CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Tecnólogo em Segurança da Informação

Douglas Ramos Inácio Neves

A SEGURANÇA DOS DADOS EM UM AMBIENTE CORPORATIVO

Americana, SP

2015

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Tecnólogo em Segurança da Informação

Douglas Ramos Inácio Neves

A SEGURANÇA DOS DADOS EM UM AMBIENTE CORPORATIVO

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Tecnológo em Segurança da Informação, sob a orientação do (a) Prof.(o) Esp. Antonio Lacerda.

Área de concentração: Segurança da Informação

Americana, S. P.

2015

Neves, Douglas Ramos Inácio

N423s A segurança dos dados em um ambiente corporativo. / Douglas Ramos Inácio Neves. – Americana: 2015.

42f.

Monografia (Graduação em Tecnologia de Análise de Sistemas e Tecnologia da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Esp. Antônio Alfredo Lacerda

1.Segurança de sistemas de informação I. Lacerda, Antônio Alfredo II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

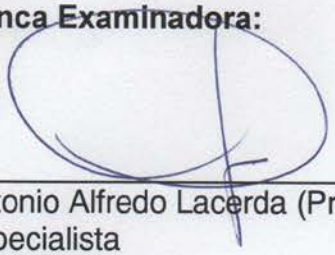
Douglas Ramos Inácio Neves

SEGURANÇA DOS DADOS EM UM AMBIENTE CORPORATIVO

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.

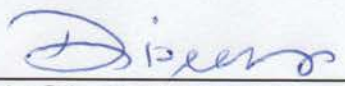
Americana, 23 de junho de 2015.

Banca Examinadora:



Antonio Alfredo Lacerda (Presidente)
Especialista
FATEC Americana

Clerivaldo José Roccia (Membro)
Mestre
FATEC Americana



Diógenes de Oliveira (Membro)
Especialista
FATEC Americana

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus pela realização deste projeto, meu pai Valter Batista Neves e minha namorada Vanessa Fachini Dellagnese que me apoiaram durante esse meu trabalho.

DEDICATÓRIA

Dedico e agradeço em primeiro lugar a Deus, por estar me guiando durante todo caminho.

Em especial ao meu pai Valter Batista Neves e minha namorada Vanessa Fachini Dellagnese que me apoioram e incentivaram.

A Fatec-AM, pelos professores e amigos que conquistei durante este curso, certamente aprendi muito com todos.

RESUMO

Muito se fala sobre a proteção dos dados online, que estão em risco diariamente – é necessário proteção e atenção na hora da manipulação de certos dados, como por exemplo, dados bancários. As empresas (grandes ou pequenas) devem ter um cuidado redobrado com os dados que elas manipulam e armazenam, pois são dados de clientes, parceiros, fornecedores e a falta de segurança desses dados colocam em risco a estratégia da empresa e claro, todos os envolvidos. A presente pesquisa aborda a segurança dos dados em ambientes corporativos, e ressalta que as empresas, (mesmo com toda a tecnologia disponível) muitas vezes não estão totalmente preparadas para proteger de forma eficiente e eficaz os seus dados ou não dão a devida importância à sua proteção, resultando em vários prejuízos, tanto ideológicos quanto financeiros; ele mostra também que parte da vulnerabilidade dos dados existe por conta do comportamento dos colaboradores, que muitas vezes acreditam que é dever apenas da própria organização zelar e proteger seus dados, sigilosos ou não. Este trabalho mostra também a importância desses dados para as grandes empresas, bem como os riscos inerentes à proteção desses dados; é discutido também os principais métodos e tecnologias para defesa existentes no cenário tecnológico atual de modo geral, e também encerra com um estudo de caso, onde é abordado como esses métodos e tecnologias funcionam na realidade.

Palavras Chave: Segurança; dados; informação, segurança dos dados.

ABSTRACT

It's said a lot about the protection of online data, which is at risk on a daily basis – protection and attention is required when handling certain data such as bank account details. Companies (large or small) should have a care with the data they manipulate and store, as they handle data from customers, partners, suppliers and the lack of data security endanger the company's strategy and of course, everyone involved.
The present research addresses data security in corporate environments, noting that companies (even with all the technology available) often are not fully prepared to protect efficiently and effectively your data or do not give needed importance to its protection, resulting in many losses, both financial and ideological; it shows also that part of data vulnerability exists because of the behavior of employees, who often believe that only the organization itself must ensure and protect your data, sensitive or not. This work shows the importance of these data for large enterprises, as well as the risks inherent in the protection of such; it's discussed also the main methods and technologies to existing defense in the current technological landscape in general, and also concludes with a case study, where it is discussed how these methods and technologies work in reality.

Keywords: *Security; data; information; enterprises, data safety.*

SUMÁRIO

LISTA DE FIGURAS E DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CPD: Centro de Processamento de Dados

TI: Tecnologia da Informação

SI: Segurança da Informação

RH: Recursos Humanos

FTP: File Transfer Protocol (em português, Protocolo de Transferência de Arquivos)

DNS: Domain Name System

HD: Hard Disk (Disco Rígido)

1 INTRODUÇÃO

A Tecnologia da Informação vem avançando de forma rápida e contínua atualmente, e se tornou praticamente inviável para grandes empresas e companhias tratar de seus negócios sem que ela própria não esteja totalmente informatizada. Até mesmo as pequenas empresas encontram uma maneira de informatizar seus processos internos, seja utilizando um ERP ou uma simples planilha em Excel para armazenar dados; se estes dados se perdem ou se corrompem de alguma forma, a empresa perde informações valiosas que fazem com que seu negócio prospere.

Dado, de acordo com Setzer (2001) é:

> "[...] uma seqüência 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 seqüência de dados."

Setzer (2001) 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. Por exemplo, na frase: "A Lua é linda", a palavra **Lua** pode fazer sentido para alguém que saiba o que é a Lua, mas para um computador, esta mesma frase seria apenas um conjunto de caracteres.

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 seu 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.

Atualmente, grande parte do patrimônio das empresas sejam elas multinacionais ou micro, é digital, e está relacionada aos dados e informações mantidas por elas; dados de clientes, de movimentos estratégicos, novas tecnologias e serviços adquiridos – estes são só alguns exemplos dos tipos de dados e informações valiosíssimas para as empresas.

