Universidade Federal do Rio de Janeiro

Escola Politécnica

MBA em Governança, Projetos e Serviços de TI
(MBGPS)

# MECANISMOS DE PREVENÇÃO CONTRA *RANSOMWARE* UM ESTUDO DE CASO NA EMPRESA MÉDICO-HOSPITALAR


Autor:

Diego Ramos Fonseca

Orientador:

Manoel Villas Bôas Júnior, M. Sc.

Examinador:

Cláudio Luiz Latta de Souza, M. Sc.

Examinador:

José Airton Chaves Cavalcante Junior, D. Sc.

Examinador:

Vinicius Drumond Gonzaga, M. Sc.



**Rio de Janeiro**
**Junho de 2021**

# Declaração de Autoria e de Direitos

Eu, **Diego Ramos Fonseca** CPF 096.603.537-23, autor da monografia ***MECANISMOS DE PREVENÇÃO CONTRA RANSOMWARE: UM ESTUDO DE CASO NA EMPRESA MÉDICO- HOSPITALAR***, subscrevo para os devidos fins, as seguintes informações:

1. O autor declara que o trabalho apresentado na defesa da monografia do curso de Pós-Graduação, Especialização MBA - Governança, Projetos e Serviços de TI da Escola Politécnica da UFRJ é de sua autoria, sendo original em forma e conteúdo.

1. Excetuam-se do item 1 eventuais transcrições de texto, figuras, tabelas, conceitos e ideias, que identifiquem claramente a fonte original, explicitando as autorizações obtidas dos respectivos proprietários, quando necessárias.

1. O autor permite que a UFRJ, por um prazo indeterminado, efetue em qualquer mídia de divulgação, a publicação do trabalho acadêmico em sua totalidade, ou em parte. Essa autorização não envolve ônus de qualquer natureza à UFRJ, ou aos seus representantes.

2. O autor declara, ainda, ter a capacidade jurídica para a prática do presente ato, assim como ter conhecimento do teor da presente Declaração, estando ciente das sanções e punições legais, no que tange a cópia parcial, ou total, de obra intelectual, o que se configura como violação do direito autoral previsto no Código Penal Brasileiro no art.184 e art.299, bem como na Lei 9.610.

2. O autor é o único responsável pelo conteúdo apresentado nos trabalhos acadêmicos publicados, não cabendo à UFRJ, aos seus representantes, ou ao(s) orientador(es), qualquer responsabilização/ indenização nesse sentido.

1. Por ser verdade, firmo a presente declaração.

Rio de Janeiro, _____ de _____ de _____.

_____

Nome Completo

**UNIVERSIDADE FEDERAL DO RIO DE JANEIRO**

Av. Athos da Silveira, 149 - Centro de Tecnologia, Bloco C, sala - 212,
Cidade Universitária Rio de Janeiro – RJ - CEP 21949-900.

## RESUMO

Os ataques de *ransomware* têm aumentado significativamente nos últimos tempos. Neste sentido, este projeto identificou vulnerabilidades que contribuem para o ataque cibernético nos tempos de adequação a LGPD. Para isso, foi realizada uma análise por meio de questionário no departamento de TI, tendo como objeto de estudo o ataque de *ransomware* na empresa médico-hospitalar, cujo nome foi mantido em sigilo por questões éticas e de segurança. Com os resultados deste estudo, é possível verificar que a ausência de mecanismos de controle e prevenção de segurança, no departamento de tecnologia de uma empresa, contribuem para uma invasão, causando vazamento de dados e comprometendo a imagem do negócio, além de trazer prejuízos financeiros. Por fim, é preciso adotar ações que mitiguem essas vulnerabilidades, implementando boas práticas de segurança e trazendo investimento para a TI, com a finalidade de minimizar o impacto diante de um ataque cibernético. De acordo com a análise dos resultados obtidos, conclui-se que existem diversos pontos vulneráveis que podem facilitar uma invasão e que uma das práticas de prevenção é a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais, a começar pela reestruturação da infraestrutura de segurança, a partir do núcleo de negócio da empresa com o aprimoramento do sistema de backup. Para ações futuras, indicam-se testes de invasão monitorados com objetivo de realizar varredura na rede, em busca de vulnerabilidades e a avaliação do grau de maturidade dos processos de governança, com o uso da Framework ITIL e Cobit 5.0.



Palavras-chave: ISO 27000, Cibersegurança, LGPD, Segurança da Informação.

## ABSTRACT

Ransomware attacks have increased significantly in recent times. In this sense, this project identified vulnerabilities that contribute to cyber attack in times of adaptation to LGPD. For this, an analysis was carried out through a questionnaire in the IT department, with the object of study being the ransomware attack on the medical-hospital company, whose name was kept confidential for ethical and security reasons. With the results of this study, it is possible to verify that the absence of control and security prevention mechanisms, in the technology department of a company, contributes to an invasion, causing data leakage and compromising the business image, in addition to bringing financial losses . Finally, it is necessary to adopt actions that mitigate these vulnerabilities, implementing good security practices and bringing investment to IT, in order to minimize the impact of a cyber attack. According to the analysis of the results obtained, it is concluded that there are several vulnerable points that can facilitate an invasion and that one of the prevention practices is the adoption of technical and administrative measures capable of protecting personal data, starting with the restructuring of the infrastructure from the company's core business with the enhancement of the backup system. For future actions, monitored penetration tests are indicated with the aim of scanning the network, looking for vulnerabilities and assessing the degree of maturity of the governance processes, using the ITIL Framework and Cobit 5.0



Keywords: ISO 27000, Cybersecurity, LGPD, Information Security

## SIGLAS

**ABNT** Associação Brasileira de Normas Técnicas

**AD** *Active Diretory*

**DNS** *Domain Name System*

**LGPD** Lei Geral de Proteção de Dados

**RDP** *Remote Desktop Protocol*

**TI** Tecnologia da Informação

**TJ** Tribunal de Justiça

**UFRJ** Universidade Federal do Rio de Janeiro

**VPN** *Virtual Private Network*

**UTM** *Unified Threat Management*

**WAN** *Wide Area Network*

## LISTA DE FIGURAS


Figura 1.1 – Metodologia usada neste trabalho 14
Figura 2.1 - Inserção da cibersegurança 16
figura 2.2 - Total de incidentes reportados do CERT.br por ano 24
Figura 2.3 – Total de incidentes reportados do CERT.br por ano – tipos de ataque 24
Figura 2.4 – Gráfico de perdas financeiras com ataques de *Ransomware* 25
Figura 2.5 – Anatomia de Ataque *Ransomware* 28
Figura 2.6 - Princípios da Segurança da Informação 30
Figura 3.1 - Conexão recusada ao tentar acessar o sistema 32
Figura 3.2 - Erro de perfil temporário 33
Figura 3.3 – Serviços Encriptados pelo *Ransomware* 33
Figura 3.4 - Topologia do *Core Business* 35
Figura 3.5 – Arquitetura atual 36
Figura 3.6 – Arquitetura do Sistema Bacula *Backup* 37
Figura 3.7 – Topologia do backup com o Bacula 38
Figura 3.8 – Descentralização da TI (1) 39
Figura 3.9 – Descentralização da TI (2) 39
Figura 3.10 – Quantidade de respostas e classificação 41
Figura 3.11 – Principais pontos de vulnerabilidades 42
Figura 4.1 – Gráfico contendo percentual de dificuldade 47
Figura 4.2 – Nova arquitetura de servidores de banco de dados 48
Figura 4.3 - Composição total 1 contratação do projeto 49
Figura 4.4 – Composição 2 despesa anual 50
Figura 4.5 - Aquisição de Hardware 51
Figura 4.6 – Comparativo de investimento do projeto 52
Figura 4.7 - Composição 2 total do projeto segurança 51
Figura 4.8 – Composição de Despesa Firewall 52
Figura 4.9 - Comparativo de investimento do projeto segurança 52
Figura 4.10 - Nova arquitetura do *backup local* 54
Figura 4.11 - Composição 3 total do projeto backup local 55
Figura 4.12 - Composição de Despesa Gestão do Sistema Bacula 56
Figura 4.13 - Comparativo Gestão – Arcserver e Despesa Anual com backup 56
Figura 5.1 - Resultados alcançados percentualmente 56

Figura 5.2 - Linha do Tempo dos Investimentos Realizados 59

## LISTA DE QUADROS

Quadro 3.1 – Modelo do questionário respondido pelo comitê 40
Quadro 3.2 – Análise das respostas do questionário proposto ao comitê 41
Quadro 3.3 - Descrição da análise das respostas do questionário proposto ao comitê 44
Quadro 5.1 - Resultados obtidos 57

# Sumário

**Capítulo 1: Introdução** ..... 12

1.1 – Tema ..... 12
1.2 - Justificativa ..... 12
1.3 – Objetivo Geral ..... 13
1.4 - Delimitação ..... 13
1.5 – Metodologia ..... 13
1.6 – Descrição ..... 14

**Capítulo 2: Embasamento Teórico** ..... **16**

2.1 – Cibersegurança ..... 16
2.2 – Segurança da Informação: ISO 27000, ISO 27001 e ISO 27002 ..... 17
2.3 – Gestão da Segurança de Informação… ..... 20
2.4 – Gerenciamento de Segurança de Informação ..... 21
2.4.1 – Sistemas ..... 21
2.4.2 – Informação ..... 21
2.4.3 – Ameaças ..... 22
2.4.4 – Vulnerabilidade. ..... 23
2.4.5 – Incidentes. ..... 22
2.5 – Avaliação de Riscos ..... 26
2.6 – Aplicação no combate ao ransomware sob a ótica da Lei Geral de Proteção de Dados ..... 27
2.7 –Adoção de políticas de segurança na informação ..... 30

**Capítulo 3: Propostas Tecnológicas** ..... **31**

3.1 – Histórico do incidente ..... 32
3.2 – Infraestrutura atual ..... 35
3.3 – Estrutura do *backup*. ..... 36
3.4 – Visão da TI perante o negócio. ..... 38
3.5 – Análise do ambiente ..... 40
3.6 – Identificação dos principais pontos de vulnerabilidades. ..... 42
3.7 – Sugestão Proposta ..... 42

**Capítulo 4: Resultados Obtidos** ..... **46**

4.1 – Resultado Geral. ..... 46
4.2 – Resultado Obtido na Infraestrutura do *Data Center*. ..... 47
4.3 – Resultado Obtido na Infraestrutura de segurança da empresa ..... 50
4.2 – Resultado Obtido na operação do backup da empresa. ..... 52

**Capítulo 5: Conclusão e Trabalhos Futuros** ..... **56**

5.1 – Conclusão ..... 56
5.2 – Trabalhos Futuros ..... 60

**Referências Bibliográficas…….....……....……..…61**

# CAPÍTULO 1

# Introdução

## 1.1 – Tema

O presente estudo discorre sobre a avaliação do grau de maturidade dos processos existentes de segurança da informação em relação aos ataques de *ransomware* nos tempos de adequação à Lei n° 13.709/2018, intitulado como Lei Geral de Proteção de Dados (LGPD), em torno de uma empresa médico-hospitalar.

Diante de um ataque cibernético de *ransomware*, os prejuízos e impactos causados na operação da empresa, podem ser maiores do que as dezenas de ações judiciais provocadas pelos titulares lesados ao terem seus dados pessoais expostos.

A pesquisa tem a intenção de trazer uma reflexão diante do problema exposto para contribuir de maneira significativa no combate e prevenção destes tipos de ataques cibernéticos, que ocorrem pela ausência de boas práticas na segurança da informação e até mesmo por negligências das empresas.

## 1.2 – Justificativa

A escolha do tema se justifica pela sua relevância como potencial instrumento de combate e prevenção de ataques *ransomware*, não somente nos tempos de adequação a Lei Geral de Proteção de Dados, sobretudo nos casos de vulnerabilidades a segurança da informação que culminam em vazamentos de dados.

Assim, é possível notar que os ataques de *ransomware* nos tempos da LGPD impactam direta ou indiretamente empresas e a sociedade por meio de brechas não notadas na segurança de Tecnologia da Informação (TI) que colaboram para um ataque cibernético, causando a paralização dos sistemas da empresa, além de culminar no vazamento de dados sensíveis, comprometendo a marca perante o mercado.

Para tanto, é preciso identificar vulnerabilidades que contribuem para invasão e vazamento de dados, implementando boas práticas de segurança da informação com a finalidade de minimizar o impacto diante de um ataque cibernético.

## 1.3 – Objetivo Geral

Identificar vulnerabilidades que contribuem para o ataque cibernético, provocado por um *ransomware*, como forma de minimizar os impactos e obter ganhos na segurança da informação na empresa. Tendo como objetivos mais específicos os seguintes processos:

- Verificar vulnerabilidades que contribuem para invasão e vazamento de dados no departamento de TI;
- Implementar práticas de segurança da informação em torno das atividades do negócio;
- Aprimorar o *backup* e a segurança da rede na empresa;
- Apresentar os resultados obtidos após a implementação das boas práticas em segurança.

## 1.4 – Delimitação

Este projeto de pesquisa se delimitou no estudo de uma empresa médico-hospitalar, denominada como Alfa, especificamente no departamento de tecnologia da informação, no que se refere apenas ao setor de segurança local.

Dessa forma, este projeto de pesquisa não abrange microempresas e nem aquelas de porte global, uma vez que não alcança o debate sobre o usuário doméstico. Para tanto, com os resultados obtidos neste apontamento, serão propostas ações que visem mitigar os riscos de ataques e invasões inerentes ao negócio que comprometam sua continuidade, no que se refere a vazamento de dados no âmbito da LGPD dentro da empresa.

## 1.5 – Metodologia

Esta pesquisa se trata de uma pesquisa quantitativa e qualitativa em que será feito um levantamento de dados e informações por meio de embasamento teórico, no que tange a medidas de segurança da tecnologia da informação e questionários aplicados a empresa médico-hospitalar. Assim sendo, a pesquisa assume como estudo de caso por proporcionar maior familiaridade com a problemática, tornando-o explícito por meio de um levantamento bibliográfico para aprofundar o conhecimento. Por ser um tipo de pesquisa muito específica, quase sempre ela assume a forma de um estudo de caso, de acordo com Antonio Carlos Gil [1]. A figura 1.1 demonstra como será o processo de metodologia deste trabalho.

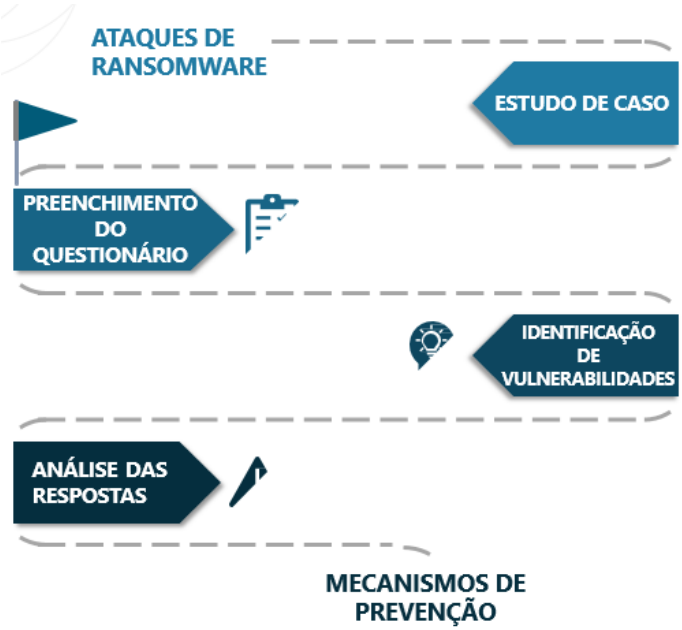


Figura 1.1 – Metodologia usada neste trabalho
Fonte: Autor

Para um melhor tratamento dos objetivos e melhor apreciação desta pesquisa, observou-se que ela é classificada como pesquisa descritiva exploratória. Detectou-se também a necessidade da pesquisa bibliográfica no momento em que se fez uso de materiais já elaborados: livros, artigos científicos, revistas, documentos eletrônicos, enciclopédias e normas técnicas da família ISO/IEC 27000 e na busca e alocação de conhecimento sobre boas práticas de segurança da informação como forma de instrumento no combate e prevenção de ataques cibernéticos de *ransomware* na empresa médico-hospitalar, correlacionando o conhecimento científico com abordagens já trabalhadas por outros autores. Dessa forma, será feito o uso de gráficos para visualização analítica dos dados.

## 1.6 – Descrição

No capítulo 2, será realizado o embasamento teórico da pesquisa, definindo o conceito cibersegurança e ransomware, apresentando a LGPD, suas consequências, a aplicação das boas práticas de segurança no combate ao ransomware, a gestão e gerenciamentos de Segurança da Informação. Além disso, há apresentação de informações sobre ameaças, vulnerabilidade, incidentes, avaliação de riscos, aplicação da Lei Geral de Proteção de Dados no combate ao ransomware e adoção de políticas de segurança na informação.

O capítulo 3 serão apresentadas as propostas tecnológicas.

O capítulo 4 serão apresentados os resultados obtidos.

