UNIVERSIDADE DO SUL DE SANTA CATARINA

RICARDO BORDIN

SALVAGUARDA DOS DADOS DA EMPRESA ANÁLISE.PRO
BACKUP ON LINE DE DADOS

Palhoça

2018

RICARDO BORDIN

SALVAGUARDA DOS DADOS DA EMPRESA ANÁLISE.PRO
BACKUP ON LINE DE DADOS

Relatório apresentado ao Curso **Tecnólogo em Gestão da Tecnologia da Informação,** da Universidade do Sul de Santa Catarina, como requisito parcial à aprovação na unidade de aprendizagem de Estudo de Caso.

Orientadora: Profa. Nilce Miranda Ayres,

Palhoça

2018

RICARDO BORDIN

SALVAGUARDA DOS DADOS DA EMPRESA ANÁLISE.PRO
BACKUP ON LINE DE DADOS

Este trabalho de pesquisa na modalidade de Estudo de Caso foi julgado adequado à obtenção do grau de Tecnólogo em Gestão da Tecnologia da Informação e aprovado, em sua forma final, pelo Curso Superior de Tecnologia em Gestão da Tecnologia da Informação, da Universidade do Sul de Santa Catarina.

Palhoça, 09 de novembro de 2018.

Profa. Orientadora Nilce Miranda Ayres, Profa. Ma.
Universidade do Sul de Santa Catarina

AGRADECIMENTOS

Agradeço primeiramente a Deus, pois a vida e a saúde são os dons mais preciosos que uma pessoa pode ter, e ele é muito benevolente em me proporcionar exatamente isto.

Aos meus pais, Enio Bordin e Maria Otália Bordin já falecidos, que mesmo não estando mais presente fisicamente na minha vida, tenho certeza de que estão ao meu lado me incentivando nos momentos de fraqueza.

Agradeço com muito amor e carinho aos meus filhos Rafael, Bruna, Lyza e Ricardo, pela compreensão e paciência e por permitirem a clausura diária, para poder estudar e chegar até aqui.

A minha amada e querida esposa Sandra Yegros agradeço com todo amor pelo carinho, atenção, compreensão e paciência ao longo do curso para que pudesse atingir este objetivo.

RESUMO

Os dados produzidos e custodiados são de extrema importância e vitais para saúde de uma empresa. E para que estes dados mantenham sua integralidade, há a necessidade de serem armazenados de forma correta. Como ainda é pouco difundida a cultura de acesso seguro a rede mundial de computadores, é enorme a incidência de crimes virtuais. Como os bens a serem sequestrados são os dados que uma empresa produz e possui, há a necessidade destes dados serem guardados e custodiados de uma maneira segura. Neste contexto as empresas devem considerar seriamente a contratação de serviços terceirizados de armazenamento em nuvem por empresas especialistas, e que possuam excelente estrutura. Há diversas empresas com alta capacitação no mercado nacional e no exterior. Neste trabalho, é apresentada uma abordagem baseada na mudança da estrutura de TI e nos procedimentos realizados de backup online de dados da Análise.PRO, mantendo-se sua confidencialidade e integridade. A abordagem proposta mostra os danos que podem ocorrer pela incidência de ataques cibernéticos de um cenário real, e como podem ser minimizados estes ataques. Mostra também que com as profundas mudanças que ocorreram durante todo o processo, ocorreram enormes benefícios na manutenção da integridade dos dados custodiados.

Palavras-chave: Armazenamento. Ataques. Backup. Confidencialidade. Dados. Integridade.

SUMÁRIO

1 INTRODUÇÃO

Diante do cenário atual, a ameaça cibernética mais utilizada mundialmente é o chamado Ransomware, um malware que ao ser executado criptografa todos os arquivos do seu dispositivo requerendo um resgate financeiro, geralmente em bitcoins, para poder recuperá-los. Seu principal objetivo é sequestrar dados importantes de usuários desprotegidos, o que aumenta as chances destes usuários cederem às exigências de pagamento para poderem ter seus arquivos de volta.

Um dos principais focos dos ataques são as empresas, porém deve-se considerar, como regra geral, que elas possuem ferramentas de proteção e detecção de ameaças, bem como o assessoramento de um setor de TI qualificado.

Partindo desse pressuposto, o foco desse trabalho será direcionado à empresa que atua na área contábil, a Análise.PRO que não possui qualquer informação, auxílio ou proteção contra esses tipos de ataque.

Após descrever as etapas padronizadas do trabalho como Introdução, Tema, Descrição dos Objetivos Geral e Específico, e os procedimentos metodológicos adotados, será apresentada uma análise realizada da empresa Análise.PRO, bem como a estrutura encontrada. Após detalhamentos, será discorrida a proposta de mudanças, e por fim serão descritas as mudanças realizadas pela empresa.

Para a realização deste trabalho foram realizados estudos sobre vulnerabilidades das redes, sequestro e resgate de dados, a situação atual da empresa Análise.PRO, as reestruturações necessárias, análise dos equipamentos e serviços necessários de contratação.

Destaca-se que o presente estudo de caso não esgota o assunto abordado, mas incita a permanente busca por novas formas de proteção dos dados gerados, bem como incentiva novas pesquisas tecnológicas sobre guarda e armazenamento.

2 TEMA

Os dados produzidos são bens extremamente valiosos que uma empresa possui e mantém. Eles podem ser na forma de dados financeiros, de cadastros de recursos humanos, contábeis, estoques, projetos, pesquisa, enfim de uma infinidade de tipos que uma empresa pode produzir.

Diariamente vemos na imprensa notícias de vazamentos e de sequestros de dados reservados de clientes e de empresas, seja por ataques cibernéticos, seja pela falta de política de privacidade da empresa, ou até mesmo pela manipulação inadequada por algum funcionário mal intencionado.

A salvaguarda desses dados é um fator muito preocupante e delicado para o setor de TI da empresa, o qual deve manter íntegras todas as informações produzidas e os dados custodiados dos clientes com a confidencialidade necessária para que não sejam expostos.

Segundo a LUMIUN (2017), crime cibernético é assunto que precisa estar presente e ser debatido no cotidiano, mas que ainda é pouco discutido, e principalmente, são poucas as empresas que sabem a importância de entender sobre esse assunto e manter a segurança para evitar invasão e roubo de dados.

