INSTITUTO DE ENSINO SUPERIOR DO ESPÍRITO SANTO
FACULDADE DO ESPÍRITO SANTO – MULTIVIX CACHOEIRO DE ITAPEMIRIM
CURSO DE SISTEMAS DE INFORMAÇÃO

DANIEL HEMERLY DE BACKER
ESTELA PIN CANAL

DIAGNOSTICANDO A SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS DE MÁRMORES E GRANITOS NA CIDADE DE CACHOEIRO DE ITAPEMIRIM, EM CONFORMIDADE COM A NBR ISO/IEC 17799:2005

CACHOEIRO DE ITAPEMIRIM
2014

DANIEL HEMERLY DE BACKER
ESTELA PIN CANAL

DIAGNOSTICANDO A SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS DE MÁRMORES E GRANITOS NA CIDADE DE CACHOEIRO DE ITAPEMIRIM, EM CONFORMIDADE COM A NBR ISO/IEC 17799:2005

Trabalho de Conclusão de Curso apresentado ao curso de Sistemas de Informação na Faculdade do Espírito Santo – MULTIVIX Cachoeiro de Itapemirim, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Prof. Me. Jocimar Fernandes.

CACHOEIRO DE ITAPEMIRIM
2014

DANIEL HEMERLY DE BACKER
ESTELA PIN CANAL

DIAGNOSTICANDO A SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS DE MÁRMORES E GRANITOS NA CIDADE DE CACHOEIRO DE ITAPEMIRIM, EM CONFORMIDADE COM A NBR ISO/IEC 17799:2005

Trabalho de Conclusão de curso apresentado ao curso de Sistemas de Informação na Faculdade do Espírito Santo – MULTIVIX Cachoeiro de Itapemirim, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Aprovado em 01 de dezembro de 2014.

COMISSÃO EXAMINADORA

_____
Prof. Me. Jocimar Fernandes
Orientador

_____
Prof. Me. Bruno Missi Xavier

_____
Prof. Esp. Marcelo Costalonga

_____
Prof. Me. Thiago Caliman

Dedicamos exclusivamente à nossa família.

AGRADECIMENTOS

Agradecemos a Deus acima de tudo.
Às organizações que colaboraram para a realização da pesquisa deste trabalho.
E ao nosso orientador pelo apoio.

“*O objetivo fundamental dos sonhos não é o sucesso, mas nos livrar do fantasma do conformismo.”*
Augusto Cury.

BACKER, Daniel H. de; CANAL, Estela P. **Diagnosticando a segurança da informação nas empresas de mármores e granitos na cidade de Cachoeiro de Itapemirim, em conformidade com a norma ISO/IEC 17799:2005.** 2014. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) – Faculdade do Espírito Santo – MULTIVIX Cachoeiro de Itapemirim, Cachoeiro de Itapemirim, 2014.

RESUMO

A informação atualmente é usada como base para tomadas de decisões, que pode alavancar um grande sucesso no mercado competitivo. É asseverada como um do ativo mais importante da organização, sendo por isso necessário, uma imprescindível preocupação com a existência e cumprimento de políticas de segurança da informação, para que este bem seja corretamente resguardado. O objetivo principal deste trabalho é por meio de pesquisa descritiva com método quantitativo, baseado em questionário e aplicado através do *survey,* levantar e identificar a existência de políticas de segurança da informação em conformidade com a norma NBR ISO/IEC 17799:2005 nas empresas dos setores de rochas ornamentais no município de Cachoeiro de Itapemirim e mensurar o grau de aderência de acordo com a norma citada. Os objetivos da pesquisa foram alcançados a partir da análise de dados e ficou evidenciado que não há forte relação entre as práticas da segurança da informação e as características relevantes das empresas participantes da pesquisa. Ficou evidenciado também, que as práticas de segurança aderidas pelas empresas pesquisadas em conformidade com a norma, variaram entre 20% e 100%. Foi constatado vistosamente o apoio de 79,2% da alta direção aos princípios de segurança da informação nas empresas. Aos participantes da pesquisa, houve uma convergência aceitável da satisfação geral com o nível de formalização das práticas e o grau das aderências das práticas de segurança. De forma geral, as práticas de segurança destacaram-se satisfatoriamente na maioria das empresas com pontuações acima da média.

Palavras-chave: NBR ISO/IEC 17799:2005. Segurança da informação. Empresas no ramo de rochas ornamentais.

BACKER, Daniel H. de; CANAL, Estela P. **Diagnosticando a segurança da informação nas empresas de mármores e granitos na cidade de Cachoeiro de Itapemirim, em conformidade com a norma ISO/IEC 17799:2005.** 2014. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) – Faculdade do Espírito Santo – MULTIVIX Cachoeiro de Itapemirim, Cachoeiro de Itapemirim, 2014.

ABSTRACT

The information is currently used as a basis for decision making, which can leverage a great success in the competitive market. It is asserted as one of the most important asset of the organization, so it is necessary, an essential concern with the existence of and compliance with information security policies, so that the well is properly safeguarded. The main objective of this work is through descriptive research with quantitative method, based on questionnaire and applied through the survey, survey and identification of the existence of information security policies in accordance with the standard ISO / IEC 17799: 2005 in the Companies ornamental stone sector in the municipality of Itapemirim and measure the degree of compliance in accordance with this standard. The research objectives were achieved from analysis of data and it was evident that there is no strong relationship between the practices of information security and the relevant characteristics of the study participants companies. We also demonstrated that the safety practices adhered to by the companies surveyed in accordance with the standard, ranged between 20% and 100%. Was flamboyantly found the support of 79.2% of top management to the principles of information security in organizations. To research participants, there was an acceptable convergence of overall satisfaction with the level of formalization of the practices and the degree of adherence to safety practices. In general, safety practices stood out satisfactorily in most companies with above average scores.

Key words: NBR ISO/IEC 17799:2005. Information security. Companies in the field of ornamental.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

SUMÁRIO

1 INTRODUÇÃO

A informação como base para tomada de decisão tem alavancado um grande diferencial para o mercado competitivo entre as organizações, sendo que se a sua utilização for feita de forma correta, poderá garantir a sobrevivência e crescimento de qualquer empresa, mas se a informação não for administrada cuidadosamente, poderá inverter o sucesso no mercado competitivo e enraizar prejuízos e fracassos.

Com o advento da tecnologia da informação, esse quadro tem facilitado a gestão da informação como base para tomada de decisão, pois a velocidade e quantidade com que os dados são processados foram aumentadas consideravelmente e uma confiança maior foi estabelecida. Antigamente era comum (ou ainda é) as informações e os negócios serem tratados e movimentados manualmente, porque a tecnologia de antigamente não passava muita confiança e o armazenamento das informações eram carentes. E, com isso, perdia-se então muito tempo manipulando os dados e era mais suscetível ao erro e certamente pouco ou nenhum controle era usado.

A tecnologia tem melhorado não somente a capacidade de processamento e armazenamento da informação, mas também a sua disseminação. Os sistemas distribuídos, como a Internet, por exemplo, têm contribuído estupendamente para com a propagação da informação, e este fator evoluí cada vez mais.

A Internet é um conjunto de computadores interligados no mundo inteiro com diversos recursos para quem a explora, todavia, a facilidade de usuários de acesso a ela, desnudou a exigência de componentes de hardwares, softwares e políticas com relação à segurança eletrônica digital. Com esse acesso sem fronteiras de seus usuários a tudo e em qualquer momento, a própria comunidade desenvolvedora não percebeu que deixara passar um assunto importante: a segurança. A segurança na Internet é falha, os meios pelos quais a informação trafega não é seguro e têm riscos, e um grande risco é achar que não se corre riscos (CERT, acesso em 01 out. 2014). Contudo, entendendo que a base de dados de uma empresa é um grande potencial ou se não o ativo mais importante para sobrevivência no mercado, o

vazamento de informações estratégicas, seja por falhas involuntárias ou falhas intencionais, é um grande risco que a empresa deve considerar e se preocupar.

1.1 Problema de Pesquisa

As empresas precisam atentar-se para a segurança das informações que fazem parte dos negócios e estratégias internas. Controles e políticas de segurança devem ser estabelecidos nas empresas para, ao menos, os riscos serem reduzidos.

A cidade de Cachoeiro de Itapemirim, no estado do Espírito Santo, realiza todo o ano a grande feira internacional do mármore e granito, a *Stone Fair*, e segundo os seus realizadores, Cachoeiro "[...] é conhecida nacionalmente pelo seu parque industrial de beneficiamento de rochas ornamentais, o maior do Estado, e pioneiro nesse mercado em todo país, com cerca de 1.000 empresas atuando no setor [...]" (CACHOEIROSTONEFAIR, 2013, acesso em 3 mar. 2014).

A partir desse fato, percebe-se pelo grande número de empresas atuando no setor, que há um grande número de concorrência. Nesse meio competitivo a informação pode ser um fator diferencial de sucesso. Mas será que os gestores têm conhecimento disso e sabem da importância de ter uma política de segurança para preservar as informações da empresa?

Métodos de segurança, como as políticas de segurança são usadas para orientar todos os envolvidos a utilizarem adequadamente desde o espaço físico de trabalho até os sistemas de processamento de dados, deste modo, a sua ausência motiva ameaças às informações. A ausência também de *backups* pode ser um risco no caso de perda de alguma informação por conta de uma queda de energia ou queima de equipamentos. Dados publicados no site do aeon.com.br, de uma pesquisa decorrente no ano de 2012, mostram estatísticas referentes às consequências relacionadas às perdas de informações nas empresas. "[...] gestores entendem que as perdas da informação geram consequências [...] não entendem é que este impacto pode ser muito maior do que eles imaginam" (MORAES apud AEON, 2012, acesso em: 3 mar. 2014). Ainda de acordo com os dados citados na pesquisa, 93 % das empresas que perdem seus servidores de dados por qualquer motivo, quebram

em um ano, 50 % das empresas que perdem seus servidores e não possuem gerenciamento de dados quebram imediatamente quando do incidente, 94 % das empresas que sofrem com perdas catastróficas jamais reabrem suas portas, 77 % das empresas que testam seus sistemas de *backup* encontram falhas operacionais, 50 % das fitas de *backup* falham durante o processo de restauração, 96 % das estações de trabalho que possibilitam a guarda de dados não sofrem *backup* periódico, 70 % das empresas que sofrem grande perda de dados quebram em um ano.

1.2 Objetivos

1.2.1 Geral

O objetivo geral é verificar através de pesquisa descritiva, o nível de segurança da informação, juntamente com uma análise de conformidade com as normas estabelecidas pela NBR ISO/IEC 17799:2005 nas empresas de mármores e granitos na cidade de Cachoeiro de Itapemirim, Espírito Santo, Brasil.

1.2.2 Específicos

a) Avaliar o nível de segurança da informação nas empresas de mármores e granitos, na cidade de Cachoeiro de Itapemirim, ES;
b) Avaliar as características relevantes das empresas de mármores e granitos, na cidade de Cachoeiro de Itapemirim, ES;
c) Quantificar o número de empresas que possuem políticas de segurança e quantas se preocupam em realizar *backup* das suas informações;
d) Analisar a conformidade das políticas de segurança com a norma NBR ISO/IEC 17799:2005;

1.3 Pressupostos

Foi possível no desenvolvimento do trabalho criar uma visão antecipada através dos seguintes pontos observados, como prováveis respostas para a pesquisa de campo:

a) Existem políticas de segurança da informação formalizadas nas empresas de mármores e granitos, na cidade de Cachoeiro de Itapemirim, ES;
b) As politicas de segurança da informação das empresas estão em conformidade com a norma NBR ISO/IEC 17799:2005;
c) As empresas com maior número de funcionário e de faturamento anual, possuem melhores práticas de segurança da informação.

1.4 Justificativa

De acordo com os dados levantados pelo Portal do Governo do Estado do Espírito Santo (acesso em 3 mar. 2014), o ES é o principal produtor e um importante estado de maior processamento e exportação de rochas ornamentais no Brasil. É nele a maior concentração de rochas ornamentais no país, e há estimativas de crescimentos e investimentos grandes no setor.

Ainda de acordo com o Portal do Governo, a cidade de Cachoeiro é a maior cidade do Brasil processadora e detém o maior parque industrial do estado. Pode-se então notar o prestígio que a cidade de Cachoeiro de Itapemirim possui. “Para se ter uma idéia (sic) da importância do polo processador de Cachoeiro, 25 milhões de metros quadrados de rochas ornamentais que o Espírito Santo processa por ano, 70% é beneficiado em empresas cachoeirenses” (CACHOEIROSTONEFAIR, 2013, acesso em 4 mar. 2014).

Essas empresas totalizam 1.000 somente na cidade de Cachoeiro de Itapemirim. E se levarmos em conta a grande concorrência neste ramo, a empresa que não resguardar suas informações e obter prejuízos pelas suas perdas, o erro pode ser crucial para o seu fechamento.

Empresas no setor de rocha, assim como quaisquer outras, que possui funcionários, seja na grande proporção, pequena ou média, estão sujeitas a riscos envolvendo as suas informações. Logo, é recomendado a adoção de políticas de segurança da informação para instruir os funcionários e todos os envolvidos com orientações do que pode ou não fazer na empresa. Mesmo independente dos funcionários, nos meios pelos quais as informações trafegam, os riscos também são iminentes, além dos riscos externos que as empresas estão sujeitas, como os riscos de desastres naturais (incêndios, avalanches, enchentes e etc.). Contudo, existem muitas medidas de segurança que prometem resguardar ou reduzir a um nível aceitável os riscos às informações.

> [...] uma empresa se propõe a oferecer serviços de qualidade, buscando o constante aprimoramento nesse quesito, necessita, sempre, estar preparada para lidar com os cuidados que a segurança da informação exige, defendendo seu próprio patrimônio e não sofrendo, no futuro com erros cometidos por omissão (CNASI, [20--], acesso em: 4 mar. 2014).

É importante enfatizar que há muitas empresas no setor de rochas na cidade de Cachoeiro, e aquela que ignorar a segurança de suas informações poderá ter prejuízos irreparáveis e abrir as portas para a grande concorrência neste setor.

2 REVISAO DE LITERATURA

2.1 Conceitos e Características da Informação

Atualmente discute-se muito a respeito dos valores que a informação agrega às organizações, bem como para toda a sociedade. O que é chamado pelos autores Audy, Andrade e Cidral (2007, p. 93) de “sociedade da informação”. A informação por si só tem um importante papel na tomada de decisões, como trata o autor Andrade (2009), as decisões são ações para resolver algum problema ou chegar a algum objetivo, mas essas decisões, sejam elas racionais ou administrativas, são tomadas com base no fator de incerteza, ou seja, em previsões não perfeitas. E ainda segundo o autor, mesmo que a previsão seja completa, outro aspecto que pode tornar mais difícil a tomada de decisão é a falta de informação. E com embasamento nessa objeção, o autor Rascão (2006) trata e relaciona o grau de incerteza com o conceito de probabilidade, na qual pode ser reduzida com o efeito de que a informação pode causar, seja através da sua utilização ou percepção.

Logo, fica inteligível que a informação tem sim um papel importante. As organizações, os gestores precisam tomar decisões, e precisam das informações para tomar decisões.

A informação nada mais é, de acordo com Audy, Andrade e Cidral (2007), um conjunto de dados organizados e processados, que apresentam alguma significação precisa, diferentemente dos dados puros, que por si só não apresentam um significado ou valor adicional. Rascão (2006, p. 36) simplifica que a “informação é o dado com significado atribuído”. E a partir da informação, é possível extrair conhecimentos, onde Dantas (2011, p. 9), descreve que o conhecimento “[...] é a informação cuja relevância, confiabilidade e importância, foram avaliadas, e é obtido pela interpretação e integração de vários dados e informações para iniciar a construção de uma situação”.

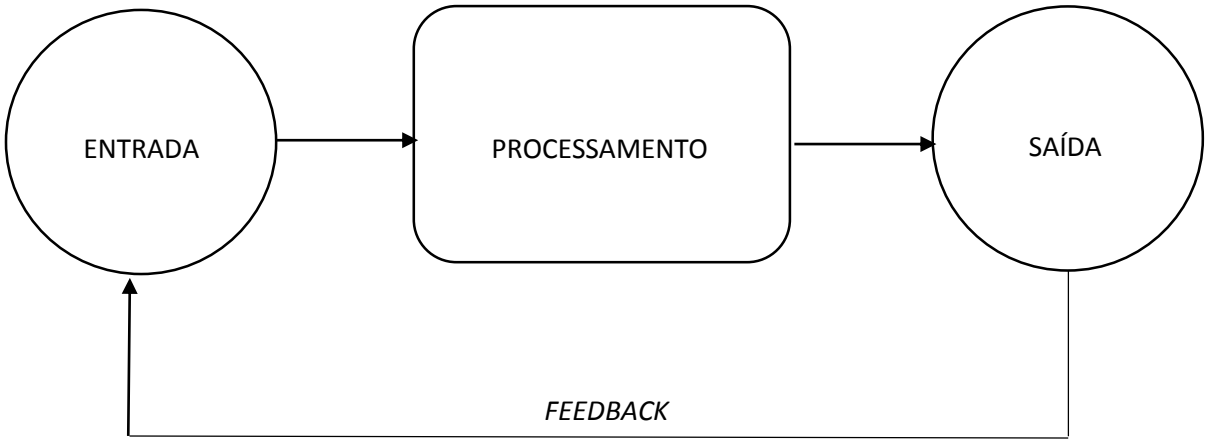
Outros conceitos da informação são descritos por Laudon e Laudon (1998, apud AUDY; ANDRADE; CIDRAL, 2007, p. 94) onde dizem que “[...] são dados que foram moldados em um formato que possui um significado e utilidade para o homem”, e

por Davis (1974, apud AUDY; ANDRADE; CIDRAL, 2007, p. 94) que também conceitua a informação como “[...] um dado processado de uma forma significativa para o usuário e que tem um valor real ou percebido para decisões correntes e posteriores”. Estes conceitos refletem para o reforço de que a informação resulta de um processamento que têm valores significativos e importantes para o homem e tomadas de decisão.

2.1.1 Sistemas de Informação

O tratamento dos dados que resultam em informações é geralmente feito a partir de um Sistema de Informação, descrito por Dantas (2011, p. 10), “[...] como um conjunto de elementos ou componentes inter-relacionados, que coletam (entrada), manipulam (processamento) e disseminam (saída) os dados e a informação e fornecem um mecanismo de *feedback* para atender um objetivo”.

Figura 1 – Componentes básicos de um Sistema de Informação



Fonte: Ralph (2002) apud Dantas (2011), adaptado pelos autores.

Existem vários tipos de Sistemas de Informações disponíveis para as organizações, como mostra o Quadro 1, que devem ser selecionados e implantados de acordo com a necessidade da empresa.

Quadro 1 – Tipos de Sistemas de Informação

Tipos de sistemas	Sigla	Descrição
Sistemas de informações gerenciais	SIG	Contém as operações básicas da empresa, atendendo às necessidades dos gerentes de nível médio de monitorar e controlar a empresa, prevendo também seu desempenho futuro.
Sistemas de apoio à decisão	SAD	Auxiliam gerentes de nível médio a tomar decisões que fogem da rotina. Focam em um único problema, que se altera com rapidez e para o qual não existe uma resolução totalmente predefinida.
Sistemas de apoio ao executivo	SAE	Ajudam os executivos da gerência sênior a tomar decisões em relação à questões como tendências de custo do setor em longo prazo e como a empresa se encaixará nesse cenário. Abordam decisões não rotineiras que exigem bom senso e capacidade de avaliação e percepção, uma vez que não existe um procedimento previamente estabelecido para se chegar a uma solução.
Sistemas integrados	ERP	Coleta dados de vários processos fundamentais da organização, como: manufatura e produção, finanças e contabilidade, vendas e marketing e recursos humanos. Esses dados são então armazenados em um único repositório central. Assim, a informação que estava fragmentada em diferentes sistemas passa a ser compartilhada em toda a empresa, permitindo que os diferentes setores da organização possam cooperar de forma mais próxima.
Sistemas de gerenciamento de cadeia de suprimentos	SCM	Ajudam a empresa a administrar sua relação com os fornecedores. O objetivo fundamental desses sistemas são o de levar a quantidade certa de produtos da fonte ao local de consumo, com menor uso possível dos recursos de tempo e custo.
Sistemas de gerenciamento do relacionamento com o cliente	CRM	Fornecem informações sobre o cliente para que seja possível coordenar todos os processos de negócios a ele relacionados, em termos de vendas, marketing e serviços. Tem como objetivo maximizar a receita, a satisfação e retenção de clientes.
Sistemas de gestão do conhecimento	SGC	Possibilitam que as organizações administrem melhor seus processos, capturando e aplicando conhecimentos. Coletam todo o conhecimento e a

		experiência relevantes na empresa e os tornam disponíveis onde e quando forem necessários para melhorar os processos de negócio e as decisões administrativas.
Sistemas de processamento de transações	SPT	Registra as transações de rotina necessárias para o funcionamento da empresa como, por exemplo, registro de vendas, sistemas de reservas em hotéis, folha de pagamento, registro de funcionário. O objetivo dos é responder (sic) perguntas de rotina e monitorar o fluxo de transações da organização.