Entretanto, grandes corporações têm se tornado alvo de *hackers* e estes invadem seus sistemas e roubam quaisquer informações que acharem relevantes. O ataque mais recente foi à empresa Sony, que ocorreu no final de novembro de 2014, e expôs dados pessoais de funcionários e ex-funcionários da Sony. É necessário atentar ao fato de que a Sony não é uma empresa qualquer, mas sim uma multinacional renomada no mundo todo, e nem mesmo ela foi isenta do ciber ataque.

É preocupante ver que não somente empresas no Brasil, mas algumas espalhadas pelo mundo não priorizam a segurança das informações que detêm, mesmo sendo reconhecidamente seu maior patrimônio. Sendo assim, esta pesquisa discutirá sobre a segurança dos dados em ambientes empresariais, de forma a mostrar que mesmo com toda a tecnologia disponível, ainda sim existem riscos enormes para manter os dados sigilosos. Uma vez que a área mais sensível à perda de dados seja identificada, fica muito mais fácil e eficiente direcionar os esforços para as áreas adequadas, para então minimizar os danos tanto físicos quanto patrimoniais, de perda, vazão ou roubo de dados.

Esta pesquisa analisa a aplicação e a importância da Segurança da Informação em ambientes corporativos, e também:

- Realiza um breve estudo da Segurança da Informação e discutirá principais riscos e ameaças, e formas de defesa para minimizar estes riscos;
- Estuda um ambiente corporativo real através de um estudo de caso, a fim de mostrar como as políticas de segurança, regras internas e outros atuam na proteção dos dados.

O trabalho foi realizado utilizando pesquisa bibliográfica, utilizando principalmente livros, artigos de periódicos e material disponibilizado na Internet; ele foi estruturado em cinco capítulos, sendo que o primeiro – esta introdução - apresenta o tema da pesquisa; o segundo conceitua os princípios básicos da Segurança da Informação. O capítulo terceiro apresenta os mecanismos existentes para a proteção dos dados; o capítulo quarto apresenta os riscos e ameaças existentes no ambiente corporativo; e o capítulo quinto apresenta um estudo de caso, que mostra como esses métodos de defesa realmente atuam em um ambiente corporativo real.

2 A SEGURANÇA DA INFORMAÇÃO

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 (ISO/IEC 27002, 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 dessas informações, pois são de grande importância ao usuário e as empresas.

De acordo com a norma ISO/IEC 27002 (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.

2.1 O AMBIENTE CORPORATIVO

Esta pesquisa trata da Segurança da Informação em Ambientes Corporativos; esses ambientes consistem em uma rede local em uma empresa, conectada à Internet por um ou mais links.

Se em uma rede doméstica a proteção dos dados é muito importante, em uma rede corporativa essa proteção exige o triplo proteção, pois a empresa guarda informações sigilosas (do próprio negócio e de clientes) que, em mãos erradas, podem gerar um grande prejuízo monetário e de propriedade intelectual.

A questão é: mesmo com essa consciência, os dados estão totalmente seguros em ambiente corporativo?

Um recente estudo da *Edelman* (2015), realizado no mundo todo, ressalta que há três problemas graves que concernem à segurança dos dados:

> **“Falta de prioridade:** Mais de metade (59%) dos respondentes dizem que a sua organização não considera privacidade e segurança de informações pessoais uma prioridade da empresa. No Brasil esse número sobre para 78%. Com relação ao cumprimento da legislação vigente neste tema, 40%

> dos entrevistados no mundo têm certeza de que isso é feito, e no Brasil, apenas 21%
> **Falta de recursos:** No Brasil, 81% acreditam que a sua organização não tem a experiência, treinamento ou tecnologia para proteger informações pessoais, e 73% dizem não contar com os recursos adequados. No mundo, os número são, respetivamente, 62% e 54%.
> **Falta de Transparência:** Apenas 26% dos entrevistados brasileiros acreditam que a sua empresa é transparente sobre o que faz com as informações de clientes e de funcionários, em contraste com os 44% globalmente. No que diz respeito à rapidez para responder a queixas de consumidores e de órgãos regulatórios, no Brasil, 77% informam que sua organização não é eficiente e, no mundo, 42% dos respondentes não estão satisfeitos.” De Edelman (2015).

Como visto na pesquisa, ainda há lacunas graves na Segurança da Informação, mesmo em redes corporativas, e a mais grave é a falta de prioridade, quando esta deveria ser o item mais importante – é da prioridade que surge a preocupação em manter os dados íntegros e confidenciais, como será abordado ainda neste capítulo.

2.2 PRINCÍPIOS BÁSICOS

De acordo com Brook (2010), a Segurança da Informação possuí seus princípios básicos e é representada por três fatores, a Tríade conhecida por CIA (Confidencialidade, Integridade e Disponibilidade) conforme figura a seguir.

Figura 1 – Segurança da Informação: Tríade CIA

Fonte: ISO/IEC 27002 (2005)

Esses atributos são os primordiais na Segurança da Informação, pois através deles que é orientado a analise, 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 mal comportamento de usuários e até mesmo devido à 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, Segundo Brook (2010):

Confidencialidade: Esta relacionado a disposição dos dados somente para partes apropriadas que requerem o acesso e confiáveis, somente quem tem a permissão de acessa-los, garantindo assim que os dados não sofra alterações e que informações não sejam comprometidas.

Integridade: É a garantia que os dados não sofram alteração e que suas informações fiquem falhas e corrompidas. A integridade possui dois pontos em seu processo que pode ser comprometida, que é no carregamento ou no armazenamento desses dados, sendo que á causa pode ser atribuída a vários fatores.

Disponibilidade: A disponibilidade dos dados significa que o mesmo deve estar disponível para acesso sempre que necessário. Nesse processo é envolvido software, hardware e vários fatores, onde todos devem ser bem planejados para que qualquer falha que ocorra, exista uma redundância para que esses dados não fiquem indisponíveis. A disponibilidade é um grande desafio em ambientes coorporativos, pois a informação deve sempre estar disponíveis e ser rapidamente transmitida quando solicitada.

É importante ressaltar, que além desses três principais atributos, aplicam na Segurança da Informação também, o não repúdio, autenticidade e a privacidade. (STONEBURNER, 2011).