Torres (2009, p.492), enfatiza que o maior problema em relação a ataques e roubo de dados é que muita gente pensa que isso só ocorre em ambiente virtual, o que não é verdade e pode ocorrer pela ação de funcionário ou pessoa mal intencionada.

Ulbrich e Della Valle (2009) descrevem várias formas de ataques que podem ser realizados pela internet para acessos não autorizados a computadores com a finalidade de furto dos dados vitais das empresas.

2.1 TEMA ESPECÍFICO

Salvaguarda e implantação de sistema de backup online dos dados produzidos pela Análise.PRO.

2.2 PROBLEMA DE PESQUISA

Como investir e manter um plano de backup online seguro e confiável para evitar possíveis perdas por invasões e sequestros de dados?

2.3 JUSTIFICATIVA DA PESQUISA

Diante de tantas adversidades encontradas diariamente como perda acidental de dados, crimes cibernéticos e furtos internos, é de suma importância que as empresas desenvolvam e mantenham atualizados programas de confidencialidade e manutenção dos dados produzidos, bem como a guarda em local confiável.

Com tantas ameaças encontradas diariamente, surgiu a motivação para desenvolver um trabalho de mudanças de procedimentos e de prevenção de perdas de dados junto a empresa Análise.PRO.

Para que este trabalho pudesse ter êxito, foi realizado um estudo de viabilidade de mudanças e de implantação de novos sistemas, os quais foram realizados com sucesso, permitindo à empresa manter intactos e confiáveis todos os dados gerados.

3 OBJETIVOS

3.1 OBJETIVO GERAL

Propor a implantação de uma política de tratamento e salvaguarda de dados, bem como da implantação de um sistema de backup online.

3.2 OBJETIVOS ESPECÍFICOS

- Descrever como funcionam os sistemas de backup online.
- Analisar e descrever as vantagens da implantação de uma política de tratamento de dados para que não ocorram perdas irreversíveis e desastrosas.
- Analisar os pontos positivos e negativos da implantação ou não de um sistema de backup online nas empresas
- Analisar os benefícios da realização do backup online de dados por uma empresa certificada terceirizada.
- Identificar os dados da empresa Análise.PRO que necessitam serem tratados com um grau maior de atenção e sigilo.
- Identificar a necessidade de salvaguarda dos dados da empresa Análise.PRO em um sistema de backup online.
- Mostrar os benefícios para a empresa Análise.PRO ao produzir e manter, e constantemente aperfeiçoar, um plano de salvaguarda para que os dados e informações se mantenham íntegros e confiáveis por intermédio de backup online diários.

4 PROCEDIMENTOS METODOLÓGICOS

4.1 CAMPO DE ESTUDO

O campo de estudo para a realização deste trabalho foi baseado na empresa Análise.PRO – Assessoria Empresarial, que trabalha na área de consultoria contábil, fiscal, financeira, tributária e auditorias, com uma vasta carteira de clientes físicos e empresariais onde são desenvolvidos todos os trabalhos referentes às áreas citadas.

Para atingir aos objetivos deste trabalho, foi realizada uma pesquisa exploratória que, quanto aos seus objetivos gerais, proporciona maior familiaridade com o problema e visa torná-lo mais explícito (GIL, 2002, p. 41), e também foi realizada pesquisa bibliográfica em sites de tecnologia que tem enfoque nas informações necessárias sobre os temas, além de livros especializados na área de TI. Após a pesquisa do material teórico, foi realizada uma síntese dos aspectos mais relevantes abordados sobre backup online e salvaguarda de dados.

A análise do trabalho foi realizada de forma qualitativa verificando-se as necessidades da empresa de assessoria contábil geradora de dados e as disponibilidades das empresas que realizam backup online.

4.2 INSTRUMENTOS DE COLETA DE DADOS

Para a realização deste trabalho, foram utilizados os instrumentos conforme descrito no Quadro 1:

Quadro 1 – Instrumento de coleta de dados:

Instrumento de coleta de dados	**Universo pesquisado**	**Finalidade do Instrumento**
Questionário	Pessoas que trabalham diretamente com a manipulação dos dados vitais da empresa.	Levantar os dados vitais e como são mantidas as integridades destes dados.
Observação Direta	Ambiente de trabalho e modo como são tratados os dados.	Levantar possíveis falhas nos procedimentos utilizados na geração, manutenção e guarda dos dados.
Pesquisa bibliográfica	Sites especializados em segurança e em backup online.	Conhecer e analisar as formas de ataques e as opções disponíveis de backup online.

Fonte: Do autor

5 APRESENTAÇÃO E ANÁLISE DA REALIDADE OBSERVADA

5.1 ESTRUTURA DA ORGANIZAÇÃO

A Análise.PRO é uma empresa especializada em Assessoria Contábil, Planejamento Tributário, Assessoria Societária, Auditorias Tributárias e Internas, Contabilidade Escrita e Gerencial, suporte e assessoramento de empresas.

Tem como missão:

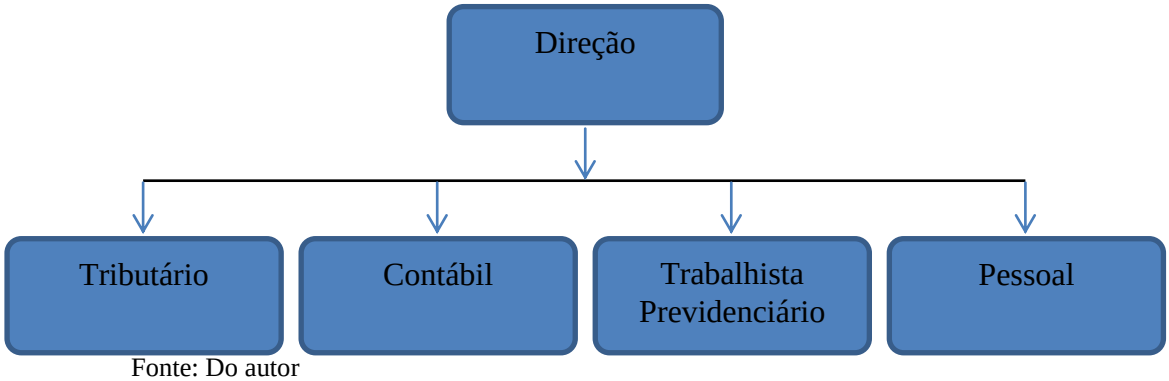
> A Análise.PRO Assessoria Empresarial é uma empresa especializada no suporte e assessoramento de empresas.
> Com o espírito inovador e respeitando a ética profissional, possui o diferencial de atuar voltada para individualidade de seus clientes desenvolvendo um conjunto de procedimentos específicos capazes de gerar soluções inteligentes para o desenvolvimento empresarial. O foco no comprometimento e qualidade do atendimento aumenta a confiança dos clientes, fortalecendo a marca e a credibilidade da empresa no mercado. (Análise.PRO, 2018).