Fonte: Laudon e Laudon (2004) apud Santos, Quatrin, Pinto, Stefanan, Costa, 2012.

É válido que a informação em si é essencial para uma organização, e sendo um sistema de informação que tratará da informação, este deve ser bem estruturado e implantado corretamente, caso não, o feito pode gerar prejuízos em vez de bons resultados, e os autores Oliveira, Ponchio, Neto e Pizzinatto (2009) reforçam este argumento através de uma pesquisa com 375 organizações de várias nações, onde revelaram que o mau gerenciamento dos sistemas de informação pode realmente acarretar em grandes perdas.

2.1.2 Ativo da informação e informação valiosa

O site da Realiso (acesso em 24 mar. 2014) discute um ativo como qualquer componente que auxilia os processos de negócio de uma organização, seja o componente humano, software, tecnológico e etc. Ou mais simplificadamente, ainda de acordo com o site, o ativo é tudo o que pode agregar valor para uma entidade. Como também é descrito na norma ISO/IEC 13335-1:2004 citada pela NBR ISO/IEC 17799:2005 (2005, p. 1), onde o ativo é “qualquer coisa que tenha valor para a organização”.

Ativo é “qualquer coisa que precisa ser protegida, porque tem valor para a organização e contribui para que a organização tenha sucesso em atingir seus objetivos” (STALLINGS; BROWN, 2014, p. 448).

A NBR ISO/IEC 17799:2005 (2005, p. 21) cita os tipos de ativos:

> a) Ativos da informação: base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;
>
> b) Ativos de *software:* aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
>
> c) Ativos físicos: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;
>
> d) Serviços: serviços de computação e comunicações, utilidades gerais, por exemplo aquecimento, iluminação, eletricidade e refrigeração;
>
> e) Pessoas e suas qualificações, habilidades e experiências;
>
> f) Intangíveis, tais como reputação e a imagem da organização.

Analisando o conceito de ativos e os tipos de ativos, é notório que a informação é um ativo de grande mérito para a organização, uma vez que as tomadas de decisões são feitas sobre as informações que circulam por toda organização, assim assevera a Acioli (2011). Dados de uma pesquisa publicada no site Mundo en Línea (2004) reforçam o mérito da informação como principal ativo da organização, onde se destaca que 94 % das empresas que perdem seus dados, seja por má gestão da informação, erro humano, falhas de segurança ou catástrofes naturais, cedo ou tarde elas desaparecem.

“Como a informação tem ocupado um papel de destaque no ambiente de negócios, e também tem adquirido um potencial de valoração para as organizações e para as pessoas, ela passou a ser considerada o seu principal ativo” (DANTAS, 2011, p. 21).

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente (sic) necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado (NBR ISO/IEC 17799:2005, p. ix).

Campos (2006) enfatiza que, a informação como ativo é por muitas vezes mais valiosa do que o valor dos bens físicos, uma vez que as organizações garantem seus bens patrimoniais como ativos.

Sendo as informações os ativos mais importantes para a organização, percebe-se que elas se tornam valiosas. O conceito de informação valiosa “está diretamente ligado a como ela auxilia os tomadores de decisões a atingir seus objetivos organizacionais” (STAIR; REYNOLDS, 2006, p. 7.). Por exemplo, o valor de uma informação poderia ser medido de acordo com o grau de probabilidade de acerto em uma tomada de decisão ou pelo retorno de lucros adquiridos após a tomada de decisão, a partir da informação valiosa.

Quadro 2 – Características de informações valiosas

Características	**Definições**
Precisas	Informações precisas não contém (sic) erros. Em alguns casos, informações imprecisas são geradas quando dados imprecisos são fornecidos durante o processo de transformação. Isto é comumente denominado lixo entra, lixo sai (GIGO – *garbage in, garbage out*).
Completas	Informações completas contêm todos os fatos importantes. Por exemplo, um relatório de investimentos que não inclua todos os custos importantes não é completo;
Econômicas	Informações devem também ser relativamente econômicas de produzir. Os tomadores de decisões devem sempre equilibrar o valor das informações e o custo de produzi-las.
Flexíveis	Informações flexíveis podem ser usadas para diversos propósitos. Por exemplo, informações sobre os itens em estoque para uma peça específica podem ser usadas por um representante de vendas para fechar uma venda, por um gerente de produção para determinar se é preciso repor os estoques e por um executivo financeiro para determinar o valor total que a companhia investiu em estoque.
Confiáveis	Podemos depender de informações confiáveis. Em muitos casos, a confiabilidade de informações depende da confiabilidade do método de coleta de dados. Em outros, a confiabilidade depende da fonte de informações. Um boato de fonte desconhecida de que o preço do petróleo pode subir pode não ser confiável.
Relevantes	Informações relevantes são importantes para o tomador de decisões. A informação de que o preço do tecido pode cair talvez não seja relevante para um fabricante de dispositivos para computadores.
Simples	Informações devem também ser simples, e não exageradamente complexas. Informações sofisticadas e detalhadas podem ser

	desnecessárias. De fato, informações em demasia podem provocar uma sobrecarga de informações e o tomador de decisões, por sua vez, talvez não consiga determinar o que é de fato importante.
Apresentadas no momento exato	É preciso apresentar as informações no momento exato. Saber das condições climáticas da semana anterior não o ajudará a decidir qual roupa vestir hoje.
Verificáveis	Informações devem ser verificáveis. Isso significa que você pode checa-las para garantir que estejam corretas, talvez pela checagem de muitas fontes para a mesma informação.
Acessíveis	Informações devem ser de fácil acesso para usuários autorizados, obtidas no formato correto e no momento correto segundo suas necessidades.
Seguras	Informações devem ser seguras quanto ao acesso de usuários não autorizados.

Fonte: Stair e Reynolds (2006).

De acordo com Stair e Reynolds (2006) os dados apresentados no Quadro 2 são características essenciais para informações serem valiosas e consequentemente, além de serem valiosas para os tomadores de decisões, tornam-se também para toda a organização. E ainda segundo os autores, as informações podem causar grandes prejuízos às organizações, se elas forem imprecisas e vagas, pois com informações erradas, as decisões também se tornam erradas.

2.2 Gestão do Risco

2.2.1 Conceito do risco

No contexto empresarial, as ameaças e as oportunidades podem acarretar perdas ou ganhos para o negócio. O sucesso de uma empresa pode ser alcançado através de uma boa gestão do risco, tendo como objetivo de aperfeiçoar as suas oportunidades estabelecendo estratégias voltadas para um maior crescimento, assim como também para a maximização de seus resultados. Com a ausência da gestão do risco, as empresas passam a obter grandes resultados de perdas e danos em especial à informação. A norma da NBR ISO/IEC 17799:2005 (2005, p. 2), define o risco como uma “combinação da probabilidade de um evento e de suas consequências”.

Os riscos de segurança da informação são as possibilidades de uma ameaça explorar vulnerabilidades dos seus ativos, comprometendo assim a confidencialidade, integridade e a disponibilidade das informações de uma organização (NBR ISO/IEC 27005, 2008).[1] Por outro lado, Oliveira (2006) classifica os riscos sendo uma oportunidade, uma incerteza ou uma ameaça. Essa classificação de Oliveira é considerada a mais preocupante, pois está associada às ocorrências de efeitos negativos como, por exemplo, perda de recursos financeiros, fraudes, roubos, comprometimento da imagem, infração legal, indisponibilidade de serviços, dentre outros (VASILE; STUPARU; DANIASA, 2010).

> O risco é compreendido como algo que cria oportunidades ou produz perdas. Com relação à segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas. É medido pela possibilidade de um evento vir a acontecer e produzir perdas (DANTAS, 2011, p.41).

De acordo com Moraes (2010), a gestão de risco envolve diversos processos como a identificação, o reconhecimento, a avaliação e gradação dos riscos. Esses processos são seguidos de aplicações de recursos econômicos que possuem o objetivo de realizar a implementação de controles capazes de minimizar, monitorar e controlar a probabilidade de ocorrer efeitos negativos dentro da organização. Dessa forma, é possível corrigir as não conformidades da empresa e implementar novas oportunidades de melhorias.

Gerenciar os riscos é um dos principais processos da gestão da segurança da informação, pois visa identificar, analisar, avaliar e controlar os riscos inerentes à segurança da informação. Gerenciar os riscos pode ser um processo complexo e oneroso, contribuindo para que as empresas não priorizem esse processo em projetos de segurança da informação (OLIVEIRA *et al.*, 2009).

[1] É importante ressaltar que os termos como vulnerabilidade, confidencialidade, integridade e disponibilidade, serão destrinchados em tópicos posteriores.

2.2.2 Processo de gestão do risco

Aumentar a capacidade de gerir o risco e aperfeiçoar o seu retorno faz parte dos integrantes de uma abordagem sistêmica, que proporciona um processo formal para a melhoria da capacidade de identificação e avaliação dos riscos. Bezerra (2013) afirma que essa abordagem deve estar de acordo com os objetivos da organização, atendendo assim às suas necessidades especificas conforme os requisitos de segurança da informação.

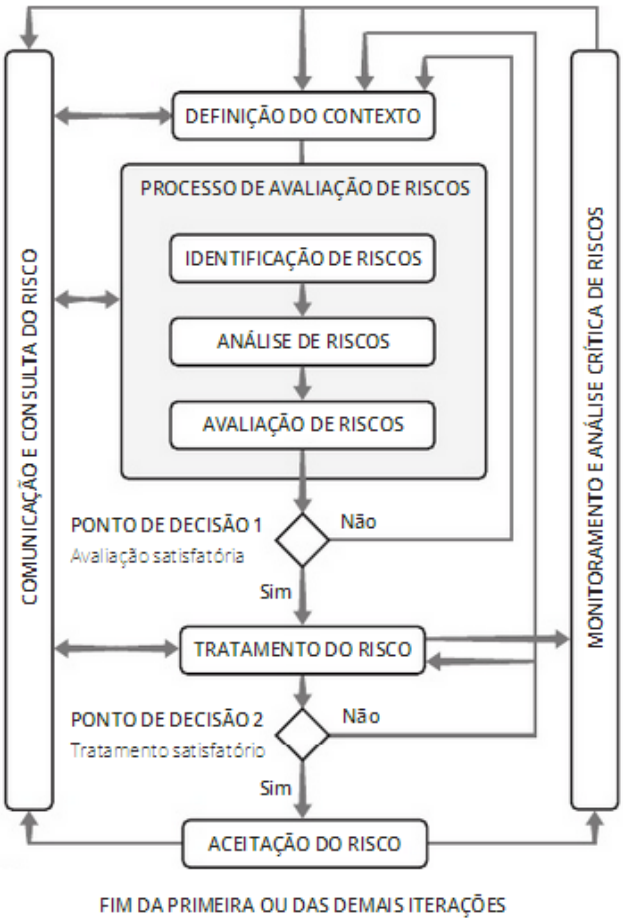
Ainda de acordo com Bezzera (2013, p.12) “[...] a gestão de riscos é composta de atividades formalizadas e coordenadas para controlar e dirigir um conjunto de instalações e pessoas com relações e responsabilidades entre si e com o ambiente externo”.

Konzen *et al.* (2012) afirma que existem diversas normas e metodologias que auxiliam o desenvolvimento de uma gestão de riscos, onde cada uma disponibiliza um conjunto de diretrizes distintas voltadas para o gerenciamento dos riscos. Dentre os modelos e referência encontrados para a gestão dos riscos que visam nortear as implementações necessárias está a ISO/IEC 27005 (2008). O processo descrito nesta norma estabelece um embasamento para a construção de metodologias para gestão de riscos informando o que a organização deve fazer, mas não detalha suficientemente como executar as atividades, dificultando a sua implementação por partes das organizações.

A ISO/IEC 27005 define o processo de gestão de risco como atividades coordenadas para dirigir e controlar o risco de uma organização (LUND; SOLHAUG; STOLEN, 2010).

Dessa forma, o processo de gestão de riscos é definido por oito atividades, como pode ser observado na Figura 2.

Figura 2 – Processo de gestão de riscos de segurança da informação



Fonte: ABNT NBR ISO/IEC 27005, 2008.

O ciclo de vida da gestão de riscos de segurança da informação é iterativo, conforme demonstra a Figura 2, onde a gestão se desenvolve de maneira incremental, através de uma sucessão de iterações, e cada iteração libera uma entrega para a seguinte, reduzindo o tempo e o esforço.

Para cada atividade da norma são propostas diretrizes para implementação, conforme descritas no Quadro 3 a seguir.

Quadro 3 – Principais grupos do processo de gestão de risco

Processo	**Descrição**
Definição do Contexto	Responsável pela definição do ambiente, escopo, critérios de avaliação, entre outras. Etapa essencial para equipe realizar a gestão de risco e conhecer todas as informações sobre a organização.
Análise/Avaliação de riscos	Permitirá a identificação dos riscos e a determinação das ações necessárias para reduzir o risco a um nível aceitável.
Tratamento do risco	A partir dos resultados obtidos na análise e avaliação do risco são definidos os controles necessários para o tratamento do risco, com base nos controles que deverão ser especificados de acordo com a norma da ABNT NBR ISO/IEC 27001.
Aceitação do risco	Assegura os riscos aceitos pela organização, ou seja, os riscos que por algum motivo não serão tratados ou serão tratados parcialmente.
Comunicação do Risco	É feita a comunicação do risco de forma como será tratado, para todas as áreas operacionais e seus gestores.
Monitoramento e analise critica	São as atividades de acompanhamento dos resultados, implementados dos controles e de análise crítica para a melhoria contínua do processo de gestão de riscos.

Fonte: Bezerra (2013) adaptado pelos autores.

No Quadro 3, descreve-se com mais detalhe cada atividade do processo de gestão do risco, indicada pela norma NBR ISO/IEC 27005.

A norma ISO/IEC 27005 não inclui uma metodologia específica para a gestão de riscos de segurança da informação, dessa forma, cabe a cada organização definir qual será a melhor abordagem de acordo com o contexto na qual está inserida.

2.2.3 Classificação da gestão do risco

Dantas (2011) entende que o risco pode ser classificado como oriundo de possíveis eventos da natureza ou decorrente de problemas técnicos, assim como também, resultar de uma ação intencional.

Diante disso, Dantas (2011) classifica os riscos em três categorias distintas, como: riscos naturais que são aqueles oriundos de fenômenos da natureza; os riscos involuntários que resultam das ações não intencionais, relacionados com vulnerabilidades humanas, físicas, hardware, de software entre outros; e os riscos intencionais que são aqueles derivados de ações deliberadas para causarem danos.

2.2.3.1 Riscos Naturais

De acordo com Sêmola (2003) os riscos classificados por naturais são decorrentes de fenômeno da natureza, como por exemplo, os incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição etc.

Landoll (2011) entende que a determinação de riscos de segurança da informação para a construção de uma organização inclui uma análise dos riscos naturais e humanos.

Segundo Dantas (2011) dependendo da ocorrência do evento pode ser difícil estabelecer uma proteção que seja eficaz, por outro lado, caso os eventos sejam comuns em uma determinada região, por exemplo, pode facilitar o processo de planejamento e estabelecimento de medidas para realizar a prevenção desses impactos assim como a sua concretização. Dantas (2011) destaca alguns fatores que devem ser considerados em relação aos riscos naturais:

- A instalação da empresa é passível de eventos da natureza que podem ser constantes e de proporções catastróficas;
- Carência de boletins meteorológicos;
- Estrutura da empresa com materiais de baixa qualidade ou resistência;

- Equipamentos de combate a catástrofes de má qualidade ou sem manutenção periódica;
- Falta de plano de contingência;
- Falta de preparo em ações inesperadas.

2.2.3.2 Riscos Involuntários

Dantas (2011) afirma que, a identificação da sua origem tem relação direta com as vulnerabilidades humanas, físicas, de hardware e de software. Sêmola (2003) concorda com a afirmação de Dantas (2011), porém acrescenta que os riscos involuntários quase sempre podem ser causados por desconhecimento, assim como também por acidentes, erros, falta de energia, dentre outros.

De acordo com Dantas (2011), alguns fatores devem ser considerados em relação aos riscos involuntários, tais como:

- Falha nos equipamentos para uso de detecção e prevenção;
- Não cumprimento das normas para controle de materiais inflamáveis;
- Estrutura da empresa com materiais de fácil combustão;
- Equipamentos ligados 24 horas;
- Carência de treinamento em medidas controvérsias;
- Inexistência de processos de qualidade;
- Inexistência de controles internos;
- Inexistência de programa de capacitação continuada;
- Cultura organizacional.

2.2.3.4 Riscos Intencionais

O risco intencional, ou seja, aquele concernente a uma ação proposital, podem ser motivados por vários fatores, como o tipo do negócio ou tipo do produto, que geram ações deliberadas a fim de provocar danos a algum ativo da organização, após detectar alguma brecha no sistema de proteção da empresa (DANTAS, 2011).

Dantas (2011) descreve alguns fatores que devem ser considerados em relação aos riscos intencionais, tais como:

- Situação do sistema de controle interno;
- Produtos atrativos no mercado;
- Instalação da empresa sujeita a eventos naturais de proporção catastróficas;
- Ocorrência de crimes na região em que a empresa está situada;
- Sensação de impunidade;
- Remuneração dos funcionários em espécie;
- Funcionários insatisfeitos;
- Mercado competitivo;
- Informações de nível estratégico.

2.2.4 A importância da segurança da informação

Os riscos, como citados, existem. Um bom motivo para segurança da informação ser de grande importância, é que os sistemas computacionais hoje em dia não são tão seguros. Um artigo publicado no site Tecmundo, por Amoroso (2009), comparando sistemas operacionais seguros, resulta em uma pesquisa que enfatiza que não há sistemas blindados e as brechas nos diversos sistemas operacionais vêm crescendo exponencialmente. Até nos sistemas e aplicativos para dispositivos móveis a segurança é muito falha e estão ficando cada vez menos seguros, como mostra a pesquisa publicada no site Ecopag (2013), onde desnudou o aumento na quantidade de *malwares* em 614%, nos últimos 12 meses anteriores a data de publicação do artigo.

> A segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infra-estruturas (sic) críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como o governo eletrônico (e-gov) ou o comércio eletrônico (e-business), e evitar ou reduzir os riscos relevantes. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída reduz a eficácia da implementação de um controle de acesso centralizado (NBR ISO/IEC 17799:2005, p. ix).

Nos sistemas distribuídos a segurança da informação é de grande importância, pois os recursos de informação que são mantidos e circulam pelos sistemas distribuídos

têm um excessivo valor real para os usuários que os usam (COULOURIS; DOLLIMORE; KINDBERG. 2007).

2.3 Segurança da Informação

Com embasamento da importância da segurança da informação, é significante para as organizações e todos os envolvidos de uma organização, que o conceito de segurança da informação seja desdobrado.

2.3.1 Conceito

De antemão, Calouris, Dollimore e Kindberg (2007, p. 30) informam que a segurança da informação possui três componentes: “confidencialidade (proteção contra exposição para pessoas não autorizadas), integridade (proteção contra alteração ou dano) e disponibilidade (proteção contra interferência com os meios de acesso aos recursos)”, como representado na Figura 3.

Figura 3 – Componentes básicos da segurança da informação.

Fonte: Claudiododt, 2011.

Com isso, a ABNT NBR ISO/IEC 17799:2005 (2005, p. 1) utiliza os componentes da segurança da informação para descrevê-la, e enfatiza que a segurança da informação é a “preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como

autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas". Ainda de forma mais simplista, a mesma norma cita que a segurança da informação é "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

Soares, Lemos e Colcher (1995) complementam que a segurança, além de estar relacionada ao caráter de preservação da informação contra a manipulação indevida de informações restritas por pessoas não autorizadas, está relacionada também com a necessidade de proteger os computadores e dispositivos periféricos. Este conceito certificado pelos autores reflete na realidade de que, por mais que tem-se toda uma preocupação com a preservação da informação, nada adianta se os meios pelos os quais as informações são armazenadas ou processadas, estiverem desprotegidos ou que dispõe de acesso livre.

Já Barrett e King (2010) não tratam a segurança da informação apenas como normas ou procedimentos a serem seguidos, os autores asseveram que a atitude mental do pessoal que lidar com a informação é o ponto chave para segurança. Segundo os autores, os funcionários de uma empresa precisam estar cientes das responsabilidades e atentarem para a segurança, pois o ser humano é o principal responsável pela preservação da informação.

Anteriormente foram citadas as características de uma informação valiosa. E com o fundamento de segurança da informação, para que a informação seja considerada valiosa, além das outras características que a compõe, ela particularmente deve ser segura. Não é fiável uma decisão ser tomada sobre informações duvidosas, informações danificadas ou informações modificadas por outrem não autorizados, porém, mesmo que os gestores utilizem informações não seguras como base para a tomada de decisões, o risco de cometerem erros é grande. Sendo assim, para que a informação seja considerada segura, deve-se basicamente preservar os componentes citados anteriormente: integridade, confidencialidade e disponibilidade. Destrinchados a seguir.