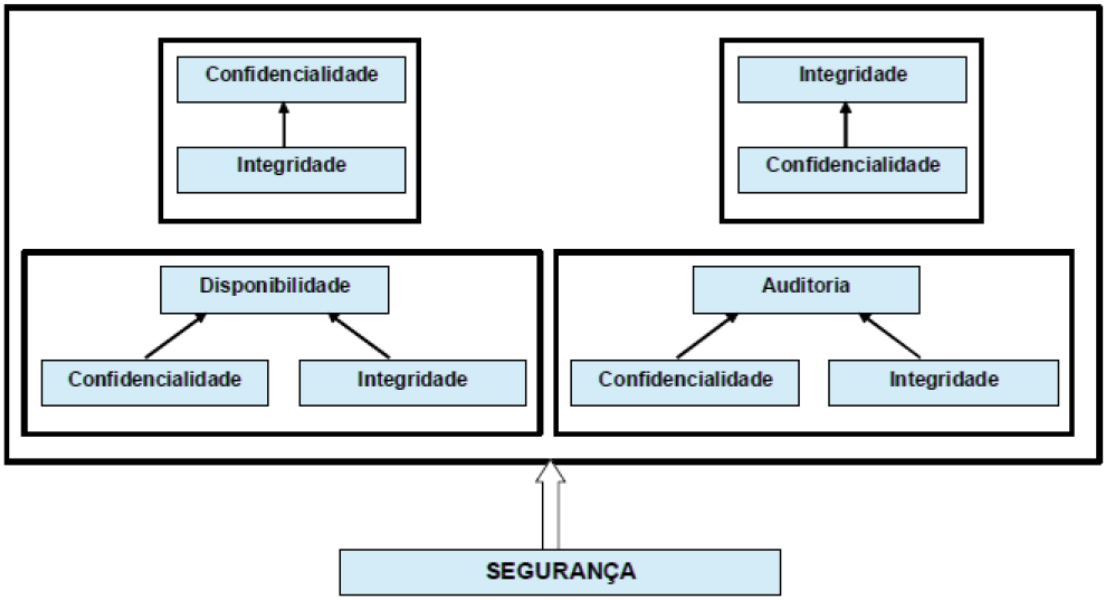
O não repúdio ou irretrabilidade pode ser definido como a junção de autenticidade com integridade, pois visa garantir a informação origem de forma que

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, de acordo com figura 2.

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

Figura 2 – Relação dos princípios da segurança



Fonte: STONEBURNER, (2001)

2.2 NORMAS E REGULAMENTAÇÃO ISO

De acordo com as normas da ISO/IEC 27002 (2005), são abordados requisitos de Gestão da Segurança para que sejam adotadas na empresa, entre elas esta a ISO 27001 e 27002, certificação para a organização e para o profissional respectivamente, ideal que as duas sejam solicitadas e utilizadas em conjunto em uma organização, empresa capacitada e atendendo as normas, e com profissionais capacitados para manter a organização e politica de segurança de acordo com as normas.

2.2.1 ISO 27001

Norma Internacional que define os Requisitos para Sistemas de Gestão de Segurança da Informação. Auxilia a empresa aplicar um sistema de Segurança da Informação que permita inibir os riscos de segurança e adequar os atributos da norma para a empresa construir assim um sistema seguro e com uma política definida.

Benefícios da Norma

- Diminui 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;
- Combina recursos com outros Sistemas de Gestão;
- Métodos e mecanismos para verificar sucesso do sistema.

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 a regulamentação das normas e auditada para receber o certificado.

2.2.2 ISO 27002

É recomendável que a ISO 27001 seja utilizada em conjunto com a 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.

3 MODELOS E MECANISMOS DE SEGURANÇA

Segundo as normas da ISO/IEC 27002 (2005), esses modelos são meios de aplicar os princípios triviais de Segurança da Informação, utilizando mecanismos de controle (físicos e lógicos).

3.1 CONTROLES FÍSICOS

É o controle definido como barreiras que limitam o acesso direto a infraestrutura, que garante a existência dos dados e informações, como por exemplo, portas, trancas, sistemas de autenticação, paredes, entre outros.

3.2 CONTROLES LÓGICOS

Talvez o que nos traz mais preocupação e atenção, o controle lógico pode ser definido como barreiras para impedir e limitar acesso a informação em todo o meio eletrônico, exemplos como criptografia, autenticação, senhas, entre outros meios abordados a seguir.

3.3.1 Contas e Senhas

“É por meio das suas contas e senhas que os sistemas conseguem saber quem você é e definir as ações que você pode realizar”(CERT.BR, 2006).

Muitas empresas de Tecnologia da Informação, quando se utiliza de aplicativos próprios, seus usuários devem ter uma conta e uma senha para cada aplicativo, e cada senha geralmente é elaborada com requerimentos diferentes (por ex: caracteres maiúsculos e/ou minúsculos, caracteres alfanuméricos, tamanho específico, etc.).

3.3.2 Cópias de Segurança

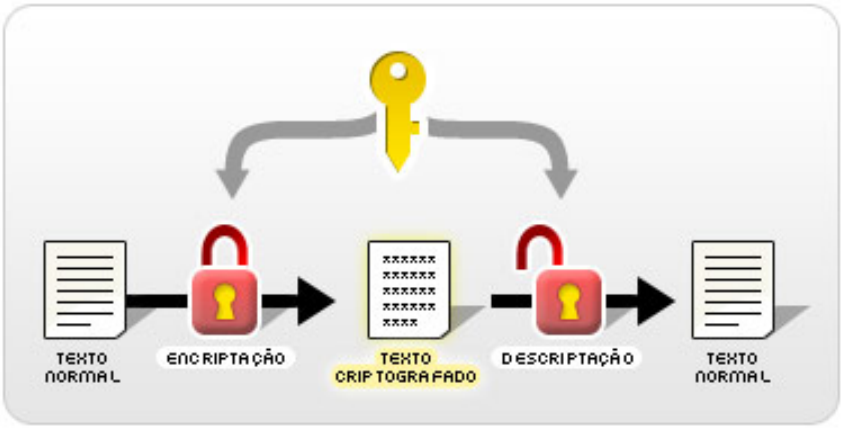
As cópias de segurança são conhecidas como backups, ajudam a proteger dados de perdas, seja de formas acidentais por usuários e até mesmo por falhas em armazenamento ou hardware (CERT.BR, 2006).

3.3.3 Criptografia

São técnicas aplicadas em informações que são transformadas de sua forma original para outra ilegível, onde somente os responsáveis e destinatários corretos da chave de segurança consigam acesso e leitura da informação.

Segundo a norma da ISO 27002 (ISO/IEC,2005), a criptografia é um dos aspectos mais importantes na segurança de informações e vem se tornando um componente básico de proteção de dados, pois com o aumento de infraestrutura de TI nas empresas e utilização de sistemas em inúmeras operações na empresa, aumentou o risco de roubo de informações dentro de uma organização. Dessa forma a criptografia é um dos principais métodos de proteger informações eletrônicas e uma das mais importante na segurança dos dados. A figura a seguir ilustra o objetivo da criptografia.