O variado leque de operações realizadas pela Análise.PRO, demanda a geração de um vasto campo de informações reservadas de empresas e pessoas físicas, os quais devem ser tratados por colaboradores com elevado índice de confidencialidade.

Desde sua fundação a mais de 10 anos por três sócios proprietários a empresa busca aumentar seu quadro de colaboradores, e permanentemente investe em suas qualificações.

A estrutura da empresa antes da proposta de mudança pode ser representada pela Figura 1:

Figura 1: Estrutura da empresa antes da proposta de mudança.



Fonte: Do autor

E direção da Análise.PRO é compartilhada entre os três sócios fundadores da empresa.

Os planos de trabalho são elaborados, debatidos e definidos em reuniões semanais com todo o efetivo, e atos que demandem decisões extras são tomados em reuniões da diretoria a qualquer tempo.

Cada sócio é especializado em uma área, sendo que o sócio da área trabalhista e Previdenciária atua conjuntamente no setor de pessoal.

O quadro de trabalho é complementado por colaboradores encarregados de realizarem os trabalhos específicos de cada área.

Inicialmente os trabalhos eram realizados em estações de trabalho não conectadas em rede. Como a empresa não possuía em seu quadro de colaboradores uma pessoa qualificada na área de TI contratou um técnico para realizar a interligação em rede destas estações de trabalho, mas sem que fosse instalado e configurado um servidor dedicado. Este procedimento tornou mais ágil à condução dos trabalhos até então realizados.

5.2 DESCRIÇÃO E ANÁLISE DA REALIDADE OBSERVADA

Conforme dados coletados da forma de trabalho e como são tratadas as informações geradas e também as necessidades da empresa Análise.PRO, iniciou-se a análise das informações compiladas pelo questionário proposto na empresa.

Com base no questionário pode-se levantar que:

O total de tipo de dados gerados pela empresa é desconhecido da maioria dos colaboradores. Cada um tem ciência somente dos dados com os quais trabalha.

Os dados que são gerados backups são definidos pela direção conforme a relevância dos mesmos.

O armazenamento dos dados são HDs externos, pendrives e CDs, os quais são guardados na própria empresa e em alguns casos algum membro da direção leva para casa.

A frequência com que são realizados os backups não é bem definida. Inicialmente era para ser diária, mas ocorre que às vezes não é realizado.

Com relação à perda de dados, a empresa já contabiliza histórico de grande incidência de perda de dados em função de CD arranharem e/ou quebrarem, pendrives queimarem e/ou perdidos, HDs externos caírem no chão danificando-os e/ou queimarem, gerando com isto uma enorme dor de cabeça e retrabalho para todos do escritório.

Os equipamentos utilizados pela empresa estão muito defasados das necessidades atuais. A empresa possui 08 estações de trabalho compostas de: CPU Pentium III, 512 MB de memória RAM, HD 80Gb, tela TRC.

Possui também uma impressora multifuncional DeskJet antiga em rede.

Somados a todos estes fatores, a empresa não dispõe de colaborador com conhecimento específico na área de TI para que possa ficar encarregado da realização da assistência à rede e aos equipamentos.

Com estes relatos pode-se perceber que o nível de segurança e de confiabilidade dos dados é quase inexistente, gerando uma grande insegurança quanto à integridade dos dados.

Após a análise da situação e com as observações diretas registradas durante vários dias, pode-se perceber que a empresa necessitava urgentemente encontrar uma solução para os problemas enfrentados com os constantes retrabalhos e com a insegurança no tocante a confidencialidade dos dados.

A Análise.PRO gera e manipula muitos dados confidenciais dos clientes como CNPJ/CPF, conta corrente, banco, agência, saldos, extratos bancários, variação patrimonial, e muitos outros dados significativos para a condução de uma empresa.

A preocupação no tratamento das informações geradas pela Análise.PRO deve-se ao fato de que os resultados da perda da integridade dos dados ou vazamento das informações neles contidas, seja de que forma for, pode ser catastrófico, visto tratarem-se de informações relevantes e confidenciais dos clientes.

Se as perdas forem causadas por ataques cibernéticos, diversas são as forma como estes ataques ocorrem, mas basicamente estes são realizados na forma de invasão e instalação de programas nocivos no computador da vítima para que seja realizada uma função específica.

Segundo Angelo (2016):

> Trata-se de um malware – malicious software – software nocivo destinado a se instalar em sistema de computador alheio, de forma ilícita (sem o consentimento consciente do usuário), e tem a função de causar danos, alterações na funcionalidade do sistema, ou mesmo roubo de informações.
> O ransomware vai um pouco além: após realizar todo o procedimento de um malware, restringe e bloqueia o acesso a dados e informações, via sistema, infectando e emitindo uma "cobrança", pedindo um valor de "resgate" para que o acesso seja plenamente reestabelecido. É uma chantagem virtual. Existem diversos tipos de ransomware, e apesar dos termos técnicos e a alta complexidade em defini-los com palavras mais simples, eles (os "ransomware") são mais comuns do que você imagina.

Após ocorrer a invasão do computador alvo, o programa malicioso inicia a encriptação dos dados, tornando-os incompreensíveis para quem não tiver o código para reverter a criptografia. Com os dados criptografados, o ransomware armazena-os em um servidor de comando, para uso e controle futuro, pois mesmo pagando o resgate (figura 2), você ainda corre riscos de subornos no futuro.