O capítulo 5 apresenta a conclusão do trabalho e pesquisas futuras.

# CAPÍTULO 2

# Embasamento Teórico

## 2.1 - Cibersegurança

A segurança na internet é um tema que cresce junto com a preocupação em utilizar o espaço cibernético. Enquanto alguns indivíduos são extremamente cuidadosos quando estão online, mas a maioria compartilha seus dados em sites que não são seguros e que podem fazer o mau uso dos dados coletados. Assim, os desafios colocados pelas questões de segurança, como o vazamento de dados pessoais, fizeram com que fossem traçados mecanismos para melhorar a cibersegurança.

De acordo com a ISO/IEC 27032 [2], que apresenta as diretrizes para a segurança cibernética, alinhadas com a segurança da informação, inerente à família das normas internacionais 27000, a segurança cibernética (*cybersecurity* ou *cyberspace security*) é definida "como preservação da confidencialidade, da integridade e da disponibilidade da informação no espaço cibernético" [2].

Adicionalmente, a norma apresenta outras propriedades que podem estar envolvidas nesse contexto, "tais como: autenticidade, responsabilidade, não repúdio e confiabilidade também podem estar envolvidos" [3]. Deste modo, a figura 1.1 a seguir, extraída da norma ISO/IEC 27032 [2], ilustra de forma simples, a abrangência e inserção da cibersegurança no campo da segurança da informação.

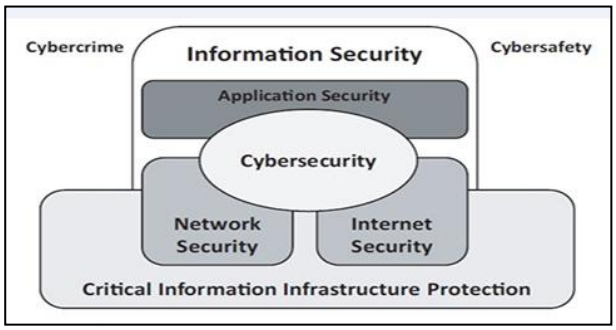


Figura 2.1 – Inserção da cibersegurança
Fonte: ABNT, 2015.

Nesse sentido, a cibersegurança envolve uma infraestrutura de informações como medidas de segurança em que:

> (...) a relação entre os domínios é complexa, por exemplo, alguns serviços de infraestrutura não precisam afetar a segurança cibernética diretamente (como água e transporte). Contudo, a falta de segurança cibernética pode ter impacto negativo sobre a disponibilidade de sistemas críticos de infraestrutura de informação, proporcionados pelos provedores de Infraestrutura críticas [2].

Em relação ao espaço cibernético, ele "não pertence a alguém; todo mundo pode fazer parte e tem uma participação nele" [2]. Assim, a rápida conexão que deveria trazer benefícios para as pessoas pode auxiliar quem tem planos de fazer ataques *ransomware* a dados alheios. Assim, baseando-se na escalabilidade das novas tecnologias nas relações pessoais, e nas gigantescas fraudes e prejuízos que estão atreladas a elas, a cibersegurança deve ser, cada vez mais, um tema importante presente nas organizações.

Por fim, podemos chegar à conclusão de que a maioria das pessoas desconhecem os perigos dos compartilhamentos de seus dados em sites que não são seguros, tais sites podem vender os dados sensíveis para cibercriminosos na *Deep Web* ou até mesmo na *Dark Web*. Logo, é indiscutível que, mesmo promovendo boas práticas em cibersegurança na infraestrutura de segurança de TI, o elo mais fraco sempre serão as pessoas. Nesse sentido, é possível minimizar tal impacto com ações de conscientização regulares na empresa no bom uso da internet.

## 2.2 - Segurança da Informação: ISO 27000, ISO 27001 e ISO 27002

As boas práticas da família ISO 27000 norteiam técnicas de gestão e controles de segurança da informação, auxiliando diversas empresas independente do seu volume, tipo ou natureza.

Segundo a norma ABNT NBR ISO/IEC 27002 [4],

> A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados,

> quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos.

O mais preocupante é que na maioria dos ataques e invasões percebe-se nas empresas a fragilidade pela ausência de boas práticas que possibilitem garantir a continuidade do negócio. Assim, é essencial que as organizações identifiquem na segurança da informação se os requisitos básicos estão sendo cumpridos. De acordo com a ISO 27002, existem três fontes principais de segurança da informação.

> A primeira é a avaliação de riscos para a organização. Leva-se em conta os objetivos e as estratégias globais de negócios da empresa. Por meio da avaliação de riscos, as ameaças e as vulnerabilidades são identificadas, e assim, é realizada a estimativa da probabilidade de ocorrências das ameaças e do impacto potencial ao negócio [4].

Por seguinte, "a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural" [4].

O último requisito para a segurança da informação diz respeito aos "conjuntos de processamento, armazenamento, comunicação e arquivo da informação que uma organização precisa manter para desenvolver suas operações" [4]. Assim como, "A ISO/IEC 27000 apresenta uma introdução geral de um sistema de gestão da segurança da informação e da família de normas da série ISO/IEC 27000" [4].

Pode-se dizer que uma das melhores práticas é avaliar os riscos sob a ótica dos processos críticos de negócio. Tendo como referência a ISO/IEC 27000, os resultados serão satisfatórios tendo menor chance de não alcançar os objetivos desejados pela organização.

O Sistema de Gestão de Segurança da Informação (SGSI) para a ISO 27001 estabelece em seus requisitos gerais que

> A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta. Para os efeitos desta Norma, o processo usado está baseado no modelo de PDCA. [5]

Assim, para implementar e operacionalizar o SGSI, a organização deve formular um plano de tratamento de riscos, identificando a gestão apropriada, bem como os recursos, responsabilidades e prioridades. Implementar plano de tratamento de riscos, além de definir medidas de eficácia dos controles dos grupos selecionados.

A ISO 27002 afirma que a segurança da informação seja definida pela organização, sendo "aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação". [4]. De acordo com a ISO, "as políticas de segurança da informação contemplam: a estratégia do negócio, regulamentações, legislação e contratos e o ambiente de ameaça da segurança da informação, atual e futuro". [4]

> A necessidade de políticas internas de segurança da informação varia entre organizações. Políticas internas são especialmente úteis em organizações maiores e mais complexas onde aqueles que definem e aprovam os níveis esperados de controle são segregados daqueles que implementam os controles, ou em situações onde uma política se aplica a muitas pessoas ou funções diferentes na organização. Políticas de segurança da informação podem ser emitidas em um único documento, "política de segurança da informação" ou como um conjunto de documentos individuais, relacionados. Se qualquer uma das políticas de segurança da informação for distribuída fora da organização, convém que cuidados sejam tomados para não divulgar informações confidenciais. Algumas organizações usam outros termos para estes documentos da política, como "Normas", "Diretrizes" ou "Regras". [4]

Não menos importante que essa consideração, entretanto, é que os riscos relacionados podem partir independente de políticas internas de segurança definidas pela empresa, exemplo clássico, pode ser considerado, a ausência de investimento em segurança no setor de TI. Diante disso, vale considerar que há divergência de modelos propostos, quando o assunto é investimento em segurança. Espera-se, portanto, que as empresas criem maturidade não somente em sua atividade fim, mas em investimento de tecnologia e capital intelectual.

Por seguinte, a ISO 27002 afirma que deve ser estabelecido a cópia de segurança das informações com o objetivo de proteger contra perda de dados. "Convém que cópias de segurança das informações, dos s*oftwares* e das imagens do sistema sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida." [4]. E ainda,

> Convém que a política de *backup* seja estabelecida para definir os requisitos da organização relativos às cópias de segurança das informações, dos *softwares* e dos sistemas. Convém que a política de *backup* defina os requisitos para proteção e retenção. Convém que os recursos adequados para a geração de cópias de segurança sejam disponibilizados para garantir que toda informação e os *software*s essenciais possam ser recuperados após um desastre ou a falha de uma mídia […] [4].

Assim, "convém que as cópias de segurança sejam armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal." [4].

Conforme explicado acima o que importa, portanto, é assegurar a proteção contra perda de dados por meio de um sistema que atenda aos requisitos de negócio. Esse, porém, é um requisito que envolve recursos de hardware e a escolha de um bom sistema. Vê-se, pois, que a escolha depende de levantamento por parte terceiros seja por fabricante ou com a contratação de uma consultoria especializada. É preciso ressaltar que não é um processo trivial a construção de um plano de backup, infelizmente, tem outros entraves como orçamento limitado das empresas. Por final, a importância deve ser defendida pelo resultado da ausência do backup numa possível invasão.

## 2.3 - Gestão da Segurança de informação

A segurança da informação abrange tanto os aspectos tecnológicos (mundo virtual) quanto os aspectos físicos (mundo real). Nesse contexto, a gestão da segurança da informação também considera conceitos de administração para garantir o melhor controle das informações, dentro dos princípios de segurança (confidencialidade, integridade e disponibilidade) e minimizar os riscos.

Segundo Manoel [6], "Gestão da Segurança da Informação, tem como objetivo alinhar a estratégia com os objetivos da empresa, dando mais valor aos responsáveis pela empresa, e ainda garante que os riscos da informação sejam direcionados aos responsáveis". Segundo Fontes [7], segurança da informação, deve estar ligada diretamente aos objetivos de negócio e não deve existir para ela mesma.

Segundo descreve Ulmann [8] "Com as normas da família ISO 27000 podemos entender os requisitos, as necessidades de se implantar uma Política de Segurança de Informação, programar e operar controles de riscos, para assim monitorar o desempenho dentro da empresa." A autora faz um levantamento das descrições das normas conforme Manoel [6] e relata as atualizações ocorridas e publicadas no catálogo da ABNT até o ano de 2013.

Norma ABNT NBR ISO/IEC 27001:2013: abrange requisitos de estabelecimento, manutenção, implementação, além de melhoria contínua da SGSI com avaliação e tratamento dos riscos de segurança da informação conforme as necessidades das empresas.

Norma ABNT NBR ISO/IEC 27004:2010: Orientação para melhoria na eficiência das empresas através de indicadores de medição para mensurar os riscos inerentes ao negócio, segundo Ulmann [8] *apud* Manoel [6].

Norma ABNT NBR ISO/IEC 27005:2008: define como a proteção da informação minimizando o risco e maximizando o retorno sobre os investimentos em TI. A segurança é adquirida com controles apropriados de políticas, de incidentes, continuidade e conformidade dos negócios, conforme ABNT [5].

O ponto de compreensão do processo de gestão de risco na gestão da segurança da informação e suas particularidades, considera os principais conceitos trazidos pela norma ABNT mensurando os riscos para assim minimizar os impactos na organização.

## 2.4 - Gerenciamentos de Segurança da Informação

Segundo Roher [9]

> hackers podem usar diversas técnicas específicas, mas todas podem ser enquadradas em três categorias: falha de configuração, falha de software e falha humana. O sistema em si está inseguro e pode ser diretamente atacado. A senha de fábrica do equipamento não foi modificada, as opções de segurança não foram ajustadas ou uma permissão indevida foi dada. As falhas de segurança podem ser corrigidas atualizando os programas instalados. Os softwares incluem um recurso de atualização automática que pode ser ativado para que as falhas de segurança sejam corrigidas o quanto antes. As falhas humanas basicamente convence quem usa o computador a executar um programa desenvolvido pelo criminoso. Por isso, é preciso ficar sempre atento na hora de clicar em links e, especialmente, ao abrir programas. Manter o navegador web, sistema operacional e outros programas atualizados diminui bastante as chances de ser atacado por golpes na primeira categoria

### 2.4.1 - Sistemas

Sistema são os meios físicos e lógicos, humanos, financeiros, organizacionais e consumíveis diversos, que de maneira racional interagem entre eles, se integram e se combina com vista à produção, memorização, distribuição e consulta de informação, objetivando satisfazer determinadas necessidades, como dito em [10].

Conforme Amaral e Varajão [11], um sistema de informação reúne, guarda, processa e faculta informação relevante para esta seja acessível e útil para aqueles que fazem parte da organização incluindo gestores, funcionários e clientes.

### 2.4.2 – Informação

A informação pode ser considerada como os conjuntos de dados que geram conhecimento sobre um determinado assunto, fato ou fenômeno. O dado não define significado relevante e não produz compreensão.

Como afirma Beal [12], tudo aquilo que, diminuindo o nosso grau de incerteza, ou indefinição, nos potencializa a racionalidade para tomada de decisão é informação.

Amaral e Varajão [11] concordam que informação é junção de dados que, quando provido de forma e tempo apropriado, melhora o conhecimento da pessoa que o recebe, ficando ela mais capacitada a desenvolver determinada atividade ou a tomar determinada decisão em qualquer setor que atue.

Independentemente de como as informações estão armazenadas, se física ou virtualmente, seu valor é incomensurável para todos que dela fazem parte. Ainda que não necessitem de sigilo para certas operações, se relacionam às rotinas da empresa que podem paralisar com sua falta, segundo Neto e Solanca [13].

### 2.4.3 – Ameaça

A ameaça é a possibilidade do acontecimento de um incidente com algum ativo da organização, podendo levar danos à organização, como por exemplos inundação, roubo, erro de usuário, falha de hardware, dentre outros.

Para Sêmola [14], representam agentes dentro ou fora das organizações, que podem encontrar vulnerabilidades, causando incidentes que impactem os negócios.

Segundo Amaral e Varajão [11] podem se originar de fenômenos da natureza como terremotos ou enchentes; podem ser voluntárias por ações mal-intencionadas de funcionários insatisfeitos, vazamento de informação e ataque de vírus que venha corromper o funcionamento dos sistemas, como também pode ser involuntárias por negligência ou imprudência de colaboradores despreparados.

### 2.4.4 – Vulnerabilidade

A vulnerabilidade é um ponto da organização que contém debilidade de segurança e pode ser afetado por uma ameaça, causando danos a empresa. Exemplos: portas destrancadas, erro na alocação de privilégios para alguns usuários, falta de manutenção, configuração incorreta.

Para Beal [12], representa um elemento ou conjunto de falhas com possibilidade de ser explorados por uma ameaça e causar danos às informações e à organização. Para Baruque e Santos [10], é uma fragilidade que possibilita uma ameaça a efetivar um ataque.

Vulnerabilidade constitui a "fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças", conforme Norma ABNT NBR ISO/IEC 27002:2005 [4].

### 2.4.5 – Incidentes

Os incidentes de segurança podem ser definidos como quaisquer eventos adversos, confirmados ou não, relacionados a segurança de sistema de computação como também de redes de computadores.

Segundo Manoel [6], trata-se de um "fato imprevisível que ocorre no decurso de um acontecimento principal e pode ou não influir no seu desenvolvimento."

Godim [15] define incidente computacional como sendo qualquer ação ilegal, não autorizada ou inaceitável que envolve um sistema computacional ou rede de computadores causando danos.

O CERT (Centro de Estudos, Resposta e Tratamentos de Incidente de Segurança no Brasil) [16] apresenta dados estatísticos reportados pelas empresas brasileiras e as análises apontam para um crescimento alarmante, como mostra as figuras 2.2, com o total de incidentes reportados do CERT.br por ano e a figura 2.3, com total de incidentes reportados do CERT.br por ano separados por tipos de ataque.