2.3.1.1 Integridade

A integridade segundo Peixoto (2006) citado por Alves (2012, p. 18) “é a garantia de que as informações não sofreram nenhuma modificação durante o trajeto entre a pessoa que enviou e a pessoa que recebeu a informação, garantindo assim a sua real veracidade após chegarem ao destino”. Ou seja, é quando a informação recuperada possui o mesmo valor da informação original.

Uma informação íntegra, é uma informação que não foi modificada, alterada ou destruída por alguém não autorizado e que seja legítima. Uma informação não íntegra é quando a informação foi corrompida, modificada, roubada ou destruída ou qualquer interferência no valor da informação original (DANTAS, 2011).

O que pode facilitar para a quebra da integridade são as modificações, bem como inserir, alterar ou excluir parte do conteúdo da informação; as alterações dos espaços físicos ou lógicos onde as informações estão armazenadas ou alterações nos meios físicos ou lógicos por onde a informação trafega; ou quando os sistemas que armazenam as informações são acessados irrestritamente e a partir disso as informações modificadas (DANTAS, 2011).

2.3.1.2 Confidencialidade

A confidencialidade segundo Peixoto (2006) citado por Alves (2012, p. 18) “é a garantia de que as informações transmitidas chegarão ao seu destino sem que se dissipem para outro lugar onde não deveriam passar [...]”. Ou seja, compartilhar a informação, mas de forma segura e protege-la de acesso irrestrito.

Quando pessoas sem permissões conseguem acesso às informações restritas, ocorre a quebra da confidencialidade. Quando a informação passa a ser conhecida por outrem, ocorre também a perda da confidencialidade. E garantir a confidencialidade é preservar o valor da informação com restrições e não permitir que o acesso indevido ocorra (DANTAS, 2011).

Casos que se encontram com facilidade também é, quando funcionários de uma determinada empresa conversam em público ou com pessoas que não integram à organização, assuntos do trabalho e passam despercebidamente informações que não podem ser divulgados, este é um caso comumente das informações vazadas com o envolvimento dos funcionários da própria empresa (MENDES, 2011).

2.3.1.3 Disponibilidade

A disponibilidade segundo Peixoto (2006) citado por Alves (2012), é manter a informação disponível. O autor ressalta um grande desafio que é manter a estrutura por onde a informação trafega, confiável e íntegra, e ao mesmo tempo, que a informação esteja sempre disponível.

A quebra da disponibilidade ocorre quando a informação não está acessível ou não disponível para ser usada pelos usuários autorizados em qualquer momento em que for preciso utilizar. Já garantir a disponibilidade é assegurar-se de que a informação estará pronta para ser utilizada em qualquer momento, e também quando durante no percurso ou no armazenamento não ocorrer nenhum erro (DANTAS, 2011).

2.3.2 Ameaças

Tanenbaum (2003) discute que o maior problema relacionado à segurança, é oriundo de pessoas muito inteligentes e dedicadas, porém mal intencionadas, maliciosas que tentam através do roubo, manipulação ou destruição da informação, obter algum benefício, causar prejuízos ou simplesmente chamar a atenção. Com essa abordagem, é introduzida uma preocupação para a segurança: as ameaças.

Ameaça segundo a ISO/IEC 13335-1:2004 citado pela NBR ISO/IEC 17799:2005 (2005, p.3) é a “causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização”. A NBR ISO/IEC 17799:2005 (2005, p. ix) cita algumas ameaças à segurança da informação, como: “fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, *hackers* e ataques de *denial of service*”.

Enquanto Tanenbaum (2003) enfatiza que as ameaças resultam do fator humano, ataque de *crackers*[2], por exemplo, que expõe riscos à segurança da informação, a NBR ISO/IEC 17799:2005 destaca que ameaças podem originar, além do fator humano, também de incidentes como catástrofes, o que tem parecenças com o que Dantas (2011) cita, em que as ameaças podem ser naturais, a partir de eventos da natureza, como fenômenos de terremotos, inundações, furacões e etc.

Os autores Soares, Lemos e Colcher (1995), complementam e caracterizam as ameaças como acidentais e não acidentais. Ameaças acidentais, segundo os autores, são as ameaças que não foram feitas com intenção ou propósito, como falhas no *hardware* ou descuidos, adverso das não acidentais, que estão associados às intenções premeditadas e variam de interceptação e monitoração das informações aos ataques sofismados.

Já Barrett e King (2010, p. 295) são mais genéricos quando citam que “uma ameaça é qualquer coisa que coloque em perigo a segurança da rede”. Elas variam de formas e tamanhos. E os autores asseveram que as possibilidades de ameaças precisam ser analisadas a partir da configuração do servidor, pois a grande parte dos servidores possuem diversidades de serviços e protocolos ativos por padrão, assim sendo, brechas que permitem as ameaças podem ser evidentes.

Quadro 4 – Consequências de ameaça

Ameaça	**Descrição**
Revelação não autorizada	Circunstância ou evento pelo qual uma entidade obtém acesso a dados que não está autorizada a acessar.
Fraude	Circunstância ou evento que pode resultar no recebimento, por uma entidade autorizada, de dados falsos na crença de que sejam verdadeiros.
Disrupção	Circunstância ou evento que interrompe ou impede a operação correta de serviços e funções de sistemas.
Usurpação	Circunstância ou evento que resulta no controle de serviços ou funções do sistema por entidade não autorizada.

Fonte: Stallings e Brown (2014), adaptado pelos autores.

[2] Segundo Tanenbaum (2003), são invasores que promovem ataques e ações de má fé contra qualquer entidade ou sistema de seu interesse, a fim de causar transtornos, prejuízos ou roubar dados.

O Quadro 4 desnuda quatro tipos de consequências de ameaças comuns, especificados pelos autores Stallings e Brown (2014) que violam os pilares da segurança da informação, assim como a quebra de confidencialidade, integridade e disponibilidade.

2.3.3 Vulnerabilidades

A NBR ISO/IEC 17799:2005 (2005, p. 3) conceitua a vulnerabilidade como uma “fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças”.

Os autores Soares, Lemos e Colcher (1995) usam o termo segurança como uma medida para minimizar as vulnerabilidades de qualquer coisa de valor e recursos. Dessa forma, os autores citam que a vulnerabilidade é qualquer debilidade que será explorada a fim de acessar sistemas ou informações ilegalmente.

Sêmola (apud DANTAS, 2011) associa a vulnerabilidade às fragilidades dos ativos de informação, que se forem exploradas, permitem que as ameaças ocorram.

Campos (2007) citado por Mendes (2011) enfatiza que as vulnerabilidades estão relacionadas na maioria das vezes com os ativos da informação e tampouco aos fatores externos. Dessa forma é válido alvitrar que a informação é o ativo de grande mérito para a organização e para a continuidade dos negócios, somada a sensibilidade que ela sofre com as vulnerabilidades inerentes, reflete a necessidade de haver uma preocupação com a segurança das informações. Todavia, Dantas (2011) enfatiza que as vulnerabilidades ocorrem como consequência de várias maneiras, inclusive por fatores externos, e as classificam como:

- Naturais: está relacionado com o meio ambiente, que podem de alguma maneira levar riscos às informações, como por exemplo, uma mata pegar fogo ou um barranco desmoronar sobre a organização;
- Organizacional: está relacionado às políticas, planos e procedimentos da organização, como por exemplo, a falta de controle de acesso às

determinadas áreas da empresa ou à falta de políticas que assegura as informações de pessoas não autorizadas;

- Física: está relacionada às instalações físicas a qual compõe o ambiente de processamento ou armazenamento das informações, como por exemplo, instalações impróprias ou sistema de combate a incêndio;
- *Hardware*: está relacionada aos equipamentos que por alguma falha de fabricação ou falha de configuração podem pôr em riscos as informações;
- *Software*: está relacionado às falhas e brechas nos sistemas que podem facilitar o acesso irrestrito e à modificação das informações. Outro ponto que pode também tornar vulnerável os sistemas, é o mau uso ou uso inadequado;
- Meios de armazenamento: meios pelos quais as informações são gravadas, como discos, CD ROM e etc. E que podem ser vulneráveis, se esses meios forem usados inadequadamente ou estarem expostos em área que podem danificá-los, e assim perder ou danificar informações;
- Humanas: está relacionado ao pessoal de toda organização, que pela falta de consciência, de conhecimento, de responsabilidade, de preocupações, ou por atos errôneos, podem colocar em risco a segurança da informação ou a própria informação;
- Comunicação: está relacionado às vias pelas quais as informações trafegam, toda a sua infraestrutura, e que se mal preservadas ou mal preparadas ou mal protegidas, podem também colocar em risco as informações no momento em que trafegam e até mesmo impedir a disponibilidade da informação.

2.3.4 Políticas de Segurança da Informação

“A primeira etapa para planejar serviços e mecanismos de segurança é desenvolver uma política de segurança” (STALLINGS; BROWN, 2014, p. 27).

Segundo a NBR ISO/IEC 17799:2005 (2005, p. ix) “a segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas [...]”. Estabelecer uma boa política de segurança pode garantir a preservação dos pilares da segurança ou ao menos dificultar as ameaças de agirem, que ainda é definido pela NBR ISO/IEC 17799:2005 (2005, p. 2) como “intenções e

diretrizes globais formalmente expressadas pela direção". A mesma norma cita ainda que as políticas são usadas como uma forma de controle de gerenciamento dos riscos à segurança.

Stallings e Brown (2014) definem políticas de segurança como regras e práticas que norteiam como a organização deve usar medidas de segurança para proteger os seus ativos críticos.

Soares, Lemos e Colcher (1995, p. 450), em uma definição próxima, citam que "uma política de segurança é um conjunto de leis, regras e práticas que regulam como uma organização gerencia, protege e distribui suas informações e recursos". Para completar, segundo Barrett e King (2010, p. 296) "[...] políticas que não possuem suporte da gerência podem ser impraticáveis, e aquelas que os usuários não têm conhecimento são ineficazes".

Acima, pode ser notado brevemente a necessidade de uma gerência no suporte às políticas de segurança da informação. Para reforçar, Imoniana (2010) aduz que, para que os objetivos sejam vencidos é indispensável estabelecer de modo claro as políticas, e que são necessários os gerentes traduzi-las e detalha-las em linguagem operacional, evitando a dupla interpretação.

As políticas como leis, regras e práticas, agem sobre as informações que uma entidade possui, limitando-as em seu uso e restringindo acesso e manipulação da mesma a determinadas pessoas, e ainda funciona como um manual de como as pessoas envolvidas devem trabalhar de forma que garanta a segurança da informação. Para isso, é de extrema importância que os usuários estejam cientes do uso da política de segurança e como trabalharem com ela, pois, já fora citado que o fator humano é uma grande ameaça à segurança da informação, logo, se os usuários não estiverem por dentro das políticas, se não forem treinados ou se não forem capazes de seguir as normas à risca, podem acidentalmente contribuir para com as ameaças (BARRETT; KING, 2010).

De acordo com Stallings e Brown (2014), os seguintes fatores devem ser ponderados ao desenvolver uma política de segurança:

- O valor dos ativos que estão sendo protegidos;
- As vulnerabilidades do sistema;
- Ameaças potenciais e probabilidade de ataques.

Fontes (2012) assevera que as políticas devem ser formalizadas e devem ter regras explícitas que atendam todas as áreas da organização e que seja definida para todos os envolvidos da organização. Sendo que, se houver a necessidade de estabelecer regras diferentes para determinados usuários, isto deve ser explícito e formalizado nos regulamentos da política.

Um ponto importante a ser observado, levantado pelos autores Barret e King (2010), é de que ao estabelecer políticas e trabalha-las de forma correta em uma organização, seguindo seus conceitos e práticas, a segurança pode ser garantida de forma eminente. Todavia, estabelecer políticas para algumas empresas sairia muito caro, pois é um investimento sem nenhum retorno financeiro (receitas), sendo assim, algumas organizações adotam a medida de esperar alguma situação acontecer e posteriormente tomar a iniciativa de solucionar o problema, mas isso é uma medida muito arriscada e os prejuízos são iminentes.

2.3.5 Backup

Mesmo com todo aparato de segurança, mesmo com grandes investimentos, é inevitável assegurar as informações totalmente e priva-las de qualquer desastre. E mesmo que ocorra algum desastre ou alguma ameaça venha destruir a informação, é possível que através do *backup* essa informação seja recuperada. Dessa maneira, o *backup,* dentre vários métodos de segurança, é o mais básico e indispensável. Fialho (2007) assevera que esta é a melhor forma de proteger os dados de um sistema.

Backup nada mais é do que uma cópia de segurança das informações importantes da organização. Através da cópia de segurança é possível garantir a integridade e disponibilidade das informações, recuperando-as após alguma ocorrência que as tenha danificado ou afetado a disponibilidade das mesmas (MENDES, 2011, NBR ISO/IEC 17799:2005).

São pontos consideráveis, referentes ao item 10.5.1 da norma NBR ISO/IEC 17799:2005, no que diz respeito as diretrizes para geração das cópias de segurança: as cópias de segurança da informação devem ser mantidas em locais seguros, preferivelmente em locais distantes o suficiente para que não sejam atingidos em casos de desastres; e que estas cópias sejam testadas regularmente para garantir a confiabilidade no caso de emergência.

A NBR ISO/IEC 17799:2005 aduz que as cópias de segurança das informações sejam regularmente efetuadas. Fialho (2007, p. 7) corrobora com a norma e diz que "a freqüência (sic) dos *backups*, ou seja, o número de vezes que você fará as cópias, depende diretamente da relevância que os dados possuem [...], assim como da quantidade de informações processadas [...]" O autor ainda destaca que a frequência dos *backups* depende da importância que a organização dá a segurança da informação, e levanta a atenção de que não se pode confiar na sorte, ou seja, não é fiável acreditar que nada vai acontecer e então deixar de fazer o *backup.*

> É preciso estabelecer uma periodicidade para fazer backup de todas as máquinas [...], preferencialmente em fitas DAT (armazenam de 4 GB a 12 GB), ou qualquer outro tipo de fita que se adéqüe (sic) a sua necessidade (fitas podem comportar muito mais de 12 GB). As mídias de backup devem ser renovadas constantemente, isto é, não se deve regravar sobre uma mesma fita por muitas vezes seguidas. As fitas já gravadas devem ser guardadas em local seguro, normalmente um cofre à prova de incêndio. As fitas jogadas no lixo deverão ser destruídas (TORRES, 2001, p. 413).

Além dos *backups* em fitas, como citado pelo autor acima, há outros meios em que algumas ocasiões, dependendo da velocidade da conexão com a Internet e da quantidade de dados, pode ser uma alternativa mais viável, que são serviços de *backups online*, que permitem armazenar os dados em servidores remotos ou servidores nas nuvens, como é mais conhecido popularmente (NADEL, 2012).

O que deve ser claro a respeito dos *backups* nas nuvens é que, como os *backups* são feitos por acessos via Internet e para que seja possível armazenar e recuperar os dados de forma eficiente, é necessária uma conexão também eficiente com a Internet. Entretanto, algumas vantagens são evidentes, como: não há perigo dos servidores remotos serem danificados e os dados perdidos, as empresas que prestam este tipo de serviço possuem diversos servidores que distribuem entre outros as cópias das informações; como o serviço de *backup* é *online*, é possível

portabilidade para acessar os dados em qualquer local, que tenha conexão com a Internet (VELLIS, 2013).

Lembrando que fazer apenas um *backup* não é confiável.

2.3.6 Norma NBR ISO/IEC 17799:2005

É significante qualificar o conceito de norma para uma melhor compreensão dos seus objetivos. Dessa forma, a Associação Brasileira de Normas Técnicas (ABNT) caracteriza a norma como um documento que fornece orientações para realização de atividades ou para seus resultados. A norma assegura a conformidade de um processo, por exemplo, através de regras e objetos de controle.

A ABNT ainda aponta os objetivos da norma. Que são:

- Comunicação: visa pôr seguro a confiabilidade nas relações comerciais, através de meios adequados para a troca de informações;
- Simplificação: visa tornar simples o relacionamento entre consumidor e fornecedor, através da redução de variedades de procedimentos e produtos;
- Proteção ao consumidor: visa requisitos para a percepção da qualidade de serviços e produtos;
- Segurança: visa meios para a proteção da saúde humana e do meio ambiente;
- Economia: visa a racionalização dos processos de produção ou atividades produtivas de modo que reduza o custo de produtos e serviços;
- Eliminação de barreiras: visa facilitar o intermédio comercial com cortes de regulamentos conflitantes.

Para completar,

> a Associação Brasileira de Normas Técnicas (ABNT) é o Fórum Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais Temporárias (ABNT/CEET), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros) (ABNT NBR ISO/IEC 17799:2005, p. vii)

Um documento de segurança da informação foi publicado na Inglaterra em 1989, por um grupo do Departamento de Indústria e Comércio, com o objetivo de atribuir valor à segurança da informação, promover a certificação, e estabelecer códigos de boas práticas que deveriam ser usados para prover a segurança da informação (CAMPOS, 2006).

Com a cooperação da indústria inglesa e a evolução do trabalho, impulsionaram em 1995, a publicação da norma de segurança da informação *British Standard* BS7799:1995, e uma posterior publicação em 1998. No ano de 2000, após sugestões e revisões, a norma BS779 ganhou destaque internacional, após ser homologada pela *International Organization for Standardization* (ISO) e efetivado a publicação da norma na forma da ISO/IEC 17799:2000 (INFORMABR, acesso em 19 de jul. 2014, CAMPOS, 2006).

Segundo o site da segurança da informação, a Informabr (acesso em 19 jul. 2014), relata que “[...] em setembro de 2001, a ABNT homologou a versão brasileira da norma, denominada NBR ISO/IEC 17799”.

“A ABNT NBR ISO/IEC 17799 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Segurança Física em Instalações de Informática (CE-21:204.01) [...]” (NBR ISO/IEC 17799:2005, p. vii).

Para completar, Ferreira e Araújo (2006), esclarecem que foi publicada no ano de 2005, uma nova versão da norma NBR ISO/IEC 17799, na qual, foram incluídos capítulos referentes ao gerenciamento de riscos e também sobre a gestão de incidentes de segurança.

A *insight* Sinfic (2006) caracteriza a norma ISO/IEC 17799:2005 como um instrumento de práticas de gestão da segurança da informação, cujo os objetivos são determinar uma referência para as organizações praticarem a gestão da segurança da informação e desenvolver, entre as organizações a confiança nas transações comerciais. A *insight* Sinfic (2006) ainda aponta os onze tópicos contidos na documentação da referida norma:

1) Política de segurança: enfatiza os principais assuntos que devem ser abordados em uma política de segurança;
2) Segurança organizacional: enfatiza o emprego de responsabilidades, incluindo terceiros e fornecedores de serviços e toda uma estrutura de gestão da segurança da informação;
3) Classificação e controle de ativos de informação: visa o gerenciamento, a organização e controle dos ativos da organização;
4) Segurança relacionada com as pessoas: tem enfoque nos riscos oriundos das pessoas, que provocam atos intencionais ou acidentais à segurança da informação. Também incluem responsabilidades, descrição de cargos, medidas para contratação e formação, visando sempre a segurança da informação;
5) Segurança ambiental e física: está relacionado com as necessidades de estabelecer áreas de circulação restrita, bem como a proteção dos equipamentos e toda a infraestrutura da tecnologia da informação;
6) Gestão das operações e comunicações: segundo autor, este tópico aborda as principais áreas, na qual devem ter especial atenção da segurança. Está relacionado com os procedimentos operacionais e responsabilidades, bem como a homologação e implantação de sistemas, gestão de redes, controle e prevenção de vírus, controle de mudanças, controle de documentação, execução e armazenamento de backups, segurança de correio electrónico, entre outras;
7) Controle de acesso: visa o controle de acesso aos sistemas, monitoração de acesso e uso, entre outros;
8) Desenvolvimento e manutenção de sistemas: aqui são tratados os requisitos de segurança dos sistemas: uso e controle de criptografia; segurança de desenvolvimento; controle de arquivos e outros;
9) Gestão de incidentes de segurança: dispõe de dois itens: notificação de instabilidade e acontecimentos de segurança da informação; e gestão dos incidentes da segurança da informação e melhorias;
10) Gestão da continuidade do negócio: visa o estabelecimento de um plano de contingência, testado e atualizado;
11) Conformidade: visa o exame das propriedades intelectuais e a proteção das informações dos clientes.

2.4 Requisitos da Política de Segurança da Informação e Segurança da Informação Estabelecidos Pela Norma NBR ISO/IEC 17799:2005

Anteriormente foi descrito pormenorizadamente sobre as políticas de segurança, mas é válido alvitrar que uma política de segurança deve ser formalizada, atender a todos e a todas as áreas de uma organização. Como descrito no item 5.1 da norma NBR ISO/IEC 17799:2005, o objetivo da política da segurança é “promover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes”.

A política de segurança da informação é necessária para que a construção da proteção da segurança da informação seja efetivada. Ela norteará nas diretrizes e limites que a organização precisará para implantar a segurança das informações (FONTES, 2012).

A norma NBR ISO/IEC 17799:2005 (2005, p. 8) ainda sugere que a política de segurança da informação seja uma “política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação [...]”.