Figura 2: Pagamento de resgate

Fonte: Ceschini (2016)

Como exemplo de ransomware temos o Fantom, que ataca os sistemas operacionais da plataforma Windows passando-se por uma atualização de sistema, com novas rotinas e

implementações de funcionalidades, comunicação e principalmente de segurança. Por se fazer passar exatamente por uma atualização, está infectando muitos computadores impondo resgate (figura 3).

Figura 3: Imposição de resgate

Fonte: Ceschini (2016)

As invasões provocam um grande prejuízo para os usuários domésticos e maiores ainda para as empresas, bancos, instituições públicas, etc, que tem seus valiosos dados sequestrados e sem a certeza de que serão recuperados. No meio corporativo é fundamental que os gestores, profissionais de TI e responsáveis, notifiquem e preparem seus funcionários, técnicos e mesmo clientes, para o uso correto dos sistemas instalados nos equipamentos.

Outro ransomware muito conhecido que tem feito muitas vítimas é o Arhiveus-A, que compacta os arquivos no computador invadido, e os criptografa.

Os pedidos de resgate variam de débitos em conta corrente, pagamento no crédito, bitcoins (ou outra moeda virtual), e pagamentos on-line por transações diversas.

A melhor forma de evitar um pagamento de resgate pelos dados perdidos é a manutenção de um programa diário de backup online de dados, os quais podem ser restaurados a qualquer momento.

Atualmente existem diversos sites especializados em programas antivírus, que dispõem de programas gratuitos para recuperação de dados criptografados por diversos tipos de ransomware em suas mais diversas variantes. Tais programas e os procedimentos de recuperação são descritos nos sites das empresas.

Diversas são as telas de ransomware (figura 4) registradas por Ceschini (2016) que poderão aparecer nas telas dos computadores infectados.

Figura 4: Telas de ransomware

Fonte: Ceschini (2016)

Após pesquisa constatou-se muitas notícias referentes a invasões de computadores, servidores e sistemas com o intuito de copiarem os dados vitais da empresa e também com a intenção de "sequestrar" a máquina do cliente e criptografar todo o seu conteúdo, não permitindo qualquer acesso e impondo-lhes uma forma de resgate, na maioria das vezes de alto valor monetário, para que seja liberada uma chave de segurança para liberação dos dados.

Diversos são os registros e como exemplo de ocorrência segue fato ocorrido no Governo do Distrito Federal em 2017 conforme reportagem do portal de notícias G1 (2017):

> Serviços públicos do Distrito Federal foram afetados, na tarde desta segunda-feira (24), por um ataque cibernético a computadores do governo. Até as 19h, o governo confirmava problemas em máquinas da Secretaria de Saúde e de administrações regionais. Segundo o GDF, não houve acesso a dados de contribuintes.

> Maior unidade de saúde da rede pública, o Hospital de Base suspendeu os exames de raio X por tempo indeterminado (entenda abaixo). O mesmo também aconteceu no Hospital Regional de Samambaia.
> Responsável pela tecnologia do governo, a Secretaria de Planejamento afirma que o setor está "trabalhando em regime de plantão" para resolver o problema e normalizar a rede.

O portal de notícias G1 (2018) também noticiou outro ataque cibernético ao sistema de rede do Governo do Distrito Federal.

> Os sistemas de informática do Governo do Distrito Federal sofreram 2.043.551 tentativas de invasão em 2017. Em 18 casos, "hackers" conseguiram acessar os servidores, informou a Secretaria de Planejamento – pasta que administra a infraestrutura tecnológica do GDF. Os dados foram obtidos pelo G1 por meio da Lei de Acesso à Informação.
> Comparando com os números de 2016, a quantidade de tentativas de invasão cresceu 3.927%. Naquele ano, foram registradas 52.031 iniciativas frustradas e 12 ataques efetivos.
> (...) Entre as estratégias usadas pelos hackers está a de "força bruta", quando são tentadas todas as possibilidades de senhas. Outra técnica é a conhecida como "ataque do dicionário". Segundo o consultor Antônio Martino, cientista da computação, o método consiste em usar as senhas mais frequentes – como "123" – para tentar acesso ao sistema.
> "O ataque do dicionário é mais refinado que o de força bruta. Ele pega palavra comuns da língua portuguesa ou termos frequentes e tenta combinações", explicou Martino ao G1. "Com o método do dicionário, o ataque fica mais efetivo e aumentam as chances de invadir os servidores."
> Outro meio usado contra os sistemas do GDF é o ataque conhecido como "de negação de serviço" ou simplesmente DDoS. "Neste caso, é como se todo mundo tentasse ligar para um telefone e essa pessoa não conseguisse mais receber ligações sérias. Ou seja, você não invade o sistema, mas acaba o derrubando por sobrecarga", disse o especialista.

Estes foram somente dois exemplos dos inúmeros casos ocorridos em diversas áreas onde existam computadores conectados em redes.

Existe atualmente uma série de ferramentas que podem evitar desastres como esses. Todos os dias arquivos, fotos, filmes e uma incontável quantidade de informações importantes que são armazenadas em computadores, notebooks, celulares e tablets empresariais sofrem algum tipo de ameaça.

O objetivo do backup é manter essas informações seguras, possibilitando a pronta recuperação numa eventual perda dos arquivos em uso, seja por erro humano, sabotagem, sequestro de dados e de máquinas ou mau funcionamento dos equipamentos. Pode ocorrer alguma perda inesperada de informação. Nessa hora, uma cópia de segurança externa dos dados é essencial para a continuidade de operações de uma empresa.

Tais procedimentos podem perfeitamente serem usados não somente por empresas, mas por todos que precisarem salvaguardar seus dados, evitando perdas inesperadas.

O procedimento de salvaguarda de dados, reservados ou não, baseia-se na necessidade de manter um registro de todas as ações tomadas pela empresa, bem como salvaguar-

dar todos os registros, dados, documentos, programas e toda forma de conteúdo digital que são a essência da empresa.

