018.

CISCO. 2018. **O que é um firewall? .** Disponível em: <https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html>. Acesso em: 27 Out. 2018

FILHO, Hayrton Rodrigues do Prado. **Os riscos e os prejuízos causados pela vulnerabilidade da segurança da informação.** Revista AdNorma, 2018. Disponível em < https://revistaadnormas.com.br/2018/05/29/os-riscos-e-os-prejuizos-causados-pela-vulnerabilidade-da-seguranca-da-informacao/ > Acesso em: 10 Nov. 2018

FONSECA, Paula Fernanda. **Gestão de segurança da informação**: o fator humano. Curitiba. 2009. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula%20Fernanda%20Fonseca%20-%20Artigo.pdf>. Acesso em: 18 abr. 2018.

FONTES, E. . **Segurança da Informação**: **o usuário faz a diferença**! . Editora Saraiva, 2017. Disponível em: <https://books.google.com.br/books?id=FyprDwAAQBAJ>. Acesso em: 22 Out. 2018
GONÇALVES, Sérgio Ricardo M. ***Hackers*, *Crackers* e *Spammers*: quem são e o que fazem?** . Mundo Jurídico, 2003.

GUIMARÃES, Matuzalém. **Segurança da informação na Internet.** Viva o Linux, Brasil, 2008. Disponível em < http://www.vivaolinux.com.br/artigo/Seguranca-da-Informacao-na-Internet?pagina=1>. Acesso em: 24 abr. 2018.

JESUS, Guilherme Bindi Alencar; SCHIMIGUEL, Juliano. **Implementação de Backup Como Processo De Segurança Da Informação**. 2018. Disponível em < http://www.eumed.net/2/rev/atlante/2018/02/backup-seguranca-informacao.html >. Acesso em 29 Out. 2018

KASPERSKY. Blog Kaspersky. **10 principais ameaças a Cibersegurança em 2013**. Disponível em: < https://www.kaspersky.com.br/blog/10-principais-ameacas-a-ciberseguranca-em-2013/1806/ >. Acesso em: 04 Set. 2018.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de gestão da informação que armazenam imagens digitais de documentos com fidedignidade e confiabilidade**. Gestão da Informação, 2005.

LIMA, Fernando. **ISO 27001 e ISO 27002. 2011**. Disponível em: <http://www.portalgsti.com.br/2011/05/iso-27001-e-27002.html>. Acesso em: 16 Abr. 2018.

MENKE, Fabiano. **Assinaturas Digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a ICP alemã**. Revista de Direito do Consumidor, v. 12, n. 48, 2003. Disponível em: < http://egov.ufsc.br/portal/sites/default/files/anexos/4375-4369-1-PB.pdf>. Acesso em: 06 Dez. 2018

MICROSOFT. 2012, **O que é software antivírus? .** Disponível em: <https://www.microsoft.com/pt-br/security/resources/antivirus-whatis.aspx>. Acesso em: 27 Out. 2018

PEIXOTO, Mário C. P. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro: Brasport, 2006.

PINTO, Andre Munhoz. **Pesquisa mostra que ataques online a micro e pequenas empresas é crescente**. Disponível em < https://blog.avast.com/pt-br/2014/09/15/pesquisa-mostra-que-ataques-online-a-micro-e-pequenas-empresas-e-crescente/ > Acesso em: 11 Set. 2018.

PINTO, Pedro. **Complacência e desconhecimento colocam em risco os dados corporativos**. 2014. Disponível em: < https://empresashoje.pt/informacao/complacencia-e-desconhecimento-colocam-em-risco-dados-corporativos/ >. Acesso em: 29 Out. 2018.

SÊMOLA, Marcos. **Gestão de segurança da informação:** visão executiva da segurança da informação: aplicada ao Security Officer. Rio de Janeiro: Elsevier, 2003.

SETZER, V.W. **Dado, informação, conhecimento e competência.** São Paulo, Depto. de Ciência da Computação, Universidade de São Paulo, 2015.