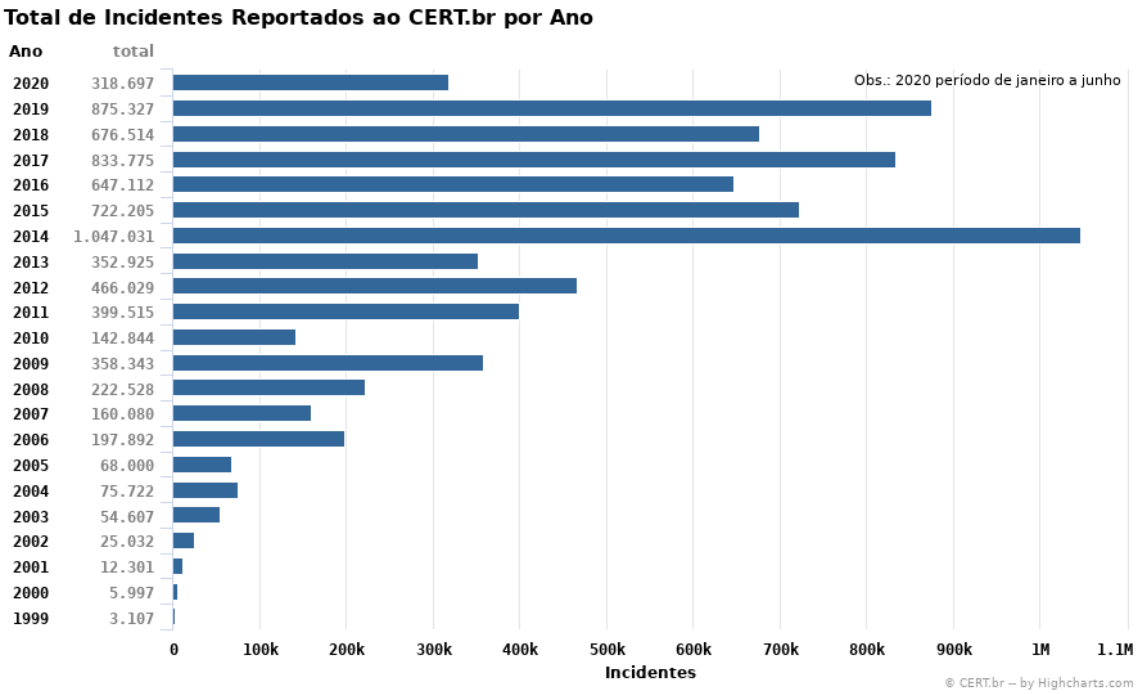


Figura 2.2 – Total de incidentes reportados do CERT.br por ano
Fonte: CERT.BR (2020)

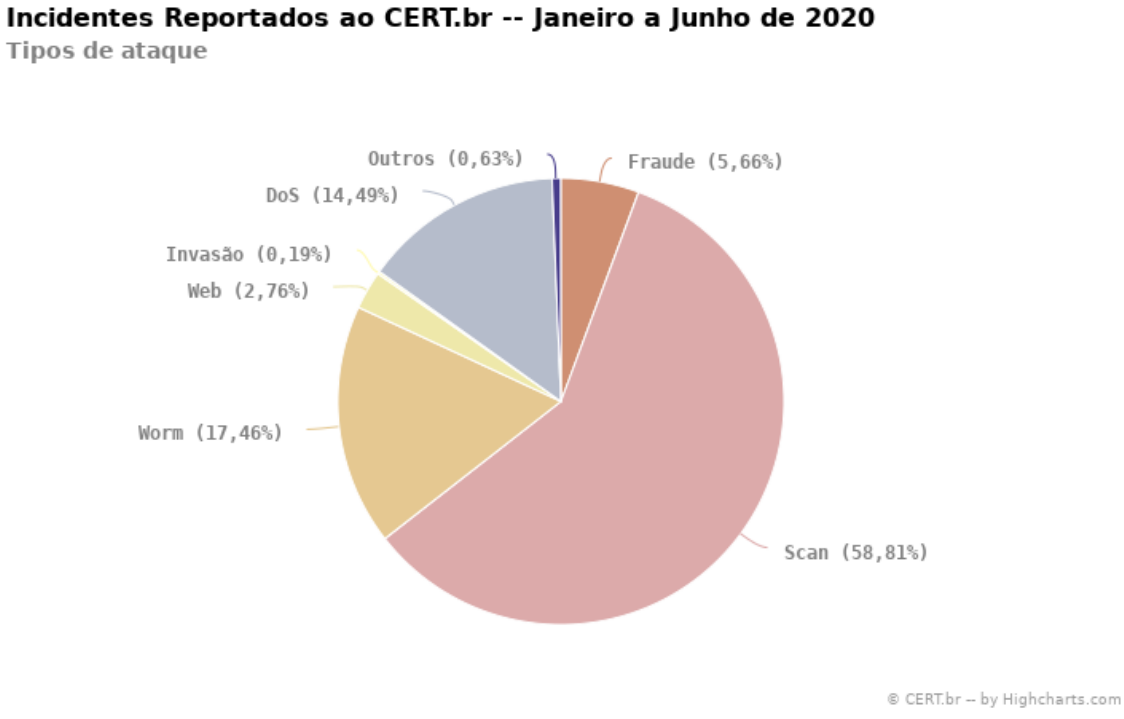


Figura 2.3 – Total de incidentes reportados do CERT.br por ano – tipos de ataque

Fonte: CERT.BR (2020)

CERT. BR [16] ainda apresenta informações detalhadas sobre os tipos de incidentes.

- ***worm***: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **invasão**: um ataque bem-sucedido que resulte no acesso não autorizado a um computador ou rede.
- ***web***: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- ***scan***: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

A figura 2.4 apresenta perdas financeiras em milhões de dólares provocados pelo ataque de Ransomware em grandes empresas.

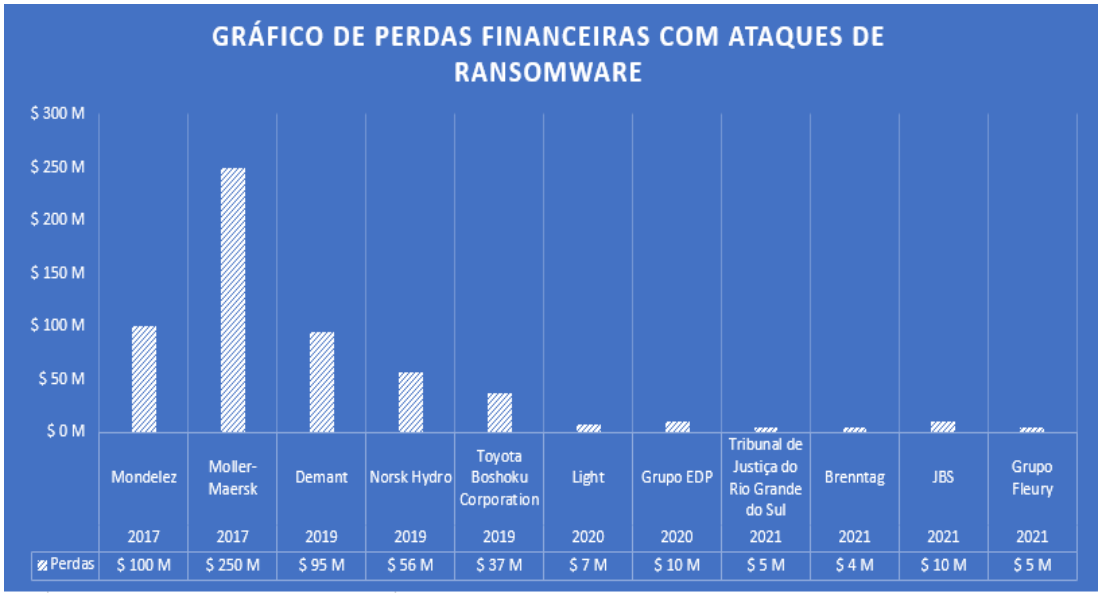


Figura 2.4 – Gráfico de perdas financeiras com ataques de *Ransomware*

Fonte: Autor

A Mondelez [17] empresa American Food, Confeitaria e Beverage Company em 2017, teve perda de 100 milhões de dólares, no mesmo ano, A Moller-Maersk [18] maior companhia de transportes marítimos do mundo foi vítima do vírus Petya com perda de 250 Milhões de dólares. Em 2019 a Demant [19] maior empresa fabricantes mundiais de aparelhos auditivos teve perda de 95 milhões de dólares, no mesmo ano a Norsk Hydro [19] produtora mundial de

alumínio teve perda de 56 milhões e a Toyota Boshoku Corporation [20] fornecedora de autopeças 37 milhões de doláres nesse mesmo ano provocados pelo ataque de *Ransomware*.

Em 2020 a Light [21] empresa de geração e distribuição de energia do Rio de Janeiro foi invadida por meio de um malware *Ransomware* tendo perda de 7 milhões de dólares, seguido do Grupo EDP [21] responsável pela transmissão e comercialização de energia em 11 estados brasileiros sofreu um ataque sendo exigido 10 milhões de dólares para o pagamento do resgate.

Em 2021 o Tribunal de Justiça do Rio Grande do Sul [22], sofreu um ataque de Ransomware, oficialmente o TJ RS não revela se pagou ou não resgate aos hackers para recuperar os dados criptografados no ataque hacker. O mercado especula que os hackers teriam cobrado 5 milhões de dólares. A Brenntag [23] empresa de distribuição de produtos químicos também desembolsou o equivalente a 4,4 milhões de doláres em um ataque executado pelo DarkSide.

A JBS gigante mundial do setor de carnes [24] teve 10 milhões de dólares de prejuízo para o resgate de seus dados, e a Fleury [24], que gastou 5 milhões de dólares. Ambas ocorrências foram registradas em Junho deste ano.

Hintzbergen et al [25] comenta que

> Uma exposição é a circunstância de estar exposto às perdas provenientes de um agente ameaçador. Uma vulnerabilidade expõe uma organização a possíveis ameaças. Se a gestão de senhas for fraca e as regras para senhas não forem aplicadas, a empresa fica exposta à possibilidade de ter a senha de usuários capturada e usada de forma não autorizada. Se uma empresa não tem seu cabeamento inspecionado e não estabelece medidas proativas de prevenção contra incêndios, ela se expõe a incêndios potencialmente devastadores.

## 2.5 Avaliação de Riscos

O processo de tratamento da gestão de riscos em segurança da informação, considerando as particularidades das normas da ABNT, os aspectos de definição de contexto, análise e avaliação de riscos, tratamento, aceitação, monitoramento e análise crítica dos riscos, comunicação e melhoria contínua.

Segundo a ABNT NBR ISO 27005:2019 [26]

> (...) abordagem sistemática de gestão de riscos de segurança da informação ê necessária para se identificar as necessidades da organização em relação aos requisitos de segurança da informação e para criar um sistema de gestão de segurança da informação (SGSI) que seja eficaz. Convém que esta abordagem seja adequada ao ambiente da organização e em particular esteja alinhada com o processo maior de gestão de riscos corporativos.

A ABNT NBR ISO 27005:2011 [27] "reafirma a importância da gestão de risco na segurança da informação para gerenciamento de incidentes e redução de prejuízos futuros. Tal associação destaca o quão fundamental é a comunicação dos processos de gestão de riscos não só entre gestores, mas também em áreas operacionais". De acordo com ABNT (2011) [27], "não basta implementar tratamentos de gestão de riscos, é preciso também comunicar os riscos e a natureza dos controles de riscos aplicados a todos os colaboradores que lidam com os sistemas".

Segundo a ABNT NBR ISO 27005:2019 [26], "Algumas formas de tratamento do risco podem lidar com mais de um risco de forma efetiva (por exemplo: o treinamento e a conscientização em segurança da informação)". De acordo com a ABNT (2019) [26], "Convém que um plano de tratamento do risco seja definido, identificando claramente a ordem de prioridade em que convém que as formas especificas de tratamento do risco sejam implementadas, assim como os seus prazos de execução. Prioridades podem ser estabelecidas usando várias técnicas, incluindo a ordenação dos riscos e a análise de custo-benefício. É de responsabilidade dos gestores da organização equilibrar os custos da implementação dos controles e o orçamento".

De acordo com a ABNT NBR ISO 27005:2019 [27], "Um incidente envolvendo a segurança da informação pode trazer consequências a vários ativos ou apenas a parte de um único ativo. O impacto está relacionado à medida do sucesso do incidente. Por conseguinte, existe uma diferença importante entre o valor do ativo e o impacto resultante do incidente. Considera-se que o impacto tem um efeito imediato (operacional) ou uma consequência futura (relativa ao negócio como um lodo), a qual inclui aspectos financeiros e de mercado".

## 2.6 - Aplicação no combate ao *ransomware* sob a ótica da Lei Geral de Proteção de Dados

Para compreender o termo *ransomware*, os autores Fornasier, Spinato e Ribeiro [20] explicam que "é utilizado genericamente para que se possa identificar um tipo de malware comumente usados para a prática de crimes de extorsão, quando ameaçam as vítimas por meios digitais''. Assim, o malware obriga as vítimas a fazer o pagamento de valores específicos para que elas recuperem os seus dados que foram roubados.

O conceito de *ransomware* não é algo novo, tendo suas origens encontradas no início da década de 1990, quando Joseph Popp escreveu os primeiros "códigos maliciosos", que infectariam computadores, criptografando suas informações. Fica claro que as tecnologias usadas naquela época não podem (nem devem) ser comparadas com as atualmente disponíveis ficando cada vez mais difícil coibir essa tipologia de crime [28]. A figura 2.5 apresenta as etapas do processo de um ataque de *ransomware*.

Conforme destacado na figura 2.5 a anatomia de um ataque *ransomware* inicia com a implantação no hospedeiro por meio de um download, phishing e exploração de vulnerabilidades, após o malware infectar o computador, são redefinidas as chaves do Windows para iniciar todas as vezes automaticamente. O comando e controle é estabelecido da geração de duas chaves de criptográficas, sendo uma mantida no computador da vítima e a outra enviada para o cibercriminosos. Com a comunicação estabelecida começa o processo de encriptação de todos os arquivos do computador da vítima. E por fim, o *ransomware* poderá exibir uma tela com limite de tempo para pagamento do resgate em forma de bitcoins não rastreáveis.

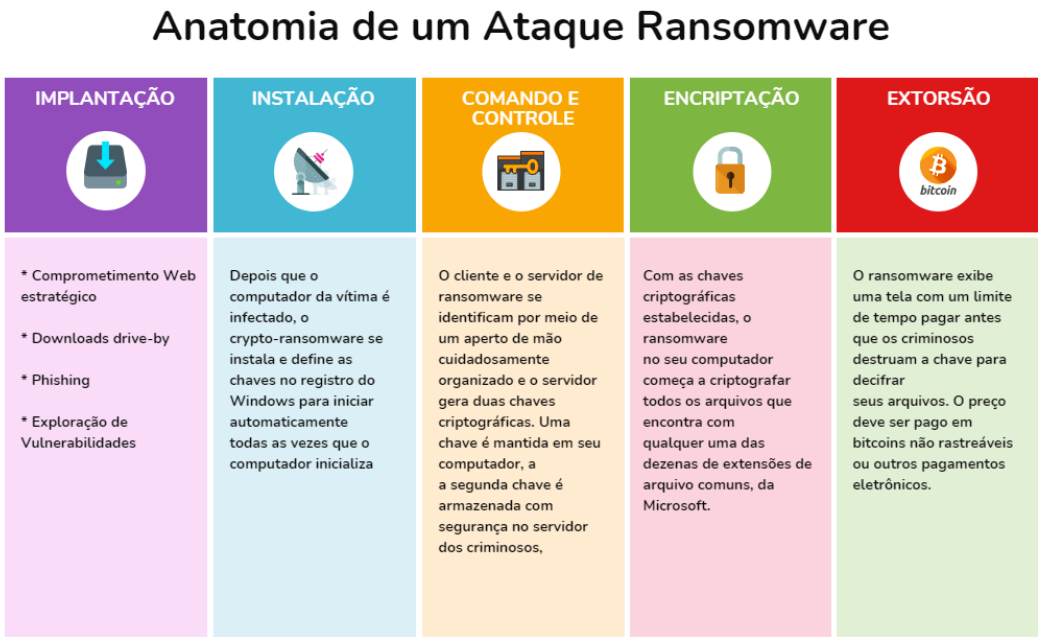


Figura 2.5 – Anatomia de Ataque *Ransomware*

Fonte: LISKA, A.; GALLO, 2017

Dessa forma, a Lei Geral de Proteção de Dados Pessoais (LGPD) de número 13.709 [22] altera a Lei n 12.965 – o Marco Civil da Internet. A partir da Medida Provisória (MP) n. 869/2018, a LGPD entrou em vigência em agosto de 2020, visto que "em 2020, devido à crise global provocada pela pandemia do novo coronavírus (Covid-19), […] foi aprovada uma nova MP para que as empresas não sejam penalizadas por não se adequarem à lei [31]. Isso ocorreu porque recomendações de isolamento social foram adotadas como parte de combate a pandemia, assim, a lei começou a valer no dia 03 de maio de 2021.

O artigo 6º da LGPD traz dez princípios da boa-fé que devem ser levados em consideração no tratamento dos dados pessoais, são eles: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e, a responsabilização e prestação de contas.

Entre os dez princípios citados, o da segurança afirma que é preciso "adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" [31]. Junto à segurança, é necessário adotar medidas para prevenir a ocorrência de danos, além de adotar medidas eficazes de comprovar o cumprimento das normas de proteção de dados pessoais.

> Hoje, a lei abre espaço para um novo perfil profissional, que é o Data Protection Officer (DPO), profissional de extrema importância, pois tem conhecimento sobre como deve ser executada a proteção de dados pessoais e sobre as regras e os regulamentos brasileiros em matéria de privacidade e proteção dos dados em ambiente corporativo [23].

Esse profissional organiza ações de proteção de dados em ambientes coorporativos, além de treinar a empresa para que ela tenha disciplina e saiba tratar os dados pessoais que têm em mãos à luz da legislação vigente.

Por conseguinte, a Lei de Geral de Proteção de Dados apresenta a forma de mapear dados com segurança: identificar o fluxo desses dados, avaliar a necessidade do seu armazenamento, mapear os controles de segurança utilizados, analisar o risco e possíveis vulnerabilidades e monitorar quem está acessando e de onde está acessando [31]. Para tanto, o artigo 5 da Lei ressalta que o tratamento de dados é

> X - Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração [30].

Dessa maneira, a proteção da informação em conformidade com a LGPD perpassa por: *hardening* dos servidores (conjunto de ações que deixa os servidores protegidos), proteção das estações de trabalho (por meio da criptografia, softwares de antivírus atualizados e ativos permitir uma conexão via VPN segura e criptografada com a rede da empresa e manter a política de senhas atualizada) [31].