Figura 3 – Contexto Básico da Criptografia



Fonte: SANTANDER (2015).

3.3.4 Logs

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT.BR, 2006), as logs são registros de eventos e atividades geradas por programas ou serviços do computador operada por usuários. Geralmente são armazenados em arquivos e em base de dados.

Os logs são importantes, pois neles constam detalhes como horário, data, operação realizada, alterações e usuário responsável pela alteração, entre outros pontos relevantes.

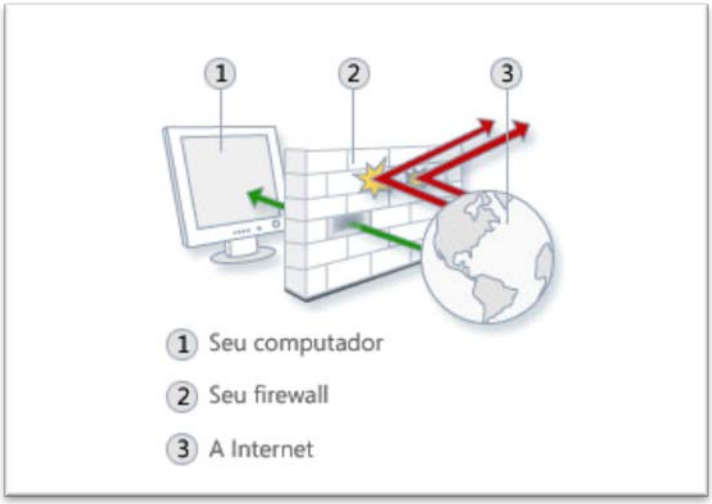
3.3.5 Controle de Acesso

Controle de acesso pode ser aplicado em mecanismo lógico como físico, sendo que o intuito é proteger dados de partes não autorizadas. No mecanismo físico é utilizado salas reservadas, com portas, trancas e no mecanismo lógico, como senhas, bloqueios de sistema para determinados usuários, entre outros.

3.3.6 Firewall

Firewall é um sistema de proteção de redes internas contra acessos que não são autorizados, dessa forma o acesso é controlado pelo firewall, que funciona como uma barreira entre a rede interna (organização) e Internet, de acordo com figura 4. (MICROSOFT, 2015)

Figura 4 – Funcionamento do Firewall



Fonte: MICROSOFT, (2015)[1]

3.3.7 Filtro Spam

Spam é o termo dado para e-mails não solicitados, que são enviados a um grande número de pessoas (ANTISPAM, 2015).

Esses filtros são utilizados e configurados para impedir que esses e-mails indesejáveis cheguem a sua caixa de entrada, sendo que em um ambiente

[1] **Fonte: Disponível em: <http://windows.microsoft.com/pt-br/windows/what-is-firewall#1TC=windows-7>, acesso em 07 mar. 2015**.

coorporativo isso se torna indispensável, ainda mais com o risco de comprometer máquinas de trabalho.

3.3.8 Antimalwares

Segundo o CERT.BR (2006), antimalwares são ferramentas que procuram e detectam ameaças, anulando ou removendo o que prejudique o computador. São os famosos antivírus, antispyware, entre outros.

Todos esses métodos de defesa lógicos podem ser utilizados para usuários comuns e principalmente em ambientes coorporativos, no qual todos os pontos devem ser abordados com muito cuidado, bem planejados e estabelecidos dentro da empresa, documentados e executados corretamente, com o intuito de diminuir os riscos dentro da organização.

4 RISCOS E AMEAÇAS NO AMBIENTE CORPORATIVO

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 *PCs* 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.

Como, em se falando em Segurança da Informação, são inúmeros os riscos e ameaças possíveis, o autor desta pesquisa se valeu em dividi-los em riscos físicos e lógicos.

4.1 RISCOS FÍSICOS

4.1.1 Comportamento dos Colaboradores

Segundo um estudo da Cisco (2014), toda a região da Europa, Ásia e Rússia está em risco por que as empresas se preocupam mais com os riscos externos às empresas (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 advinda da complacência e do desconhecimento; os colaboradores creem que os mecanismos de segurança protegem totalmente suas atividades online.

De acordo com essa pesquisa, 35% dos colaboradores (dentre mais de 12000 entrevistados) tem esta esperança, enquanto que 42% tem consciência de que também é responsável por manter os dados da empresa seguros. Para piorar o cenário, 62% não estão conscientes sobre reais ameaças, e não acreditam que seu comportamento online impacta alguma coisa na segurança dos dados (CISCO, 2014).

Outro estudo, feito pela Gantech (2014), reforça a ideia que os colaboradores são a vulnerabilidade final, vulnerabilidade esta que é explorada pelos *hackers* ou crackers. Emails capciosos, uma propaganda que seja clicada por acidente e pronto, já se tem uma possível porta aberta na rede da empresa para acesso indevido.

Este estudo da Gantech (2014) mostra, em sua página, um exemplo clássico da ameaça exposta acima:

> “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.”

4.1.2 Políticas de Segurança

A Política de Segurança (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 [...]” (FAUSTINI, 2015); 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, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Na teoria, a grande maioria das empresas hoje adotam algum tipo de Política de Segurança.

Ainda segundo o estudo da Cisco (2014) citado no item 3.1.1, denotou 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.

4.1.3 Acesso Não Autorizado

Esta é uma forma de prevenir roubo ou a corrupção de dados: restringindo o acesso a *data centers*, por exemplo, somente à pessoal autorizado; uma das formas de se restringir o acesso seria através de crachás com leitura biométrica: somente as pessoas com a biometria cadastrada poderia acessar determinada parte do edifício.

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, p.169):

> “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, estudado no tópico 3.1.1.

4.2 RISCOS LÓGICOS

Como mencionado no capítulo anterior, há certos mecanismos que previnem determinados riscos e ameaças, tanto físicos quanto lógicos. Os mais relevantes para as corporações na visão do autor desta pesquisa seguem abaixo:

4.2.1 Senhas

Diretamente relacionado com o item 3.2.3, Ataques Virtuais, as senhas são tão importantes quanto as Políticas de Segurança, pois são consideradas umas das maneiras de acesso ao sistema ou às informações confidenciais por invasores.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT.BR, 2012) define:

> “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, o que deixa o sistema vulnerável à ataques; o CERT.BR (2012) aconselha que se “evite nomes, sobrenomes, contas de usuário, números de documentos, placas de carros, números de telefones”, bem como sequências de teclado e nomes de personagens famosos.

