UNIVERSIDADE FEDERAL DO PARANÁ
DEPARTAMENTO DE CIÊNCIA E GESTÃO DA INFORMAÇÃO

ANGELA DA SILVA LOCH

A QUALIDADE DA INFORMAÇÃO NO AMBIENTE CORPORATIVO: UMA ANÁLISE CRÍTICA COM ÊNFASE NA SEGURANÇA DA INFORMAÇÃO À LUZ DA ABNT NBR ISO/IEC 17799/2005

CURITIBA
2015

ANGELA DA SILVA LOCH

A QUALIDADE DA INFORMAÇÃO NO AMBIENTE CORPORATIVO: UMA ANÁLISE CRÍTICA COM ÊNFASE NA SEGURANÇA DA INFORMAÇÃO À LUZ DA ABNT NBR ISO/IEC 17799/2005

Trabalho de conclusão de curso apresentado à Disciplina SIN119 – Pesquisa em Informação, do Curso de Gestão da Informação do Departamento de Ciência e Gestão da Informação do Setor de Ciências Sociais Aplicadas da Universidade Federal do Paraná.
Orientador: Prof. Dr. Mauro José Belli

CURITIBA
2015

Dedico este trabalho as pessoas que sempre estiveram ao meu lado em todos os momentos, aos meus pais.

AGRADECIMENTOS

Agradeço primeiramente a Deus por me confortar nos momentos mais difíceis e por mostrar que valia a pena ir em frente.

Aos meus pais, Pedro e Silmara, que dedicaram suas vidas para me proporcionar a melhor educação possível, além de todo o amor dado a mim, o qual me deu forças para seguir até o fim.

Aos meus amigos, Gilmar, Joceli e Silmara, que acompanharam minha jornada durante esses quatro anos, pelas experiências vividas em conjunto, pela companhia durante os longos finais de semana de estudo e pela amizade construída.

Ao meu orientador, professor Mauro, o qual me acolheu em um momento difícil e acreditou em meu trabalho. Agradeço também por toda a paciência que teve comigo, pela constante ajuda durante as orientações, pelo conhecimento transmitido e pelo grande exemplo de ser humano que é.

Agradeço a todos que acreditaram na minha capacidade de cumprir esse desafio e fizeram parte dessa etapa tão importante da minha vida.

“A menos que modifiquemos a nossa maneira de pensar, não seremos capazes de resolver os problemas causados pela forma como nos acostumamos a ver o mundo”.

(Albert Einstein)

RESUMO

Analisa os processos de gestão documental em uma unidade informacional na empresa X, de forma a identificar suas fragilidades em relação à como assegurar a qualidade da informação por meio da segurança da informação. Utiliza o estudo de caso e a pesquisa-ação como técnicas de pesquisa, a qual é caracterizada como exploratória e qualitativa e possui a entrevista estruturada como instrumento de coleta de dados. Faz uma comparação entre a realidade da unidade informacional com a norma ABNT NBR ISO/IEC 17799:2005 que define o código de prática para a gestão da segurança da informação. Conclui que existem pontos a serem melhorados no que diz respeito à segurança da informação e a visão de tê-la como um ativo estratégico para a empresa. Propõe ações a serem adotadas para obter melhores práticas na segurança da informação e assim garantir sua qualidade, das quais os resultados da implantação das mesmas poderão ser analisados em um futuro estudo.

Palavras-chave: Gestão da informação. Gestão de documentos. Qualidade da informação. Segurança da informação.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas.
BSI	*British Standard Institute.*
DVD	*Digital Versatile Disc*, ou Disco Digital Versátil.
GED	Gestão Eletrônica de Documentos.
ISO	*International Organization for Standardization*, ou Organização Internacional para Padronização.
ISMS	*Information security management system*, ou Sistema de Gestão de Segurança da Informação.
PDCA	*Plan, Do, Check e Act,* ou Planejar, Fazer, Checar e agir.
PLR	Participação de Lucros e Resultados.
PSI	Política de Segurança da Informação.
SGSI	Sistema de Gestão de Segurança da Informação.
VHS	*Vídeo Home System*, ou Sistema Doméstico de Vídeo.