Assim, tem-se o princípio do menor privilégio (a ideia é limitar privilégios, especificando o que um usuário pode fazer de maneira muito granular), o controle de acesso (atribuições de permissões de acesso a todos os tipos de objetos – pastas, arquivos, banco de dados), a auditoria (é um controle de segurança dissuasivo, pois usuários mal-intencionados não irão se arriscar em ambientes que eles sabem que estão sendo monitorados), a análise de vulnerabilidades e os planos de recuperação de desastres. Não se pode esquecer da tríade que compõe a segurança da informação: confidencialidade, integridade e disponibilidade [31]. Na figura 2.6, podem-se ver explicações sobre cada um dos pontos desta tríade.

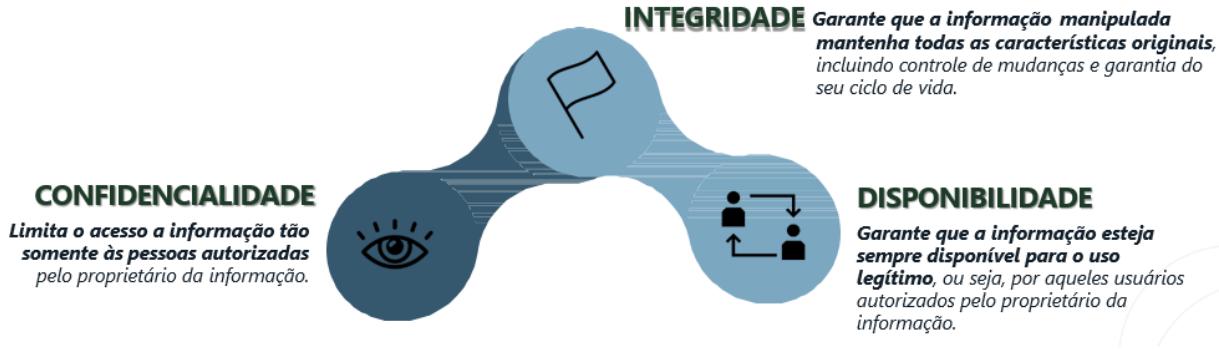


Figura 2.6 - Princípios da Segurança da Informação

Fonte: Autor

## 2.7 - Adoção de políticas de segurança na informação

Com base na análise de dados e de *ransomware*, conclui-se que a melhor forma de se proteger desses ataques é realizar um *backup* regularmente, "Convém que cópias de segurança das informações, dos s*oftwares* e das imagens do sistema sejam efetuadas e testadas

regularmente conforme a política de geração de cópias de segurança definida.” [4]. Assim como “Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra malware, combinados com um adequado programa de conscientização do usuário. [4]. Diretrizes para implementação “Convém que a proteção contra malware seja baseada em software de detecção e resposta a malware, na conscientização da segurança da informação, no controle de acesso adequado e nos controles” [4].

“As informações pessoais diariamente despejadas nas redes compartilhadas, são inúmeras e fazem com que bancos de dados tenham uma visão praticamente completa de vidas, interesses, gostos e poder de compra” [28]. No mercado, esse tipo de informação é extremamente valioso, porque quem a detêm sabe como deve proceder para que seu produto venda mais.

Desta forma, é possível entender que a moeda mais cara atualmente é a informação que empresas e indivíduos fornecem a organizações que exploram as redes – e que monetizam esses dados para auferir lucro e fazer suas ações de marketing. O que acontece é que cada vez mais criminosos tentam roubar esses dados, para conseguir, com chantagens e ameaças, valores para que a vítima tenha de volta aquilo que é seu por direito [28].

# CAPÍTULO 3

# Propostas Tecnológicas

## 3.1 - Histórico do incidente

A empresa utilizada neste estudo pertence ao segmento de importação e distribuição de material médico hospitalar, de médio porte, situada no Rio de Janeiro, a qual, com o ataque do vírus *ransomware*, teve o servidor de banco de dados Oracle e seus *backups* criptografados, acarretando enormes prejuízos. Assim, a empresa deixou de honrar seus compromissos com clientes e fornecedores por ter suas atividades suspensas. Dessa maneira, a figura 3.1 mostra que a conexão ao sistema não pôde ser realizada.

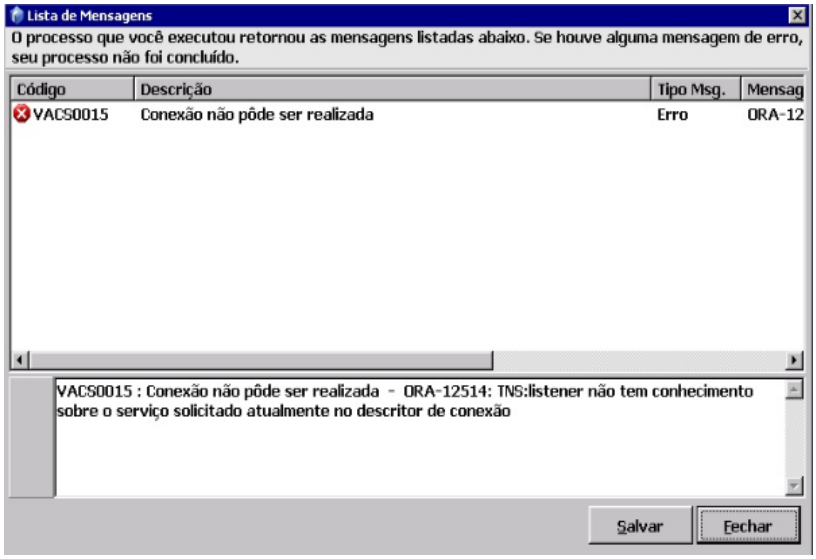


**Figura 3.1** - Conexão recusada ao tentar acessar o sistema
Fonte: Servidor Empresa Alfa

Sem restabelecer uma conexão com o sistema de gestão da empresa, o próximo passo da TI foi identificar no próprio servidor hospedado no *data center* a causa raiz do problema.

A equipe de TI acessou o servidor de produção do banco de dados sendo identificado erro de perfil temporário, que ocasiona acesso limitado aos recursos do servidor. Quando tentou-se acessar o utilitário de administração de ferramentas do servidor de banco de dados para um diagnóstico mais assertivo, apresentou outro erro, sendo impedido de se executar a ferramenta de diagnóstico, conforme ilustrado abaixo na figura 3.2:

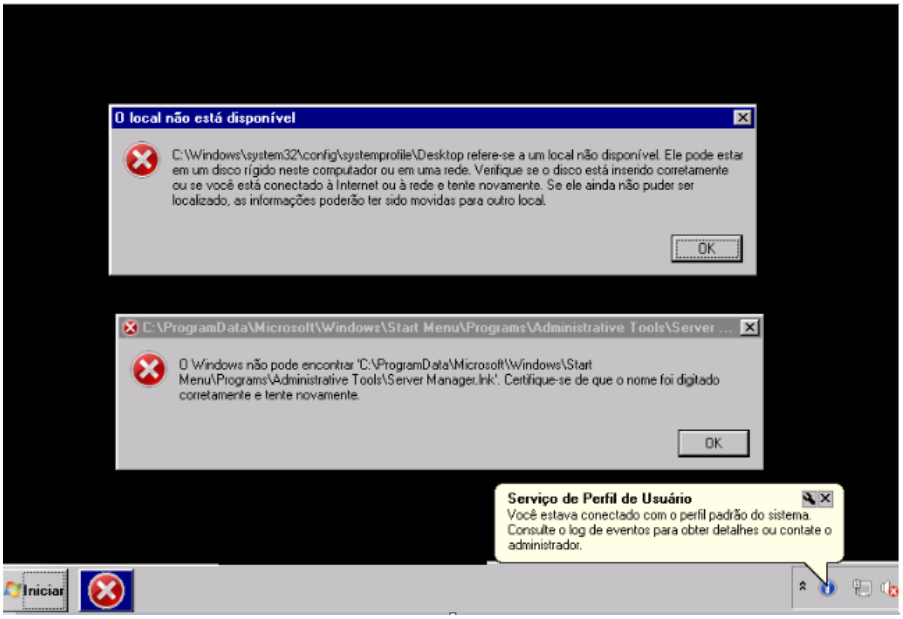


**Figura 3.2** - Erro de perfil temporário

Fonte: Servidor Empresa Alfa

Uma nova tentativa foi feita pela equipe a fim de verificar o servidor de produção do banco de dados, com o intuito de acessar as ferramentas de sistema, porém sem sucesso, pois foi identificado que todo o sistema havia sido criptografado por um ataque de *ransomware*, cuja ID-5A6BCD61. conforme figura 3.3:

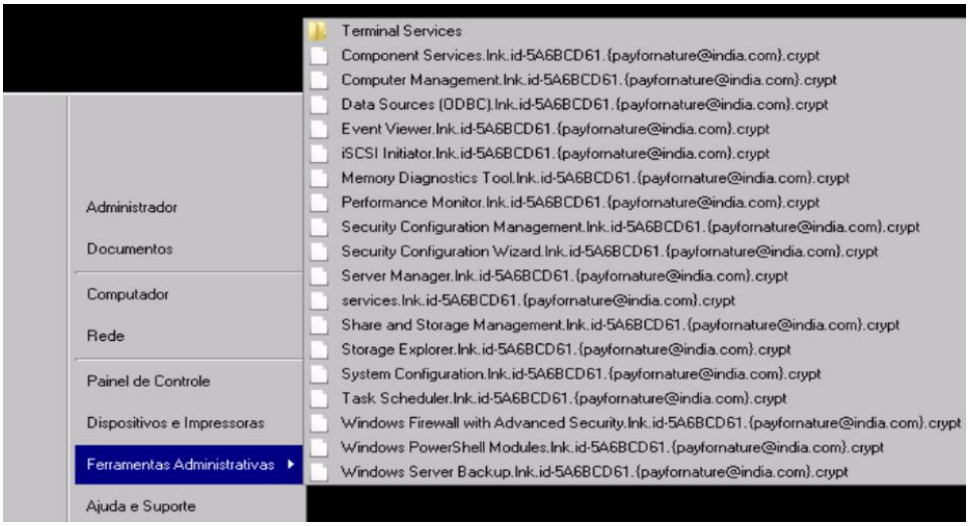


**Figura 3.3** – Serviços Encriptados pelo *Ransomware*

Fonte: Servidor Empresa Alfa

A criptografia gerada deixou os serviços do sistema operacional inoperantes, assim como o serviço de banco de dados da empresa inacessíveis para operação. A estrutura de diretório do servidor de produção também foi impactada, impedindo qualquer tipo de acesso ou cópias.

Os profissionais tentaram realizar o *decrypt* dos arquivos infectados pelo *malware Ransomware* (CRYPT), sem sucesso. O plano de restauração do sistema operacional com ferramentas específicas, fracassaram. Uma varredura do sistema operacional foi executada com as ferramentas BitDefender e Avira, contudo, também sem sucesso.

Como os procedimentos realizados pelos funcionários não foram bem-sucedidas, a direção decidiu instaurar um comitê de crise para aprovar a liberação de recursos financeiros com a finalidade de criar um servidor de contingência no *data center* e restaurar o último *backup* da base de dados.

Por meio da abertura de chamado, foi acionado o fornecedor terceiro que administra o banco de dados do servidor produção. Em paralelo foi aberto o chamado com a Equinix, que faz a gestão do ambiente e administra o *backup* do banco de dados, com a finalidade de verificar o último *backup* realizado e apoiar na atividade de remoção do *ransomware*.

Em resposta ao chamado aberto, a Equinix informou ao cliente que não possui em contrato nenhum gerenciamento proativo, consequentemente, não poderia ser prestado o devido suporte para remoção e configuração do servidor infectado.

Diante da reposta do ticket, a equipe de TI fez nova abertura de chamado, solicitando a evidência do último *backup* full realizado. Conforme resposta do ticket, o último *backup* íntegro disponível, tinha sido feito há 12 dias do ataque.

Quando foi verificado o *backup* pelo administrador do banco de dados, constatou-se, que não serviria para a restauração, pois o sistema de I não estava fazendo dos diretórios corretos. Os diretórios onde os dados eram acessados pelo sistema, haviam sido alterados e o setor de infraestrutura de TI da empresa não foi comunicado para revisão da política de *backup*. Portanto, a empresa Alfa estava descoberta tanto na segurança de TI, quanto na gestão de contrato, que supostamente estabelecia a gestão de infraestrutura onde hospedavam os servidores, como também na continuidade do negócio, pois não havia o *backup* do banco de dados para restauração da operação na empresa.

## 3.2 – Infraestrutura Atual

O contrato de aluguel de *firewalls* atende todas as unidades com equipamentos únicos, sem nenhum tipo de contingência. Não existem VPNs entre as filiais e tampouco no sistema da empresa. O acesso ao servidor do sistema é realizado por meio do *Remote Desktop Protocol* (RDP).

O contrato de gerenciamento do ambiente de servidores é serviço de *Co-location* que significa que o *data center* hospeda os ativos de infraestrutura sem gerenciamento proativo. *Co-location* é um serviço que o *data center* oferece para guardar o servidor na infraestrutura deles. A figura 3.4 apresenta a topologia da infraestrutura do Core Business.

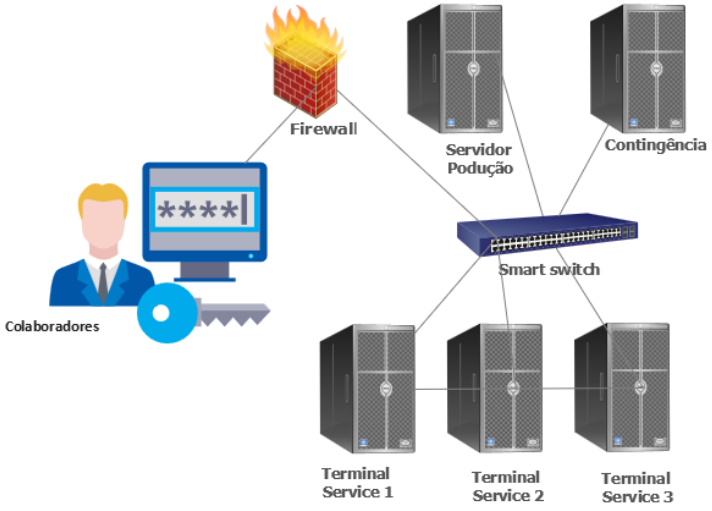


**Figura 3.4 -** Topologia do *Core Business*

Fonte: Autor

Os colaboradores acessam o sistema por meio da conexão RDP e o serviço *load balancing microsoft terminal services* é encarregado de dimensionar a carga de usuários a partir dos três servidores para não comprometer o desempenho do acesso. A arquitetura atual está composta, de acordo com a figura 3.5:

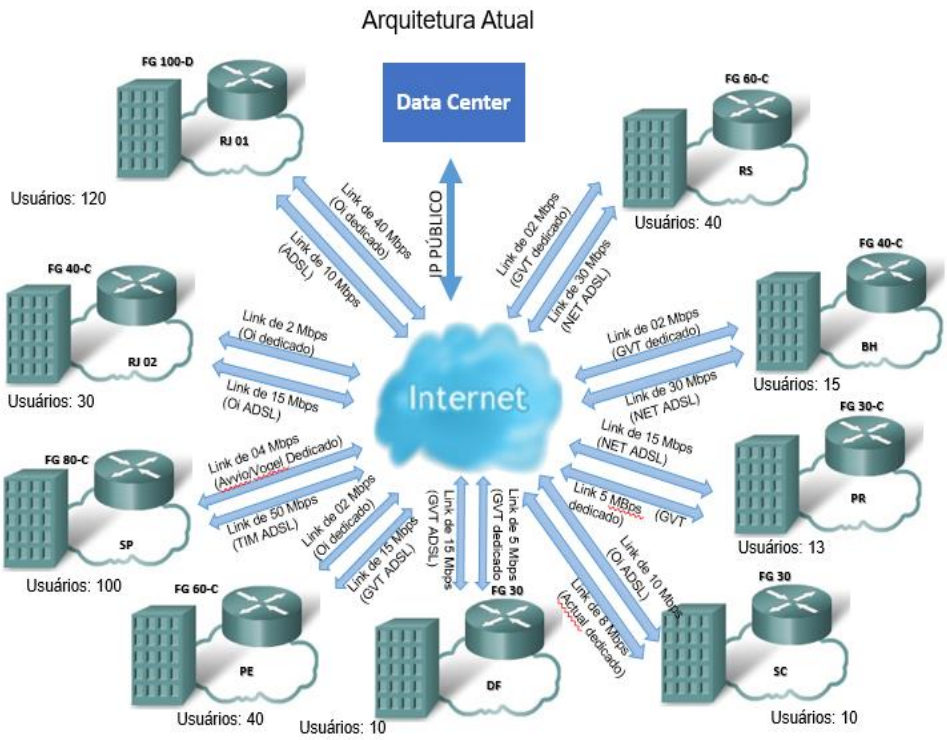


**Figura 3.5** – Arquitetura atual

Fonte: Autor

A infraestrutura de rede Wi-Fi não permite a configuração de uma rede específica para os visitantes que seja totalmente separada rede interna. Não há nenhum tipo de gestão estratégica dos *firewalls* no ambiente por parte do fornecedor ou da equipe responsável.