Para que se faça este procedimento, há a necessidade de se criar a cultura de arquivamento correto e diário, para que a empresa não seja surpreendida com surpresas desagradáveis. Segundo CONTROLENET (2018) existem algumas regras que devem ser seguidas para que os objetivos sejam atingidos com sucesso:

- Como principal regra de segurança, as cópias não podem estar no mesmo equipamento que mantém os arquivos originais e em sistemas de backup instalados fisicamente próximos para evitar que computadores, servidores e sistemas de backup de um mesmo ambiente sofrerem sinistros simultâneos como furto, mau funcionamento, vandalismo, incêndio ou outros desastres;

- Jamais realize backup por intermédio de equipamentos instalados ao lado do computador como HDs Externos, pendrives ou mídias em geral; e

- O sistema de backup de fitas LTO, RDX ou DLT como alternativa, mas com o inconveniente de poderem ser transportadas para fora do âmbito da empresa, e serem perdidos e/ou danificados, bem como incorrer no fato de que os dados ali contidos podem ficar desatualizados rapidamente.

Pelos fatos descritos acima é que uma empresa deve se preocupar constantemente em armazenar corretamente os dados produzidos para que não incorram em uma trágica parada na produção em função de algum desastre ocorrido inesperadamente.

A Análise PRO, pelo grande volume de informações geradas, deve estudar a viabilidade da criação do setor de TI de forma que ele seja atuante e inovador, ou ter em seu quadro de colaboradores os serviços de técnico especializado da área. Desta forma o setor poderá desenvolver políticas de implementações de segurança dos dados gerados pela empresa. Políticas estas que podem compreender de que forma serão feitas a salvaguarda e guarda, onde serão arquivadas, politicas de acesso aos dados, gerenciamento dos backups, etc.

O setor de TI tem uma função primordial no controle de desastres onde, se não tratados corretamente, poderão ser perdidos definitivamente, tornando-os irrecuperáveis.

Em empresas onde não há o setor de TI ou técnico da área, como uma empresa de contabilidade, por exemplo, é primordial a contratação de empresa especializada em realizar backup.

Como citado anteriormente, os backups devem ser realizados e armazenados em locais distantes da empresa, preferencialmente nas nuvens, em empresas com sistemas de hardware e software confiáveis, com sistema de redundância, agendamento diário automático

de sincronização e alta velocidade de conexão, especializadas na salvaguarda de dados corporativos, onde serão armazenados com sistemas de criptografia e senhas para acesso.

A PHONOWAY (2018) por ser uma empresa que trabalha com soluções de armazenamento descreve os pilares básicos para investimento em backup na nuvem:

> Ao investir em uma solução de backup na nuvem você precisa ter certeza que ela atenderá os 3 pilares básicos : Integridade, disponibilidade e confidencialidade.
> Uma solução de backup na nuvem tem que ir além da simples recuperação de dados. Ela precisa garantir o arquivamento das informações por tempo indeterminado com segurança e confidencialidade.
> Permitir que você armazene e recupere a informação de forma simplificada, com rotinas simples e preservadas de desastres naturais ou ações provocados pelo homem.

Os sistemas atuais permitem realizar uma seleção de quais pastas devem ser sincronizadas com o sistema de backup, permitindo assim uma maior agilidade do sistema e a realização de cópias de segurança de todos os dados necessários, além de geralmente manter os últimos 07 backups ativos, o que dá uma grande margem de segurança.

Segundo PENSO TECNOLOGIA (2018):

> A cada dia, o uso da nuvem torna-se mais popular, seja entre as pessoas ou no âmbito empresarial. Mesmo que não tenhamos consciência disso, todos nós temos algo na nuvem. Seja um e-mail, um aplicativo, um perfil em uma rede social. E por que as tecnologias caminham cada vez mais em direção à nuvem? Porque o ambiente da nuvem é mais confiável frente aos internos das empresas e seus recursos são ilimitados.

A realização de backup por empresas especializadas em backup em nuvem é uma tendência que está se tornando cada vez mais rotineira em virtude das políticas segurança implementadas por elas, confiabilidade e política de privacidade na salvaguarda dos dados, além da economia que a empresa faz em relação ao investimento em hardware e software específico e pessoal treinado somente para manter guarda dos dados.

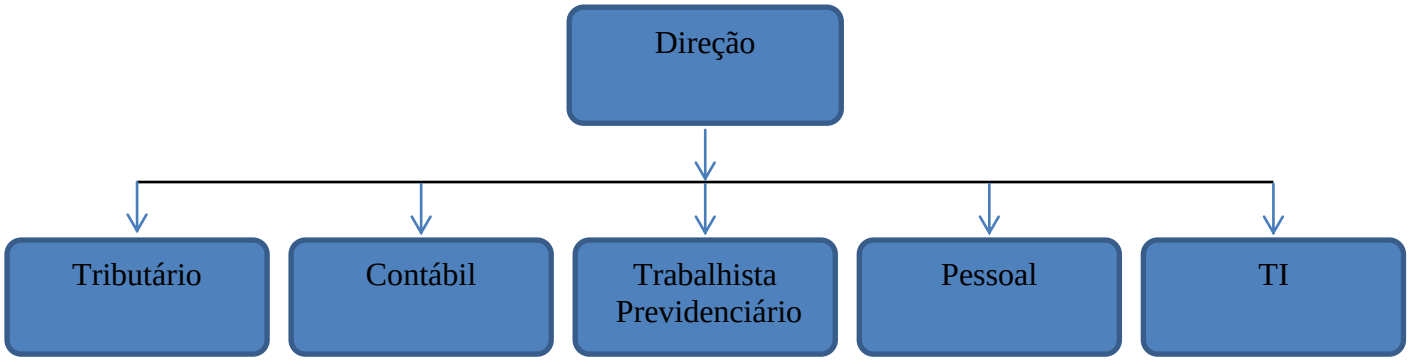
O manuseio dos dados eram realizado pela Análise.PRO sem os devidos cuidados, deixando com isto a confidencialidade e a integridade comprometidas.

Conforme relatado anteriormente, é muito preocupante a grande incidência de ocorrências de perda e/ou de sequestro de dados das empresas por pessoas e/ou programas maliciosos com o intuito de auferir vantagens financeiras criminosas com resgates digitais.