SUMÁRIO

1 INTRODUÇÃO

A informação, independente do seu formato e suporte, é um patrimônio estratégico em qualquer empresa, além de ser um recurso de extrema importância, como Fontes (2012, p.1) assegura:

> A informação é um recurso essencial para toda organização, independente do seu porte e do seu segmento de atuação no mercado. É utilizando-a que processos organizacionais funcionam, as pessoas podem realizar suas atividades profissionais, a geração do conhecimento acontece e o compartilhamento desse conhecimento é realizado. Enfim, a informação possibilita que a organização atinja seus objetivos. (FONTES, 2012, p.1)

Além disso, a norma ABNT NBR ISO/IEC 17799/2005 afirma 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”.

Portanto, a segurança da informação objetiva preservar a qualidade da informação e também a forma de gestão, como afirma Blue Phoenix (2008): "A segurança da informação de uma empresa garante, em muitos casos, a continuidade de negócio, incrementa a estabilidade e permite que as pessoas e os bens estejam seguros de ameaças e perigos”, sendo que essas ameaças e perigos podem ocorrer de diferentes formas, como afirma Santo (2010, p.3):

> As ameaças a segurança podem ser de diferentes formas como incêndios, inundações, falhas de energia, sabotagem, vandalismo, roubo, e outros. O uso da Internet nas organizações trouxe novas vulnerabilidades na rede interna. Se não bastassem as preocupações existentes com espionagem comercial, fraudes, erros e acidentes, agora as empresas também precisam se preocupar com os hackers, invasões, vírus e outras ameaças que penetram através desta nova porta de acesso. (SANTO, 2010, p.3)

Nesse sentido, garantir a qualidade da informação, a gestão documental e a segurança dos documentos sigilosos é um desafio para qualquer organização, pois as mesmas estão inseridas em um ambiente tecnológico, em que a rede é de fácil acesso e está disponível para a maioria das pessoas, além dos problemas humanos da segurança, no qual pessoas podem fazer uso de informações das quais não possuem autorização para acesso, ou ainda divulgá-las sem permissão. Portanto, é de extrema importância manter um processo gerencial bem definido para garantir a

segurança da informação e de documentos que contenham informações de caráter sigiloso, pois sua divulgação ou acesso não autorizado pode gerar danos irreparáveis à mesma. Dessa forma, com a gestão de informações e de documentos, e com uma segurança da informação bem definida, segura e objetiva, busca-se evitar vazamentos, fraudes, espionagem, uso indevido e demais problemas que possam prejudicar a empresa.

Esse trabalho apresentado à disciplina de Pesquisa em Informação visa abordar o tema qualidade e segurança da informação na gestão de documentos e informações sigilosas, com foco na empresa X. Este relatório de pesquisa está estruturado em cinco partes: A primeira dedicada a introdução, que apresenta o problema de pesquisa, a justificativa e a contribuição, tanto para no âmbito pessoal, quanto para o âmbito acadêmico e para a empresa pesquisada. Em seguida, ainda como parte da introdução, descrevem-se os objetivos, geral e específicos. A literatura pertinente integra o segundo capítulo, abordando assuntos como: A informação como recurso estratégico; A qualidade da informação; A gestão da informação; A gestão de documentos; A classificação de informações e documentos segundo o grau de sigilo; e, a segurança da informação, esta que esta dividida em duas partes, normas e melhores práticas e, política de informação. Em seguida, a parte três, descreve a metodologia utilizada para a realização da pesquisa, seguida da análise e discussão dos resultados, e por fim, as considerações finais no capítulo cinco.