O monitoramento dos *firewalls* e *links* de internet está ausente de qualquer responsabilidade. Os chamados nas operadoras de telecomunicações são feitos nas primeiras horas da manhã, quando então inicia o prazo de SLA acordado com as operadoras.

Os relatórios operacionais e gerenciais de consumo de internet não existem para uma gestão eficiente dos links de Internet. O *service level agreement* ou acordo de nível de serviço (SLA) para atendimento em casos críticos são de oito horas úteis.

## 3.3 – Estrutura do *backup*

O sistema de *backup* em cada filial é o Bacula® *Open Source Network Backup Solution*. Uma solução de gerenciamento de *backup Open Source*. O Bacula é gerenciado e monitorado diariamente por um fornecedor terceiro, garantindo assim que todos os procedimentos de *backup* estejam de acordo com as políticas estabelecidas no que tange aos backups dos servidores locais e caixas de e-mails da gerência e supervisão.

A política de *backup* de cada filial, define o armazenamento em uma estrutura local, garantindo a autonomia do seu funcionamento. Para cada filial, estão definidos os meios de armazenamento do *backup*. Desta forma, o funcionamento do *backup* será independente de *link* de internet, bastando apenas a conexão da rede local. O sistema faz o *backup* apenas de diretórios dos servidores de arquivos.

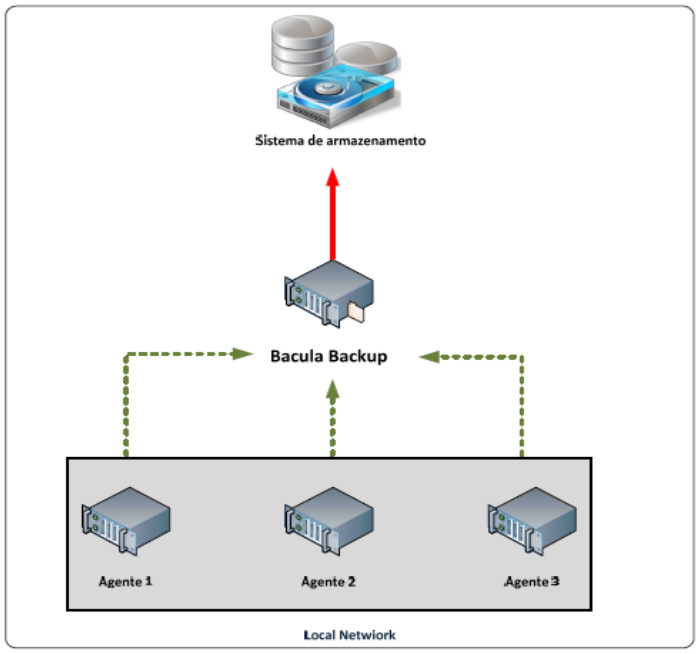


**Figura 3.6** – Arquitetura do Sistema Bacula *Backup*
Fonte: Autor

Em concordância com o que está ilustrado na figura 3.6, é instalado um agente do Bacula em cada servidor alvo designado. Após esta instalação, o sistema transfere os dados para um dispositivo de armazenamento local conforme a topologia do *backup* apresentado na figura 3.7.

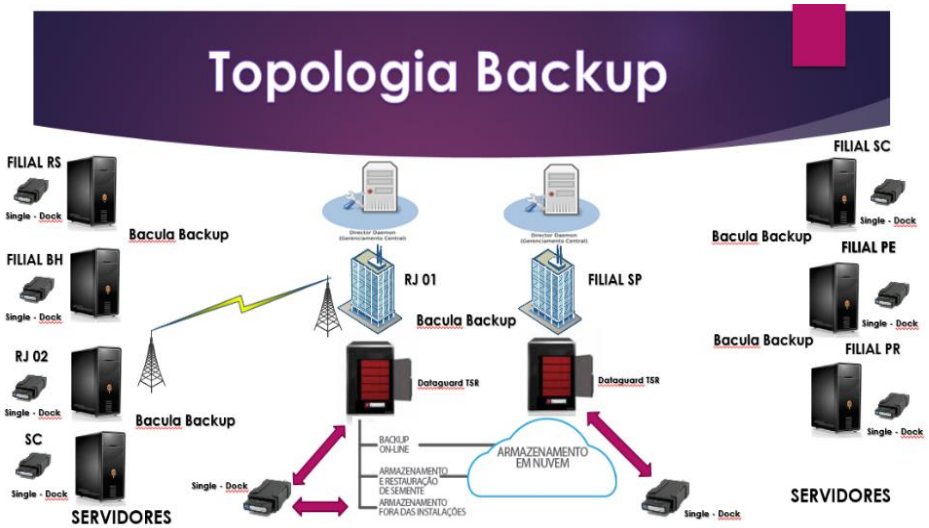


**Figura 3.7** – Topologia do *backup* com o Bacula
Fonte: Autor

O sistema possui limitações técnicas envolvidas, pois, conforme destacado na política de *backup*, ele cópia e restaura as informações apenas de pastas do servidor de arquivos em um dispositivo local.

## 3.4 – Visão da TI perante o negócio

Diante da situação atual da área de TI, não existe um responsável claro para os incidentes, assim como a ausência de procedimentos e processos padronizados. Esta ausência causa dificuldade no treinamento de novos colaboradores da área nas filiais.

As equipes do segmento das filiais não se sentem obrigadas a discutir previamente com a TI da matriz a implementação de novas tecnologias ou execução de investimentos, causando impacto na organização como um todo.

Por conta da falta de alinhamento estratégico, os departamentos de TI das filiais não têm nenhuma sinergia com a matriz. Periodicamente, a TI da Matriz é surpreendida por incidentes nas filiais onde que atuam sem nenhum conhecimento prévio sobre o assunto, conforme a ilustração da figura 3.8.

Tipos de ausência de alinhamento estratégico: desligamento de colaborador sem a TI ser previamente avisada, compras de equipamentos sem padronização e alinhamento, softwares fora do padrão de licenças, falhas na comunicação e processos que são decididos nas filiais e não são repassados para a TI da matriz.

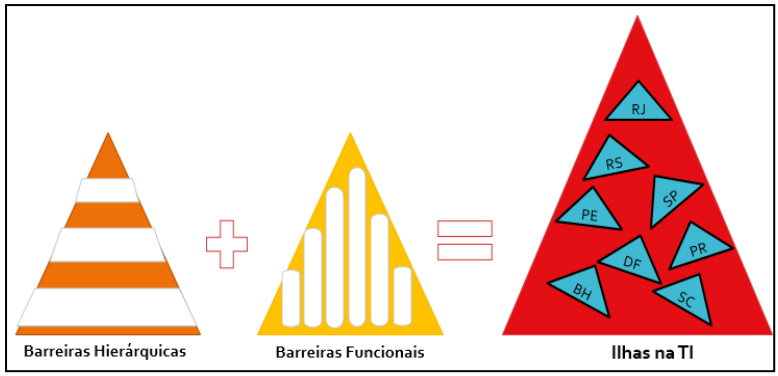


**Figura 3.8** – Descentralização da TI (1)
Fonte: Autor

A falta de clareza na responsabilidade dos processos tem prejudicado o atendimento às demandas dos usuários. Estamos falando de situações referentes ao dia a dia que ocorrem na Matriz e nas filiais, e não nos projetos, pois é no dia a dia em que se nota a necessidade de atribuição de responsabilidade, delegar de forma clara quem é o responsável por determinado processo e quem é o responsável por executar determinada atividade.

Para confirmar esta análise, outro problema recorrente na empresa Alfa é falta de comunicação entre as equipes da matriz e das filiais, antes destas executarem algum investimento ou fazer alguma aquisição. Por diversas vezes a TI da matriz teve que atuar em projetos já em andamento para corrigir ou padronizar tecnologias, devido à ausência de diálogo antes de iniciarem os trabalhos. Outro aspecto desta falta de interação é a demora na atuação da TI da matriz em incidentes nas filiais, devido a falha de comunicação é necessário se inteirar do acontecimento antes de tomar medidas de contorno e solução.

A diretoria da organização não vê a TI como agregador de valor ao negócio, apenas como suporte operacional dos usuários. Os conflitos de responsabilidade entre matriz e filiais são comuns, obrigando à diretoria a atuar como mediadora conforme ilustrado na figura 3.9.

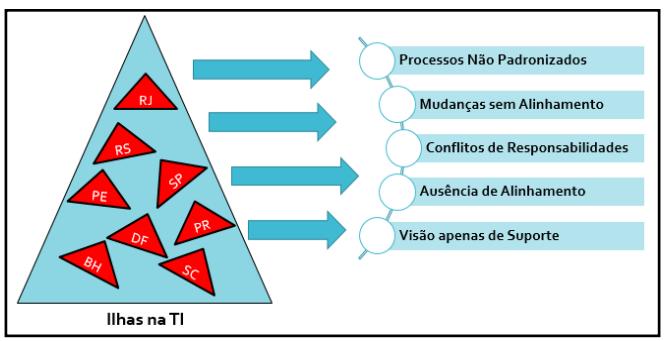


**Figura 3.9** – Descentralização da TI (2)
Fonte: Autor

## 3.5 – Análise do ambiente

Para compreender melhor o cenário que culminou o ataque de *ransomware*, onde o servidor e seus *backups* foram criptografados, foi aplicado um levantamento, por meio de um questionário com os membros do comitê de TI, visando identificar as vulnerabilidades que contribuíram para o ataque cibernético na infraestrutura de TI, conforme no quadro 3.1.

Quadro 3.1 – Modelo do questionário respondido pelo comitê

| | **Questionário Realizado** | SIM | NÃO |
|---|---|---|---|
| 1 | A empresa possui sistema de backup eficiência que possibilidade replicação para outro local? | | x |
| 2 | A empresa possui contrato de gestão proativa dos servidores no data center? | | x |
| 3 | A empresa faz uso de algum sistema de monitoramento dos servidores no data center? | | x |
| 4 | O departamento de TI da empresa faz uso de controle para monitoramento de fornecedores? | | x |
| 5 | O departamento de TI da empresa faz uso de boas práticas na gestão de service desk? | | x |
| 6 | Na organização os acessos ao sistema da empresa são por meio de VPN? | | x |
| 7 | A organização possui contratos de gestão proativa da infraestrutura de servidores? | | x |
| 8 | Na organização o antivírus é gerenciado pelo setor de Tecnologia? | | x |
| 9 | Na organização os processos de TI são padronizados? | | x |
| 10 | A infraestrutura de rede Wi-Fi permitem a configuração de uma rede específica para os visitantes? | | x |
| 11 | A organização possui monitoramento dos firewalls? | | x |
| 12 | Na organização existem relatórios operacionais e gerenciais de consumo de internet? | | x |
| 13 | Na organização possui sistema que realiza o backup completo dos servidores virtualizados? | | x |
| 14 | A organização possui procedimento ou sistema para a gestão de patches de segurança? | | x |
| 15 | A TI da empresa ocorrem mudanças sem alinhamento? | | x |
| 16 | A empresa possui firewall de redundância em caso de incidentes? | | x |
| 17 | Existem problemas por falta de treinamento? | | x |
| 18 | No departamento de TI existe ausência de definição de papéis? | | x |
| 19 | O departamento de TI é realiza a gestão de contratos com fornecedores? | | x |
| 20 | O departamento de TI possui sistema de inventário de ativos? | | x |
| 21 | O active diretory da empresa é integrado com todas as filiais? | | x |
| 22 | Os usuários possuem bloqueios para instalar programas? | | x |
| 23 | A empresa possui balanceamento de link de internet? | | x |
| 24 | A empresa possui políticas de firewall completas para navegação? | | x |
| 25 | O departamento de TI possui o controle do licenciamento? | | x |

Fonte: Autor

O segundo passo após o preenchimento do questionário é a apresentação de um mapa de riscos com base na probabilidade de impacto em relação a cada pergunta. Os resultados podem ser acompanhados no quadro 3.2 e na figura 3.10:

Vale ressaltar que o questionário abordou a análise da situação atual do ambiente de infraestrutura local da empresa apontando vulnerabilidades que levarão a conclusão de resultados significativos que serão apresentados a partir da matriz risco versus impacto.

**Quadro 3.2** – Análise das respostas do questionário proposto ao comitê

Impacto (- / +)

Probabilidade (+ / -)

| | Muito Baixo | 2. Baixo | 3. Moderado | 4. Alto | 5. Muito Alto |
|---|---|---|---|---|---|
| Quase Certo | Significante | Pouco Crítico | Crítico | Muito Crítico | Muito Crítico |
| Muito Provável | Significante | Muito Significante | Pouco Crítico | Crítico | Muito Crítico |
| Pouco Provável | Pouco Significante | Significante | Muito Significante | Pouco Crítico | Crítico |
| Improvável | Insignificante | Pouco Significante | Significante | Muito Significante | Pouco Crítico |
| Raro | Insignificante | Insignificante | Pouco Significante | Significante | Muito Significante |

Fonte: Autor

Não existe um modelo ideal pronto, a empresa deve preparar um projeto de segurança da informação combinando estratégias de acordo com o tipo de negócio, ambiente operacional. O processo de gestão de riscos, inclui identificação, análise, avaliação e tratamento dos riscos que causem a interrupção de seus negócios.

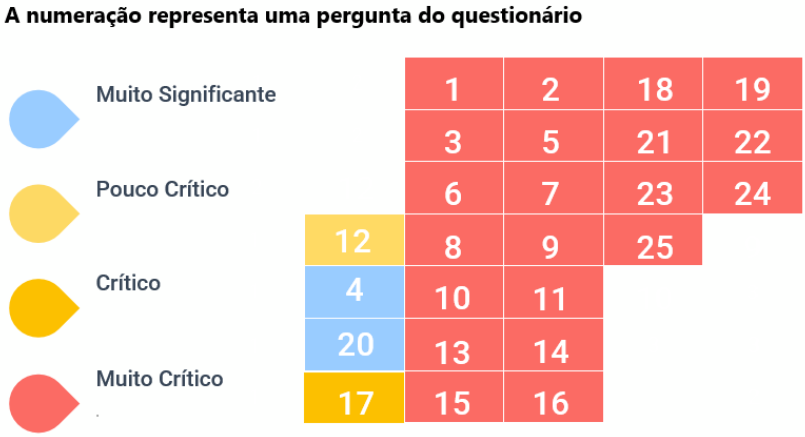


**Figura 3.10** – Quantidade de respostas e classificação.

Fonte: Autor

O incidente de segurança da informação, ocorre a partir da ação de ameaça, explorando uma ou mais vulnerabilidades, causando a perda da segurança da informação e comprometendo o negócio. Quanto aos impactos muito críticos conforme apresentado na figura 3.10, deve promover a identificação dos principais pontos de vulnerabilidades e tratar os riscos que causem interrupções do negócio por meio da identificação, análise, avaliação e tratamento dos riscos.

## 3.6 – Identificação dos principais pontos de vulnerabilidades

A figura 3.11 demonstra de uma forma sintética os principais pontos de vulnerabilidades identificados que precisarão de atenção para ser estabelecido um plano de ação.

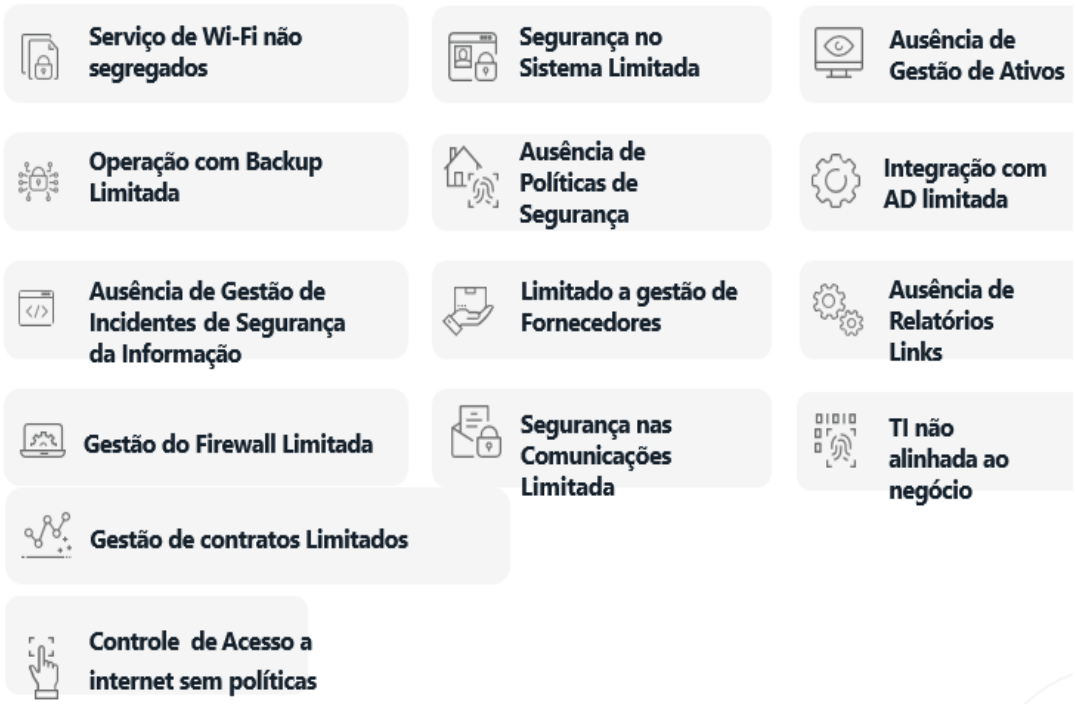


**Figura 3.11** – Principais pontos de vulnerabilidades

Fonte: Autor

## 3.7 – Sugestão Proposta

Logo após o evento que sucedeu a invasão no servidor de banco de dados foi avaliado que o impacto da parada no sistema por 12 dias, causou a organização prejuízo direto de R$ 6.5 milhões, além disso, levou meses até a empresa se restruturar com seu faturamento, comprometendo as rotinas de vendas, estoque, financeiro contas a pagar e receber. Ao mesmo tempo que os processos estávam sendo restruturados medidas tiveram que serem tomadas, como a avaliação do ambiente no *data center* da Equinix, pois devido a invasão a conclusão que se chega, é que o ambiente não seria seguro. Portanto, torna-se necessário avaliação para troca tanto do ambiente de infraestrutura dos servidores como da gestão e monitoramento dos ativos.