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, 2012).

Uma forma de evitar que sejam criadas senhas fracas, a empresa pode determinar uma série de regras que devem ser observadas, do contrário, a senha não será aceita. Por exemplo: "a senha deve ter de seis a doze caracteres, ter um caractere maiúsculo, um número e um caractere especial"; se o colaborador não digitar a senha dentro desses padrões, ela não é criada – é uma forma simples mas eficaz de garantir que as senhas sejam fortes o suficiente para evitar (ou dificultar) sua descoberta.

4.2.2 Vírus, Pendrives e Ataques Virtuais

Intimamente ligado com os dispositivos móveis (tais como *pendrive* e outros dispositivos de armazenamento), os vírus ou *malwares* têm crescido e com isso, os ataques às redes corporativas também. Um estudo realizado pela Kaspersky Lab e pela B2B International, mostra que 91% das organizações sofreram algum tipo de ataque cibernético nos últimos 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 roubo de informações e também foram identificados ataques contra colaboradores, como já mencionado no item 3.1.1; 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 Troia 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.”

Um número preocupante publicado em uma pesquisa da grande Symantec revela que 30% das empresas do Brasil não utilizam softwares antivírus (COMPUTERWORLD, 2009).

Esta pesquisa mostra, pelo menos considerando as pequenas e médias Empresas (PMEs) do Brasil, a preocupação com a Segurança da Informação é descuidada. O estudo também pesquisou as causas desse número tão alto: 28% das empresas não possuem um pessoal dedicado à Tecnologia da Informação, e outros 37% alegam falta de verba para comprar os *softwares*, como equipamentos necessários para efetuar cópias de segurança.

Grandes empresas com certeza se utilizam de uma versão paga e voltada para ambientes corporativos.

Como visto até agora, há vários mecanismos de Segurança da Informação disponíveis, de acordo com cada necessidade existente. Alguns estudos mostram que, apesar da Segurança da Informação ser algo vital para o negócio atualmente, ainda sim há alguns comportamentos que precisam ser desencorajados dentro e fora de empresas (uso da Internet para questões pessoais, pendrives, acesso de e-mails pessoais dentro da empresa, dentre outros), a conscientização é muito importante.

O próximo capítulo fará uma análise de um ambiente corporativo real e discutirá sobre como esses mecanismos de defesas e os riscos existentes atuam em um ambiente real.

5 ESTUDO DE CASO

5.1 ÂMBITO ABORDADO

A Empresa fictícia TMT Telecomunicações, atualmente provê serviços para o estado de São Paulo, possui sete unidades, sendo a Matriz na cidade de Americana, onde se localiza o Centro de Processamento de Dados (CPD).

Nesta unidade estão localizado os principais servidores da empresa, onde os negócios da empresa são baseados em um sistema cujo nome é TQualy; este aplicativo funciona em todas unidades da TMT, através de um *link* dedicado que a empresa possui. Esse sistema atende a todas as áreas de negócio da empresa, cada setor possui determinadas funções e autorizações de acordo com o serviço a ser desempenhado pelo colaborador.

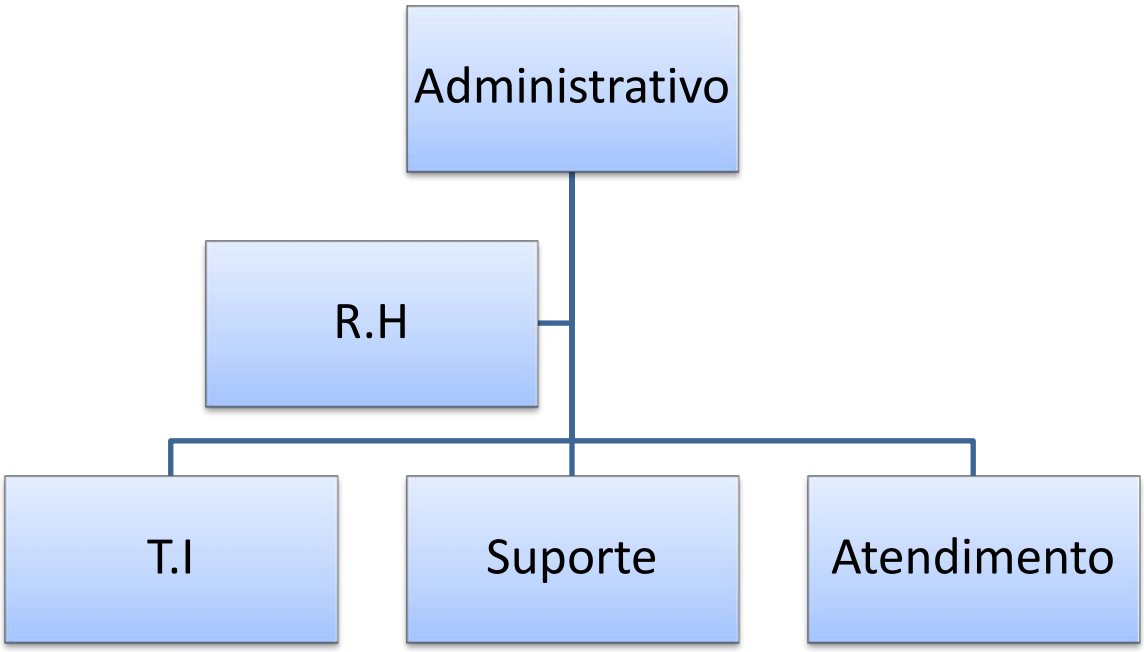
É possível diagnosticar o grande risco de perda ou roubo de informações, dentro um sistema que aborda todas áreas de negócio da empresa, primordial para que todas as unidades funcionem adequadamente. A consequência de comprometimento desses dados é refletida financeiramente e causar grandes danos a organização.

5.2 SITUAÇÃO INICIAL DA EMPRESA

A Empresa TMT Telecomunicações não possui uma Política de Segurança, não possui um firewall na conexão com o link dedicado, localizado na Matriz (CPD).

A TMT possui em sua Matriz cerca de 250 funcionários em 5 departamentos, conforme figura 5, sendo eles, administração, TI, recursos humanos, suporte, atendimento. A empresa conta com 110 microcomputadores, com plataforma predominante Microsoft Windows 7. Para os servidores da empresa é utilizado o Microsoft Windows Server 2003.

Figura 5: Organograma da empresa TMT Telecomunicações



Fonte: Elaborado pelo Autor.