1.1 PROBLEMA DE PESQUISA

Como visto no tópico anterior, é imprescindível que se tenha um processo gerencial bem definido para garantir a qualidade da informação, pois a informação é um ativo da empresa. No caso da empresa X, o departamento estudado contêm documentos sigilosos, portanto para que a qualidade da informação desses documentos seja assegurada é necessária uma gestão da informação e de documentos, além de processos relacionados à segurança da informação, que pode ser analisada através de algumas dimensões, como afirma Fontes (2012, p.2): “O grau de disponibilidade, integridade e confidencialidade (sigilo) protegerá a

informação para que a organização operacionalize os seus negócios e atenda aos seus objetivos".

Partindo dessa premissa, levantam-se alguns questionamentos para que a qualidade da informação possa não ser protegida na empresa X: Os colaboradores podem desrespeitar a política de segurança da empresa; a política de segurança de informação pode possuir fragilidades; a informações e documentos podem estar armazenados de forma incorreta; o prazo de guarda pode não ser respeitado; Pessoas não autorizadas podem ter acesso às informações e documentos sigilosos; pode ocorrer erro humano ou catástrofes como incêndio ou inundação e a empresa não estar preparada.

Portanto, diante de tais questionamentos, o problema de pesquisa desse trabalho é: Dada a importância do acervo informacional da unidade observada, os processos de gestão documental da empresa X possuem fragilidades? Como tratá-las?

1.2 JUSTIFICATIVA

De acordo com a norma ABNT NBR ISO/IEC 17799/2005 a informação " é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida".

Ao passo que, segundo o Manual de Gestão de Documentos (2012, p.31) " os documentos podem ser classificados como sigilosos em razão de sua imprescindibilidade à segurança da sociedade, à defesa do Estado ou que possam":

> Pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional; Prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou os que tenham sido fornecidos em caráter sigiloso por outros Estados e organismos internacionais; Pôr em risco a vida, a segurança ou a saúde da população; Oferecer elevado risco à estabilidade financeira, econômica ou monetária do País; Prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas; Prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional; Pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou Comprometer atividades de inteligência, bem como de investigação ou fiscalização e mandamento, relacionadas com a prevenção

> ou repressão de infrações. (MANUAL DE GESTÃO DE DOCUMENTOS, 2012, p.31).

Nesse sentido, considera-se importante garantir a qualidade da informação nos documentos sigilosos, pois a falta de um processo que assegure sua confidencialidade, disponibilidade e a integridade acarreta riscos à segurança da própria empresa, a qual pode ocorrer por meio de espionagem, sabotagem, dissimulação e outras ações que afetem a qualidade de informações que subsidiam a tomada de decisão, a qual norteia o futuro da empresa e de seus colaboradores, sendo que a segurança das informações e documentos sigilosos também garantem o segredo do negócio da organização e sua competitividade no mercado.

A realização desta pesquisa possibilita auxiliar os responsáveis pela qualidade e segurança das informações dos documentos sigilosos nos procedimentos e cuidados a serem tomados para a segurança informacional no departamento de documentos e informações corporativas da empresa X, demonstrando que é primordial reconhecer o valor da informação e utilizá-la da melhor forma estratégica possível para alcance de bons resultados na sua proteção. Não existiu a pretensão de assegurar total sucesso, mas sim, de reduzir as possibilidades de risco, vazamento e perda.

A motivação da pesquisa veio por meio do interesse pessoal da pesquisadora tanto no tema de documentação quanto em segurança da informação, pois a mesma já trabalhou na biblioteca da empresa pesquisada e se identifica com o assunto. Além de poder colaborar com uma empresa renomada, há interesse de posteriormente fazer uma pós-graduação na área pesquisada. Poder contribuir com um dos possíveis campos de atuação do gestor da informação é um motivo de incentivo para o desenvolvimento da pesquisa, além de poder incentivar futuros estudantes de gestão da informação ou até mesmo pessoas formadas a realizarem pesquisas na área. Também é interessante a oportunidade de poder correlacionar conhecimentos adquiridos a partir de algumas disciplinas do curso de Gestão da Informação, tais como: Gestão de Documentos, Tópicos em Gestão de Documentos, Segurança da Informação, Políticas de Informação e Tópicos em Gestão da Informação.