Os procedimentos realizados antes da contratação de uma empresa especializada em backup de dados, eram realizados pela Análise.PRO de forma não confiável, visto não haver uma política de segurança e de correto trato com as informações geradas e com os dados sigilosos dos clientes.

Ao analisar todas as evidências primeiramente foi proposto à Análise.PRO que inicialmente passasse a ter em seu quadro um setor de TI com no mínimo 1 profissional. Setor este criado e incorporado à estrutura organizacional da empresa conforme figura 5 abaixo.

Figura 5: Estrutura da empresa após proposta de mudança



Fonte: Do autor

Como segundo tópico foi orientado para que o setor de TI realizasse a implantação de um servidor dedicado e a reestruturação do sistema de rede e a atualização das estações de trabalho obsoletas atualmente utilizadas.

Como passo seguinte, o setor de TI realizou levantamento de empresas especializadas em salvaguarda de dados.

Após análise das propostas de soluções apresentadas pelas empresas interessadas na prestação dos serviços solicitados, e também detalhamento de implantação de uma estrutura de rede confiável, foi explanado à diretoria a proposta mais viável à empresa. Com isso foram contratados os serviços de uma empresa especializada e conceituada.

Os serviços oferecidos pela empresa escolhida para implantação incluem backups automáticos online diários agendados para iniciar em horário pós-expediente, guarda dos dados com alto índice de confiabilidade e confidencialidade, e garantia de restauração integral dos últimos 07 backups a qualquer hora, fatos estes que deram tranquilidade à empresa.

Após instalação e configuração de servidor com software dedicado, em reunião com todos os integrantes da Análise.PRO, foram definidas as pastas com os dados do servidor que havia necessidade de backup.

A Análise.PRO formalizou contrato com empresa especializada em realização de backups online, onde mantém todos os dados resguardados da incidência de qualquer sinistro que possa ocorrer.

A empresa contratada mantém os últimos sete backups realizados custodiados, pois em casos de ocorrência de sinistros, poderão ser restaurados imediatamente e integralmente.

Ressalta-se que, conforme informação de um dos diretores da Análise.PRO, meses após a configuração do servidor e a contratação dos serviços de backup, a empresa sofreu sequestro e criptografia de seus dados por software malicioso, fato este verificado no início

dos trabalhos de certo dia. Ocorre que no dia anterior, por ser feriado, não houve lançamentos, gerando perdas zero aos dados.

Diante disso o setor de TI imediatamente trocou os HDs e restaurou cópia dos sistemas, além de baixar a última cópia dos dados tutelados à empresa de backups, o que consumiu em torno de uma hora todo o processo.

Ressalta-se que esta ocorrência deu-se em várias empresas e repartições de serviços públicos naquela mesma semana.

Atualmente a Análise.PRO mantém em sua estrutura um setor de TI muito ativo e responsável pela integridade dos dados da empresa.

Como pontos fortes e fracos da realização de backups online de dados, entre muitos, podemos destacar os mostrados no quadro 2 abaixo:

Quadro 2: Pontos fortes e fracos.

Problema	Pontos fortes	Pontos fracos	Justificativa
Quais os pontos fortes e fracos da implantação de um sistema de backup online de dados?	Segurança: Pois possibilita que toda a logística da informação seja feita de forma criptografada, automatizada e digital. Dessa forma, reduz riscos de esquecimento ou violação da informação. A segurança fica armazenada em datacenter seguro e espalhado em localizações que garantem que a informação continuará existindo.	Insegurança: Apesar dos arquivos serem criptografados, a partir do momento em que são armazenados na nuvem, muitas pessoas ainda sentem-se inseguras ao salvarem seus dados nestas ferramentas. Isso porque, seus usuários podem sofrer ataques de cibe criminosos e ter logins e senhas capturadas, o que pode gerar um grande transtorno para a empresa no futuro.	Apesar do medo de inserir arquivos na nuvem, os sistemas de criptografia e os data centers atualmente disponíveis são bastante confiáveis.
	Flexibilidade: Seja uma empresa de pequeno porte, com dois computadores, ou uma grande companhia com milhares, o sistema em nuvem tem capacidade de atender. E mesmo que a empresa comece pequena, e aumente gradativamente sua necessidade por backup, a nuvem acompanhará esse crescimento.	Velocidade da internet: Para transferir os dados para a nuvem, é necessário ter acesso a uma internet de qualidade, com uma banda que lhe ofereça uma velocidade razoavelmente boa, caso contrário, dependendo do tamanho dos arquivos ou caso a conexão caia no meio da transferência, a empresa será prejudicada.	Para que se mantenha a integridade dos dados é de vital importância que a velocidade de conexão seja bem elevada, para que não ocorram perdas de dados durante a comunicação. Desta forma manteremos uma boa flexibilidade do sistema.
	Disponibilidade: O sistema em nuvem está disponível 100% do tempo, independente de qualquer situação de falta de energia, mudança física da empresa, aumento de estações de trabalho. etc.	Custo: Para cada ação realizada pela empresa, existe um custo a ser adicionado no orçamento. No caso da computação em nuvem não seria diferente, já que terá que dispor de um servidor para atender especificamente às necessidades de seus colaboradores e da organização como um todo. Assim, é importante verificar qual a solução ideal, para não gastar demais.	Os custos de manutenção de um sistema em nuvem são justificados pela alta disponibilidade dos dados em tempo integral para o cliente, gerando com isto um grande diferencial no quesito confiabilidade.

Fonte: Do autor.

Mesmo diante de alguns fatores negativos, os pontos positivos superam com elevada vantagem, pois os pontos fracos têm soluções e podem ser resolvidas e/ou minimizadas.

6 PROPOSTA DE SOLUÇÃO DA SITUAÇÃO-PROBLEMA

6.1 PROPOSTA DE MELHORIA PARA A REALIDADE ESTUDADA

Como base para a descrição e análise da realidade observada, e nos procedimentos anteriormente descrito, tem-se um parâmetro fundamentado da forma como tratar dados reservados gerados pela empresa Análise.PRO.