No item 5.1.1, a NBR ISO/IEC 17799:2005 orienta para que a direção aprove o documento da política de segurança da informação e que este documento seja de conhecimento de todos da organização, inclusive partes externas. Observa-se que o papel da direção é de grande significância para agregar valores à política de segurança, quiçá enraizar docência a todos os envolvidos, levando a fundar o comprometimento com a segurança da informação.

A direção exerce o seu compromisso com a segurança da informação através da política da segurança da informação, além de influenciar no comportamento de todos os usuários no que diz respeito a identificação e tratamento dos riscos. (BEAL, 2005).

Para Fontes (2012) é fundamental que a direção participe da segurança da informação para haver uma proteção das informações estável, e justifica que a

direção tem que dar exemplo utilizando uma parte do seu tempo com o compromisso com a segurança da informação.

Nas diretrizes para implementação, a NBR ISO/IEC 17799:2005 (2005, p. 8) aponta as declarações que devem conter no documento da política:

> a) uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação;
>
> b) uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhada com os objetivos e estratégias do negócio;
>
> c) uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco;
>
> d) breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo:
>
> 1) conformidade com a legislação e com requisitos regulamentares e contratuais;
>
> 2) requisitos de conscientização, treinamento e educação em segurança da informação;
>
> 3) gestão da continuidade do negócio;
>
> 4) conseqüências (sic) das violações na política de segurança da informação;
>
> e) definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança da informação;
>
> f) referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que os usuários devem seguir.

Referente ao comprometimento com a segurança da informação, a direção deve apoiar efetivamente a segurança da informação dentro da organização, deve definir atribuições e tornar conhecimento de suas responsabilidades, conforme descrito no item 6.1.1 da norma NBR ISO/IEC 17799:2005 (2005, p. 10). Em paralelo a isto, a norma cita algumas diretrizes para a direção, na qual, convém que:

> a) assegure que as metas de segurança da informação estão identificadas, atendem aos requisitos da organização e estão integradas nos processos relevantes;
>
> b) formule, analise criticamente e aprove a política de segurança da informação;

> c) analise criticamente a eficácia da implementação da política de segurança da informação;
>
> d) forneça um claro direcionamento e apoio para as iniciativas de segurança da informação;
>
> e) forneça os recursos necessários para a segurança da informação;
>
> f) aprove as atribuições de tarefas e responsabilidades específicas para a segurança da informação por toda a organização;
>
> g) inicie planos e programas para manter a conscientização da segurança da informação;
>
> h) assegure que a implementação dos controles de segurança da informação tem uma coordenação e permeia a organização.

A última diretriz da direção citada pela norma faz alusão ao item 6.1.2 da NBR ISO/IEC 17799:2005 (2005, p. 11), na qual é destacado o papel de representantes para coordenação das atividades de segurança das informações, sendo estes com exercícios de atribuições importantes dentro das organizações. Também para a coordenação da segurança da informação, há diretrizes que convém que esta atividade:

> a) garanta que as atividades de segurança da informação são executadas em conformidade com a política de segurança da informação;
>
> b) identifique como conduzir as não-conformidades;
>
> c) aprove as metodologias e processos para a segurança da informação, tais como análise/avaliação de riscos e classificação da informação;
>
> d) identifique as ameaças significativas e a exposição da informação e dos recursos de processamento da informação às ameaças;
>
> e) avalie a adequação e coordene a implementação de controles de segurança da informação;
>
> f) promova, de forma eficaz, a educação, o treinamento e a conscientização pela segurança da informação por toda a organização;
>
> g) avalie as informações recebidas do monitoramento e da análise crítica dos incidentes de segurança da informação, e recomende ações apropriadas como resposta para os incidentes de segurança da informação identificados.

As responsabilidades pela segurança da informação devem ser claras, definidas, e especificadas no documento da política de segurança da informação. As responsabilidades devem ser explanadas para que assegure o cumprimento dos processos da segurança da informação. As responsabilidades podem ser delegadas a outros envolvidos, mas sem perda da obrigação pelas ações de segurança da informação. Por fim, cada local da organização deve possuir os responsáveis para o

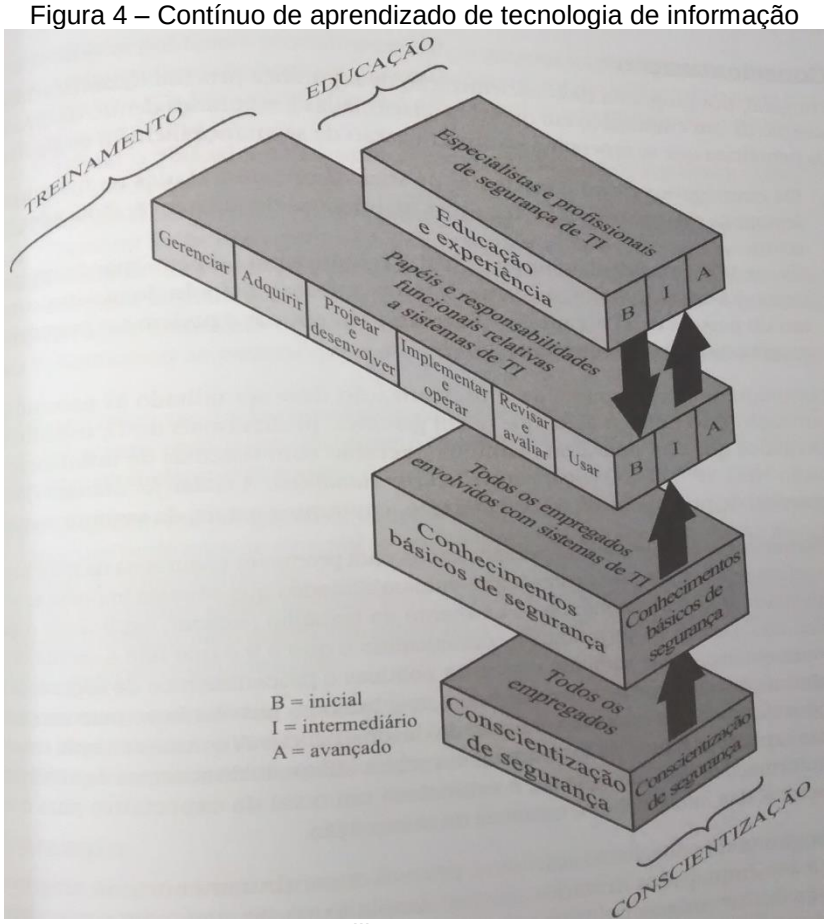
zelo dos ativos e cumprimento dos processos da organização, sendo claramente definidas (NBR ISO/IEC 17799:2005).

2.4.1 Requisitos para educação em segurança da informação e de conformidade com normas e regulamentos

Para os autores Stallings e Brown (2014), a aprendizagem da segurança da informação deve ser alcançada por programas contínuo de aprendizado, onde deve ser iniciado através de conscientização, treinamento e educação, seguindo uma linha temporal, como mostrado na Figura 4. Alguns benefícios desses programas são citados pelos autores:

- Estado melhor no comportamento dos colaboradores;
- Maior capacidade de responsabilizar os colaboradores pelos seus atos;
- Debilitar as responsabilidades da organização no ato civil e criminal, em relação ao comportamento do colaborador;
- Cumprimento das regras e obrigações formalizadas no contrato.

Figura 4 – Contínuo de aprendizado de tecnologia de informação



Fonte: Stallings e Brown, 2014.

Esses programas podem diminuir fraudes, falhas intencionais ou não, pois fica evidente as responsabilidades de cada funcionário e penalidades pertinentes (STALLINGS; BROWN, 2014).

“Do ponto de vista da segurança, contratar apresenta desafios significativos à gerência” (STALLINGS; BROWN, 2014, p. 507).

Para reforçar a ideia dos autores acima, antes da contratação, os candidatos ao emprego devem ser analisados especialmente ao se tratar de atribuições a cargos que envolvam informações sensíveis, e as suas responsabilidades devem ser definidas e atribuídas de acordo com as condições de contratação e cargos. Uma vez atribuída as responsabilidades, os funcionários e terceiros devem assinar acordos e contratos sobre suas obrigações confiadas (NBR ISO/IEC 17799:2005).

É importante que nos contratos de emprego, tenha-se uma cláusula declarando a confidencialidade dos ativos de informação da organização e que é de responsabilidade do empregado zelar por isto (STALLINGS; BROWN, 2014).

Durante a contratação, “um nível adequado de conscientização, educação e treinamento nos procedimentos de segurança da informação [...] seja fornecido para todos os funcionários, fornecedores e terceiros, para minimizar possíveis riscos de segurança da informação” (NBR ISO/IEC 17799:2005, p. 28). Aos envolvidos, é importante a participação nas práticas de segurança da informação em conformidade com as políticas e aos processos da organização.

“Os principais problemas associados ao comportamento de empregados são erros e omissões, fraude e ações executadas por empregados insatisfeitos. Programas [...] de educação de segurança podem reduzir o problema de erros e omissões” (STALLINGS; BROWN, 2014, p. 502).

> Convém que o treinamento em conscientização comece com um processo formal de indução concebido para introduzir as políticas e expectativas de segurança da informação da organização, antes que seja dado o acesso às informações ou serviços.
>
> Convém que os treinamentos em curso incluam requisitos de segurança da informação, responsabilidades legais e controles do negócio, bem como o treinamento do uso correto dos recursos de processamento da informação [...].
>
> Convém que a conscientização, educação e treinamento nas atividades de segurança da informação sejam adequados e relevantes para os papéis, responsabilidades e habilidades da pessoa, e que incluam informações sobre conhecimento de ameaças, quem deve ser contatado para orientações sobre segurança da informação e os canais adequados para relatar os incidentes de segurança da informação.
>
> O treinamento para aumentar a conscientização visa permitir que as pessoas reconheçam os problemas e incidentes de segurança da informação, e respondam de acordo com as necessidades do seu trabalho. (NBR ISO/IEC 17799:2005, p. 29)

Para o bem estar da segurança da informação entre o recurso humano e a organização, é importante atentar para os requisitos ao se tratar de encerramento ou mudança de contratação. É preciso que estabeleça controles para que a saída dos funcionários seja de forma ordenada, dessa forma, garantir a devolução dos equipamentos, ativos e a anulação dos direitos de acesso. Ao se tratar de mudanças

de contratação, a responsabilidade anterior deve ser desapropriada e uma nova responsabilidade deve ser controlada (NBR ISO/IEC 17799:2005).

Todos devem ser envolvidos na segurança da informação, inclusive, a parte externa (clientes ou fornecedores), como cita o item 6.2 da NBR ISO/IEC 17799:2005 em que não se deve abrandar com segurança da informação quanto a introdução de produtos ou serviços originados da parte externa, deste modo, os acessos aos ativos por partes externas devem ser controlados e os riscos identificados.

2.4.2 Requisitos disciplinares

“Convém que exista um processo disciplinar formal para os funcionários que tenham cometido uma violação da segurança da informação” (NBR ISO/IEC 17799:2005, p. 29).

Durante as contratações, como abordado, os cuidados devem ser reparados para que as responsabilidades sejam definidas, atribuídas e controladas. Como parte das obrigações, os funcionários, assim como os terceiros, precisam entrar em comum acordo com suas obrigações e condições relativas à segurança da informação e assinem termos. É necessário que estes termos estejam em conformidade com a política de segurança da informação e que fiquem claro as “ações a serem tomadas no caso de o funcionário [...] desrespeitar os requisitos de segurança da informação da organização” (NBR ISO/IEC 17799:2005, p. 27).

De forma alguma, o processo disciplinar deve ser aplicado sem antes uma averiguação das ações de violação da segurança da informação. Neste caso, evidências devem ser levantadas, armazenadas e apresentadas em concorde com as políticas e normas, como descrito no item 13.2.3 da NBR ISO/IEC 17799:2005.

> Convém que o processo disciplinar formal assegure um tratamento justo e correto aos funcionários que são suspeitos de cometer violações de segurança da informação. O processo disciplinar formal deve dar uma resposta de forma gradual, que leve em consideração fatores como a natureza e a gravidade da violação e o seu impacto no negócio, se este é ou não o primeiro delito, se o infrator foi ou não adequadamente treinado, as legislações relevantes, os contratos do negócio e outros fatores conforme requerido. Em casos sérios de má conduta, convém que o processo permita, por um certo período, a remoção das responsabilidades, dos

> direitos de acesso e privilégios e, dependendo da situação, solicitar à pessoa, a saída imediata das dependências da organização, escoltando-a (NBR ISO/IEC 17799:2005, p. 29).

É uma boa prática também, usar o processo disciplinar como referência para dissuadir os envolvidos da organização para evitar que os mesmos violem a segurança da informação (NBR ISO/IEC 17799:2005).

2.4.3 Requisitos de continuidade de negócio

Os aspectos da gestão da continuidade do negócio com relação à segurança da informação são importantes para não obstar a interrupção das atividades e processos de negócio críticos contra eventualidades inesperadas e danosas, e se for o caso, garantir o retorno das atividades em tempo hábil e sem maiores perdas (NBR ISO/IEC 17799:2005).

Continuidade do negócio é conhecida e citada por Imoniana (2010) como plano de contingência ou plano de recuperação, na qual, reuni meios para a organização de continuar o processamento das suas transações financeiras e econômicas, posterior às falhas ou desastres.

Esta gestão de continuidade do negócio, deve ser colocada em prática para minimizar o impacto sobre a organização e recuperar as perdas em um nível aceitável dentro de uma requerida escala de tempo, com uso de ações de prevenção e recuperação. Os processos críticos devem ser identificados pela gestão de continuidade do negócio e devem ser formalizados e integrados no plano de continuidade. E após um possível acontecimento de falha ou desastre que afete a segurança da informação, é necessária uma análise de impacto nos negócios na organização (NBR ISO/IEC 17799:2005).

Mas, a continuidade de negócio é muito mais que recuperação das atividades. Como assevera Imoniana (2010, p. 167), a continuidade de negócio “contempla também as preocupações concernentes à vida dos funcionários, impactos sobre meio ambiente, imagens junto aos clientes e fornecedores e o público em geral”.

Anteriormente foi apresentado a gestão dos riscos. Para uma gestão de continuidade do negócio, é necessário que a organização entenda e esteja ciente dos riscos à ela exposta e das suas probabilidades de acontecimentos, além disso, deve-se também entender qual poderá ser o impacto que os incidentes poderão causar sobre os negócios. Estas são orientações para análise e avaliação dos riscos correspondentes aos itens 14.1.1 e 14.1.2 da NBR ISO/IEC 17799:2005. A norma ainda faz uma chamativa para que análises e avaliações dos riscos sejam feitas com total envolvimento dos responsáveis pelos negócios da organização e forte apoio da direção na participação para validação de planos estratégicos para assegurar a continuidade dos negócios.

Ao implementar um plano de continuidade, é necessário de imediato definir os responsáveis. Em um ambiente complexo, a diretoria deve ser responsável, porém, com apoio técnico, uma vez que a direção possui medidas de fim estratégico. Em um ambiente regular, o gerente de TI deverá ser o responsável. Em um ambiente diminuto, os analistas de sistemas devem ser responsabilizados (IMONIANA, 2010).

Os responsáveis, no momento do desastre, não são profissionais que possuem funções operacionais dentro do ambiente de tecnologia da informação. É recomendado que estes responsáveis sejam definidos, formalizados e divulgados para a equipe de contingência (IMONIANA, 2010).

A norma NBR ISO/IEC 17799:2005 (2005, p. 104), no seu item 14.1.3 aponta os elementos que deve considerar o processo de planejamento da continuidade de negócio:

> a) identificação e concordância de todas as responsabilidades e procedimentos da continuidade do negócio;
>
> b) identificação da perda aceitável de informações e serviços;
>
> c) implementação dos procedimentos que permitam a recuperação e restauração das operações do negócio e da disponibilidade da informação nos prazos necessários; atenção especial precisa ser dada à avaliação de dependências externas ao negócio e de contratos existentes;
>
> d) procedimentos operacionais que permitam a conclusão de restauração e recuperação que estejam pendentes;

e) documentação dos processos e procedimentos acordados;

f) educação adequada de pessoas nos procedimentos e processos definidos, incluindo o gerenciamento de crise;

g) teste e atualização dos planos.

Para certificar de que todos os planos são consistentes, para considerar os requisitos de segurança e para apontar preferencias de testes e manutenção, é necessária uma estrutura dos planos de continuidade do negócio, uma lista de procedimentos a serem seguidos. E também como requisito, os planos devem ser testados, monitorados e atualizados regulamente, assim necessário para garantir a sua diligência para operar. (NBR ISO/IEC 17799:2005, IMONIANA, 2010).

2.4.4 Requisitos de avaliação da política de segurança da informação

“Convém que a política de segurança da informação seja analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia” (NBR ISO/IEC 17799:2005, p. 9).

A norma ainda aponta para a necessidade de um gestor para análise crítica e avaliação da política, nesse embasamento, deve-se extrair oportunidades para melhoria da política de segurança da informação da organização e garantir mudanças de adequação ao ambiente organizacional e aos negócios (NBR ISO/IEC 17799:2005).

Além de um gestor responsável pela análise, é importante a participação da direção também na análise crítica. A análise crítica da informação deve seguir considerações e procedimentos referentes a uma posterior análise crítica da direção, incluindo um período para os acontecimentos da análise (NBR ISO/IEC 17799:2005).

3 MÉTODO DE PESQUISA

De forma mais simples, pesquisar “[...] significa procurar respostas para indagações propostas” (MORESI, 2003, p. 8).

“A pesquisa é a atividade nuclear da Ciência. Ela possibilita uma aproximação e um entendimento da realidade a investigar. [...] Processa-se por meio de aproximações sucessivas da realidade, fornecendo-nos subsídios para uma intervenção no real” (GERHARDT; SILVEIRA, 2009, p. 31).

O delineamento da pesquisa foi através da pesquisa descritiva, que tem por objetivo, segundo Duarte (acesso em 27 jul. 2014) “[...] descrever as características de uma população, de um fenômeno ou de uma experiência. Esse tipo de pesquisa estabelece relação entre as variáveis no objeto de estudo analisado”. Ainda segundo a autora, as variáveis podem se alterar por meio do processo de pesquisa.

Duarte (acesso em 27 jul. 2014) afirma que a pesquisa descritiva tem similaridades com a pesquisa exploratória, destacando a diferença, na qual, o assunto na pesquisa descritiva é conhecido e a contribuição nada mais é do que adaptar novas visões sobre a realidade.

O método de pesquisa foi através da abordagem quantitativa. A razão por esta pesquisa não é entender os “porquês”, o objetivo é para questões diretas e facilmente quantificáveis (MORESI, 2003). Com embasamento nessa objeção, Fonseca (2002, apud GERHARDT; SILVEIRA, 2009) aduz que ela se centra na objetividade, e como o nome sugere, os resultados da pesquisa são quantificados.

Para Moresi (2003), o objetivo de uma pesquisa quantitativa é obter, dentro de uma determinada população, a quantidade de pessoas que compartilham uma ou mais características. E ainda segundo o autor, os resultados permitem gerar uma análise estatística.

A pesquisa quantitativa é usada também para traçar o perfil de um grupo de pessoas, a partir das características em comum a todos (MORESI, 2003).

3.1 População e Amostra

De acordo com Moresi (2003), a amostra é uma parcela selecionada de uma população, e a população representa seres que compartilham de uma mesma característica, conhecido também como universo, sendo assim, a amostra é um subconjunto de um universo.

Moresi (2003) aduz uma amostragem conceituada por conglomerados ou grupos, onde este tipo de amostragem determina um grupo da população, no caso, a amostragem desta pesquisa representa um grupo de empresas dos setores de rochas ornamentais da cidade de Cachoeiro de Itapemirim.

A amostra desta pesquisa tem uma proporção de 103 empresas, cuja população, segundo o site Cachoeiro Stoner Fair 2013, representa aproximadamente 1.000 empresas do setor de rochas ornamentais da cidade de Cachoeiro de Itapemirim.

Para proceder com a pesquisa, foi orientado para que os profissionais de tecnologia da informação tomassem a frente de responder a pesquisa. Entretanto, é de entendimento que há falta de setores ou mesmo de profissionais de tecnologia da informação em algumas empresas, sendo assim, foram abertas as possibilidades para que outros profissionais de outros cargos (que absorvam o conhecimento de gestão de risco da informação ou dos assuntos levantados na pesquisa) respondessem o questionário.

3.2 Coleta de Dados

Moresi (2003) conceitua a coleta de dados como uma observação sistemática. Mais detalhadamente, é a forma de usar os sentidos para coletar os dados da realidade, sentidos estes como: ouvir, ver, examinar fatos ou fenômenos. O autor ainda assevera que para a coleta de dados, deve-se fazer uso de algum instrumento de coleta.

O método usado para coleta de dados é o *survey*, e este método, segundo Babbie (1999) citado por Martins e Ferreira (2011), “[...] examina uma amostra da população

[...]" e também permite descobrir "a distribuição de certos traços e atributos da população estudada". Corroborando com este autor, Santos (acesso em 30 jul. 2014), assevera que esta modalidade para coleta de dados "[...] consiste na coleta de dados seguida de uma descrição dos mesmos, por meio das técnicas da chamada estatística descritiva".