1.3 OBJETIVOS

Este projeto é caracterizado pelo objetivo geral e pelos objetivos específicos, descritos na sequência.

1.3.1 Objetivo geral

Investigar como assegurar a qualidade da informação dos documentos sigilosos da empresa X, tendo como referência as normativas de segurança da informação.

1.3.2 Objetivos específicos

- Identificar os processos relacionados com as informações do setor de guarda de documentos na unidade;
- Identificar os cuidados, quanto ao acesso e a guarda, que a organização possui em relação aos documentos e informações sigilosas;
- Identificar as boas práticas e os procedimentos adotados para garantir a segurança da informação;
- Identificar possíveis fragilidades de segurança da informação na organização; e,
- Identificar procedimentos a serem adotados para objetivar a melhoria da segurança da informação.

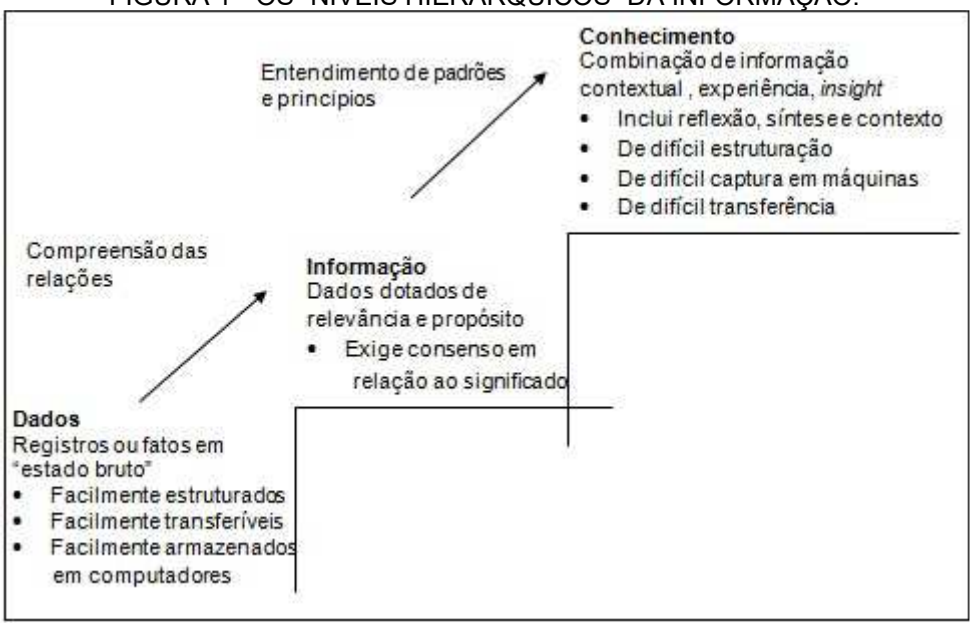
2 LITERATURA PERTINENTE

A revisão de literatura visa orientar a pesquisa, fornecendo embasamento de autores da área envolvida para a execução do projeto. Apresenta-se uma contextualização para o tema da pesquisa sobre gestão de documentos e informações sigilosas no âmbito organizacional, sobre segurança da informação e alguns subtemas que dão suporte para o mesmo.

2.1 A INFORMAÇÃO COMO RECURSO ESTRATÉGICO

A informação difere-se de dado e de conhecimento em relação ao grau de complexidade e relevância como Beal (2004, p.11) afirma: “Transformam-se dados em informações agregando-se valor a eles; e informação em conhecimento acrescentando a elas vários outros elementos”. Beal (2004, p.12) criou um esquema para melhor representar essa diferenciação entre dado, informação e conhecimento, conforme mostra a figura 1:

FIGURA 1 - OS “NÍVEIS HIERÁRQUICOS” DA INFORMAÇÃO.