A infraestrutura de segurança local teve que ser avaliada e o comitê técnico propos com o levantamento interno realizado, a contratação de uma consultoria especializada com o objetivo de identificar as necessidades de segurança de borda e vulnerabilidades do ambiente. As políticas de segurança do AD precisarão que ser revistas para uma solução de gerenciamento unificado, assim como o *firewall.*

Na arquitetura, atualmente os sites não funcionam com alta disponiiblidade causando problemas na operação do negócio. A nova proposta prevê que todos os sites funcionarão em alta-disponibilidade de forma a permitir a criação de uma WAN englobando a Matriz, as filiais e o ambiente do sistema Oracle. Toda as conexões site to site serão feitas com túneis VPN.

A infraestrutura de rede Wi-Fi, é um item com grande vulnerabilidadde, pois não estão segregadas atualmente. Os colaboradores acessam pelo mesmo ambiente da rede principal, não havendo distinção de rede interna ou rede convidado. A proposta é que seja implmentado a segregação da redes Wi-Fi evitando, assim, que conexões móveis se conectem a rede interna principal.

O grau de maturidade do backup local está limitado por conta do sistema atual bacula que não atende aos requisitos de negócio, como replicação, backup de máquinas virtuais, desduplicação e backup em núvem. A solução proposta com base no levantamento técnico por meio de uma consultoria especializada, a indicação de um sistema de mercado e se necessário for a compra de hardware.

O controle de incidentes de segurança da informação deve ser instuído por meio de controles no ambiente *windows* e gestão dos *firewalls* de modo que seja possível, aplicação também de patchs de segurança para a atualização dos sistemas operacionais como forma de mitigar os impactos causados por brechas de segurança por conta da não aplicação dos patchs.

A gestão dos ativos de forma manual como é realizada atualmente, pode resultar em inumeras falhas quando um ativo é removido do parque de máquinas. A ausência de controle por falta de um sistema de inventário resulta na ineficiência da operação de TI quando tem que analisar e dimensionar a perfomance do hardware. A solução proposta prever a necessidade de um sistema de inventário para o departamento de TI.

Cabe ressaltar que nem todos os pontos identificados no relatório proposto pelo comitê de TI serão implementados a curto prazo, pois requerem aprovação no orçamento de TI, é o caso de treinamentos, sistema de controle de digitalização de contratos, e implementação de governança de TI.

Quadro 3.3 – Descrição da análise das respostas do questionário proposto pelo comitê

| Cód. | Severidade | Descrição do risco | Tipo | Probabilidade | Impacto | Descrição do Impacto | Ação | Descrição da ação | GAP IDENTIFICADO |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Muito Crítico | A empresa possui um sistema de backup eficiência que possibilidade replicação para outro local? | Ameaça | Muito Provável | Muito Alto | Em caso de falha no local, não há outro backup. | Mitigar | Propor troca do sistema de backup atual. | BACKUP |
| 2 | Muito Crítico | A empresa possui um contrato de gestão proativa dos servidores no data center? | Ameaça | Quase certo | Muito Alto | Em caso de incidente no local não há equipe no local disponível. | Mitigar | Propor troca para um modelo de contrato de gerenciamento ativo. | GESTÃO |
| 3 | Muito Crítico | A empresa faz uso de algum sistema de monitoramento dos servidores no data center? | Ameaça | Muito Provável | Alto | Em caso de falha de hardware e no sistema não há como prever. | Mitigar | Propor a revisão do contrato ou troca do ambiente. | MONITORAMENTO |
| 4 | Muito Significante | O departamento de TI da empresa faz uso de controle para monitoramento de fornecedores? | Ameaça | Pouco Provável | Moderado | Sem gestão dos entregáveis não se tem como medir o desempenho dos serviços | Prevenir | Digitalizar todos os contratos e inclui-los em um sistema de controle. | MONITORAMENTO |
| 5 | Muito Crítico | O departamento de TI da empresa faz uso de boas práticas na gestão de service desk? | Oportunidade | Muito Provável | Moderado | Sem inclusão de boas práticas, não é possível avaliar o desempenho do serviço. | Prevenir | Incluir treinamento para o time técnio ITIl, Cobit. | BOAS PRÁTICAS |
| 6 | Muito Crítico | Na organização os acessos ao sistema da empresa são por meio de VPN? | Ameaça | Quase certo | Muito Alto | Possibilidade de invasão provocado por um malware. | Mitigar | Incluir controle de acesso mais seguro. | FIREWALL |
| 7 | Muito Crítico | O departamento de TI possui gestão proativa do orçamento de TI? | Oportunidade | Quase certo | Alto | Dificuldade de realizar o orçamento previsto conforme planejado, trazendo imagem negativa para TI. | Mitigar | Instituir responsável para o controle do orçamento. | GESTÃO |
| 8 | Muito Crítico | Na organização o antivírus possui gerenciamento proativo? | Ameaça | Quase certo | Alto | Pode ocorrer risco de contaminação por vírus. | Mitigar | Estabeler os controles necessários no gerenciamento. | MONITORAMENTO |
| 9 | Muito Crítico | Na organização os processos são padronizados? | Oportunidade | Pouco Provável | Baixo | Processos sem definição de um padrão, causando descontrole. | Prevenir | Incluir boas práticas de governança de TI. | GESTÃO |
| 10 | Muito Crítico | Na organização a infraestrutura de rede Wi-Fi permitem a configuração de uma rede específica para os visitantes? | Ameaça | Quase certo | Muito Alto | Risco de contaminação na rede interna. | Mitigar | Instituir segmentação da rede interna com a rede visitantes | BOAS PRÁTICAS |
| 11 | Muito Crítico | Na organização possui monitoramento dos firewalls? | Ameaça | Muito Provável | Muito Alto | Risco de invasão na rede interna. | Mitigar | Instituir uma consultoria para gestão compartilhada do ambiente. | MONITORAMENTO |
| 12 | Pouco Crítico | Na organização existem relatórios operacionais e gerenciais de consumo de internet? | Oportunidade | Pouco Provável | Moderado | Não há métricas para os riscos de incidentes de quedas de internet. | Prevenir | Instituir controle no firewall. | MONITORAMENTO |
| 13 | Muito Crítico | A organização possui sistema que realiza o backup completo dos servidores virtualizados? | Ameaça | Quase certo | Muito Alto | Risco identificado na restauração e no tempo de recuperação do backup. | Mitigar | Substituir sistema de backup por uma solução que atenda a empresa. | BACKUP |
| 14 | Muito Crítico | A organização possui procedimento ou sistema para a gestão de patches? | Ameaça | Muito Provável | Alto | Risco de contaminação dos computadores por falta da aplicação de patchs de segurança. | Mitigar | Instituir solução para o controle de patches. | BOAS PRÁTICAS |
| 15 | Muito Crítico | Na TI da empresa ocorrem mudanças sem alinhamento? | Oportunidade | Quase certo | Alto | O departamento não é visto como estratégico, causando descontrole e falta de motivação da equipe. | Prevenir | Instuir boas prática de Governança. | GESTÃO |
| 16 | Muito Crítico | A empresa possui firewall de redundância em caso de incidentes? | Ameaça | Muito Provável | Muito Alto | Em caso de falha do firewall principal a organização fica vulnerável. | Mitigar | Propor redundância de firewall. | FIREWALL |
| 17 | Crítico | Na organização existem problemas por falta de treinamento? | Oportunidade | Muito Provável | Moderado | Sem capacitação adequada os profissionais não conseguem atender aos desafios crescentes de Tecnologia dentro | Mitigar | Incluir programa de treinamento anual. | GESTÃO |
| 18 | Muito Crítico | No departamento de TI existe ausência de definição de papéis? | Ameaça | Quase certo | Muito Alto | Quase sempre ocorre causando desorganização nas atividades e incidentes do dia a dia. | Mitigar | Incluir Matriz RACI para definição de papéis e responsabilidades | GESTÃO |
| 19 | Muito Crítico | No departamento de TI é realizado o controle de fornecedores? | Ameaça | Quase certo | Alto | O impacto é que não se consegue mensurar as entregas causando insatisfação e ausência de qualidade. | Mitigar | Incluir pesquisa de satisfação quanto os serviços prestados. | GESTÃO |
| 20 | Muito Significante | No departamento de TI possui sistema de inventário de ativos? | Oportunidade | Muito Provável | Moderado | A falta de conhecer o ambiente causa problema na operação do negócio. | Mitigar | Incluir um sistema de inventários de TI. | BOAS PRÁTICAS |
| 21 | Muito Crítico | O active diretory da empresa é integrado com todas as filiais? | Ameaça | Quase certo | Muito Alto | Não há controle do ambiente sem adoção de políticas de usuários. | Mitigar | Realizar a integração com o AD. | BOAS PRÁTICAS |
| 22 | Muito Crítico | Os usuários possuem bloqueios para instalar programas? | Ameaça | Quase certo | Muito Alto | Os usuários podem instalar qualquer programa sem autorização. | Mitigar | Instituir controle de usuários. | BOAS PRÁTICAS |
| 23 | Muito Crítico | Na empresa possui balanceamento de link de internet? | Ameaça | Muito Provável | Alto | Na queda de um link de internet não política de balanceamento. | Mitigar | Instituir funcionalidadde de balanceamento. | FIREWALL |
| 24 | Muito Crítico | Na empresa possui políticas de firewall completas para navegação? | Ameaça | Muito Provável | Alto | O usuário pode acessar qualquer site proibido. | Mitigar | Instituir novos controles na política de navegação. | FIREWALL |
| 25 | Muito Crítico | O departamento de TI possui o controle do licenciamento? | Ameaça | Muito Provável | Alto | Pode causar impacto em uma auditoria gerando multas. Serviço de suporte sem garantia ou atualizações futuras de | Mitigar | Instituir auditórias com o uso de um sistema de inventário e realizar renovação | GESTÃO |

**Figura 3.12** – Descrição da análise das respostas

Fonte: Autor

O tratamento do risco consiste na adoção de medidas para diminuir os riscos que foram avaliados no passo anterior. As medidas podem ser preventivas ou corretivas. Confome representado no quadro 3.3 da figura 3.12 com base no mapeamento realizado da figura 3.10, das 25 perguntas respondidas obtermos 21 processos muito críticos, 01 crítico, 02 muito significantes e 01 não crítico.

Todos os dados levantados no mapeamento na etapa de avaliação e análise de risco servirão como subsídio para a correção e tratamento no caso de alguma ocorrência a partir do gaps identificados. As medidas baseiam-se em tratar a causa raiz do risco bem a adoção dos procedimentos de segurança exigidos pela organização.

# CAPÍTULO 4

# Resultados Obtidos

## 4.1 – Resultado Geral

A partir do resultado da análise das respostas percebeu-se, que existem diversos pontos de vulnerabilidade na infraestrutura que podem facilitar uma invasão. Essas fragilidades podem estar relacionadas com a invasão no servidor de banco de dados, que resultaram na criptografia do sistema e *ba*ckups.

Baseado neste último incidente e nos levantamentos obtidos, decidiu-se rever a reestruturação da infraestrutura de segurança a partir do núcleo de negócio da empresa, onde ficam hospedados os servidores banco de dados e o sistema. Dessa forma poderá minimizar os riscos de ataques e vazamento de dados, pois observa-se que atualmente as regras da empresa não se baseiam em políticas de segurança, demonstrando a necessidade de mudanças.

A análise da situação atual do ambiente de infraestrutura local, demonstrada a partir da matriz risco versus impacto, levou às seguintes conclusões gerais: a empresa possui dificuldades para gerenciar sua infraestrutura de segurança (monitoramento, *firewall*, *backup*), ausências de boas práticas de segurança da informação, falta de ferramentas de gestão e monitoramento, conforme figura 4.1, contendo gráfico de dificuldade com base no mapeamento obtido no questionário do quadro 3.3, figura 3.12. Estes fatores podem gerar vulnerabilidades na infraestrutura, favorecendo invasões e vazamento de dados, inviabilizando o tempo hábil de resposta para retorno das operações, caso ocorram.

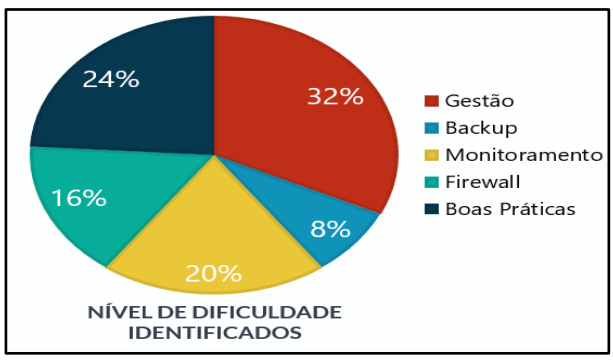


**Figura 4.1** – Gráfico contendo percentual de dificuldade
Fonte: Autor

## 4.2 – Resultado Obtido na Infraestrutura do *Data Center*

Com base no levantamento obtido após a invasão, a direção da empresa optou pela mudança de sua infraestrutura, conforme a seguir:

Migração dos seguintes serviços para o *Data center* Oracle:

- Servidores em ambiente Virtualizado em Cloud;
- Dados das aplicações em *storage*;
- Atualização dos sistemas operacionais para Windows 2012;
- Implantação de monitoramento proativo;
- *Backup*;
- Antivírus;
- *Active directory*;
- Oracle (Licenciado em cloud);
- DNS;
- *Firewall*;
- Sistema de gestão integrada.

Principais diferenciais:

- Todas as unidades operacionais se comunicarão direto ao *data center* Oracle ficando independentes da Matriz;
- Não haverá a necessidade de aquisição de novos equipamentos;
- Escalabilidade do parque sob demanda;
- Alta disponibilidade dos serviços instalados no *data center*.

A infraestrutura teve que ser redimensionada para atender aos requisitos de performance da operação. De acordo com a figura 4.2, segue nova arquitetura.

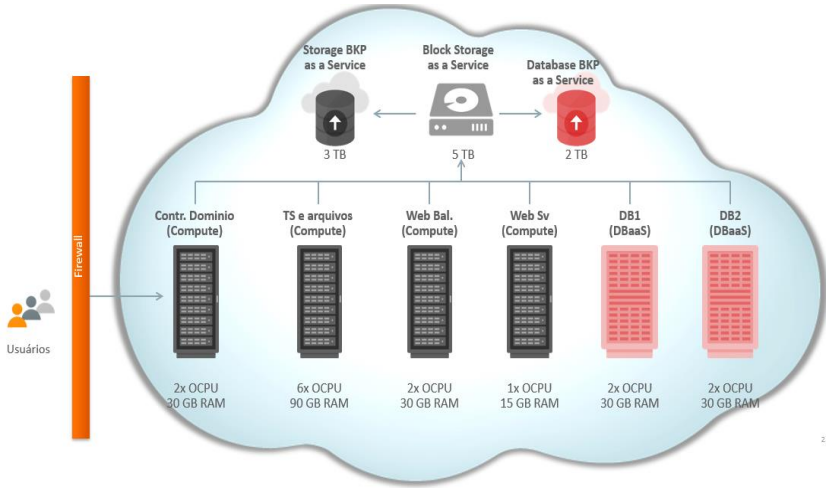


**Figura 4.2** - Nova arquitetura de servidores de banco de dados
Fonte: Autor

O custo do projeto, referente à solução proposta, pode ser verificado na figura 4.3.

| Composição Total do Projeto | |
|---|---|
| **CONTRATAÇÃO** | |
| Infraestrutura Cloud | R$ 145.996,86 |
| Serviços de Inicialização em Cloud Computing - Implantação e Consultoria | R$ 24.000,00 |
| Suporte e Gerenciamento mensal | R$ 72.000,00 |
| Total ano | R$ 241.996,86 |
| Tempo de implantação | 3 meses |

**Figura 4.3** – Composição total 1 contratação do projeto
Fonte: Autor

| Composição | |
|---|---|
| **Despesa Anual (antes do projeto)** | |
| Locação Mensalidade Datacenter | R$ 63.985,56 |
| Prestação de Serviço Datacenter | R$ 45.974,64 |
| Suporte e Gerenciamento Banco de Dados | R$ 30.296,04 |
| Licenciamento Oracle | R$ 25.408.26 |
| Custo total ano | R$ 165.664,50 |

**Figura 4.4** – Composição 2 despesa anual (antes do projeto)
Fonte: Autor

Percebe-se que se compararmos a contratação do projeto conforme figura 4.4 com os gastos antes do projeto, temos o aumento de 31,54 % no orçamento de TI representando a diferença de R$ 76.332,36 ano.