Todas as máquinas possuem conexão à Internet via proxy, contudo sem monitoração e restrições a qualquer tipo de site.

A situação é bem preocupante, sendo que no último semestre o número de manutenções corretivas em máquinas devido a vírus e falhas causadas por usuário aumentou em 60%.

5.3 POLÍTICA DE SEGURANÇA

5.3.1 Responsabilidade

A responsabilidade pelo desenvolvimento da política de segurança fica por conta do pessoal de TI, será definida uma célula dentro do setor para realizar o estudo organizacional e constantemente atualizar e manter a execução desta política.

O cumprimento da política cabe a todos os funcionários, tanto gerentes como diretores e empregados, visando sempre garantir integridade das informações e também de recursos físicos da organização.

5.3.2 Análise de Risco

A Análise de risco será o processo de identificação e avaliação dos riscos e fatores presentes na organização em questão, possibilitando através desses riscos, uma visão do impacto antes que aconteça. Ao aplicar esse processo, será estabelecido prioridades de ação, investimento necessário para prevenir, e o tamanho do risco, evitando quedas de performance e interrupção dos recursos triviais da empresa.

5.3.3 Processos Críticos

Todos setores possuem seus processos, e a partir da análise risco, esses processos precisam ser levantados e estabelecidos.

É preciso levantar todas informações confidenciais dos setores e também as falhas humanas, conforme tabela 1.

Tabela 1 – Processos x Setores

Setor	Risco de Vazamento de Dados	Risco Humano
RH	Salário de Funcionários	Digitação / Vírus / Internet
Administrativo	Processos Jurídicos	Digitação / Vírus / Internet
T.I / Suporte	Processos de Segurança / Senhas / Sistemas Integrados	Internet / Vírus / Acessos Ilegais
Atendimento	Dados Empresariais	Internet / Vírus / Digitação

Fonte: Elaborado pelo Autor.

5.3.4 Classificação das Informações

A classificação da informação é muito importante, pois a partir desta, é enfatizado os pontos que devem priorizados e quais controles adotar. Há informações de uso interno que os setores as relacionam, e cada um possui

suas informações confidenciais que precisam de proteção de dados maior e individual.

5.3.5 Política de Senhas

Será alinhado entre as Equipes que uma senha segura deverá conter no mínimo seis caracteres alfanuméricos, com letras maiúsculas e minúsculas, números e símbolos.

Essas senhas terão um prazo estabelecido pela organização, e após certo período de tempo é solicitado a alteração da mesma.

Senhas com nomes de usuário, datas e combinações simples não serão aceitas pela segurança, dessa forma devem ser evitadas.

5.3.6 Política de uso da Internet/ E-mail

É estabelecido a forma correta do uso de e-mail coorporativo e Internet, onde e-mails são arquivados em um servidor, com filtros de defesas pré estabelecidos pela equipe de TI, porém é solicitado aos usuários não utilizar para comunicação externa e também extra trabalho.

Para a Internet somente acesso a sites são permitidos, contudo não qualquer tipo de site, será utilizado sistemas de controles de acesso e logs, bloqueando também redes sociais, sites pornográficos, categorias especificas como games, esporte, onde cabe a empresa definir.

É proibido o uso de ferramentas P2P (ponto a ponto), e também ferramentas de mensagens instantâneas. Somente será permitido ferramentas homologadas pela organização.

5.3.7 Política de Acesso

O Acesso a determinados locais da rede e funções estabelecidas para cada setor no sistema integrado TQualy será planejado também na política de

acesso, dessa forma cada perfil de usuário terá acesso a locais específicos e somente poderá visualizar no sistema o que lhe é permitido e importante para desenvolver seu trabalho dentro de seu setor.

O sistema TQualy, que é um software desenvolvido especificamente para o trabalho da TMT Telecomunicações, também possuirá perfis de usuários de acordo com o cargo e setor que o colaborador se encontra.

Para acesso aos servidores, também será de acordo com o login do colaborador, equipe responsável terá acesso. Em caso de manutenções de terceiros, será necessário alinhar com Gestor da área.

5.3.8 Política de Uso dos Computadores

O Uso da estação fica totalmente restrita aos usuários, não sendo permitido instalação de softwares, e alterações em configurações, sem ser solicitado pela que equipe de T.I.

Uso de pen drives, conteúdos de fotos e vídeos também será bloqueado não comprometendo assim a integridade nos serviços prestados.

5.3.9 Política de Monitoração de Logs

Os logs são muito importantes para uma boa monitoração de eventos e para identificar possíveis fraudes na segurança, e até mesmo desvio de processos.

Para monitoração dos logs é importante que cada colaborador da empresa possua uma “ID” (Identificação), seja ela numérica ou alfanumérica. Com essa identificação, toda alteração realizada no ambiente de rede ou até mesmo para processos executados dentro do sistema da empresa fica registrado, sendo possível saber quem a executou e quando foi realizado.

5.3.10 Política de uso de Drives

Fica proibido o uso de qualquer mídia física dentro da empresa, visto que os dados importantes estarão presentes nos servidores.

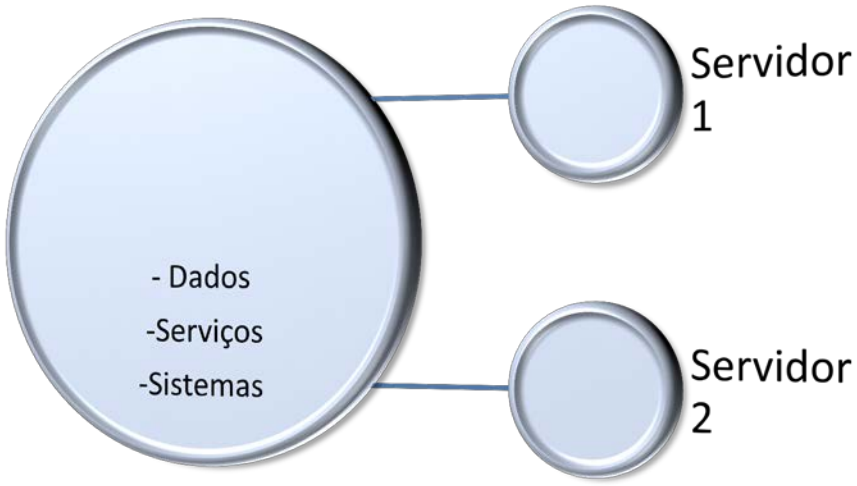
5.4 PLANO DE CONTINGÊNCIA

No plano de Contingência, há necessidade de manter os dados e serviços da empresa sempre disponíveis e funcionando, em qualquer fatalidade é preciso de um segundo plano, uma redundância para que não ocorra nenhum impacto.