Santos (acesso em 30 jul. 2014) ressalta para a instigação de Moresi (2003) que o questionário é o instrumento de coleta de dados mais comum. O autor cita a Internet como o meio mais facilitador para o delineamento da pesquisa, frisa na agilidade de comunicação e uma aproximação maior entre os participantes da pesquisa. Esse procedimento foi a princípio adotado justamente pela dificuldade de se entrevistar pessoalmente todos os participantes alvos da pesquisa, entretanto na prática, a pesquisa através da Internet não teve resultados tão satisfatórios, o retorno foi pequeno para uma grande expectativa, sendo assim, foi necessário também a pesquisa presencial nas organizações, obviamente comparado com a pesquisa na Internet, a pesquisa presencial fora mais dificultosa e mesmo assim, os resultados foram mais satisfatórios do que a pesquisa remota.

O questionário é "constituído por uma série ordenada de perguntas pré-elaboradas, sistemática e sequencialmente dispostas em itens que constituem o tema da pesquisa, que devem ser respondidas por escrito e sem a presença do pesquisador" (MORESI, 2003, p. 65).

O questionário foi *online*, trabalhado através da ferramenta Google Forms (vide APÊNDICE A). Com esta ferramenta, era possível gerar um *link* com o endereço do questionário, facilitando assim o envio pelos meios de comunicação de forma mais prática e direta. O questionário foi respondido também *online* e após a resolução das questões, o participante enviou as respostas e estas foram armazenadas em uma planilha on-line também gerenciada pela ferramenta do Google Forms.

O questionário foi dividido em duas partes, objetivando:

- Parte 1, composta por 6 (seis) perguntas que ajudara a caracterizar a empresa e o colaborador respondente de forma geral e agrupá-los,

desnudando o cargo do colaborador, o seu grau de escolaridade e tempo de anos trabalhado na empresa, o tamanho da empresa no que diz respeito ao seu faturamento anual, número de colaboradores e a sua área geográfica de atuação;

- Parte 2, composta por 15 (quinze) perguntas que ajudara a compreender a satisfação quanto a aderência dos procedimentos da segurança da informação pela empresa em conformidade com a norma NBR ISO/IEC 17799:2005.

As duas partes totalizam 21 (vinte e uma) questões, sendo 1 (uma) delas aberta, a qual se trata da indagação do cargo do colaborador. As outras questões são objetivas.

Os procedimentos de coleta de dados foram os seguintes:

1. Por *e-mail*:
    a. Foi feito um contato prévio por telefone com a empresa para divulgação da pesquisa;
    b. O *link* do questionário foi enviado via *e-mail*;
    c. Um contato posterior foi efetuado para assegurar o recebimento do e-mail e opcionalmente sanar dúvidas referente ao questionário;
    d. O prazo de 1 (um) dia foi estabelecido para o tempo de resposta dos participantes, se eles não puderam responder no mesmo instante;
    e. Depois do prazo foi efetuado outro contato para assegurar que os participantes tenham respondido.
2. Via redes sociais:
    a. O contato foi estabelecido e o participante foi esclarecido sobre a pesquisa;
    b. Em concordância, através da própria rede social, o *link* do questionário foi enviado;
    c. Ao mesmo tempo foram passadas as instruções para a resolução do questionário;
    d. O contato foi permanecido até que o participante confirmasse o entendimento e envio das respostas.

3. Presencial:
    a. O entrevistador se dirigiu até a organização;
    b. Foi feita uma explanação sobre a pesquisa e solicitado a participação de algum representante da organização;
    c. Sendo aceito, foi entregue o questionário impresso para o participante responder;
    d. O entrevistador permaneceu no local até que o participante terminasse de responder o questionário;
    e. O questionário foi recolhido e as respostas foram repassadas posteriormente para o questionário online, para que as respostas fossem armazenadas no banco de respostas do Google Forms.

No que tange o envio do questionário via rede social é justificado pela maior facilidade de um contato direto e interação maior com o participante. Silveira (2011) complementa que através das redes sociais, é possível uma pesquisa quantitativa com trocas de informações quase instantâneas e precisas.

3.2.1 Constructo da pesquisa

Foi estruturado o constructo da pesquisa em um quadro (vide Quadro 5), de forma a facilitar a visualização dos objetivos da pesquisa e a análise dos resultados, expondo as variáveis e questões inerentes do questionário, que permitisse também, uma melhor forma de visualizar os resultados obtidos e uma forma de obtê-los.

Quadro 5 – Constructo da pesquisa

OBJETIVOS DA PESQUISA	VARIÁVEIS	QUESTÕES
Caracterizar a empresa e o colaborador respondente de forma geral e agrupá-los, e a partir disto avaliar e comparar as diferenças relevantes das características das empresas dos setores de rochas ornamentais da cidade de Cachoeiro de Itapemirim.	✓ Cargo ou função do participante; ✓ Grau de formação do participante; ✓ Tempo de trabalho do participante na empresa; ✓ Faixa de faturamento anual da empresa; ✓ Número de funcionários; ✓ Área geográfica de atuação comercial da empresa.	1 2 3 4 5 6
Identificar a existência de políticas de segurança da informação formalizada na empresa.	✓ Escala de satisfação quanto ao questionamento sobre a existência da política de segurança.	7
Mensurar a aderência das práticas de segurança da informação conforme a norma NBR ISO/IEC 17799:2005	✓ Escala de satisfação quanto aos questionamentos referentes as diretrizes de implementação constadas nos itens 5.1.1 e 5.1.2 da norma NBR ISO/IEC 17799:2005.	7, 8, 9, 10, 11, 12, 13, 14, 17 e 20
	✓ Escala de satisfação quanto ao questionamento referente as diretrizes de implementação constadas nos itens 9.1.1 e 9.1.4 da norma NBR ISO/IEC 17799:2005.	16
	✓ Escala de satisfação quanto aos questionamentos referentes as diretrizes de implementação constadas no item 10.5.1 da norma NBR ISO/IEC 17799:2005.	18, 19
Mensurar o grau de satisfação do participante quanto a formalização das políticas de segurança da informação da empresa.	✓ Escala de satisfação quanto a formalização das políticas de segurança da informação aderidas pela empresa.	21

Fonte: Elaborado pelos autores

Conforme salientado, e conforme tratam os objetivos da pesquisa, de acordo com o Quadro 5, o questionário foi preparado em duas partes, sendo a primeira para caracterizar a empresa e a outra para verificar a aderência de diretrizes da segurança da informação conforme a NBR ISO/IEC 17799:2005. Para atingir o

objetivo de mensurar a aderência à segurança da informação em conformidade com a norma citada, foi proposto no questionário para que o participante escolhesse o seu grau de satisfação a cada item, através de uma escala.

A escala de satisfação do participante quanto a aderência da segurança da informação pela empresa foi enumerada de 1 (um) a 5 (cinco), onde 1 (um) é para representar uma total insatisfação e 5 (cinco) para representar uma total satisfação com a aderência de diretrizes.

3.3 Análise de Dados

Após a coleta de dados, o procedimento de análise de dados deve ser estabelecido para apresentar os resultados da pesquisa. Consiste especificamente na descrição dos dados, apresentando as características das variáveis e seus relacionamentos. (GERHARDT; SILVEIRA, 2009).

Os dados da pesquisa foram armazenados pelo gerenciador do Google Forms e foi utilizado o *software Microsoft Excel* 2013 para sumarizar os dados em planilhas.

Com base na análise descritiva para o procedimento de estudo do resultado da pesquisa, foi utilizado a técnica de estatística descritiva, a fim de organizar, descrever e resumir os dados coletados, e dessa forma, as respostas obtidas foram tabuladas (REIS e REIS, 2002). A tabulação das respostas foi feita de forma ordenada, na sequência do questionário. Cada resposta foi apresentada em cada tabela, juntamente com a questão, as opções e a quantificação das opções respondidas pelos participantes da pesquisa. Cada tabela foi submetida a uma descrição.

Em um outro momento, foi aplicado a análise de *clusters* ou agrupamento, que segundo Hair *et al.* (2006), é uma técnica analítica multivariada de dados, usado para classificar os indivíduos em subgrupos. Ainda de acordo com Hair *et al*. (2006, p. 35), “[...] o objetivo é classificar uma amostra de entidades (indivíduos ou objetos) em um número menor de grupos mutuamente excludentes, com base nas similaridades entre as entidades”.

Para efeito da análise de agrupamento, foi construído uma tabela para evidenciar as pontuações e a classificação individual das empresas pesquisadas, de acordo com as práticas de segurança da informação adotadas em conformidade com a NBR ISO/IEC 17799:2005. Esta tabela foi submetida ao *software Action* 2.7 para a efetiva análise de agrupamento, explanando os grupos para descrição dos relacionamentos entre os objetos.

3.4 Limitações da pesquisa

As limitações oriundas da pesquisa consistem nas dificuldades encontradas durante a realização da pesquisa descritiva do nível de segurança da informação. Apesar de ter sido realizada com uma amostragem significativa de 103 empresas do setor do mármore e granito da cidade de Cachoeiro de Itapemirim, a pesquisa apresentou as seguintes limitações:

a) Procedimento da pesquisa: como a pesquisa foi realizada por meio de um questionário *online* e presencial, no caso da amostragem alcançada através do procedimento *online*, no qual o participante respondeu o questionário sem a presença do entrevistador, não foi possível identificar se o entendimento do mesmo em relação às perguntas foi correto, ao contrário do procedimento presencial, com a presença do entrevistador as dúvidas foram sanadas possibilitando ao colaborador uma melhor avaliação. Além disso, após o contato prévio com o participante da pesquisa e o encaminhamento do questionário, poucos participantes responderam as questões.

   No procedimento presencial a principal limitação encontrada pelo entrevistador foi a falta de algum colaborador da área de tecnologia da informação na empresa, o que dificultou o entendimento das questões por parte dos colaboradores. Além disso, houve dificuldade de atendimento pelas empresas, uma vez que elas informavam não possuírem tempo naquele momento para participar da entrevista e solicitavam um retorno posterior ou que não tinha interesse em participar por falta de conhecimento no assunto;

b) Identificação dos participantes: tendo em vista os procedimentos que foram utilizados para a realização da pesquisa, foi efetuado um contato prévio com as empresas para divulgar a pesquisa e identificar o melhor colaborador de cada empresa. Porém nos procedimentos *online* que foram utilizados, não foi possível identificar se o questionário realmente foi respondido pelas empresas que solicitaram o envio, assim como também se quem respondeu era a pessoa responsável pela área de tecnologia da informação da empresa.

   No procedimento presencial, encontrar um responsável pela área de tecnologia da informação na empresa foi a maior limitação. Dessa forma, buscou-se pelos gestores das empresas, que quando encontrados, ao longo do questionário apresentaram carência de conhecimento em relação a área tecnológica em especial a segurança da informação. Dessa forma, em todos os procedimentos utilizados não foi possível identificar se quem respondeu realmente era a pessoa mais indicada para participar da pesquisa.

c) Confiabilidade da informação: devido o procedimento *online* não contar com a presença do entrevistador e a identificação da empresa no questionário, não foi possível averiguar se as respostas realmente corresponderam com a realidade da gestão da segurança da informação da empresa pesquisada. Por outro lado, o procedimento presencial contribuiu para com essa identificação, uma vez que o entrevistador foi até a empresa e auxiliou o colaborador a responder cada questão.

4 ANÁLISE DE DADOS

A partir daqui serão expostos os resultados da pesquisa, a começar com a análise descritiva das organizações e posterior a análise descritiva das práticas da segurança da informação. No item 4.3 será possível observar a análise de *clusters* ou agrupamento, no qual as cento e três empresas pesquisadas foram particionadas em grupos para uma descrição dos seus relacionamentos. E por fim, o item 4.4 revela uma análise descritiva geral das questões relacionadas com as práticas de segurança da informação.

4.1 Análise Descritiva das Organizações Pesquisadas

A Tabela 1 apresenta os cargos ocupados pelos participantes das empresas pesquisadas.

Tabela 1 – Cargo ocupado pelo colaborador participante da pesquisa

Qual o seu cargo ou função?		
Cargos	**%**	**Nº**
Operador de Logística	1%	1
Não respondeu	1%	1
Gerente Financeiro	1%	1
Faturista	1%	1
Diretor Comercial	1%	1
Almoxarifado	1%	1
Sócio	2%	2
Gerente Comercial	2%	2
Consultor de Vendas	3%	3
Analista de Sistema	3%	3
Gerente de Departamento Pessoal	3,80%	4
Contador	3,80%	4
Administrador	4,80%	5
Gerente Geral	5,80%	6
Financeiro	6,80%	7

Gerente Administrativo	7,60%	8
Auxiliar de Escritório	11,60%	12
Diretor Presidente	13,60%	14
Auxiliar Administrativo	26,20%	27
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

Com base na pesquisa, apenas dezessete (16,6%) dos participantes responderam ocupar cargos da alta direção, sendo dois (2%) Sócios, quatorze (13,6%) Diretores Presidentes e um (1%) Diretor Comercial.

A expectativa quanto a ocupantes de cargos da área especificamente da tecnologia da informação foi baixa, somente três (3%) dos participantes responderam ocupar a função de Analista de Sistemas.

Dos participantes, vinte e seis (25%) representam cargos de administradores e gerência nas empresas pesquisadas, que subdividem Gerente Administrativo, Gerente Comercial, Gerente Financeiro e Gerente Geral, no entanto, nenhum Gerente de Tecnologia da Informação.

Os maiores índices se concentram entre os Auxiliares Administrativos e Auxiliares de Escritório, totalizando trinta e nove (37,8%) dos participantes da pesquisa.

Dos outros participantes, três (3%) responderam ocupar cargos de Consultores de Vendas, sete (6,8%) responderam ocupar cargos de Financeiros, quatro (3,8%) responderam ocupar cargo de Contador, um (1%) respondeu ocupar cargo de Almoxarifado, assim como um (1%) respondeu ocupar cargo de Operador de Logística e por fim, um (1%) respondeu ocupar cargo de Faturista.

A Tabela 2 mostra o grau de escolaridade dos colaboradores respondentes da pesquisa. O objetivo disto é analisar se há relação entre o grau de escolaridade do respondente, quanto à sua contribuição e satisfação com o nível da segurança da informação da empresa.

Tabela 2 – Grau de escolaridade do colaborador participante da pesquisa

Qual o seu grau de escolaridade?		
Alternativas	**%**	**Nº**
2º grau completo	26 %	27
3º grau incompleto	20 %	20
3º grau completo	33 %	34
Especialização	18 %	19
Mestrado	3 %	3
Doutorado	0 %	0
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

Nenhum dos participantes das empresas pesquisadas responderam possuir doutorado. Os maiores índices se concentram entre participantes que são concluintes do ensino médio e graduação superior, onde vinte e sete (26%) dos representantes possuem até o 2º grau completo, vinte (20%) possuem o 3º grau incompleto, enquanto a maioria, representando trinta e quatro (33%) dos participantes, possuem o 3º grau completo. Dezenove (18%) possuem especialização e apenas três (3%) possuem mestrado.

Para fim de análise dos colaboradores respondentes da pesquisa, a Tabela 3 mostra a faixa que corresponde ao número de anos trabalhados do colaborador na empresa pesquisada.

Tabela 3 – Número de anos trabalhados do colaborador participante da pesquisa

Qual a faixa que corresponde ao número de anos trabalhados na empresa?		
Alternativas	**%**	**Nº**
Até 3 anos	45 %	46
Superior a 3 e inferior ou igual a 5 anos	19 %	20
Superior a 5 e inferior ou igual a 10 anos	17 %	17
Superior a 10 anos	19 %	20
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

A maior concentração foi de colaboradores que trabalham até 3 anos na empresa, representando quarenta e seis (45%) dos participantes. Mesmo assim, não houve muita variação entre as alternativas, onde, vinte (19%) responderam terem o tempo de trabalho superior a 3 e inferior a 5 anos, outros também vinte (19%) responderam terem o tempo de trabalho superior a 10 anos, enquanto outros dezessete (17%) responderam terem o tempo superior a 5 e inferior a 10 anos trabalhados.

A Tabela 4 desnuda o resultado da pesquisa com a classificação das empresas pelo faturamento anual.

Tabela 4 – Classificação das empresas diante o faturamento anual

Qual a faixa de faturamento anual a empresa está classificada?		
Alternativas	**%**	**Nº**
Até R$ 2,4 milhões	44 %	45
Superior a R$ 2,4 milhões e inferior ou igual a R$ 16 milhões	30 %	31
Superior a R$ 16 milhões e inferior ou igual a R$ 90 milhões	15 %	16
Superior a R$ 90 milhões e inferior ou igual a R$ 300 milhões	5 %	5
Maior que R$ 300 milhões	6 %	6
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

A classificação das empresas pelo faturamento anual, foram com base no Banco Nacional de Desenvolvimento (BNDES), a classificação de porte das empresas adotada por ela, se aplica a todos os setores.

E com base na tabela do BNDES, quarenta e cinco (44%) das empresas pesquisadas são consideradas microempresas, por possuírem um faturamento anual de até R$ 2,4 milhões. Trinta e um (30%) das empresas são consideradas pequenas empresas, por possuírem um faturamento anual superior a R$ 2,4 milhões e inferior a R$ 16 milhões. Dezesseis (15%) das empresas são consideradas médias empresas, por possuírem um faturamento anual superior a R$ 16 milhões e inferior a R$ 90 milhões. Apenas cinco (5%) das empresas pesquisadas são consideradas média-grande empresa por possuírem um faturamento anual superior a R$ 90 milhões e inferior a R$ 300 milhões, enquanto as outras seis (6%) empresas,

representam as grandes empresas, por possuírem um faturamento maior que R$ 300 milhões.

A Tabela 5, classifica as empresas quanto ao seu quadro de número de funcionários.

Tabela 5 – Classificação das empresas pela quantidade de funcionários

Qual o número de funcionários que a empresa se enquadra?		
Alternativas	**%**	**Nº**
Até 10 funcionários	40 %	41
De 11 a 100 funcionários	51 %	53
De 101 a 500 funcionários	8 %	8
Acima de 500 funcionários	1 %	1
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

Apenas uma (1%) empresa participante respondeu ter acima de 500 funcionários, próximo disso, apenas oito (8%) das empresas responderam ter de 101 a 500 funcionários. O resultado mostrou a maioria das empresas que possuem uma variação entre 10 a 100 funcionários, onde quarenta e um (40%) das empresas responderam ter até 10 funcionários, enquanto cinquenta e três (51%) responderam terem acima de 10 até 100 funcionários.

Quanto maior o número de funcionários, maior a necessidade de controles de segurança, sendo assim, espera-se que empresas que possuem maior número de funcionários tendem a terem maior formalização de suas políticas de segurança.

A Tabela 6, representa a classificação das empresas quanto a sua área de atuação comercial.

Tabela 6 – Classificação das empresas pela área geográfica de atuação comercial

Qual a área geográfica de atuação comercial da empresa?		
Alternativas	**%**	**Nº**
Cachoeiro de Itapemirim	5 %	5
Espírito Santo	5 %	5
Brasil	63 %	65
Mercosul	0 %	0
Global	27 %	28
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

O objetivo desta questão é analisar se existe alguma relação de atuação em diferentes áreas geográficas com as diretrizes de segurança da informação ou se existe diferença das políticas de segurança entre as áreas geográficas de atuação comercial regional e global.

Nenhuma das empresas participantes responderam atuar comercialmente no Mercosul, entretanto, vinte e oito (27%) das empresas pesquisadas atuam no âmbito global. O maior percentual é de que sessenta e cinco (63%) das empresas atuam em todo o território nacional, enquanto apenas cinco (5%) de empresas atuam somente na cidade de Cachoeiro de Itapemirim e também outras cinco (5%) empresas responderam atuar somente dentro do estado do Espírito Santo.

4.2 Análise Descritiva das Práticas de Segurança da Informação

A partir deste ponto, as tabelas evidenciam as satisfações dos participantes da pesquisa quanto as práticas de segurança da informação adotada pela empresa.

A Tabela 7 desnuda a existência de políticas de segurança que forneçam diretrizes para a segurança da informação.

Tabela 7 – Estabelecimento de políticas de segurança que forneçam diretrizes para implementação da segurança da informação

Há políticas de segurança estabelecidas que forneçam de forma geral diretrizes e forma de implementação de normas da segurança?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	6 %	6
Insatisfeito	8 %	8
Regular	23 %	24
Satisfeito	34 %	35
Totalmente Satisfeito	29 %	30
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

A norma NBR ISO/IEC 17799:2005 expressa a necessidade de haver políticas de segurança, pois é considerada um fator crítico para o sucesso da implementação de segurança da informação nas empresas.

Sobre a satisfação da existência de políticas de informação nas empresas pesquisadas, seis (6%) dos participantes responderam estarem totalmente insatisfeitos com a prática de política de segurança. Um pequeno número de participantes também respondeu estarem insatisfeitos, oito (8%) participantes. Vinte e quatro (23%) afirmaram uma satisfação regular nessa questão. A maioria dos participantes, trinta e cinco (34%) responderam estarem satisfeitos, mas bem próximo disso, trinta (29%) dos participantes responderam estarem totalmente satisfeitos com a existência de políticas de segurança que oferecem diretrizes para práticas da segurança da informação.