SILVA, Carla Karine Oliveira da. **Proposta de Política de Segurança da Informação Física e Lógica para o Instituto PHOENIX de Basquetebol**. 2013. Disponível em: <http://nippromove.hospedagemdesites.ws/anais_simposio/arquivos_up/documentos/artigos/e937bba73c4c048f07e41cbe97c599a9.pdf>. Acesso em: 29 Out. 2018.

SILVA NETTO, Abner da; SILVEIRA, Marco Antônio Pinheiro da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **Revista de Gestão da Tecnologia e Sistemas de Informação**. Vol.4, No.3, 2007. Disponível em: < http://www.jistem.fea.usp.br/index.php/jistem/article/download/10.4301%252FS1807-17752007000300007/95>. Acesso em: 24 abr. 2018.

STONEBURNER, Gary. **Underlying technical models for Information technology security**. Gaithersburg, USA, NIST Special Publication 800-33, 2001.

STRONG SECURITY. **Criptografia de dados: importância para a segurança da empresa**. 2018, Disponível em: <https://www.strongsecurity.com.br/criptografia-de-dados-importancia-para-seguranca-da-empresa/>. Acesso em: 24 Out. 2018

TEIXEIRA, Tiago. **Antivírus para empresa qual a melhor escolha?** . Disponível em < https://blog.bluepex.com/antivirus-para-empresa-qual-a-melhor-escolha/ > Acesso em: 11 Set. 2018.

TELIUM NETWORKS. **Entenda as diferenças entre controles físicos e controles lógicos de uma vez por todas! .** 2016. Disponível em: <https://blog.telium.com.br/entenda-as-diferencas-entre-controles-fisicos-e-controles-logicos-de-uma-vez-por-todas/>. Acesso em: 22 Out. 2018

Apêndice

TERMO DE COMPROMISSO

O presente Termo tem como objetivo reforçar aos colaboradores da empresa fictícia HDC Service sobre as proibições e consequências do uso indevido dos equipamentos e sobre a divulgação parcial ou total de dados ou informações de operações pertinentes e de responsabilidade da empresa, conforme a Politica de Segurança adotada e apresentada em treinamento realizado por todos.

São eles:

01. O uso do *login* e a correspondente senha têm caráter pessoal e intrasferível;

02. É **expressamente proibido o compartilhamento de *login* e senha**, portanto, cabe a cada um adotar os meios necessários a manter esta informação protegida, sob pena de que caso ocorra utilização indevida do *Login*, o colaborador possa sofrer as sanções Administrativas previstas na Política de Segurança, bem como nas esferas Civil e Criminal caso julgado necessário;

03. É terminantemente proibido que o colaborador ou qualquer outra pessoa se identifiquem no sistema em nome de outro;

04. É terminantemente proibido o uso de telefones celulares ou *smartphones* no ambiente de trabalho, isto não quer dizer que o colaborador esta incomunicável, quer dizer apenas que você deve seguir uma regra de segurança e desta maneira evitar se expor à sanções contidas na Política de Segurança, portanto, se for o caso, converse com o seu gestor, explique a situação emergencial e solicite uma pausa de suas atividades para que possa atender às suas necessidades pessoais;

05. É terminantemente proibido que o colaborador ao se ausentar da sua estação de trabalho deixe o sistema aberto, possibilitado que terceiros tenham acesso ao ambiente sem a devida autenticação;

06. É terminantemente proibido o uso do *e-mail* corporativo, *softwares* de comunicação instantânea para envio de qualquer conteúdo – mensagem e/ou anexos - estranho às atividades do colaborador, ou seja, utilize os recursos que a empresa lhe dispõe somente para questões profissionais;