Como proposta de melhorias, foram elencados vários tópicos, conforme Quadro 3 – Questionário de coleta de dados, exposto no Apêndice, e descritos abaixo:

a) Implantação de Setor de TI

Inicialmente deve ser realizados estudos de viabilidade de implantação de um setor de TI com técnico habilitado e capacitado em redes, configuração de hardware e software, que ficará encarregado de prestar assistência em qualquer situação anormal que ocorrer.

b) Instalação de um servidor dedicado

O setor de TI deve pesquisar no mercado um servidor dedicado para as aplicações e para a guarda de dados gerados pela empresa, que depois de adquirido, deverá ser instalado e configurado com os aplicativos necessários.

c) Modernização dos equipamentos de hardware

Após a conclusão da instalação e configuração do servidor, o setor de TI deverá proceder a substituição das estações de trabalho obsoletas por estações mais atualizadas e configuradas.

Os aplicativos necessários aos trabalhos diários, bem como aplicativos de segurança como antivírus, firewall, e ferramentas de detecções de malware devem ser instalados e configurados em todas as estações.

d) Instalação e configuração de rede interna

O Setor de TI deverá providenciar a instalação e configuração de uma rede intranet com as novas estações de trabalho/servidor/impressoras, que deverão ser configuradas com aplicativos específicos para cada tipo de utilização, bem como devem ser atualizados constantemente.

e) Configuração e gerenciamento de níveis de acesso

Faz-se necessário o uso de aplicativo de gerenciamento de acesso, definindo níveis de acesso aos aplicativos utilizados e aos bancos de dados separadamente, bem como a configuração para o monitoramento constante, evitando com isso invasões indesejadas.

f) Contratação de serviços de backup online de dados

Após a conclusão das instalações e configurações, o setor de TI deverá realizar pesquisas de empresas especializadas em serviços de backup online de dados para apresentação à direção, para a seleção da que mais se enquadrar nos padrões exigidos pela Análise.PRO e futura contratação de serviços da área.

g) Implantação de plano de monitoramento

Como ação complementar ao serviço de backup online de dados, foi orientada a criação, manutenção e constante aperfeiçoamento pelo setor de TI, de um plano de monitoramento e atuação para o caso de ocorrer qualquer tipo de sinistro que afetem a integridade dos dados.

h) Aquisição de sistema de fornecimento de energia de emergência

Para que não ocorram interrupções por falta de energia elétrica, foi proposto que todo sistema deve estar protegido por um sistema de estabilização e de fornecimento de energia de emergência que atue automaticamente quando o fornecimento da energia comercial oscilar e/ou faltar, evitando com isso a perda de dados na hora da transferência, bem como a perda de equipamentos por queima.

As propostas de melhorias são muito importantes, e de alguma forma restringem a incidência de perdas catastróficas que possam ocorrer no decorrer do tempo.

6.2 RESULTADOS ESPERADOS

Diante do quadro atual de vulnerabilidade e das medidas corretivas propostas, a Análise.PRO mostrou-se extremamente preocupada com a confidencialidade e segurança dos dados gerados e dos dados reservados dos clientes.

Foram apresentados os resultados dos levantamentos dos equipamentos atualmente utilizados com suas configurações, as vulnerabilidades encontradas com relação à segurança, e também as propostas de melhorias.

Após análise, como passo inicial a empresa criou o setor de TI e realizou a contratação de um colaborador. Este setor realizou pesquisas e análises junto à empresas especializadas em fornecimento de equipamentos, e montou configurações específicas, as quais foram apresentadas à diretoria onde juntamente definiram a configuração a ser implantada.

Na instalação da rede física pode ser aproveitada grande parte da rede existente, exigindo somente pequenas mudanças e com isso atenderá as mudanças de configurações necessárias.

Os estudos demonstram que deve ser adquirido um servidor dedicado e com as configurações dentro das necessidades da empresa, o qual, depois de instalado e configurado, servirá como servidor de aplicativos e de dados, com aplicativos dedicados instalados para realizar os backups online nas datas e horários pré-determinados, e demandará maior segurança em todas as operações realizadas pela empresa.

As 08 estações de trabalho obsoletas não atendem mais as necessidades e devem ser substituídas por 12 estações configuradas no mínimo com processadores I5, 2Gb de memória RAM, monitores LED 24” e HD 1Tb, e com isso passariam a atender com muita eficiência a grande demanda de trabalhos realizados diariamente na empresa, bem como agilizariam todos os procedimentos realizados atualmente.

Em substituição a impressora que já estava obsoleta, como meio de agilizar os processos de impressão, scanner e fotocópias, deve ser adquirido duas impressoras multifuncionais: 01 laser colorida e uma DeskJet para melhor atender aos serviços necessários.

O setor de TI realizou o delineamento de consumo de energia para adquirir um sistema de fornecimento de energia alternativo junto a empresas especializadas. Este sistema é de vital importância e, depois de adquirido e implantado, evitará perdas de dados e de equipamentos, e manterá ininterruptos os trabalhos na empresa.

Finalizando a reestruturação, a direção deverá atualizar alguns dos mobiliários com melhor ergonomia para o conforto dos colaboradores, evitando assim futuras complicações causadas por má postura.

Depois de realizadas todas as alterações propostas, deverão ocorrer alterações significativas nos resultados finais dos trabalhos realizados.

A Análise.PRO constantemente deverá analisar os tipos de dados gerados e custodiados pela empresa, e conforme as necessidades, poderá ampliar o backup de dados.

Como local de armazenamento, será destinada uma área no servidor de aplicações e arquivos, e a contratação dos serviços de uma empresa especializada para a realização diária de backup online de dados, gerando com este procedimento um índice de confiabilidade de mais de 99%.

6.3 VIABILIDADE DA PROPOSTA

Para que as propostas apresentadas pudessem ser implantadas, havia a necessidade de mudanças de alguns paradigmas e também da disponibilidade da empresa em realizar um investimento de grande vulto.

A Análise.PRO possui uma carteira consistente de cliente e esta em larga expansão. Para que se mantenha a integralidade e confidencialidade dos dados gerados, pois são bens de suma importância, todos os tópicos e ajustes necessários que foram apresentados, com os custos conforme quadro 4, após analisados e discutidos, foram autorizados.