A Tabela 8 evidencia a satisfação dos participantes quanto à comunicação das normas de segurança da informação para todos os envolvidos das empresas pesquisadas.

Tabela 8 – Comunicação das normas de segurança da informação

As normas de segurança da informação são efetivamente comunicadas para os usuários e ao setor de processamento de dados?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	12 %	12
Insatisfeito	4 %	4
Regular	21 %	22
Satisfeito	27 %	28
Totalmente Satisfeito	36 %	37
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

É válido alvitrar que a norma NBR ISO/IEC 17799:2005 (2005, p. 8), orienta para que a política de segurança da informação seja “comunicada através de toda a organização para todos os usuários de forma que seja relevante, acessível e compreensível para o leitor em foco”.

Assim sendo, os resultados para esta questão mostram que doze (12%) dos participantes estão totalmente insatisfeitos, outros quatro (4%) estão insatisfeitos, enquanto vinte e um (21%) apresentaram satisfação regular. Apesar de ser uma porcentagem baixa, os insatisfeitos somam dezesseis (16%), o que reflete numa frívola comunicação das diretrizes da segurança e claro, a necessidade disto. No entanto, outros vinte e oito (27%) dos participantes responderam estarem satisfeitos quanto a esta questão, e por fim o maior índice de participantes, trinta e sete (36%) responderam estarem totalmente satisfeitos.

A Tabela 9 mostra a satisfação quanto a existência de um coordenador que trabalha em prol da segurança da informação, conscientizando os envolvidos e implementando controles de segurança.

Tabela 9 – Coordenação de segurança da informação

Existe um coordenador que participa ativamente implantando controles de acessos de segurança da informação e que trabalha pela conscientização da segurança da informação?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	31 %	32
Insatisfeito	12 %	12
Regular	11 %	11
Satisfeito	15 %	16
Totalmente Satisfeito	31 %	32
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

A NBR ISO/IEC 17799:2005 sugere que as atividades de segurança da informação sejam coordenadas e que a coordenação trabalhe promovendo a conscientização da segurança da informação por toda a organização.

Aos resultados da pesquisa, trinta e dois (31%) dos participantes responderam estarem totalmente insatisfeitos quanto a prática de coordenação de segurança da informação, mas por outro lado, também trinta e dois (31%) responderam estarem totalmente satisfeitos quanto a esta questão. Doze (12%) responderam estarem insatisfeitos, enquanto dezesseis (15%) afirmaram estarem satisfeitos. Outros onze (11%) apresentaram satisfação regular desta prática.

A Tabela 10 mostra a satisfação dos participantes da pesquisa, no quesito de revisão e atualização das normas de segurança da informação.

Tabela 10 – Revisão e atualização das normas de segurança da informação

As diretrizes, regras e práticas de segurança da informação são revisadas e atualizadas regularmente?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	19 %	19
Insatisfeito	7 %	7
Regular	25 %	26
Satisfeito	17 %	18
Totalmente Satisfeito	32 %	33
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

Como já tratado, a NBR ISO/IEC 17799:2005 aduz que a política de segurança da informação seja analisada em intervalos programados, a fim de garantir sua a eficácia, adequação e contínua pertinência, e promover também constantes atualizações.

A pesquisa mostrou que, dezenove (19%) dos participantes estão totalmente insatisfeitos quanto a esta questão. Sete (7%) estão insatisfeitos, enquanto vinte e seis (25%) afirmaram satisfação regular. Outros dezoito (17%) estão satisfeitos e outros trinta e três (32%) estão totalmente satisfeitos, totalizando cinquenta e uma (49%) empresas satisfeitas quanto a revisão e atualização das normas de segurança da informação.

A Tabela 11 evidencia o apoio da alta direção das empresas pesquisadas, pelos princípios da segurança da informação.

Tabela 11 – Apoio da alta direção nos princípios da segurança da informação

As metas e os princípios da segurança da informação são apoiados pela alta direção?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	9 %	9
Insatisfeito	6 %	6
Regular	19 %	20
Satisfeito	13 %	13
Totalmente Satisfeito	53 %	55
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

A NBR ISO/IEC 17799:2005 cita que a alta direção é responsável por impor políticas de segurança da informação clara, e adequada aos objetivos do negócio da organização, deve-se ainda demonstrar apoio e comprometimento com a segurança da informação. Fontes (2012) assevera que a direção participe incisivamente nos compromissos com a segurança da informação e dê exemplo para todos os envolvidos da organização.

Assim sendo, a pesquisa mostra o maior índice de cinquenta e cinco (53%) dos participantes da pesquisa, que estão totalmente satisfeitos, enquanto outros treze (13%) estão apenas satisfeitos, mas que juntos totalizam e representam sessenta e oito (66%) dos participantes satisfeitos com o apoio da alta direção. Poucos estão insatisfeitos, com um número de seis (6%) participantes e outros nove (9%) totalmente insatisfeitos. Outros vinte (19%) demonstraram terem satisfação regular.

A Tabela 12 desnuda a satisfação dos participantes da pesquisa quanto à prática de aprendizagem da segurança da informação para os envolvidos das empresas.

Tabela 12 – Aprendizagem de segurança da informação para os envolvidos da empresa

A aprendizagem da segurança da informação é promovida para todos os envolvidos da empresa?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	22 %	23
Insatisfeito	8 %	8
Regular	24 %	25
Satisfeito	15 %	15
Totalmente Satisfeito	31 %	32
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

A NBR ISO/IEC 17799:2005 ressalta a importância de promover para todos os funcionários da organização, além de todos envolvidos externos, treinamento em conscientização, informações e atualizações sobre as normas de segurança da informação.

Os dados da pesquisa apontam que vinte e três dos participantes (22%) estão totalmente insatisfeitos, pouco menos, oito (8%) dos outros participantes responderam estar apenas insatisfeitos, juntos totalizam a soma de trinta e um (30%) participantes insatisfeitos com a prática de aprendizagem. A norma citada sugere que o treinamento em conscientização da segurança da informação comece antes das atividades ou acesso às informações de um novo colaborador recente contratado e que se mantenha a conscientização ao longo da carreira na empresa. Essa abordagem da norma implica nos números altos dos participantes insatisfeitos, e reflete a teoria de que não exista em algumas das empresas pesquisadas, a conscientização depois da contratação de novos colaboradores.

Contudo, houve o maior número de participantes que estão totalmente satisfeitos, trinta e dois (31%) e quinze (15%) dos participantes apenas satisfeitos. Outros vinte e cinco (24%) mostraram satisfação regular.

A Tabela 13 evidencia a satisfação quanto às exigências em cláusulas contratuais para o comprometimento com a segurança da informação.

Tabela 13 – Comprometimento com a segurança da informação em cláusulas contratuais

O comprometimento com a segurança da informação, bem como a confidencialidade de informações críticas é exigido em cláusulas contratuais?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	39 %	40
Insatisfeito	6 %	6
Regular	21 %	22
Satisfeito	11 %	11
Totalmente Satisfeito	23 %	24
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

“Convém que os termos e condições de trabalho reflitam a política de segurança da informação” (NBR ISO/IEC 17799:2005, p. 27). A referida norma assevera que exista concordância, entre os envolvidos da organização, com as políticas de segurança da informação e estes assinem termos ou contratos, deixando claro suas responsabilidades.

E com base na pesquisa, pode-se notar que a maioria dos participantes, quarenta (39%) responderam estarem totalmente insatisfeitos quanto a esta prática e mais seis (6%) estão apenas insatisfeitos. Vinte e quatro (23%) estão totalmente satisfeitos, enquanto poucos onze (11%) participantes estão apenas satisfeitos. Por fim, vinte e dois (21%) dos participantes responderam possuírem satisfação regular.

A Tabela 14 mostra a satisfação quanto ao conhecimento de processos disciplinares em caso de violação da segurança da informação.

Tabela 14 – Consequências a violação da segurança da informação na empresa

É de conhecimento de todos os processos disciplinares, em consequência à violação da segurança da informação na empresa?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	17 %	18
Insatisfeito	6 %	6
Regular	19 %	19
Satisfeito	23 %	24
Totalmente Satisfeito	35 %	36
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

Segundo a NBR ISO/IEC 17799:2005, deve existir um processo disciplinar formal para os colaboradores que tenham violado a segurança da informação na empresa, este processo deve ser justo e correto.

Quanto a pesquisa, o maior número de participantes está satisfeito, totalizando sessenta (58%), subdivido em trinta e seis (35%) do participantes totalmente satisfeitos e vinte e quatro (23%) dos participantes apenas satisfeitos. Dezenove (19%) afirmaram satisfação regular. Os participantes insatisfeitos com esta prática são seis (6%) e os totalmente insatisfeitos são dezoito (17%).

A Tabela 15 evidencia a existência de documentação de apoio para a segurança da informação nas empresas pesquisadas.

Tabela 15 – Documentação para apoio à segurança da informação

Existe documentação, como políticas detalhadas, que apoie a segurança da informação na empresa?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	50 %	51
Insatisfeito	18 %	19
Regular	12 %	13
Satisfeito	8 %	8
Totalmente Satisfeito	12 %	12
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

As organizações devem buscar referências à documentação para apoio às políticas de segurança da informação, de acordo com a NBR ISO/IEC 17799:2005.

E a pesquisa mostra que a maioria dos participantes, cinquenta e um (50%) estão totalmente insatisfeitos quanto a prática de uso de procedimentos para apoio a segurança da informação, outros dezenove (18%) estão apenas insatisfeitos, juntos totalizando grande número de participantes insatisfeitos. Assim, doze (12%) estão totalmente satisfeitos e oito (8%) estão apenas satisfeitos. E em uma satisfação regular, treze (12%) responderam.

A Tabela 16 mostra a satisfação dos participantes da pesquisa, quanto a localização do centro de processamento de dados, considerando os riscos.

Tabela 16 – Localização do centro de processamento de dados, considerando os riscos

A localização do Centro de Processamento de Dados (CPD) é adequada, considerando os riscos?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	17 %	18
Insatisfeito	14 %	14
Regular	11 %	11
Satisfeito	21 %	22
Totalmente Satisfeito	37 %	38
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

Os itens 9.1.1 e 9.1.4 da NBR ISO/IEC 17799:2005, mostram a necessidade de utilizar perímetros de segurança para proteger as instalações físicas, como instalações de processamentos de informações, e as ações necessárias. Toda essa proteção deve ser levada em conta os riscos e desastres.

Assim, a maioria dos participantes, trinta e oito (37%) responderam estarem totalmente satisfeitos e a também grande parcela, vinte e dois (21%) dos outros participantes responderam estarem satisfeitos, juntos somam a maioria dos participantes satisfeitos. Onze (11%) responderam satisfação regular. Outros quatorze (14%) responderam estarem insatisfeitos e dezoito (17%) estão totalmente insatisfeitos com a prática de segurança do perímetro da localização do centro de processamento de dados.

A satisfação dos participantes quanto ao controle de acesso imposto pelas empresas pesquisadas é evidenciada na Tabela 17.

Tabela 17 – Controle de acesso aos equipamentos que contém informações críticas

Existe algum controle de acesso aos equipamentos que resguardam informações críticas da empresa?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	16 %	17
Insatisfeito	7 %	7
Regular	13 %	13
Satisfeito	14 %	14
Totalmente Satisfeito	50 %	52
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

A NBR ISO/IEC 17799:2005 impõe diretrizes para controles de acesso a áreas seguras para assegurar que somente pessoas autorizadas possam circular. Dessa forma, prevenir o acesso físico não autorizado é uma forma de evitar danos às instalações e informações da organização.

Os dados da pesquisa apontam um bom resultado quanto às práticas de controles de acesso nas empresas pesquisadas, de participantes satisfeitos cinquenta e dois

(50%) estão totalmente satisfeitos com esta prática e quatorze (14%) estão satisfeitos. Com números baixos, mas ainda sim consideráveis, dezessete (16%) dos participantes estão totalmente insatisfeitos e sete (7%) estão insatisfeitos. Treze (13%) dos participantes afirmaram satisfação regular.

A Tabela 18 evidencia a existência de um plano formal de *backup* nas empresas pesquisadas.

Tabela 18 – Plano formal de *backup*

Existe um plano formal de *backup*?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	10 %	10
Insatisfeito	7 %	7
Regular	19 %	20
Satisfeito	17 %	18
Totalmente Satisfeito	47 %	48
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

Backup, também conhecido como cópias de segurança, tem como objetivo, assegurado pela NBR ISO/IEC 17799:2005, de garantir a integridade e disponibilidade da informação, além dos recursos de processamento da informação.

A expectativa para esta questão foi superada, a maioria dos participantes, quarenta e oito (47%), responderam estarem totalmente satisfeito quanto a prática de *backups* na organização pesquisada e mais dezoito (17%) dos participantes responderam estarem satisfeitos, totalizando sessenta e seis (64%) dos participantes satisfeitos. Enquanto isso, dez (10%) dos participantes estão totalmente insatisfeitos e sete (7%) estão insatisfeitos. E outros vinte (19%) responderam satisfação regular com esta prática.

Ainda a respeito de *backups*, a Tabela 19 apresenta respostas à existência de práticas que asseguram o armazenamento das cópias de segurança em locais fisicamente seguros.

Tabela 19 – *Backups* guardados em locais fisicamente seguros

***Backups* são guardados em locais fisicamente seguros?**	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	17 %	18
Insatisfeito	10 %	10
Regular	17 %	18
Satisfeito	16 %	16
Totalmente Satisfeito	40 %	41
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

A expectativa para esta questão também foi superada, onde quarenta e um (40%) dos participantes estão totalmente satisfeitos e outros dezesseis (16%) estão apenas satisfeitos. A NBR ISO/IEC 17799:2005 assevera que as cópias de segurança devam ser guardadas em locais com distância suficiente para mantê-las livres de riscos e danos de um desastre que possa ocorrer no local principal da organização.

No mais, dezoito (17%) dos participantes responderam satisfação regular. Enquanto dez (10%) responderam estarem insatisfeitos e outros dezoito (17%) estão totalmente insatisfeitos quanto a prática de armazenar os *backups* em locais seguros.

A Tabela 20 evidencia a existência de plano de contingência e de recuperação em casos de interrupções das atividades, seja por falhas ou desastres.

Tabela 20 – Plano de contingência e de recuperação

A empresa leva consideração aos riscos e adota planos de contingência e de recuperação para casos de interrupções das atividades por falhas ou desastres?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	17 %	17
Insatisfeito	12 %	12
Regular	25 %	26
Satisfeito	22 %	23
Totalmente Satisfeito	24 %	25
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

O objetivo de plano de contingência, segundo a NBR ISO/IEC 17799:2005 é de não permitir que as atividades do negócio sejam interrompidas após falhas ou desastres significativos e garantir que estas atividades sejam retomadas rapidamente.

Com base nisto, a pesquisa mostra que as satisfações dos participantes foram bem distribuídas. Entretanto, o maior número, vinte e seis (25%) dos participantes afirmaram satisfação regular quanto a esta questão. A satisfação positiva teve números também altos, mas não tão distantes, vinte e três dos participantes (22%) responderam estarem satisfeitos e outros vinte e cinco (24%) responderam estarem totalmente satisfeitos. E totalmente insatisfeitos estão dezessete (17%) dos participantes e mais doze (12%) estão apenas insatisfeitos.

A última questão, juntamente com seus resultados, está exposta na Tabela 21, que identifica a satisfação geral do participante quanto às práticas de segurança da informação da empresa pesquisada.

Tabela 21 – Satisfação geral com a formalização das diretrizes de segurança

Está satisfeito(a) com o nível geral de formalização das regras de segurança de informação da empresa?	**Satisfação**	
	%	**Nº**
Totalmente insatisfeito	13 %	13
Insatisfeito	10 %	10
Regular	30 %	31
Satisfeito	20 %	21
Totalmente Satisfeito	27 %	28
Total	**100 %**	**103**

Fonte: Dados da pesquisa.

A maioria dos participantes não responderam em alto escala quanto as suas satisfações, trinta e um (30%) responderam satisfação regular quanto o nível geral de formalização das regras de segurança da informação dentro da empresa. Quanto aos totalmente satisfeitos, vinte e oito (27%) responderam e outros vinte e um (20%) responderam estarem satisfeitos. Enquanto outros treze (13%) responderam estarem totalmente insatisfeitos e dez (10%) apenas insatisfeitos.

4.3 Análise de Clusters

A Tabela 22 desnuda a pontuação atingida por cada empresa pesquisada em relação às práticas de segurança da informação. Para isso, cada grau de satisfação possui uma pontuação relacionada: totalmente insatisfeito equivale a um ponto; insatisfeito equivale a dois pontos; regular equivale a três pontos; satisfeito equivale a quatro pontos; e totalmente satisfeito equivale a cinco pontos. O resultado do somatório da pontuação foi obtido pela multiplicação dos pontos de cada grau de satisfação pelo número de vezes em que o referido grau de satisfação foi respondido em cada questão.

Ao se usar a pontuação do grau de satisfação totalmente satisfeito, multiplicando pelo número de questões, obter-se-ia o máximo de 75 pontos. Assim, este número representa 100% das boas práticas de segurança da informação em conformidade com a norma NBR ISO/IEC 17799:2005.

Tabela 22 – Satisfação das práticas de segurança das informações

Satisfação das práticas de segurança das informações nas empresas pesquisadas							
Empresas pesquisadas	Grau de satisfação					Pontuação	%
	Totalmente insatisfeito	Insatisfeito	Regular	Satisfeito	Totalmente Satisfeito		
Empresa 1	3	4	6	1	1	38	50,7 %
Empresa 2	14	0	1	0	0	17	22,7 %
Empresa 3	4	2	2	0	7	49	65,3 %
Empresa 4	9	1	3	0	2	30	40,0 %
Empresa 5	0	3	6	1	5	53	70,7 %
Empresa 6	0	0	0	3	12	72	96,0 %
Empresa 7	2	2	1	0	10	59	78,7 %
Empresa 8	2	2	3	4	4	51	68,0 %
Empresa 9	2	5	4	4	0	40	53,3 %
Empresa 10	0	0	0	14	1	61	81,3 %
Empresa 11	0	2	6	4	3	53	70,7 %
Empresa 12	0	2	6	4	3	53	70,7 %
Empresa 13	0	0	0	7	8	68	90,7 %
Empresa 14	3	5	7	0	0	34	45,3 %
Empresa 15	3	1	2	0	9	56	74,7 %
Empresa 16	3	1	2	0	9	56	74,7 %
Empresa 17	3	1	2	0	9	56	74,7 %
Empresa 18	0	0	3	6	6	63	84,0 %
Empresa 19	0	0	1	6	8	67	89,3 %
Empresa 20	0	0	2	6	7	65	86,7 %
Empresa 21	0	2	2	2	9	63	84,0 %
Empresa 22	1	0	1	0	13	69	92,0 %
Empresa 23	3	2	3	1	6	50	66,7 %
Empresa 24	3	1	5	3	3	47	62,7 %
Empresa 25	4	1	4	3	3	45	60,0 %
Empresa 26	2	1	5	5	2	49	65,3 %
Empresa 27	3	2	3	2	5	49	65,3 %
Empresa 28	2	0	2	0	11	63	84,0 %
Empresa 29	1	0	5	4	5	57	76,0 %
Empresa 30	1	0	5	5	4	56	74,7 %
Empresa 31	1	0	5	5	4	56	74,7 %
Empresa 32	4	3	2	1	5	45	60,0 %
Empresa 33	7	2	2	0	4	37	49,3 %
Empresa 34	3	2	2	0	8	53	70,7 %

Empresa 35	0	0	5	4	6	61	81,3 %
Empresa 36	12	1	0	1	1	23	30,7 %
Empresa 37	5	1	3	4	2	42	56,0 %
Empresa 38	13	0	0	1	1	22	29,3 %
Empresa 39	6	3	2	2	2	36	48,0 %
Empresa 40	15	0	0	0	0	15	20,0 %
Empresa 41	2	0	0	3	10	64	85,3 %
Empresa 42	2	1	1	7	4	55	73,3 %
Empresa 43	2	1	1	7	4	55	73,3 %
Empresa 44	2	1	1	7	4	55	73,3 %
Empresa 45	12	1	0	1	1	23	30,7 %
Empresa 46	12	2	0	0	1	21	28,0 %
Empresa 47	4	2	4	3	2	42	56,0 %
Empresa 48	4	2	4	3	2	42	56,0 %
Empresa 49	0	1	1	12	1	58	77,3 %
Empresa 50	0	2	5	5	3	54	72,0 %
Empresa 51	1	0	1	7	6	62	82,7 %
Empresa 52	1	0	1	7	6	62	82,7 %
Empresa 53	1	0	1	7	6	62	82,7 %
Empresa 54	2	0	0	1	12	66	88,0 %
Empresa 55	2	5	7	1	0	37	49,3 %
Empresa 56	2	0	1	7	5	58	77,3 %
Empresa 57	1	1	6	7	0	49	65,3 %
Empresa 58	0	1	0	3	11	69	92,0 %
Empresa 59	0	0	3	1	11	68	90,7 %
Empresa 60	0	1	3	2	9	64	85,3 %
Empresa 61	1	1	5	4	4	54	72,0 %
Empresa 62	4	0	4	4	3	47	62,7 %
Empresa 63	2	1	2	3	7	57	76,0 %
Empresa 64	0	1	5	4	5	58	77,3 %
Empresa 65	8	0	2	0	5	39	52,0 %
Empresa 66	3	0	3	3	6	54	72,0 %
Empresa 67	0	2	2	2	9	63	84,0 %
Empresa 68	0	2	2	5	6	60	80,0 %
Empresa 69	12	3	0	0	0	18	24,0 %
Empresa 70	6	3	3	2	1	34	45,3 %
Empresa 71	1	1	4	4	5	56	74,7 %
Empresa 72	0	2	6	1	6	56	74,7 %
Empresa 73	0	0	1	1	13	72	96,0 %