Tendo em vista que os servidores estavam com a garantia prestes a vencer tornando-os ativos obsolescentes, foi necessário cotação o comparativo mais detalhado. Para ser possível a tomada de decisão de uma infraestrutura *cloud* como serviço ou aquisição de ativos no caso os servidores conforme representado na figura 4.5.

| AQUISIÇÃO DE HARDWARE | | | | |
|---|---|---|---|---|
| **Item** | **Descrição** | **Qtde** | **VL Unitário** | **VL Total** |
| 01 | Servidor Dell \| PowerEdge R530 **- Oracle** | **2** | R$ 44.737,06 | **R$ 89.474,12** |
| 02 | Servidor Dell \| PowerEdge R630 - **TS1, TS2, TS3** | **6** | R$ 36.237,45 | **R$ 217.424,71** |
| 03 | Dell Storage SCv2020 – **Matriz** | **1** | R$ 108.141,18 | **R$ 108.141,18** |
| 04 | Dell Storage SCv2000 – **Filial** | **1** | R$ 70.216,47 | **R$ 70.216,47** |
| 05 | Windows Server 2012 R2, Datacenter Ed | **1** | R$ 15.903,00 | **R$ 15 903,00** |
| | **Total** | | | **R$ 501.159,48** |

**Figura 4.5** – Aquisição de *Hardware*
Fonte: Autor

Conforme cotação realizada o custo para aquisição de novos servidores em uma estrutura *on premise*, inviabilizou a construção deste cenário conforme comparativo da figura 4.6

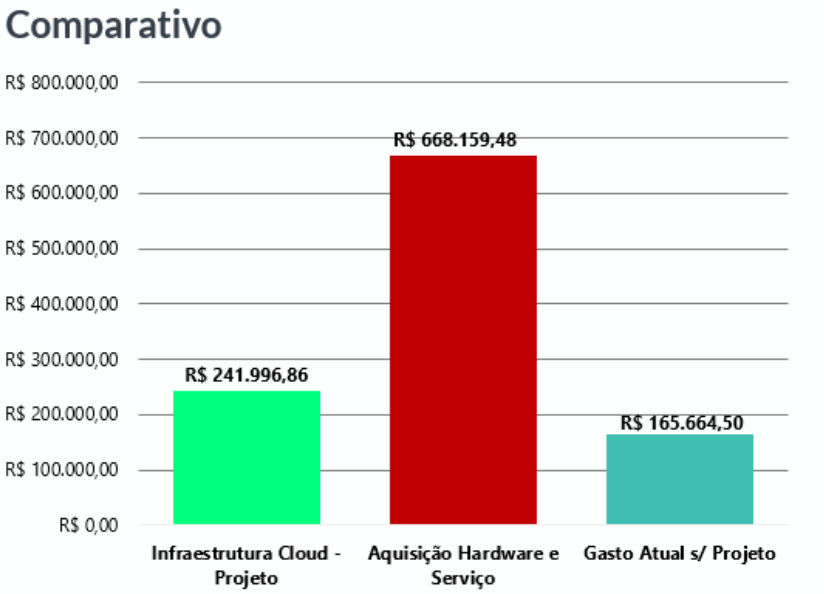


**Figura 4.6** – Comparativo e investimento do projeto
Fonte: Autor

Com base no que foi apresentado no comparativo da figurada 4.6 a estratégia de investimento, baseou-se na perspectiva da empresa de não desembolsar uma quantia significativa na aquisição de novos servidores evitando imobilizar o capital. Sob a luz do levantamento técnico que foi realizado, optou-se pela modalidade OPEX direcionando os investimento neste projeto para serviços de computação em nuvem para infraestrutura de TI com serviços de gerenciamento *cloud*.

## 4.3 – Resultado Obtido na Infraesturutra de Segurança da Empresa

Em função de uma reestruturação corporativa, foi necessária a implantação de um novo ambiente de Active Directory, nos quais os objetos foram obtidos/migrados de diferentes infraestruturas de Active Directory existentes na matriz e filiais, com o objetivo de centralizar a administração do ambiente e permitir um controle efetivo do ambiente. Para a restruturação, foi necesssário a contratação de uma consultoria especializada para implantação de um novo Active Directory em todos os sites da empresa seguindo as boas práticas de segurança da informação.

Com base no mapeamento obtido a direção da empresa por meio de um alinhamento com o comitê de TI, decidiu contratar uma consultoria especializada em segurança, que fará um mapeamento mais detalhado das necessidades de segurança de borda (Firewall) e das políticas de segurança do AD (Rede), com o objetivo de melhorar a segurança, integridade e confidencialidade tendo como premissa os gaps de vulnerabilidade identificados pelo comitê de TI através do questionário.

Para otimizar o esforço do time na segurança da empresa, houve a necessidade de contratação de Serviços de Gestão e Monitoramento dos *Firewalls* e AD, contemplando a administração criação de GPOs no AD para mitigar as vulnerabilidades internas e adoção de regras e serviços de segurança de UTM para lidar com as vulnerabilidades externas, da seguinte forma:

a) Serviço de gestão e monitoramento dos UTM e monitoração dos links de Internet a eles ligados, por meio de sistema de gerenciamento centralizado para os UTM e guarda de log por até 2 (dois] anos;

b) Serviço para abertura de chamados nas operadoras de Telecom quando houver queda nos links de Internet, 8 x 5, e nos fins de semana, a partir de horários fixos para verificação;

c) Implantação de um sistema de inventário para gestão dos ativos;

d) Suporte N3 para o AD Microsoft 8x5;

e) Aquisição de firewalls de backup como medida de proteção em caso de incidentes com o equipamento.

O custo do projeto, referente à solução proposta, pode ser acompanhado na figura 4.7.

| Composição Total do Projeto | |
|---|---|
| **CONTRATAÇÃO** | |
| Consultoria Especializada de Segurança | R$ 16.890,00 |
| Implantação de um novo Active Directory 3 meses | R$ 38.160,00 |
| Serviço de Gestão e Monitoramento Firewall e AD - 12 meses | R$ 7.600,00 |
| Aquisição de Firewalls Backup – 12 meses | R$ 4.630,00 |
| Total ano | R$ 201.810,00 |

**Figura 4.7** – Composição 2 total do projeto segurança
Fonte: Autor

O investimento para restruturação da segurança de redes teve como principais benefícios a unificação do Active Diretory, assim como a gestão e monitoramento dos firewalls aliada a aquisição de equipamentos de backup como medida de contorno em caso de falhas pontuais.

| Composição de Despesa | |
|---|---|
| **Firewall** | |
| Serviço de Licenciamento Firewall Fortinet-12 meses (RJ-SP-PE-RS-PR-DF-BH-SC) | R$ 7.436,36 |
| Total ano | R$ 89.236,32 |

**Figura 4.8** – Composição de Despesa Firewall
Fonte: Autor

A despesa antes do projeto de infraestrutura de segurança conforme figura 4.8, era somente o licenciamento dos appliances de firewall com a gestão reativa teve um salto de R$ 89.236,32 ano para R$ 146.760,00 ano, com a inclusão da gestão do firewall e AD, incorporado com equipamentos de backups, que na ocorrência de falha pontual na matriz ou filial haja a substituição do mesmo.

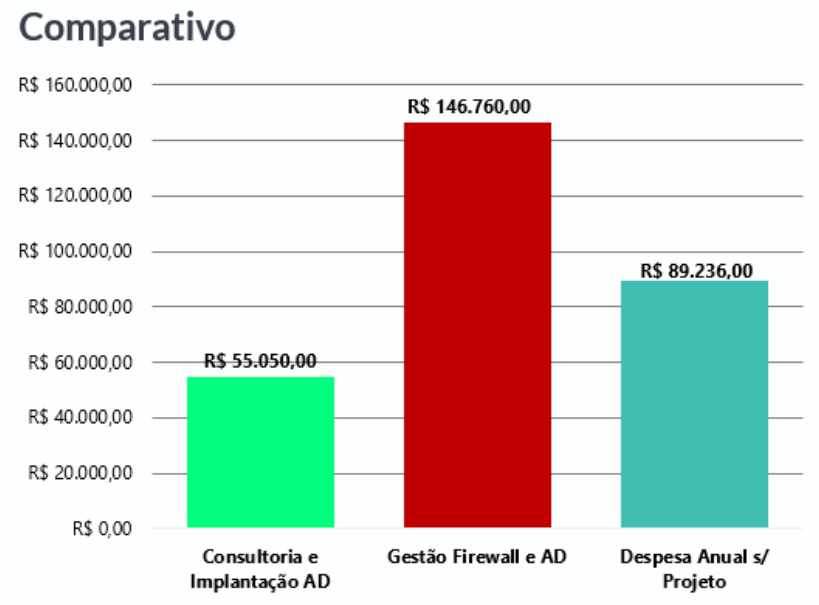


**Figura 4.9** – Comparativo de investimento do projeto segurança
Fonte: Autor

No comparativo da figura 4.9 temos o aumento de 39,20 % da despesa anual em relação a contratação do serviço de gestão de firewall e AD que justifica se comparado ao prejuízo financeiro que pode ser causado um por um ataque de *ransomware*.

## 4.4 – Resultado Obtido na operação do *backup* da empresa

Inicialmente a necessidade originou-se por meio de dois momentos que colaboraram para o aceite da restruturação do backup. O primeiro pela invasão ocorrida, pois a alta direção estava com olhar mais atento nos impactos que poderiam ocorrer por falta de investimento no setor de TI. Por outro lado, o segundo momento não menos importante pela análise obtida do sistema de *backup* Bacula que devido às limitações técnicas envolvidas e com a complexidade da infraestrutura de TI o sistema teve de ser descontinuado.

Entendemos que, sem um sistema de *backup* profissional, não temos como assegurar a continuidade dos serviços em caso de parada ou invasão. Portanto, a implantação do sistema de *backup* profissional, teve apoio de duas consultorias uma para fazer o levantamento mais detalhado do ambiente e outra para implantação da ferramenta *Arcserver*.

A execução da implementação seguiu de acordo o escopo apresentado:

- O projeto estará alinhado com o planejamento estratégico da empresa;
- As contratações seguiram o processo interno de cotação e análise;
- Contratação de uma consultoria especializada de *backup*;
- Elaboração de Políticas de *Backup*, Restauração e Retenção;
- Elaboração do Plano de Recuperação de Desastre;
- Elaboração de um Plano de Continuidade de Negócio;
- Contratação de um sistema de *backup* corporativo chamado *Arcserver*;
- Contração de um *Storage Local* e na Nuvem para armazenamento de *backup*;
- Contratação de uma empresa terceira para gestão do *backup*;

Nova arquitetura do *backup* pode ser verificada na figura 4.10:

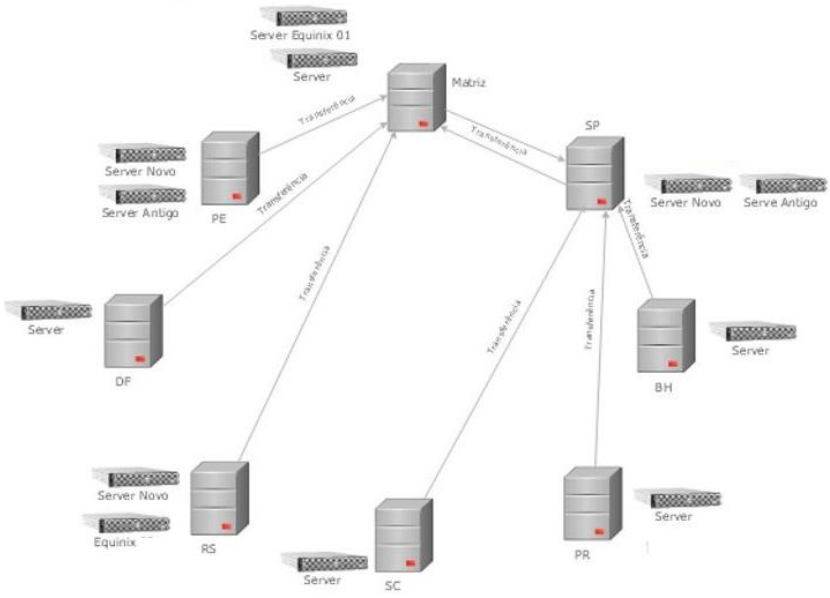


**Figura 4.10** – Nova arquitetura do *backup local*
Fonte: Autor

**Resumo do Escopo**

- Implantação do software *Arcserve* Matriz e Filiais;
- Elaboração de política de *backup* funcional para empresa;
- Implantação da política de *backup*/replicação;
- Migração de *VMwares* para os novos servidores matriz e filiais;
- Monitoramento e gestão proativa em caso de falha do sistema de *backup*;
- Gestão proativa em casos de *Disaster Recovery*;
- Suporte N3 para resolução de problemas que impactem o sistema de *backup*, *software* e *hardware*;
- Treinamento para transferência do conhecimento;
- Contrato dos Serviços pelo período de 12 meses, podendo ser renováveis por igual período;

O custo do projeto, referente à solução proposta, pode ser verificado na figura 4.11:

| Composição Total do Projeto | |
|---|---|
| **CONTRATAÇÃO** | |
| Software – Sistema (Matriz e Filiais) | R$ 158.000,00 |
| Storage Hardware - Servidores | R$ 140.000,00 |
| Consultoria | R$ 20.000,00 |
| Gestão e Governança do Backup | R$ 96.000,00 |
| Total | R$ 414.000,00 |

**Figura 4.11** – Composição 3 total do projeto backup local
Fonte: Autor

| Composição de Despesa | |
|---|---|
| **Gestão do Backup Bacula** | |
| Sistema de Backup Bacula (mês) | R$ 2.422,16 |
| Total | R$ 29.065,92 |

**Figura 4.12** – Composição de Despesa Gestão do Sistema Bacula
Fonte: Autor

A decisão da empresa com o apoio do comitê técnico e pelas análises de mercado geradas foi a escolha de um sistema profissional de backup que pudesse atender aos requisitos de negocio. Além disso, o que mais pesou para o aceite do valor de investimento conforme figura 4.11, se comparado a despesa do sistema bacula, conforme figura 4.12, foi que o sistema bacula havia sido aprovado pela alta direção no projeto anterior, sem avaliar os riscos envolvidos em relação a infraestrutura existente, como resultado a direção deciciu investir na restruturação do backup com uma ferramenta líder de mercado.

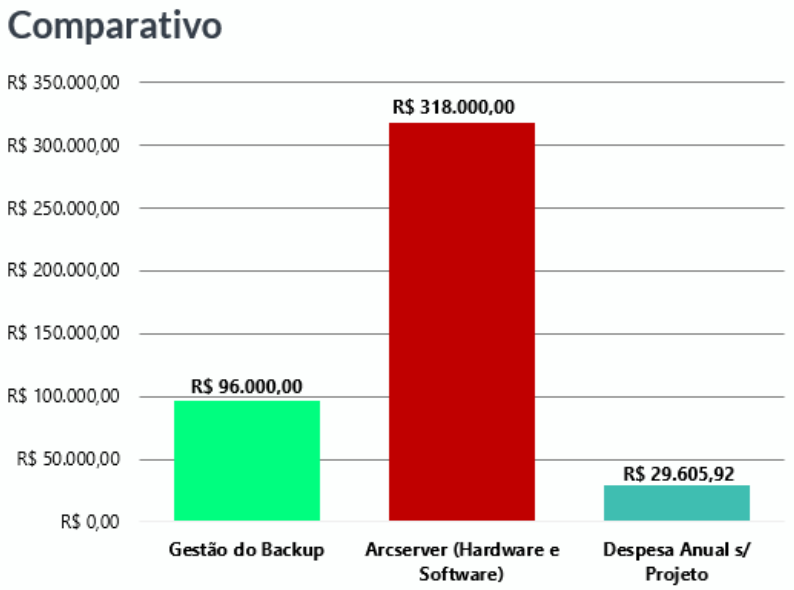


**Figura 4.13** – Comparativo Gestão – *Arcserver* e Despesa Anual com backup
Fonte: Autor

O investimento informado no gráfico comparativo da figura 4.13 representa que houve o aumento de 69,16% na gestão do backup em relação ao antigo sistema bacula que justifica-se pela aderencia complemeta do novo sistema de backup na infraestrutura do negócio.