07. É terminantemente proibida a execução de qualquer atividade ilícita que faça uso de tecnologia ou de engenharia social, como exemplo: varredura de serviços e vulnerabilidades, ataques direcionados ou distribuídos, acesso não autorizado, roubo de credencial, exploração de vulnerabilidades em infraestrutura e/ou sistemas, disseminação de vírus, *trojans*, cavalos de tróia, *softwares* maliciosos, acesso não autorizado, roubo de credencial, *keylogger* e outras variantes de ameaças;

08. É proibida a instalação de *softwares* não homologados e/ou autorizados pela Politica de Segurança e de *softwares* sem a devida licença de uso – *software* pirata – nas estações de trabalho destinadas ao trabalho profissional do usuário;

09. É proibida a divulgação de informações de qualquer natureza de que tenha conhecimento por força de suas atribuições sem a devida autorização expressa do Setor Administrativo ou de quem esse setor delegar.

Responsabilização Administrativa

Todos os atos descritos acima configuram Quebra de Procedimento, passivo de penalidades previstas na Política de Segurança, citadas abaixo:

a) Advertência;

b) Suspensão;

c) Demissão Sem Justa Causa;

d) Demissão Com Justa Causa.

No caso de infração que necessita o enquadramento nas esferas Civis e/ou Criminais, o colaborador será devidamente informado pelo Setor Administrativo.

Boas Práticas

No intuito de orientar e auxiliar nossos colaboradores no cumprimento das regras e normas exigidas pela Política de Segurança seguem algumas dicas de boas práticas que podem ser adotadas:

- Lembre que o inimigo pode “morar” ao seu lado, portanto não facilite. Esconda sua senha a sete chaves. Misture letras, números e caracteres especiais combinando-os para parecerem letras (@=a ou 0=O $=s) e também letras maiúsculas e minúsculas. Ex.: **H!)C$3Rv1c3**;

- Não deixe a senha exposta para que terceiros possam visualiza-la. Ex.: Anotar em *post it* e afixá-lo no computador ou no seu crachá;

- Quando houver *reset*, troque a senha recebida logo no primeiro acesso e desligando o computador após o uso, assim você evita que outras pessoas possam saber a sua senha, não espere 24, 48 ou 72 horas para realizar a alteração, lembre-se: segurança é prioridade número um;

- Guarde o celular na bolsa, no armário ou mantenha em modo avião, de modo que não atrapalhe o desenvolvimento de suas atividades. Use-o para recreações somente no momento de pausa e fora do seu local de trabalho;

- Faça render suas horas de trabalho. *Facebook, Twitter, Instagram* e *WhatsApp* são para os seus momentos de lazer, além de serem terminantemente proibidos dentro da empresa;

- A Internet pode te levar a mares desconhecidos e perigosos, portanto, todo cuidado é pouco, navegue somente onde você tem autorização e não se exponha a riscos desnecessários, quando menos esperar, seus dados podem ser capturados;

- A manutenção dos equipamentos e sistemas são com a equipe de TI, eles são especialistas no assunto e recebem para desempenhar esta função. Abra um chamado se tiver qualquer problema com seu equipamento ou sistema, não tente dar uma solução direta aos problemas técnicos, evite gerar mais problemas;

- Todas as informações e dados contidos nos sistemas e processos pertencem à empresa e estão sob responsabilidade da companhia, portanto, não divulgue, de maneira parcial ou integral nenhuma informação ou dados sem que exista a necessária autorização, lembre-se que a exposição de dados pode causar danos administrativos, civis e criminais, atenção e cuidado são muito importantes.

Neste ato, firma-se o presente **Termo de Compromisso**, onde o colaborador assume estar ciente, conforme condições:

1) Seguir as determinações da Política de Segurança da empresa, em razão deste Termo de Compromisso;

2) Em caso de descumprimento da Política de Segurança de forma intencional, estará sujeito às punições impostas pela política em questão;

3) Exceção a acidentes não intencionais e comprovados.

Local: _____
Data: ____/____/2018

Nome Colaborador:_____
Assinatura: _____
RG: _____ **CPF**_____

Gestor: _____
Diretoria: _____
Assinatura Gestor: _____