Empresa 74	0	0	1	1	13	72	96,0 %
Empresa 75	1	4	6	3	1	44	58,7 %
Empresa 76	1	4	6	3	1	44	58,7 %
Empresa 77	8	2	3	0	2	31	41,3 %
Empresa 78	8	2	3	0	2	31	41,3 %
Empresa 79	0	0	12	3	0	48	64,0 %
Empresa 80	1	2	4	0	8	57	76,0 %
Empresa 81	0	0	0	0	15	75	100,0 %
Empresa 82	2	2	6	2	3	47	62,7 %
Empresa 83	0	5	6	4	0	44	58,7 %
Empresa 84	0	0	0	3	12	72	96,0 %
Empresa 85	6	7	2	0	0	26	34,7 %
Empresa 86	1	1	4	8	1	52	69,3 %
Empresa 87	9	1	4	0	1	28	37,3 %
Empresa 88	0	2	5	2	6	57	76,0 %
Empresa 89	0	0	2	6	7	65	86,7 %
Empresa 90	3	0	3	4	5	53	70,7 %
Empresa 91	6	3	5	1	0	31	41,3 %
Empresa 92	1	0	0	0	14	71	94,7 %
Empresa 93	1	0	0	0	14	71	94,7 %
Empresa 94	1	0	4	4	6	59	78,7 %
Empresa 95	0	2	3	2	8	61	81,3 %
Empresa 96	1	0	0	0	14	71	94,7 %
Empresa 97	6	0	0	5	4	46	61,3 %
Empresa 98	3	0	6	2	4	49	65,3 %
Empresa 99	1	5	5	1	3	45	60,0 %
Empresa 100	7	2	3	1	2	34	45,3 %
Empresa 101	8	0	3	0	4	37	49,3 %
Empresa 102	5	3	5	0	2	36	48,0 %
Empresa 103	3	2	3	4	3	47	62,7 %

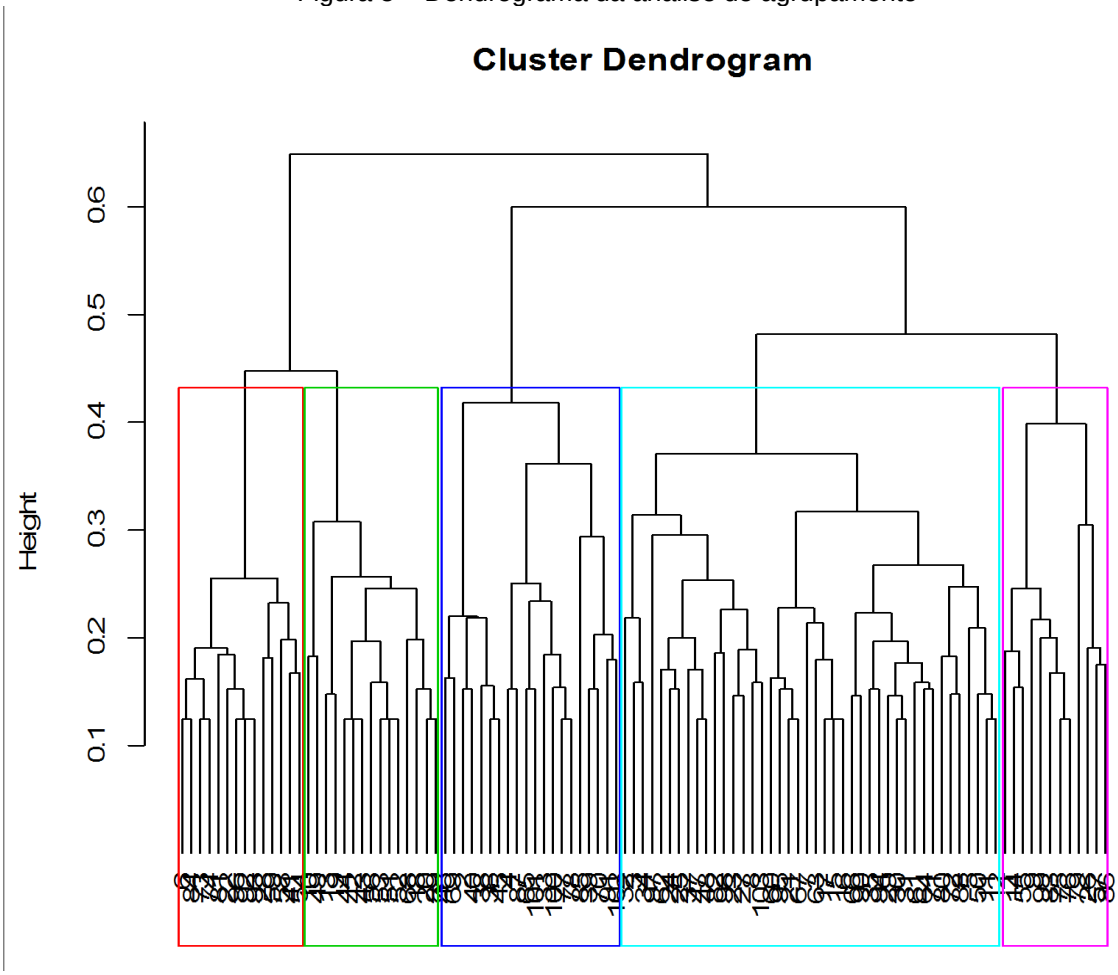
Fonte: Dados da pesquisa

Com exceção da empresa 81, a única que obteve uma pontuação de setenta e cinco, ou seja, apresentou 100% às práticas de segurança em conformidade com a NBR ISO/IEC 17799:2005, as demais empresas variaram entre quinze pontos (20%), a menor pontuação e setenta e cinco pontos (100%), a maior pontuação.

Para que a análise de clusters, também conhecida por agrupamento, se sucedesse, foi necessário submeter a tabela acima a um *software* estatístico chamado *Action*, nele foi possível aplicar uma das técnicas da análise multivariada, a análise de agrupamento.

Hair *et al.* (2006) cita três passos para análise de agrupamento. Para o primeiro passo é preciso definir alguma relação entre as entidades para separá-las em grupos, neste caso, a pontuação das práticas de segurança da informação evidenciada pelas empresas será objeto para associar as entidades e agrupá-las. O segundo passo é de fato dividir a amostra em grupos. E o terceiro passo é identificar o perfil das entidades em cada grupo, para determinar sua composição.

Figura 5 – Dendrograma da análise de agrupamento



Fonte: Dados da pesquisa.

A Figura 5 é a representação de um dendrograma gerado pela análise de clusters e se observado, as empresas foram particionadas em cinco grupos (agrupamento).

Em consequência da grande quantidade de amostra e para uma melhor visualização dos agrupamentos, a Tabela 23 evidência o resultado da análise.

Tabela 23 – Agrupamento da amostra

Agrupamento				
Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
6	10	2	3	1
22	13	4	5	9
28	18	33	7	14
41	19	36	8	26
54	20	38	11	55
58	42	39	12	57
59	43	40	15	75
73	44	45	16	76
74	49	46	17	79
81	51	65	21	83
84	52	69	23	86
92	53	70	24	99
93	56	77	25	
96	68	78	27	
	89	85	29	
		87	30	
		91	31	
		100	32	
		101	34	
		102	35	
			37	
			47	
			48	
			50	
			60	
			61	
			62	
			63	
			64	
			66	
			67	
			71	
			72	

			80	
			82	
			88	
			90	
			94	
			95	
			97	
			98	
			103	

Fonte: Dados da pesquisa.

A Tabela 23 evidencia as empresas particionadas em grupos (*clusters)*. Os grupos estão enumerados de um a cinco, que contém as empresas representadas pelos números de um a cento e três, assim indicando o total de cento e três empresas pesquisadas.

O primeiro agrupamento possui o total de quatorze empresas. Este grupo pertence as empresas com maiores pontuações, variando entre sessenta e três pontos (84%) e setenta e cinco pontos (100%), ou seja, foram as empresas que apresentaram maior grau de satisfação com as práticas de segurança da informação.

Das quatorze empresas que formam este grupo, seis respondentes da pesquisa possuem até o 3º grau completo, sendo o mesmo número de empresas que contém até 10 funcionários. A maior concentração de colaboradores que trabalham nas empresas deste grupo foi de até 3 anos. O predominante neste grupo são as empresas que atuam em todo o território nacional, com faturamento anual de até R$ 2,4 milhões e superior a R$ 2,4 milhões e inferiores a R$ 16 milhões. Apenas duas empresas estão enquadradas no âmbito global e não possuem convergências de faturamento.

O segundo agrupamento possui o total de quinze empresas. Ainda com números altos e bem próximo do primeiro grupo, as empresas correspondentes ao grupo dois possuem uma pontuação variando entre cinquenta e cinco pontos (73,30%) e sessenta e oito pontos (90,70%).

Neste grupo, existe uma convergência entre seis empresas em relação ao número de anos trabalhados pelo seu colaborador, sendo até 3 anos e o mesmo para superior a 3 anos. De acordo com oito empresas, o grau de escolaridade que os seus colaboradores se enquadram é o 3º grau completo. O predomínio neste agrupamento corresponde a onze empresas que atuam em todo o território nacional, sendo que três representam as grandes empresas, uma vez que possuem um faturamento superior a 300 milhões além de serem as únicas do grupo a possuir um quadro de colaboradores de 11 a 100 funcionários.

O terceiro agrupamento possui o total de vinte empresas. Este grupo apresenta as empresas com pontuações mais baixas, variando em média de quinze pontos (20%) a trinta e nove pontos (52%).

Das vinte empresas que compõem este grupo, nove possuem colaboradores que atuam na empresa até 3 anos. Neste agrupamento existe uma concentração de treze empresas que correspondem a um quadro de até 10 funcionários. Sete empresas possuem colaboradores com grau de escolaridade que corresponde ao 3º grau completo. Dez empresas são consideradas microempresas, por possuírem um faturamento anual de até 2,4 milhões. Observa-se, ainda, que o predominante deste agrupamento são as empresas que atuam em todo o território nacional, uma vez que apenas duas empresas atuam no âmbito global e outras três empresas atuam somente na cidade de Cachoeiro de Itapemirim.

O quarto agrupamento possui o total de quarenta e duas empresas. As empresas deste grupo apresentaram uma pontuação média, com a pontuação entre quarenta e dois pontos (56%) e sessenta e quatro pontos (85%).

Das quarenta e duas empresas que formam este agrupamento, doze empresas possuem colaboradores cujo seu grau de escolaridade corresponde até o 2º grau completo. Vinte e uma possuem colaboradores que atuam na empresa a um período de até 3 anos. Apesar do maior número de empresas deste agrupamento estarem centradas no faturamento anual de até 2,4 milhões que corresponde às microempresas, sendo que vinte e duas empresas atuam em todo território nacional,

este é o agrupamento que possui o quadro com número entre 11 até 100 funcionários.

O quinto e último grupo possui o total de doze empresas. Este grupo apresenta uma pontuação média/baixa, com o mínimo de trinta e quatro pontos (45,30%) e máximo de cinquenta e dois pontos (69, 30%).

Neste agrupamento existe uma convergência em relação ao grau de escolaridade dos colaboradores das empresas, onde quatro empresas possuem funcionários cujo seu grau de escolaridade apresentado foi o 3º grau completo sendo o mesmo número para os funcionários que apresentaram possuir especialização. De acordo com seis empresas, neste último agrupamento o número de anos trabalhados pelos colaboradores foi superior aos anteriores, sendo superior a 10 anos. Dez empresas apresentaram um faturamento anual de até R$ 2,4 milhões, já as demais corresponderam a superior R$ 2,4 milhões e inferior ou igual a R$ 16 milhões. Oito empresas apresentaram ter acima de 10 até 100 funcionários. Seis empresas atuam comercialmente em todo o território nacional, outras cinco empresas atuam no âmbito global e apenas uma empresa deste agrupamento atua na cidade de Cachoeiro de Itapemirim.

Era esperado que o grupo com maiores pontuações às práticas de segurança da informação, apresentassem um quadro de número de funcionários maiores, porque são geralmente empresas grandes e a exigência da segurança da informação nesse caso é maior, possuem maiores possibilidades de riscos.

De modo geral, não é possível em algum grupo, apontar alguma característica que sustente a pontuação do grupo, todos os grupos possuem variações de números de empresas com características diversas.

4.4 Análise Descritiva Geral das Práticas de Segurança da Informação

O objetivo desta análise é de explanar o grau de satisfação geral atingido pelas empresas com relação às práticas da segurança da informação em conformidade com a NBR ISO/IEC 17799:2005.

Para isso, a Tabela 24 evidencia a resposta de cada empresa, para cada questão das práticas de segurança da informação. É apresentado a questão, bem como sua pontuação e o percentual atingido. A contagem é da mesma forma que o agrupamento, o grau de satisfação em uma escala de um a cinco (totalmente insatisfeitos para totalmente satisfeito), contém uma pontuação de um a cinco respectivamente. Se as cento e três empresas respondessem cada questão com o grau de totalmente satisfeito, ou seja, pontuação de cinco pontos, então a satisfação de todas as empresas para uma questão seria de 100%, obtendo a pontuação total de 515 pontos.

Tabela 24 – Grau de satisfação geral para as questões das práticas de segurança da informação

Questões	**Pontuação**	**%**
Estabelecimento de políticas de segurança da informação com diretrizes para implantar a segurança da informação	384	74,5%
Comunicação das normas de segurança da informação	383	74,3%
Existência de um coordenador para o controle da segurança da informação	313	60,7%
Atualização das diretrizes da segurança da informação	348	67,5%
Apoio da alta direção com os princípios de segurança	408	79,2%
Práticas de aprendizagem em segurança da informação	334	64,8%
Exigência em cláusulas contratuais as práticas de segurança	282	54,7%
Conhecimento dos processos disciplinares em consequência da quebra de segurança da informação	363	70,4%
Existência de documentação para apoio às práticas de segurança	220	42,7%
Localização segura para o Centro de Processamento de Dados (CPD)	357	69,3%
Existência de controle de acesso físico aos equipamentos	386	74,9%
Existência de um plano de *backup*	396	76,8%
Depósito de *backups* em locais seguros	361	70,1%
Existência de planos de contingência	336	65,2%

Fonte: Dados da pesquisa.

A Tabela 24 mostra o resultado com variações pequenas. A maior pontuação é de quatrocentos e oito pontos (79,2%), para a questão no que diz respeito do apoio da alta direção para os princípios de segurança da informação nas empresas. Esse resultado é plausível, uma vez que a NBR ISO/IEC 17799:2005 enfatiza com veemência a necessidade da direção ter compromisso com a segurança da

informação, sendo a principal responsável pelo estabelecimento de políticas de segurança e o principal exemplo.

Em contrapartida, há um item com a menor pontuação, apenas duzentos e vinte pontos (42,7%), no que diz respeito da existência de alguma documentação para apoio às práticas de segurança. É válido alvitrar que, ter um documento de apoio faz parte das diretrizes para implementação de políticas de segurança e que inclusive deve estar especificado no documento da política, segundo a NBR ISO/IEC 17799:2005.

Outra pontuação baixa também foi identificado, com duzentos e oitenta e dois pontos (54,7%), referente ao item no que diz respeito a exigência de cláusulas contratuais para o compromisso com a segurança da informação. É uma porcentagem regular se considerarmos com a máxima de pontuação, e baixa, se considerarmos que os colaboradores são os maiores responsáveis por zelar a segurança dos ativos de informação da empresa.

Outro item que também teve uma pontuação satisfatória e digna de atenção, com trezentos e noventa e seis pontos (76,8%), foi a questão que evidencia a existência de planos de *backup*, caracterizado pela NBR ISO/IEC 17799:2005, como cópias de segurança, e ainda asseverado pela norma, como a forma de garantir a integridade e disponibilidade das informações após a ocorrência de algum desastre.

Ainda na faixa dos 70%, pode-se notar uma pontuação satisfatória para o estabelecimento de políticas de segurança da informação, com trezentos e oitenta e quatro pontos (74,5%) e a comunicação dessas políticas para os envolvidos das organizações, com trezentos e oitenta e três pontos (74,3%). É plausível as organizações terem políticas de segurança que são comunicadas para os seus envolvidos. O objetivo da política de segurança da informação é, segundo a NBR ISO/IEC 17799:2005, promover uma orientação para os envolvidos da organização contribuírem para com a segurança da informação, mas para isso, todos devem terem sidos comunicados e estarem cientes. Haver políticas de segurança, mas os parceiros da organização não saberem da existência ou de como trabalharem em prol da segurança, de nada vale.

Na faixa dos 60%, temos as questões que tratam da existência de um coordenador para o controle de segurança, práticas de atualização das diretrizes, as práticas de aprendizagem e conscientização da segurança, a localização segura do CPD e a existência de planos de contingência. Todas essas práticas estão acima da média, sendo assim satisfatórias para a pesquisa.

5 CONSIDERAÇÕES FINAIS

O objetivo geral deste trabalho de conclusão de curso foi verificar através de pesquisa descritiva, o nível de segurança da informação, juntamente com uma análise de conformidade com as normas estabelecidas pela NBR ISO/IEC 17799:2005 nas empresas de mármores e granitos na cidade de Cachoeiro de Itapemirim, Espírito Santo, Brasil.

5.1 Conclusões

Com base no objetivo geral, a seguir é explanada a conclusão da pesquisa, juntamente com os resultados que foram alcançados por meio dos objetivos específicos declarados na introdução deste trabalho.

a) Avaliar o nível de segurança da informação nas empresas de mármores e granitos, na cidade de Cachoeiro de Itapemirim, ES;

De acordo com os dados apresentados no item 4.3 que se referem à análise de *clusters* ou agrupamento, as empresas foram divididas em cinco grupos por meio da utilização de um *software* estatístico denominado *Action,* que apresentou diferentes níveis de aderências em relação às práticas e o nível de segurança da informação.

Neste objetivo o grau de aderência das empresas participantes esteve entre uma pontuação de quinze pontos (20%) a setenta e cinco pontos (100%), porém o grau de satisfação geral das empresas participantes que é representado pela tabela 24, demonstrou que a maioria das questões alcançaram um grau de aderência acima da média.

Conforme os resultados apresentados no decorrer da tabela 22 que representa a satisfação das práticas de segurança das informações, apenas a empresa 81 obteve grau de aderência 100%, ou seja, foi à única empresa da amostragem utilizada a apresentar um grau de 100% em relação às práticas de segurança em conformidade com a norma NBR ISO/IEC 17799:2005 com maior pontuação, setenta e cinco pontos (100%).

b) Avaliar as características relevantes das empresas de mármores e granitos, granitos, na cidade de Cachoeiro de Itapemirim, ES;

As características das empresas pesquisadas foram apresentadas no decorrer deste trabalho através dos respectivos itens: 4.1 que corresponde a análise descritiva das organizações e 4.3 representado pela à análise de clusters da pesquisa, que foi realizada com base na pontuação que cada empresa atingiu em relação às práticas de segurança da informação.

Analisando os dados existentes nestes itens, a amostragem apresentou características relevantes que foram evidenciados através dos dados da pesquisa alcançados por meio das questões de 1 a 6. Com base nesses dados, trinta e nove (37,8%) dos participantes da pesquisa ocupam cargos de auxiliares administrativos e auxiliares de escritório. Por outro lado, somente três (3%) dos participantes informaram ocupar cargos da área especificamente da tecnologia da informação.

O grau de escolaridade dos colaboradores da pesquisa predominou-se no 3º grau completo com trinta e quatro (33%) respondentes. Em relação ao período de anos trabalhados na empresa, a maior concentração foi de colaboradores que trabalham até 3 anos na empresa, representando quarenta e seis (45%) dos participantes.

Na análise referente à classificação das empresas de acordo com o seu faturamento anual, constatou-se que quarenta e cincos (44%) das empresas pesquisadas são considerados microempresas com base no Banco Nacional de Desenvolvimento (BNDES), devido possuir um faturamento anual de até R$ 2,4 milhões. Além disso, quarenta e um (40%) das empresas responderam ter até 10 funcionários.