Fonte: Beal (2004)

Segundo Silva (2000, p.7) ainda pode-se definir informação como:

> Um conjunto estruturado de representações mentais codificadas (símbolos significantes) socialmente contextualizadas e passíveis de serem registradas num qualquer suporte material (papel, filme, banda magnética, disco, compacto, etc.). (SILVA, 2000, p.7)

Já McGarry (1999, pg. 1), afirma que a informação pode ser “a matéria prima da qual se extrai o conhecimento” e entre outras avaliações também aponta que a informação é algo que reduz as incertezas em determinado momento e que realiza uma troca com o mundo exterior não sendo passivamente recebido. Ou seja, a informação é uma criação essencialmente humana e é o principal e mais valioso ativo dentro de qualquer organização. Portanto, é preciso administrar e garantir sua segurança por meio da tecnologia e das pessoas.

De acordo com Davenport (1998, p.67) há pelo menos quatro bons motivos para pensar estrategicamente a informação:

> • Os ambientes informacionais, na maioria das empresas, são um desastre;
> • Os recursos informacionais sempre podem ser mais bem alocados;
> • As estratégias da informação ajudam as empresas a se adaptar às mudanças; e,
> • As estratégicas informacionais tornam a informação mais significativa. (DAVENPORT, 1998, p.67)

Almeida e Lesca (1994, p.67) ainda afirmam que a informação de qualidade é um elemento importante na tomada de decisões pertinentes, quando a mesma é apresentada no momento adequado, ou seja, pode ser utilizada para reduzir a incerteza no referido processo. Já Beal (2004, p.75) ressalta a importância do acesso às informações adequadas para a tomada de decisão:

> Sem o acesso a informações adequadas a respeito das variáveis internas e do ambiente onde a organização se insere, os responsáveis pela elaboração da estratégia não têm como identificar os pontos fortes e fracos, as ameaças e oportunidades, os valores corporativos e toda a variedade de fatores que devem ser considerados na identificação de alternativas e na tomada de decisões estratégicas. (BEAL, 2004, p.75)

Nesse sentido, para que as empresas tenham um aproveitamento e uso adequado de suas informações é necessário que tenham informações relevantes e as transformem em instrumento de trabalho, utilizando-as para uma tomada de decisão assertiva e consequentemente transformando-as em inteligência competitiva. Desta forma, a competitividade de uma empresa seria proporcional à sua capacidade de obter informação, processá-la e disponibilizá-la de forma rápida e segura.

Para garantir que a informação seja utilizada da melhor forma possível, é necessário se preocupar com a sua qualidade, como se pode ver abaixo.

2.2 A QUALIDADE DA INFORMAÇÃO

A segurança da informação tem como objetivo garantir a qualidade da informação, e para isso existem dimensões da qualidade da informação, ou seja, características que podem ser utilizadas para análise e mensuração da sua qualidade. Porém há várias formas de categorizar essas dimensões da qualidade da informação, que segundo Sordi (2008, p.31)

> Podem ser em menor ou maior número, a depender do nível de generalização ou especialização utilizado ao se definir cada uma delas, e além do nível de decomposição definido, deve-se lembrar de que há muitos termos sinônimos para uma mesma dimensão. (SORDI, 2008, p.31)

Ainda, segundo este autor, existem quinze dimensões para analisar a qualidade da informação (quadro 1), que são:

QUADRO 1 – DIMENSÕES DA QUALIDADE DA INFORMAÇÃO

Dimensão	Definição
Abrangência/escopo da informação	Assegura que a quantidade de informação está na medida certa e suficiente às necessidades de seus leitores.
Integridade da informação	Assegura que não haja alterações ilegais do conteúdo da informação.
Acurácia/veracidade da informação	Refere-se à informação legítima, válida, constituindo uma análise fiel os fatos que representa.
Confidencialidade/privacidade da informação	Refere-se a evitar acessos não autorizados.
Disponibilidade da informação	A informação deve estar disponível as pessoas que tem direito.
Atualidade/temporalidade da informação	A informação deve ser atualizada.
Ineditismo/raridade da informação	Diz respeito à quão rara é a informação.
Contextualização da informação	Refere-se aos aspectos e componentes da informação, no sentido de serem significativos e atrativos ao público-alvo.
Precisão da informação	É definida como o nível de detalhamento ideal para seu pronto uso.
Confiabilidade da informação	Corresponde a informação à qual os usuários conferem crédito.
Originalidade da informação	Deve-se considerar o distanciamento da fonte geradora, atribuindo-se maior valor quanto mais próximo estiver da fonte original.
Existência da informação	Abrange a condição tácita ou explícita da informação, ou seja, considera-se tanto a informação de posse das pessoas, ainda não estruturadas ou estruturadas e materializadas, independente do formato e mídia utilizados.
Pertinência/Agregação de valor da informação	Implica o potencial da informação em servir e apoiar as atividades de determinado público-alvo.
Identidade da informação	Refere-se ao nome da informação, que interfere na busca e acesso da mesma.
Audiência da informação	A audiência deve ser mensurada a fim de prover subsídios a sua correta gestão.

Fonte: A autora (2015) com base em Sordi (2008)

Entretanto, na discussão sobre os critérios de qualidade da informação não há um consenso, como opina Schewuchow *apud* Paim, Nehmy e Guimarães (1996, p. 114): “qualquer critério de avaliação da qualidade da informação é, por natureza, subjetivo. É praticamente impossível encontrar um critério de mensuração simples,

preciso e satisfatório".

Ademais, alguns métodos para assegurar a qualidade da informação na organização podem ser a gestão da informação, gestão de documentos e a segurança da informação, os quais serão abordados a seguir.

2.3 A GESTÃO DA INFORMAÇÃO

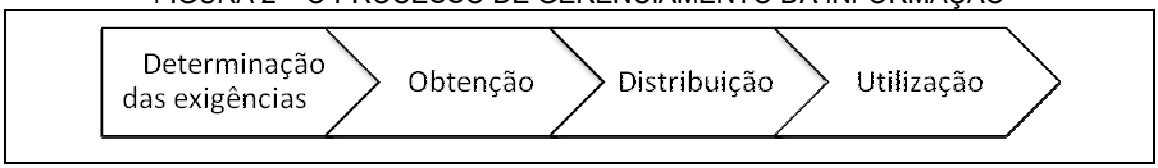
Como visto no tópico acima, a informação é um recurso estratégico importante para qualquer organização. Nesse modo, para que haja um gerenciamento adequado, segundo Alvarenga Neto (2008, p. 41) é preciso "obter a informação correta na hora certa, na forma/meio correto e endereçá-la à pessoa certa", ou seja, a informação deve estar impreterivelmente conectada com a segurança da informação, pois não pode ser acessada ou usada na hora errada, nem da forma errada e nem pela pessoa errada, pois isso poderia ocasionar problemas para a organização.

De acordo com Valentim (2008, p.1) a gestão da informação pode ser entendida como:

> Um conjunto de atividades que visa: obter um diagnóstico das necessidades informacionais; mapear os fluxos formais de informação nos vários setores da organização; prospectar, coletar, filtrar, monitorar, disseminar informações de diferentes naturezas; e elaborar serviços e produtos informacionais, objetivando apoiar o desenvolvimento das atividades/tarefas cotidianas e o processo decisório nesses ambientes (VALENTIM, 2008, p.1).

Nesse mesmo sentido, Davenport (1998, p.175) afirma que a gestão da informação é "a chave para o sucesso de qualquer organização, pois possibilita uma correta orientação dos processos e maneira que devem ser realizados". Dessa forma, o próprio autor afirma que alguns passos devem ser seguidos (figura 2) para o efetivo gerenciamento da informação: "definição das necessidades de informação, passar pela coleta, armazenagem, distribuição, recebimento e uso das informações".