# CAPÍTULO 5

# Conclusão e Trabalhos Futuros

## 5.1 – Conclusão

Com a colaboração dos responsáveis pela gestão corporativa e de TI, foram identificadas vulnerabilidades, a partir do questionário e observações de processos rotineiros, que contribuíram para que o ataque de *ransomware*, na empresa médico-hospitalar, fosse bem-sucedido. Dentre os principais Gaps encontrados estão sua infraestrutura de segurança (monitoramento, firewall, backup), ausências de boas práticas de segurança da informação, falta de ferramentas de gestão e monitoramento, conforme figura 4.1, contendo gráfico de dificuldade com base no mapeamento.

Com base no incidente, do qual a empresa foi vítima, decidiu-se reestruturar a infraestrutura de segurança de TI, atendendo as principais necessidades da empresa com relação à segurança da informação. Portanto, propõe-se aumentar a segurança dos sistemas e criar mecanismos capazes de minimizar os riscos de ataques, contaminações e proteção dos dados contra vazamentos, caso um incidente desta natureza ocorra novamente.

Os resultados alcançados atendidos a partir do quadro 5.1 estão representados percentualmente por meio da figura 5.1.

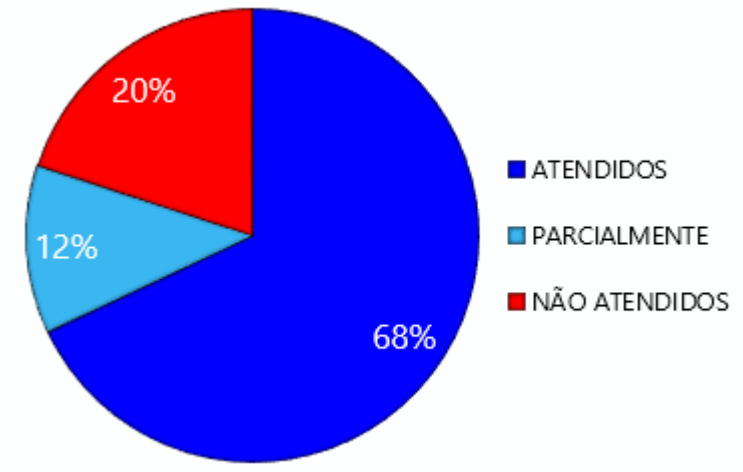


**Figura 5.1** – Resultados alcançados percentualmente.
Fonte: Autor

**Quadro 5.1** – Resultados obtidos

| Cód. | Severidade | Descrição do risco | Tipo | Probabilidade | Impacto | Resultado Alcançado |
|---|---|---|---|---|---|---|
| 1 | Muito Crítico | A empresa possui um sistema de backup eficiência que possibilidade replicação para outro local? | Ameaça | Muito Provável | Muito Alto | Atendido |
| 2 | Muito Crítico | A empresa possui um contrato de gestão proativa dos servidores no data center? | Ameaça | Quase certo | Muito Alto | Atendido |
| 3 | Muito Crítico | A empresa faz um uso de algum sistema de monitoramento dos servidores no data center? | Ameaça | Muito Provável | Alto | Atendido |
| 4 | Muito Significante | O departamento de TI da empresa faz uso de controle para monitoramento de fornecedores? | Ameaça | Pouco Provável | Moderado | Parcialmente |
| 5 | Muito Crítico | O departamento de TI da empresa faz uso de boas práticas na gestão de service desk? | Oportunidade | Muito Provável | Moderado | Não atendido |
| 6 | Muito Crítico | Na organização os acessos ao sistema da empresa são por meio de VPN? | Ameaça | Quase certo | Muito Alto | Atendido |
| 7 | Muito Crítico | O departamento de TI possui gestão proativa do orçamento de TI? | Oportunidade | Quase certo | Alto | Parcialmente |
| 8 | Muito Crítico | Na organização o antivírus possui gerenciamento proativo? | Ameaça | Quase certo | Alto | Atendido |
| 9 | Muito Crítico | Na organização os processos são padronizados? | Oportunidade | Pouco Provável | Baixo | Não atendido |
| 10 | Muito Crítico | Na organização a infraestrutura de rede Wi-Fi permitem a configuração de uma rede específica para os visitantes? | Ameaça | Quase certo | Muito Alto | Atendido |
| 11 | Muito Crítico | Na organização possui monitoramento dos firewalls? | Ameaça | Muito Provável | Muito Alto | Atendido |
| 12 | Pouco Crítico | Na organização existem relatórios operacionais e gerenciais de consumo de internet? | Oportunidade | Pouco Provável | Moderado | Atendido |

| Cód. | Severidade | Descrição do risco | Tipo | Probabilidade | Impacto | Resultado Alcançado |
|---|---|---|---|---|---|---|
| 13 | Muito Crítico | A organização possui sistema que realiza o backup completo dos servidores virtualizados? | Ameaça | Quase certo | Muito Alto | Atendido |
| 14 | Muito Crítico | A organização possui procedimento ou sistema para a gestão de patches? | Ameaça | Muito Provável | Alto | Atendido |
| 15 | Muito Crítico | Na TI da empresa ocorrem mudanças sem alinhamento? | Oportunidade | Quase certo | Alto | Parcialmente |
| 16 | Muito Crítico | A empresa possui firewall de redundância em caso de incidentes? | Ameaça | Muito Provável | Muito Alto | Atendido |
| 17 | Crítico | Na organização existem problemas por falta de treinamento? | Oportunidade | Muito Provável | Moderado | Não atendido |
| 18 | Muito Crítico | No departamento de TI existe ausência de definição de papéis? | Ameaça | Quase certo | Muito Alto | Não atendido |
| 19 | Muito Crítico | No departamento de TI é realizado o controle de fornecedores? | Ameaça | Quase certo | Alto | Não atendido |
| 20 | Muito Significante | No departamento de TI possui sistema de inventário de ativos? | Oportunidade | Muito Provável | Moderado | Atendido |
| 21 | Muito Crítico | O active diretory da empresa é integrado com todas as filiais? | Ameaça | Quase certo | Muito Alto | Atendido |
| 22 | Muito Crítico | Os usuários possuem bloqueios para instalar programas? | Ameaça | Quase certo | Muito Alto | Atendido |
| 23 | Muito Crítico | Na empresa possui balanceamento de link de internet? | Ameaça | Muito Provável | Alto | Atendido |
| 24 | Muito Crítico | Na empresa possui políticas de firewall completas para navegação? | Ameaça | Muito Provável | Alto | Atendido |
| 25 | Muito Crítico | O departamento de TI possui o controle do licenciamento? | Ameaça | Muito Provável | Alto | Atendido |

Fonte: Autor

Os resultados alcançados na implementação de melhorias na infraestrutura de segurança representam 68% atendidos totalmente e 12% atendidos parcialmente no total de 80%. Como controle de políticas de acessos, modernização do sistema de backup, substituição da infraestrutura do sistema local para nuvem, gestão e monitoramento do firewall, segmentação das redes Wi-Fi, controle e gerenciamento de patchs de segurança, redundância de firewalls, restruturação do *active directory* integrado com todas as filiais e por fim, implementação de um sistema de inventários. Assim, foram atendidos 17 resultados de vulnerabilidades, de um total de 25 itens, conforme apresentado no quadro 5.1.

Os processos que não foram atendidos foram de Gaps relacionados a gestão de TI que representaram 20% e merecem atenção para futuros projetos na empresa.

A empresa que não estabelecer mecanismos de prevenção mínimos no combate ao *ransomware*, estão sujeitas à perda, à invasão e à modificação de suas informações, além de uma possível exposição dos dados, que elevam o risco de paralização de suas atividades, gerando alto custo e prejuízos, justificando a necessidade de normas e investimentos para a prevenção e medidas de resposta caso venham a ocorrer. Não estabelecer mecanismos de segurança podem induzir a equívocos de conduta que podem acarretar consequências danosas e até mesmo ameaçar a continuidade dos negócios de uma empresa.

Um sistema eficiente de backup não resolveria sozinho este tipo de ataque, por algumas razões, pois as empresas precisam antes de mais nada, criar um roteiro de teste para validar a integridade dos dados backupeados. É importante salientar, que não é porque o backup está sendo feito, que estará bom para ser usado quando houver um incidente de segurança.

Entendendo a maturidade da segurança da empresa é possível montar um plano de gerenciamento de riscos, envolvendo pessoas, processos e tecnologia, pois não adianta ter pessoas treinadas e não ter processos de tecnologia para suportar a operação, assim como, não adianta investir muito em tecnologia e não ter processos e pessoas envolvidas.

Este estudo identificou a necessidade da utilização de uma consultoria em segurança mais especializada, assim como o investimento em capacitação e orientação que alinhem o conhecimento e aplicabilidade de todas as políticas estabelecidas na empresa. Fica evidente que o alinhamento das estratégias de gestão e controle entre os gestores corporativos e de TI é imprescindível para o sucesso e continuidade dos negócios da empresa.

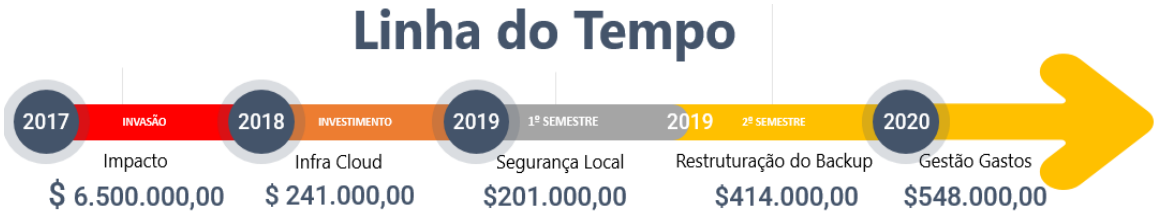


**Figura 5.2** – Linha do Tempo dos Investimentos Realizados.
Fonte: Autor

A linha do tempo da figura 5.2 apresenta o impacto obtido com a parada do sistema por 12 dias após a invasão. Os investimentos obtidos com infraestrutura cloud, restruturação da segurança local e backup superaram R$ 856.000,00 ano entre 2018 a 2020. O custo herdado de manutenção proveniente dos investimentos chega a R$ 548.000,00 ano. Não há segurança sem

investimento no setor de TI, pois nunca havia sido investido tanto com novas tecnologias para assegurar que futuros impactos não impeçam a operação de funcionar.

## 5.2 – Trabalhos Futuros

De forma geral, como trabalhos futuros, pode-se realizar um teste de invasão mediante a varredura na infraestrutura da rede interna, para simular um ataque real, com o propósito de certificar que o atual ambiente possa estar seguro contra invasão.

Em conformidade com o teste de invasão proposto, a avaliação do grau de maturidade dos processos de governança de TI torna-se essencial com a capacitação da equipe, utilizando o ITIL e Framework Cobit 5.0, como benefício no alinhamento estratégico da TI com o negócio.

O resultado da utilização de boas práticas é o controle no gerenciamento de fornecedores, assim como a definição de papéis e responsabilidades na equipe, além de instituir o processo de controle de mudanças nos ativos de infraestrutura.

# Referências Bibliográficas


[1] GIL, A. C. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 1999.

[2] ABNT. **Tecnologia da informação – técnicas de segurança – Diretrizes para Segurança Cibernética (NBR ISO/IEC 27032).** Associação Brasileira De Normas e Técnicas. Rio de Janeiro, RJ: 27000. 2015.

[3] ISO. **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Visão geral e vocabulário (ISO/IEC 27007:2018).** Versão traduzida. ISO - International Organization for Standardization. 2018.

[4] ABNT. **Tecnologia da informação – técnicas de segurança – código de prática para controles de segurança da informação (NBR ISO/IEC 27002**). Associação Brasileira De Normas e Técnicas. Rio de Janeiro, RJ: 2013.

[5] ABNT. **Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação – requisitos (NBR ISO/IEC 27001).** Associação Brasileira De Normas e Técnicas. Rio de Janeiro, RJ: Rio de Janeiro, RJ: 2006.

[6] MANOEL, S. **Governança de Segurança da Informação/Como criar oportunidades para seu negócio.** Editora Brasport, Rio de Janeiro, pp. 22-90, 2013.

[7] FONTES, E. **Políticas e Normas para a Segurança da Informação:** Como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações, on – Editora Brasport, Rio de Janeiro, pp. 9-13, 2012.

[8] ULMANN, P.E. **Políticas de Segurança da Informação:** um estudo de caso baseado nas normas ABNT NBR ISO / IEC 27014:2013 e ABNT NBR ISO / IEC 27005:2011. Trabalho de conclusão de curso da Universidade Regional do Nordeste Unijuí. Departamento de ciências exatas e engenharias/curso graduação em ciências da computação. Rio Grande do sul, pp.33-40, 2015.

[9] ROHR, Altieres. **Como um hacker invade o computador?**. Disponível em http://g1.globo.com/tecnologia/blog/seguranca-digital/post/pacotao-em-videocomo-um-hacker-invade-o-computador.html. Acesso em: 15 mai. 2020.

[10] BARUQUE, L. B.; SANTOS, L. C. **Governança em Tecnologia da Informação.** Rio de Janeiro: Fundação CECIERJ, pp. 13, 2010. BEAL, A. Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. SP: Ed. Atlas, pp 2008.

[11] AMARAL, L. e VARAJÃO, J. **Planejamento de Sistemas de Informação.** 4ª edição; Lisboa: Editora FCA, 2007.

[12] BEAL, A. **Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações**. SP: Ed. Atlas, pp 2008.

[13] NETO, A. B.; SOLONCA, D. **Auditoria de Sistemas Informatizados.** 3ª edição; Palhoça: UNISUL virtual, pp. 09-15, 2007.

[14] SÊMOLA, Marcos. **Gestão da Segurança:** Uma visão executiva. Rio de Janeiro: Campus, 2003.

[15] GONDIM, J. J. C. Gerenciamento das Operações e Comunicações: GSIC 602 (Notas de Aula). Curso de Especialização em Gestão da , e Comunicações: 2009/2011. Departamento de Ciências da Computação da Universidade de Brasília. 2010a 23 p.

[16] CERT.BR. **Incidentes reportados ao CERT.BR (janeiro a junho de 2020)**. Cert.br. Disponível em: https://www.cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html. Acesso em: 24 mai. 2021.

[17] **Perdas financeiras com *Ransomware*** https://www.foodprocessing.com/articles/2017/malware-may-have-cost-mondelez-millions/. Acesso em: 17jun. 2021.

[18] **Perdas financeiras com *Ransomware*** https://revistapegn.globo.com/Negocios/noticia/2017/11/gigante-do-transporte-maritimo-tem-prejuizo-de-us-300-milhoes-com-ataque-cibernetico.html Acesso em: 17jun. 2021.

[19] **Perdas financeiras com *Ransomware*** https://www.zdnet.com/article/norsk-hydro-ransomware-incident-losses-reach-40-million-after-one-week/ Acesso em: 17jun. 2021.

[20] **Perdas financeiras com *Ransomware*** https://gatefy.com/pt-br/blog/estatisticas-fatos-email-principal-vetor-ameacas-ciberneticas/ Acesso em: 17jun. 2021.

[21] **Perdas financeiras com *Ransomware*** https://forbes.com.br/forbes-money/2021/06/6-ataques-de-ciberseguranca-com-resgate-em-criptomoedas/#foto2 Acesso em: 17jun. 2021.

[22] **Perdas financeiras com *Ransomware*** https://www.convergenciadigital.com.br/Seguranca/TJRS-diz-que-nao-houve-perda-de-dados-com-ataque-hacker,-mas-usuarios-reclamam-da-falta-de-transparencia-56977.html?UserActiveTemplate=site&UserActiveTemplate=mobile%252Csite#:~:text=Oficialmente%20o%20TJRS%20n%C3%A3o%20revela,R%24%2026%20milh%C3%B5es%20ao%20Tribunal. Acesso em: 17jun. 2021.

[23] **Perdas financeiras com *Ransomware*** https://tecnoblog.net/459830/ransomware-mina-ouro-hackers-revil-raas-pesadelo-organizacoes/ Acesso em: 17jun. 2021.

[24] **Perdas financeiras com *Ransomware*** https://corporate.showmetech.com.br/ransomware-causa-prejuizo-enorme/ Acesso em: 17jun. 2021.

[25] HINTZBERGEN, J. et al. **Fundamentos da Segurança da Informação ISO 27001 and 27002**. Rio de Janeiro: Brasport, 2018.

[26] ABNT. **Tecnologia da informação – técnicas de segurança – gestão de riscos de segurança da informação (NBR ISO/IEC 27005).** Associação Brasileira De Normas e Técnicas. Rio de Janeiro, RJ: 2019.

[27] ABNT. **Tecnologia da informação – técnicas de segurança – gestão de riscos de segurança da informação (NBR ISO/IEC 27005).** Associação Brasileira De Normas e Técnicas. Rio de Janeiro, RJ: 2011

[28] FORNASIER, M; SPINATO, T; RIBEIRO, F. ***Ransomware* e cibersegurança:** a informação ameaçada por ataques a dados. Revista Thesis Juris, v.9, n.1, p.208-236, 2020.

[29] LISKA, A. TIMOTHY, Gallo. **Ransomware:** Defendendo-se da Extorsão Digital. NOVATEC, 2017.

[30] BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 fev. 2021.

[31] DONDA, Daniel. **Guia Prático de Implementação da LGPD.** São Paulo: Labrador, 2020.