Dessa forma para o sistema será utilizado a estratégia de Hot-site (estratégia quente), pronta para entrar em ação, o tempo de ação para isso está relacionado a tolerância a falha do objeto. No caso do sistema TQualy seria em alguns poucos segundos, pois os processos da empresa são dependentes um dos outros.

Esses sistemas e serviços triviais da empresa terão uma espécie de espelhamento simultaneamente em dois servidores de arquivos e sistemas, sendo o principal e o redundante, garantindo dessa forma o bom funcionamento, integridade e confiabilidade dos dados da organização.

Figura 6 – Plano de redundância para acesso aos dados



Fonte: Elaborado pelo Autor.

5.5 PENALIDADES

Para o não cumprimento das políticas de segurança, o funcionário acarretará penalidades, e de acordo com o nível da penalidade, podendo levar a advertências, suspensões e até mesmo desligamento, conforme tabela a seguir.

Tabela 2 – Nível de Penalidades

Infrações (Exemplos)	Nível da Infração
Mau uso do E-mail	Médio
Acesso não permitido (violação)	Grave
Uso Irregular da Internet	Médio
Vazamento de Informações	Grave

Fonte: Elaborado pelo Autor.

5.6 TERMO DE COMPROMISSO DO COLABORADOR

Será criado um termo de compromisso, onde todos os funcionários e estagiários se comprometem formalmente em cumprir as políticas de segurança estabelecidas pela empresa, tomando ciência das punições caso não seguidas, conforme anexo 1.

5.7 IMPLEMENTAÇÃO E EXECUÇÃO DA POLÍTICA DE SEGURANÇA

Será determinada a data para que as políticas entre em vigor, para isso a mesma é divulgada entre os colaboradores, por meio de e-mail, mural e folders.

Para reforçar, será solicitado a diretoria faça um comunicado a todos os funcionários a respeito das mudanças e data da implementação da nova política da empresa.

Após Implementação e execução da política de segurança, será realizado em determinado período, uma reunião entre a diretoria para estabelecer a

manutenção e melhorias da política já estabelecida, corrigindo e aperfeiçoando a mesma.

5.8 SEGURANÇA FÍSICA E PESSOAL

Para a Segurança Física, será realizado a separação dos setores onde exista necessidade, e salas onde deverá possuir trancas e alguma identificação especial, como por exemplo as salas dos hacks de servidores, diretoria, e patrimônios da empresa.

Será instalado também na empresa extintores de incêndio e hidrantes de acordo com o que é solicitado pelo corpo de bombeiros, para isso será realizado uma vistoria junto a um Engenheiro de Segurança do Trabalho, para que seja estabelecido mapas, localizações para extintores e hidrantes, pontos de encontro, sinalizações e organizado equipe de brigada de incêncio.

Para a sala de Servidores (*Datacenter*) será equipado refrigeração e extintor adequado para o local.

5.9 MANUTENÇÃO DOS EQUIPAMENTOS

Será estabelecido dento do setor de TI, responsáveis para realizar manutenções corretivas e também para as preventivas.

Para as corretivas, será necessário abrir chamado no portal de ocorrências interno, para que seja retirada maquina e realizado manutenção e correção de falha, todas as maquinas serão cadastradas também sua própria identificação.

Nas manutenções preventivas, essas precisam ser previamente agendadas, realizadas mensal, semestral, ou anual, dependendo da manutenção. As manutenções sistêmicas geralmente serão executadas com mais frequência, atualizações de software com menos, entre outros casos.

5.10 BACKUPS

O *Backup* é um dos procedimentos mais importantes para ser realizado, como a manutenção preventiva eles precisam ser realizados constantemente, para evitar qualquer perda de dados valiosos para a corporação.

Os Servidores serão todos configurados utilizando espelhamento em dois HD's, contudo será realizado backup a todo momento de logs e informações importantes, sendo elas geradas pelo sistema TQualy em todos os setores da empresa.

Um dos maiores riscos para uma organização é a perda de informações vitais, dados de clientes, dados de funcionários, informações sigilosas, valores, entre outros, o que pode acarretar grande impacto para empresa, no seu planejamento e nos seus lucros.

5.11 SERVIDORES

Para a empresa TMT Telecomunicações, serão utilizados vários tipos de servidores, servidor de e-mail, Internet, arquivos, FTP, DNS, entre outros, alguns funcionaram como servidores virtual, reduzindo custos, ambos utilizados para melhoria dos processos e facilidade de acesso a informação, conforme exemplos de tipos de servidores e suas funções de acordo com tabela 3.

Tabela 3 – Exemplo de servidores e suas funções

Servidores	Função
E-mail (Microsoft Exchange)	E-mail corporativo / Controle dos E-mails / Salvar Informações.
Servidor de Arquivos (Sharepoint)	Ambiente para centralizar informações e procedimentos da organização em apenas um lugar / Rapidez e Integridade das informações.
Servidor de Virtualização	Permiti trabalhar com servidores isoladamente, dentro de um mesmo equipamento / Economia com Infraestrutura inicial

Fonte: Elaborado pelo Autor

5.12 PLANO DE CONTINUIDADE E ATUALIZAÇÃO

Todo planejamento e política estabelecidos, precisam ser sempre revisados e atualizados, para garantir que os pontos falhos sejam corrigidos e os bem executados sejam mantidos e melhorados, dessa forma existe o plano de continuidade e atualização, para que a política de segurança na empresa se mantenha constantemente atualizada e eficaz.

5.13 CERTIFICAÇÃO

A empresa será submetida através do plano de continuidade estar sempre apta e eficaz no cumprimento das políticas, e com isso buscar a certificação ISO 27001 através das melhores praticas que deverão ser bem estabelecidas e praticadas para alcançar o objetivo, como também será oferecido treinamento a alguns colaboradores para também possuir a certificação ISO 27002.

6 CONSIDERAÇÕES FINAIS

A Segurança da Informação dispõe de várias ferramentas e métodos para proteger os dados, tanto de cidadãos comuns, quanto de grandes empresas e organizações. Firewalls, soluções antivírus, criptografia... são algumas das ferramentas ‘requintadas’ que precisaram ser desenvolvidas para proteger indivíduos contra pragas virtuais e roubo de informações por agentes mal intencionados. Sendo assim, se para um usuário comum é muito importante (e cômodo) poder realizar tarefas bancárias a partir de casa, também é igualmente importante que seus dados bancários não sejam comprometidos por vírus através da Internet; da mesma forma, uma instituição bancária, por exemplo, não pode ‘economizar’ nas medidas de proteção à Informação, do contrário somará prejuízo atrás de prejuízo.