FIGURA 2 – O PROCESSO DE GERENCIAMENTO DA INFORMAÇÃO



Fonte: Davenport, 1998

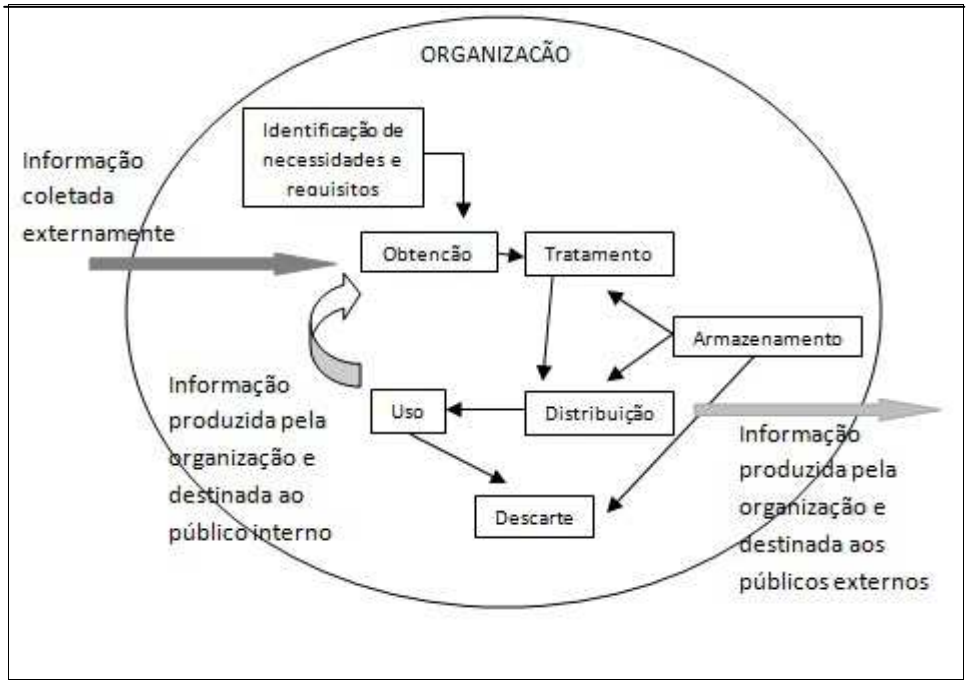
A primeira etapa (determinação das exigências), é a fase em que se devem definir as informações necessárias a determinado processo. A segunda etapa (obtenção), deve ser ininterrupta e consiste nas seguintes atividades: exploração do ambiente informacional, classificação da informação em uma estrutura pertinente, formatação e estruturação das informações. A terceira etapa (distribuição), a organização deve definir uma estratégia, podendo optar tanto pela divulgação às pessoas autorizadas, partindo da premissa de que as pessoas não conhecem o que não sabem, como pela disponibilização. Na quarta e última etapa (utilização), o uso da informação pode ser institucionalizado em uma organização, através do mecanismo de avaliação de desempenho e de recompensas e punições pessoais.

De maneira similar, Beuren (2000, p.68) afirma que circula um extenso fluxo de informações nos mais variados ambientes de trabalho, exigindo que estas informações sejam adequadamente gerenciadas quanto a sua utilidade e importância, visando evitar descartes ou acúmulos desnecessários que gerem problemas durante a tomada de decisão. A sequência de tarefas do processo de gestão da informação são, segundo Beuren (2000, p.68), equivalentes a:

> Identificação de necessidades e requisitos de informação, coleta/entrada de informação, classificação e armazenamento da informação, tratamento e apresentação da informação, desenvolvimento de produtos e serviços de informação, distribuição e disseminação de informação, análise e uso da informação. (BEUREN, 2000, p. 68).

Segundo Beal (2004, p.29) a informação (não estruturada, estruturada em papel ou estruturada em computadores) percorre um fluxo dentro das organizações que pode ser representado pela figura 3, a seguir:

FIGURA 3 – FLUXO DA INFORMAÇÃO NAS ORGANIZAÇÕES



Fonte: Beal, 2004

Nesse fluxo de informação aparece o descarte, o qual segundo Beal (2004, p.31) é:

> Quando uma informação se torna obsoleta ou perde a utilidade para a organização, ela deve ser objeto de processos de descarte que obedeçam a normas legais, políticas operacionais e exigências internas. (BEAL, 2004, p.31).