De acordo com os dados da pesquisa, à classificação das empresas pela sua área geográfica de atuação comercial, apresentou-se predominante as empresas que possuem como características atuar em todo o território nacional. Sendo o maior percentual de sessenta e cinco (63%). Enquanto que apenas cinco (5%) das empresas participantes atuam somente na cidade de Cachoeiro de Itapemirim e outras cinco (5%) atuam apenas no Estado do Espírito Santo.

c) Quantificar o número de empresas que possuem políticas de segurança e quantas se preocupam em realizar *backup* das suas informações;

As existências de políticas de segurança assim como a realização de *backups* das informações nas empresas são identificadas respectivamente através das tabelas 7 e 18, que tem como objetivo verificar a aderência de políticas de segurança, responsáveis por fornecerem diretrizes para a segurança da informação e a aderência de algum plano formal de *backup*.

A norma da ISO/IEC 17799:2005 defende as políticas de segurança como um dos fatores mais críticos que contribui para o sucesso da implementação da segurança da informação. Em relação ao uso de *backup* que também é conhecido como cópias de segurança, de acordo com a norma da ISO/IEC 17799:2005 sua principal finalidade é garantir a integridade e disponibilidade da informação assim como dos recursos de processamento de informação.

Tendo em vista a principal importância de possuir políticas de segurança e a realização dos procedimentos de *backup* nas empresas, é possível afirmar através da amostragem utilizada para a realização da análise da pesquisa, que todas as empresas participantes possuem em seu estabelecimento alguma política de segurança voltada para a informação assim como também a execução de um plano formal de *backup*.

Dessa forma, analisando a satisfação da existência dessas políticas juntamente com a realização de *backup*, quatorze (14%) empresas estão insatisfeitas com a práticas de políticas da informação, enquanto que outras oitenta e nove (86%) apresentaram um grau de satisfação de regular para totalmente satisfeita. Já em relação à existência do plano formal de *backup*, sessenta e seis (64%) empresas responderam estarem satisfeitas, vinte (19%) apresentaram satisfação regular e outras dezessete (17) estão insatisfeitas com a prática de *backups*.

Porém, de acordo com a análise geral de satisfação das práticas de segurança da informação (tabela 24), a existência de um plano formal de *backup* nas empresas

alcançou uma pontuação de trezentos e noventa e seis pontos (76,8%), apresentando um alto grau de satisfação.

d) Analisar a conformidade das políticas e práticas de segurança com a norma NBR ISO/IEC 17799:2005;

A conformidade das políticas e práticas de segurança da informação de acordo com a norma NBR ISO/IEC 17799:2005 é da análise em relação às práticas de segurança da informação identificadas através da tabela 24, que corresponde o grau de satisfação geral das empresas participantes com base nos itens de 7 a 20 do questionário.

De acordo com os dados da pesquisa, a maior pontuação é representada por quatrocentos e oito (79,2%), que se refere ao apoio da alta direção voltado para as metas e princípios de segurança da informação nas empresas, tendo como base a norma da NBR ISO/IEC 17799:2005.

Por outro lado, a menor pontuação encontrada foi de duzentos e vinte (42,7%), que corresponde à existência de documentação para apoio às práticas de segurança. Diante deste resultado, é possível afirmar que ainda existe uma carência de informação voltada para a área da segurança da informação conforme foi descrito nas limitações da pesquisa. Uma vez que segundo a norma da ISO/IEC 17799:2005 a documentação para apoio faz parte das diretrizes para implementação de políticas de segurança e, além disso, devem ser especificadas no documento da política.

Analisando de forma geral o grau de satisfação das empresas participantes da pesquisa em relação às práticas de segurança da informação, é certo de que a maioria das questões alcançaram um percentual acima da média, ou seja, apresentaram resultados a partir de 70%.

6 REFERÊNCIAS

ACIOLI, Erica. **A informação, considerada maior ativo da organização.** Sururu Digital. 30 de setembro de 2011. Disponível em <http://www.sururudigital.com.br/2011/09/a-informacao-considerada-maior-ativo-da-organizacao/>. Acesso em: 24 mar. 2014.

AEON. Segurança da informação: entenda os riscos e consequências de perder os dados. **Aeon.** 15 agosto de 2012. Disponível em: < http://www.aeon.com.br/seguranca-da-informacao-entenda-os-riscos-e-consequencias-de-perder-seus-dados>. Acesso em: 03 mar. 2014.

ALVES, Cássio B. **Segurança da informação vs. engenharia social:** como se proteger para não ser mais uma vítima. 2. ed. [S.l.:s.n., 2012]. 128 p.

AMOROSO, Danilo. **Mito ou verdade:** outros sistemas são mais seguros que o Windows? Tecmundo. 16 de outubro de 2009. Disponível em: <http://www.tecmundo.com.br/sistema-operacional/2911-mito-ou-verdade-outros-sistemas-sao-mais-seguros-que-o-windows-.htm>. Acesso em: 26 mar. 2014.

ANDRADE, Eduardo L. **Introdução à pesquisa operacional:** métodos e modelos para análise de decisões. 4. ed. Rio de Janeiro: Ed. LTC, 2009. 204 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005**: tecnologia da informação - técnicas de segurança - gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799:** tecnologia da Informação - técnicas de Segurança - código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Perguntas frequentes. [s.d.]. Disponível em: < http://www.abnt.org.br/m2.asp?cod_pagina=963#>. Acesso em: 7 maio. 2014.

AUDY, Jorge L N; ANDRADE, Gilberto K; CIDRAL, Alexandre. **Fundamentos de sistemas de informação.** Porto Alegre: Ed. Bookman, 2007.

BARRET, Diane; TODD, King. **Redes de computadores.** Tradução de Daniel Vieira. Rio de Janeiro: LTC, 2010.

BEAL, Adriana. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BEZERRA, E. K. **Gestão de riscos de TI – NBR 27005.** Rio de Janeiro: Escola Superior de Redes, 2013.

BNDES. **Porte de empresa.** [s.d.]. Disponível em: <http://www.bndes.gov.br/SiteBNDES/bndes/bndes_pt/Institucional/Apoio_Financeiro/porte.html>. Acesso em: 25 jul. 2014.

CACHOEIROSTONEFAIR. **36º feira internacional do mármore e granito:** a cidade. Disponível em: < http://www.cachoeirostonefair.com.br/site/2013/pt/cidade>. Acesso em: 03. mar. 2014.

CAMPOS, André L. N**. Sistemas de segurança da informação:** controlando os riscos. Florianópolis: Visual Books, 2006.

CERT. Segurança na Internet. **Cert**. [s.d.]. Disponível em < http://cartilha.cert.br/seguranca/>. Acesso em: 01 out. 2014.

CLAUDIODODT. Transformando sua política de segurança da informação em um ativo estratégico. **Claudiododt.** 26 de junho de 2011. Disponível em: < http://claudiododt.com/2011/06/29/transformando-sua-politica-de-seguranca-da-informacao-em-um-ativo-estrategico/ >. Acesso em: 28 mar. 2014.

CNASI. A importância de investir na segurança da informação. **Cnasi.** [s.d.]. Disponível em: < http://www.cnasi.com.br/a-importancia-de-investir-na-seguranca-da-informacao/>. Acesso em: 04 mar. 2014.

COULOURIS, G.; DOLLIMORE, J.; KINDBERG, T. **Sistemas distribuídos:** conceitos e projetos. 4. ed. Porto Alegre: Bookman, 2007.

DANTAS, Marcus L. **Segurança da informação:** uma abordagem focada em gestão de riscos. Olinda: Ed. Livro Rápido, 2011. 152 p.

DUARTE, Vânia M. do N. Pesquisas: exploratória, descritiva e explicativa. Monografias. **Brasil Escola.** [s.d.]. Disponível em: <http://monografias.brasilescola.com/regras-abnt/pesquisas-exploratoria-descritiva-explicativa.htm>. Acesso em: 27 jul. 2014.

ECOPAG. Pesquisa revela que celulares estão cada vez mais seguros. **Ecopag.** 27 de junho de 2013. Disponível em: <http://www.ecopag.com.br/blog/pesquisa-revela-que-celulares-estao-cada-vez-menos-seguros/#.U2JTdoFdXG8>. Acesso em: 26 mar. 2014.

ESGOV. Rota do mármore e granito: uma rota de bons negócios. **Portal do Governo do Estado do Espírito Santo.** [s.d.]. Disponível em: < http://www.es.gov.br/EspiritoSanto/paginas/rota_marmore_granito.aspx>. Acesso em: 03 mar. 2014.

ESPÍRITO SANTO. **Rota mármore e granito.** [s.d.]. Disponível em: <http://www.es.gov.br/EspiritoSanto/paginas/rota_marmore_granito.aspx>. Acesso em: 10 mar. 2014.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Marcio Tadeu. **Política de segurança da informação:** Guia Prático para Elaboração e Implementação. Rio de Janeiro: Editora Ciência Moderna, 2006.

FIALHO JR., Mozart. **Guia essencial do backup.** São Paulo: Digerati Books, 2007. 128 p.

FONTES, Edison. **Políticas e normas para segurança da informação.** Rio de Janeiro: Brasport, 2012.

GERHARDT, Tatiana E.; SILVEIRA, Denise T. **Métodos de pesquisa.** Rio Grande do Sul: UFRGS, 2009.

HAIR, Joseph F. et al. **Análise multivariada de dados.** 6. ed. São Paulo: Artmed, 2006.

IMONIANA, Joshua O. **Auditoria de sistemas de informação.** 2. ed. São Paulo: Atlas, 2010.

INFORMABR. Introdução: como tudo começou. **Informabr.** [s.d.]. Disponível em <http://www.informabr.com.br/nbr.htm>. Acesso em: 7 maio. 2014.

INSIGHT SINFIC. ISO IEC 17799:2005: código de boas práticas da gestão de segurança da informação. **Insight Sinfic.** 18 de dezembro de 2006. Disponível em: <http://www.sinfic.pt/SinficNewsletter/sinfic/Newsletter92/ISO17799.html>. Acesso em: 04 de maio. 2014.

KONZEN, M. P; FONTOURA, L. M; NUNES, R. C. Gestão de riscos de segurança da informação baseada na norma ISO/IEC 27005 usando padrões de segurança. In: IX SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA, 1., 2012, Resende. **Anais eletrônicos…** Resende: IX SEGeT, 2012. Disponível em: < http://www.car.aedb.br/seget/artigos12/57616827.pdf>. Acesso em: 28 mai. 2014.

LANDOLL, Douglas J. **The Security Risk Assessment Handbook:** A complete guide for performing Risk Assessment, CRC Press. [S.l.: s.n., 2011].

LUND, M. S.; SOLHAUG, B. & STOLEN, K. **Evolution in relation to risk and trust management. IEEE Computer Society.** [S.l.: s.n., 2010]. p. 49-55.

MARTINS, Claudia G.; FERREIRA, Miguel L. R. O Survey como tipo de pesquisa aplicado na descrição do conhecimento do processo de gerenciamento de riscos em projetos no segmento da construção. In: CONGRESSO NACIONAL DE EXCELÊNCIA EM GESTÃO, 7., 2011. **Anais eletrônicos**... Disponível em: <http://www.excelenciaemgestao.org/Portals/2/documents/cneg7/anais/T11_0362_1839.pdf>. Acesso em: 28 jul. 2014.

MENDES, Bráulio M. **Segurança da informação:** uma abordagem de conceitos, mecanismos e políticas de segurança. 2011. 55 f. Monografia (Especialista em Engenharia de Sistema) – Programa de Pós-Graduação em Engenharia de Sistemas, Escola Superior Aberta do Brasil, Vilha Velha, 2011.

MORAES, G. **Sistema de gestão de riscos – princípios e diretrizes – ISO 31.000/2009 comentada e ilustrada.** Rio de Janeiro:[s.n.], 2010.

MORESI, Eduardo. **Metodologia da pesquisa.** 2003. 106 f. Monografia - Programa de Pós-Graduação Stricto Sensu em Gestão do Conhecimento e Tecnologia da Informação, Universidade Católica de Brasília, Brasília, 2003. Disponível em: < http://ftp.unisc.br/portal/upload/com_arquivo/1370886616.pdf >. Acesso em: 30 ago. 2014.

MUNDO EN LÍNEA. El 94% de las empresas que pierden sus datos desaparece. **Mundo en línea.** 16 de setembro de 2004. Disponível em: <http://www.mundoenlinea.cl/noticia.php?noticia_id=638&categoria_id=35>. Acesso em: 25 mar. 2014.

NADEL, Brian. **Cinco opções de backup online**. 14 de fevereiro de 2012. Disponível em: < http://cio.com.br/tecnologia/2012/02/14/cinco-opcoes-de-backup-on-line/ >. Acesso em: 19 ago. 2014.

OLIVEIRA, M. A. F.; ELLWANGER, C.; VOGT, F. C. & R. C. NUNES. Framework para gerenciamento de riscos em processos de gestão de segurança da informação baseado no modelo DMAIC. In: XXIX Encontro Nacional de Engenharia de Produção (ENEGEP), 2009, Salvador, XXIX Encontro Nacional de Engenharia de Produção. Rio de Janeiro: Abepro, 2009. v. 1. p. 11-20. **Anais eletrônicos...** Disponível em: < http://www.abepro.org.br/biblioteca/enegep2009_TN_STP_098_661_13268.pdf >. Acesso em: 28 mai. 2014.

OLIVEIRA, Marcelo M; PONCHIO, Mateus C; NETO, Mario S; PIZZINATTO, Nadia K. Análise dos fatores de resistência na implantação de sistemas de informação na manufatura de eletrônicos. **Revista de gestão da tecnologia da informação e sistemas de informação Journal of Information System and Tecnology Management.** v. 6, n. 3, p. 507-524, 2009.

OLIVEIRA, V. L. **Uma análise comparativa das metodologias de gerenciamento de risco FIRM, NIST SP 800-30 e OCTAVE.** Dissertação (Mestrado em Engenharia de Computação) – Trabalho Final de Mestrado Profissional em Computação, UNICAMP, Campinas, 2006.

RASCÃO, José P. **Da gestão estratégica da informação:** como aumentar o tempo disponível para a tomada de decisão estratégica. Rio de Janeiro: Ed. E-Papers, 2006. 290 p.

REALISO. Ativos da informação. **Realiso.** [20--]. Disponível em: <https://sites.google.com/a/realiso.com/realiso-corp/gestao-de-risco/-3-3-ativos-de-informacao>. Acesso em: 24 mar. 2014.

REIS, E. A.; REIS, I. A. **Análise descritiva de dados:** síntese numérica. 2002. Relatório técnico RTP-02/2002. Instituto de Ciências Exatas, Universidade Federal de Minas Gerais, Belo Horizonte, 2002.

SANTOS, Andressa S; QUATRIN, Denise R; PINTO, Letícia M; STEFAN, Aline A; COSTA, Vania M F. A importância de sistemas de informação em pequenas empresas: um estudo de caso em uma agência de publicidade. In: SIMPÓSIO DE EXCELÊNCIA EM GESTÃO DA TECNOLOGIA, 4., 2012, Resende. **Anais eletrônico...** Resende: IX SEGeT, 2012. Disponível em < http://www.car.aedb.br/seget/artigos12/21616171.pdf>. Acesso em: 23 junho. 2014.

SANTOS, Luiz C. **Survey:** um delineamento de pesquisa. [s.d.]. Disponível em: <http://www.lcsantos.pro.br/arquivos/25_SURVEY01042010-171131.pdf>. Acesso em: 30 jul. 2014.

SÊMOLA, M. **Gestão da segurança da informação:** visão executiva da segurança da informação: aplicada ao Security Officer / Marcos Sêmola e Módulo Security Solutions S.A. Rio de Janeiro: Elsevier, 2003.

SILVEIRA, Emanuele. **Usando as mídias sociais como ferramenta de pesquisa de mercado.** 27 de outubro de 2011. Disponível em: < http://blog.being.com.br/index.php/consumo/midias-sociais-pesquisa-de-mercado/>. Acesso em: 30 jul. 2014.

SOARES, Luiz F. G.; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores.** 2**.** ed. Rio de Janeiro: Campus, 1995.

STAIR, Ralph M; REYNOLDS, George W. **Princípios de sistemas de informação:** uma abordagem gerencial. Tradução de Flávio Soares Corrêa da Silva; Giuliano Mega; Igor Ribeiro Sucupira. 6. ed. São Paulo: Ed. Pioneira Thomson Learning, 2006.

STALLINGS, Willian; BROWN, Lawrie. **Segurança de computadores**: princípios e práticas. Tradução de Arlete Simile Marques. 2. ed. Rio de Janeiro: Elsevier, 2014.

TANENBAUM, Andrew S. **Redes de computadores.** Tradução de Vandenberg D. de Souza. 4. ed. [S.l.]: Campus, 2003. 968 p.

TORRES, Gabriel. **Redes de computadores curso completo.** Rio de Janeiro: Axcel Books, 2001.

VASILE, T; STUPARU, D. & DANIASA, C. **The relative risk weighting process. Annals Economic Science Series.** [S.l.: s.n., 2010]. p. 540-544.

VELLIS, Davide de. **Quais são as opções para fazer backup de meus arquivos importantes.** 9 de maio de 2013. Disponível em: < http://www.reviversoft.com/pt/blog/2013/05/backup-options/>. Acesso em: 19 ago. 2014.

APÊNDICE

APÊNDICE A – Questionário de Segurança da Informação

Questionário de Segurança da Informação

Pesquisa avaliativa da segurança da informação, em conformidade com a NBR ISO/IEC 17799:2005.

1) Qual o seu cargo ou função? _____

2) Qual o seu grau de escolaridade?
( ) 2º grau completo
( ) 3º grau incompleto
( ) 3º grau completo
( ) Especialização
( ) Mestrado
( ) Doutorado

3) Qual a faixa que corresponde ao número de anos trabalhos na empresa?
( ) Até três anos
( ) Superior a 3 e inferior ou igual a 5 anos
( ) Superior a 5 e inferior ou igual a 10 anos
( ) Superior a 10 anos

4) Qual a faixa de faturamento anual a empresa está classificada?
( ) Até R$ 2,4 milhões
( ) Superior a R$ 2,4 milhões e inferior ou igual a R$ 16 milhões
( ) Superior a R$ 16 milhões e inferior ou igual a R$ 90 milhões
( ) Superior a R$ 90 milhões e inferior ou igual a R$ 300 milhões
( ) Maior que R$ 300 milhões

5) Qual o número de funcionários que a empresa se enquadra?
( ) Até 10 funcionários
( ) De 11 a 100 funcionários

( ) De 101 a 500 funcionários
( ) Acima de 500 funcionários

6) Qual a área geográfica de atuação comercial da empresa?
( ) Cachoeiro de Itapemirim
( ) Espírito Santo
( ) Brasil
( ) Mercosul
( ) Global

7) Há políticas de segurança estabelecida que forneçam de forma geral diretrizes e forma de implementação da norma da segurança?
Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.
1 2 3 4 5
( ) ( ) ( ) ( ) ( )

8) As normas de segurança da informação são efetivamente comunicadas para os usuários e ao setor de processamento de dados?
Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.
1 2 3 4 5
( ) ( ) ( ) ( ) ( )

9) Existe um coordenador que participa ativamente implantando controles de acessos de segurança da informação e que trabalha pela conscientização da segurança da informação?
Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.
1 2 3 4 5
( ) ( ) ( ) ( ) ( )

10) As diretrizes, regras e práticas de segurança da informação são revisadas e atualizadas regulamente?

Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.

1 2 3 4 5

( ) ( ) ( ) ( ) ( )

11) As metas e os princípios da segurança da informação são apoiados pela alta direção?

Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.

1 2 3 4 5

( ) ( ) ( ) ( ) ( )

12) A aprendizagem com a segurança da informação é promovida para todos os envolvidos da empresa?

Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.

1 2 3 4 5

( ) ( ) ( ) ( ) ( )

13) O comprometimento com a segurança da informação, bem como a confidencialidade de informações críticas é exigido em cláusulas contratuais?

Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.

1 2 3 4 5

( ) ( ) ( ) ( ) ( )

14) É de conhecimento de todos os processos disciplinares, em consequência a violação da segurança da informação na empresa?

Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.

1 2 3 4 5

( ) ( ) ( ) ( ) ( )

15) Existe documentação, como políticas detalhadas, que apoie a segurança da informação na empresa?
Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.
1 2 3 4 5
( ) ( ) ( ) ( ) ( )

16) A localização do Centro de Processamento de Dados (CPD) é adequada, considerando os riscos?
Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.
1 2 3 4 5
( ) ( ) ( ) ( ) ( )

17) Existe algum controle de acesso aos equipamentos que resguardam informações críticas da empresa?
Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.
1 2 3 4 5
( ) ( ) ( ) ( ) ( )

18) Existe um plano formal de *backup*?
Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.
1 2 3 4 5
( ) ( ) ( ) ( ) ( )

19) *Backups* são guardados em locais fisicamente seguro?
Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.
1 2 3 4 5
( ) ( ) ( ) ( ) ( )

20) A empresa leva consideração aos riscos e adota planos de contingência e de recuperação para casos de interrupções das atividades por falhas ou desastres?
Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.

1 2 3 4 5

( ) ( ) ( ) ( ) ( )

21) Está satisfeito(a) com o nível geral de formalização das regras de segurança da informação da empresa?
Utilize a escala de 1 a 5 para atribuir o grau de sua satisfação com este item. Onde 1 é totalmente insatisfeito e 5 é totalmente satisfeito.

1 2 3 4 5

( ) ( ) ( ) ( ) ( )