A partir da apresentação e análise dos dados, observa-se que a Segurança da Informação é um item muito importante para os Ambientes Corporativos, pois protege os dados de vários riscos. Entretanto, mesmo sendo conhecida a sua importância, estudos recentes mostram que algumas das empresas (não só do Brasil, mas ao redor do mundo todo) não dão a devida atenção, nem emprega as ferramentas necessárias para garantir a Segurança da Informação e de seus dados.

Outra questão importante diz respeito à conscientização dos empregados e funcionários de ambientes corporativos; muitos empregados nas empresas não têm nem o conhecimento se existe uma Política de Segurança ou não, e muitos acham que é dever apenas da empresa em cuidar desta parte. Estudos também mostraram que seu comportamento enquanto na Internet (como utilizar a Internet para realizar compras ou outros afazeres pessoais) é um risco tão grande quanto a falta de tecnologia empregada, pois facilita a ação de *hackers* mal intencionados, ou até mesmo *crackers*.

Atrelado às questões acima citadas, pode-se observar o efeito da falta ou da não aplicação de uma Política de Segurança em uma empresa, como foi apresentado no estudo de caso da empresa TMT Telecomunicações. Além dos danos físicos (manutenção física e lógica das máquinas, etc), há a perda de informações, que geram prejuízos monetários grandes para a empresa; com o desenvolvimento de uma Política de Segurança, feito pelo pessoal do TI, há uma melhora significativa nesses prejuízos.

De forma a dar continuidade nesta pesquisa, os assuntos que podem ser abordados são: Os Riscos das Redes Sociais em Ambientes Corporativos, que discutiria o constante uso das redes sociais dentro do ambiente de trabalho e suas implicações; e Segurança da Informação e Criptografia, que exploraria os tipos de criptografias existentes e seus usos.

REFERÊNCIAS BIBLIOGRÁFICAS

_____. **Referências**: NBR-6023/ago. 2002. Rio de Janeiro: ABNT, 2002.

BROOK, J. M. C. **CIPP guide**, CIA Triad. Estados Unidos da América, ago. 2010. Disponível em <http://www.cippguide.org/2010/08/03/cia-triad>. Acesso em: 21 fev. 2015.

CALHEIROS, R. F. **Segurança de informações nas empresas** – uma prioridade corporativa, 2002. Monografia - Universidade do Rio de Janeiro, Rio de Janeiro.

CAMPOS, A. **Sistema de segurança da informação**. 2. ed. Florianópolis: Visual Books, 2007. 218 p.

CERT.BR - Cartilha CERT.BR, 2006. Disponível em <http://cartilha.cert.br>. Acesso em: 07 mar. 2015.

CERT.BR - Cartilhas de segurança: Contas e Senhas. 2012. Disponível em: <http://cartilha.cert.br/senhas/>. Acesso em: 09 mar. 2015.

CISCO Web Page. Complacência e desconhecimento colocam em risco os dados corporativos. 2014. Disponível em: <http://www.cisco.com/web/PT/press/articles/2014/20141031.html>. Acesso em: 02 fev. 2015.

Computer World Home Page. 30% Pequenas e médias empresas usam antivírus, 2009. Disponível em: <http://computerworld.com.br/seguranca/2009/06/08/30-das-pequenas-e-medias-empresas-do-pais-nao-usam-antivirus/>. Acesso em: 22 mar. 2015.

EDELMAN. **Segurança e privacidade de dados.** Pesquisa Elaborada no Brasil e no Mundo. Disponível em: <http://www.edelman.com.br/news/privacy-risk/>. Acesso em: 16 jan. 2015.

FAUSTINI, Rodrigo. **Política de segurança da informação**. 2015. Disponível em: <http://www.faustiniconsulting.com/artigo05.htm>. Acesso em: 15 mar. 2015.

Gantech Home page. Nós somos o elo mais fraco. Disponível em: <http://www.gantech.com.br/index.php?option=com_content&view=article&id=204:voce-e-o-maior-risco-de-seguranca-da-empresa&catid=27&Itemid=41>. Acesso em: 02 fev. 2015.

GIL, A, C. **Elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas S.a, 2002. 175 p. Disponível em: <http://www.pgtur.uff.br/sites/default/files/como_elaborar_projeto_de_pesquisa_-_antonio_carlos_gil.pdf>. Acesso em: 20 fev. 2015.

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. 2011.

GUIMARÃES, Matuzalém. **Segurança da Informação na Internet.** Viva o Linux, Brasil, mai. 2008. Disponível em < http://www.vivaolinux.com.br/artigo/Seguranca-da-Informacao-na-Internet?pagina=1>. Acesso em: 21 fev. 2015.

KASPERSKY. Kaspersky Lab Page. Conheça as principais ameaças corporativas de 2013. Disponível em: <http://brazil.kaspersky.com/sobre-a-kaspersky/centro-de-imprensa/comunicados-de-imprensa/2013/kaspersky-lab-conheca-principais-amea-0>. Acesso em: 09 mar. 2015.

PALMA, 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. 2015.

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

Anexo 1

TERMO DE COMPROMISSO

TMT Telecomunicações, estabelecida à _____ n° _____, na cidade de

_____, estado de _____, CNPJ/MF n° _____,

designada **EMPRESA EMPREGADORA** e o **EMPREGADO**, Sr. _____, _____, residente à

_____, na cidade de _____, estado de

_____, e-mail _____, telefone _____, portador

da Carteira de Trabalho e Previdência Social - série _____ n° _____, CPF n°

_____, celebram o presente **TERMO DE COMPROMISSO**, que se vincula ao Instrumento Jurídico (Prestação de Trabalho) firmado entre a Empresa Empregadora e o Empregado em ____/____/____, nos termos da Lei n° 6.494/77, conforme condições a seguir:

1. O funcionário seguirá 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, o funcionário estará sujeito as punições impostas pela política em questão.

3. Salvo acidente de forma não intencional provado.

E, por estarem de acordo com os termos do presente instrumento, as partes o assinam em **3 (três) vias**, na presença de duas testemunhas, para todos os fins e efeitos de direito.

Americana, _____

Testemunhas

_____

_____

Diretor/ Gerente

_____

Funcionário

_____