Quadro 4: Custos de equipamentos

EQUIPAMENTO	**CUSTOS**
Adaptação rede física	R$ 250,00
01 Servidor dedicado	R$ 31.500,00
08 Estações de trabalho	R$ 33.600,00
02 Impressoras multifuncionais	R$ 5.200,00
01 Sistema de nobreak	R$ 12.300,00
Mobiliários	R$ 5.500,00
TOTAL	**R$ 88.350,00**

Fonte: Do autor

A origem da verba para custear a implantação da reestruturação já estava estimada no capital da empresa e vinha sendo reservada para quando fosse realizada.

Segundo a visão dos diretores, o custo benefício do investimento obteve total retorno quando da ocorrência de invasão, em que todos os dados se mantiveram intactos e as cópias de segurança puderam ser prontamente restauradas, demonstrando que realmente havia a necessidade de realizar o investimento.

Portanto o custo benefício não foi medido somente pela criação do Setor de TI e do valor gasto com a instalação da rede e dos equipamentos, mas pelos resultados finais práticos atingidos em uma situação real de invasão.

7 CONSIDERAÇÕES FINAIS

Após estudos e a contratação dos serviços de empresa especializada, ocorreu um ataque cibernético no servidor da Análise.PRO, o que não afetou as cópias de backup custodiadas em nuvem, permitindo imediato restabelecimento de todo o sistema sem registro de nenhuma perda.

Diante de todas as propostas e da ocorrência de invasão, a Análise.PRO mantém em sua estrutura um setor específico de TI com colaborador qualificado.

Como sabemos, diariamente são desenvolvidas outras técnicas e malware com o intuito de burlar as seguranças desenvolvidas até então. Esta é uma luta constante da caça se protegendo do caçador.

Com as medidas tomadas para evitar perdas de dados como a troca de equipamentos, implantação de uma rede interna de computadores bem estruturada e configurada, e a contratação de uma empresa certificada para a realização de backup online, pôde-se mitigar os ao máximo os resultados dos ataques realizados.

Diante de tantas dificuldades e incertezas, a Análise.PRO reagiu positivamente aos questionamento e as propostas de mudanças que foram indicadas.

O enorme interesse da empresa em realizar as mudanças contempladas nos vários objetivos propostos foi se suma importância para o sucesso do empreendimento.

Muitos foram os desafios quando da implantação dos objetivos propostos, onde podemos destacar:

Identificar o que realmente a empresa necessitava para que cumpra os objetivos propostos na sua a missão.

Como readequar a estrutura organizacional com a criação de mais um setor e a contratação de mais colaboradores.

Como justificar a substituição dos equipamentos por outros com mais recursos e mais atualizados, a implantação de uma nova rede física e de um sistema de servidor.

E o porquê da contratação de serviços de backup online de dados por empresa terceirizada.

Mas quando a empresa tem como meta a prestação de serviços de primeira qualidade e total responsabilidade para com os clientes, não foi difícil realizar todas as propostas apresentadas, mesmo quando os investimentos somam grande vulto, o que neste caso a em-

presa já vislumbrava uma futura modificação e já vinha reservando um aporte financeiro para tal.

Para o aprimoramento deste estudo, é aconselhável a reavaliação dos procedimentos e equipamentos, num futuro próximo, para a certificação ou realização de propostas de mudanças que se fizerem necessário.

REFERÊNCIAS

ANÁLISE.PRO, Disponível em: <http://www.analisepro.com.br/empresa>. Acessado em 07 ago. 2018.

ANGELO, Luiz, **Ransomware: Malware que sequestra dados do seu computador e pede resgate**. Disponível em <http:// www.ceschini.com.br/2016/09/ransomware-todo-cuidado-e-pouco-com-esse-malware/>. Acessado em 30 ago 2018.

CESCHINI, Comunicação e Marketing Digital, **Ransomware: Malware que sequestra dados do seu computador e pede resgate** – 2016 - <http://www.ceschini.com.br/2016/09/ransomware-todo-cuidado-e-pouco-com-esse-malware/> Acessado em 30 ago 2018.

CONTROLENET, Disponível em: <http://www.controle.net>. Acessado em: 07 ago. 2018.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa** – 4. ed. –São Paulo: Atlas, 2002.

G1, **Vírus invade computadores do GDF e suspende raio x em hospitais**. – 2017. Disponível em: <https://g1.globo.com/distrito-federal/noticia/governo-do-df-tem-pane-geral-em-sistema-e-suspende-raio-x-em-hospital-entenda.ghtml>. Acessado em 28/03/2018.

G1, **Sistemas do GDF sofrem 18 invasões e mais de 2 milhões de tentativas em 1 ano**. - 2018. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/sistemas-do-gdf-sofrem-18-invasoes-e-mais-de-2-milhoes-de-tentativas-em-1-ano.ghtml>. Acessado em 09/04/2018.

LUMIUN, **Crimes cibernéticos: Como agir em caso de invasão e roubo de dados?** – 2017 - Disponível em: <https://www.lumiun.com/blog/crimes-ciberneticos-como-agir-em-caso-de-invasao-e-roubo-de-dados/>. Acessado em: 07 ago. 2018.

PENSO TECNOLOGIA, disponível em: <http://www.penso.com.br>. acessado em: 07 ago. 2018

PHONOWAY, disponível em: <http://www.phonoway.com.br>. acessado em: 07 ago. 2018

TORRES, Gabriel. **Redes de computadores – Versão Revisada e Atualizada** – Rio de Janeiro, Novaterra Editora e Distribuidora Ltda., 2009.

ULBRICH, Henrique Cesar; DELLA VALLE, James. **Universidade Hacker** – São Paulo, Digerati Books, 2009.

APÊNDICE

Quadro 3 – Questionário de coleta de dados

Perguntas
Que tipos de dados são gerados na empresa?
Quais os dados são gerados backups?
Onde são realizados os backups?
Qual a frequência dos backups?
Histórico de perda de dados?
Qual o nível de segurança dos backups?
Qual nível de confiabilidade dos backups?
Existe setor específico responsável pelo acompanhamento dos backups?
Equipamentos atendem as necessidades?
Possui sistema de nobreak?

Fonte: Do autor