A exclusão de dados e informações desnecessárias melhora o processo de gestão da informação, segundo Beal (2004, p.32) nos seguintes aspectos:

> Economizando recursos de armazenamento, aumentando a rapidez e eficiência na localização da informação necessária, melhorando a visibilidade dos recursos informacionais importantes, etc. (BEAL, 2004, p.32).

2.4 A GESTÃO DE DOCUMENTOS

De acordo com o Dicionário Brasileiro de Terminologia Arquivística (2005, p.73) documento é a “unidade de registro de informações, qualquer que seja o suporte ou formato”.

Segundo Bellotto (2004, p.35) outra definição para documento é “qualquer elemento gráfico, iconográfico, plástico ou fônico pelo qual o homem se expressa”. Ou ainda segundo Paes (2007, p. 26) documento é “um registro de uma informação independentemente da natureza do suporte que a contém”.

Com o passar dos anos surgiu a necessidade de administrar os documentos, e para esse processo deram o nome de gestão de documentos, que segundo Rodrigues (2007, p.6) se caracteriza como:

> Um conjunto de procedimentos aplicados para controlar os documentos arquivísticos durante todo o ciclo de que incide sobre todo o seu ciclo de vida, incidindo sobre o momento da produção e acumulação na primeira e segunda idade, ou seja, no corrente e intermediária. A partir da identificação das características que apresenta a tipologia documental, são definidas as regras para sua formatação e utilização, tramitação, avaliação e classificação. (RODRIGUES, 2007, p.6).

Nesse sentido, um dos métodos utilizados para transformar a informação em recurso estratégico é o processo identificado como gestão de documentos, que pode ser definido pela Legislação Norte Americana *apud* Jardim (1987, p. 35) como:

> O planejamento, o controle, a direção, a organização, a capacitação, a promoção e outras atividades gerenciais relacionadas com a criação de documentos, sua manutenção, uso e eliminação, incluindo o manejo de correspondência, formulários, diretrizes, informes, documentos informáticos, microformas, recuperação de informação, fichários, correios, documentos vitais, equipamentos e materiais, máquinas reprográficas, técnicas de automação e elaboração de dados, preservação de centros de arquivamentos intermediários ou outras instalações para armazenagem. (Legislação Norte Americana *apud* Jardim, 1987, p. 35).

Em contrapartida o artigo 3º da Lei 8.159 (2006, p.6) considera gestão de documentos como “um conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento dos documentos em fase corrente e intermediária, visando a sua eliminação ou seu recolhimento para a guarda permanente”.

Ou ainda, segundo Rocha *et al* (2005, p.5) :

> As atividades de gestão de documentos não se restringem a evitar a produção de documentos desnecessários e a estabelecer arquivos (garantindo a organização e a preservação dos documentos), mas abrange todas as operações referentes à produção (quais são os suportes com validade, como o documento deve ser estruturado, incluindo código de classificação de assunto), à tramitação, ao uso (consulta e empréstimo), à avaliação (aplicação da tabela de temporalidade e destinação) e ao arquivamento (guarda e armazenamento). (ROCHA *et* al, 2005, p.5).

Portanto, a gestão documental garante o efetivo controle do documento, desde sua produção até sua destinação final, que seria a eliminação ou guarda permanente; Esse processo permite a localização dos documentos e acesso rápido às informações. Portanto, é importante assegurar o cumprimento de todas as tarefas em todas as fases do documento: corrente, intermediária e permanente, como mostra o quadro a seguir:

QUADRO 2 - FASES DO DOCUMENTO

1ª idade Fase Corrente	Documentos vigentes e frequentemente consultados.	Arquivo Corrente
2ª idade Fase Intermediária	Final de vigência. Aguardam prazos de precisão e precaução, raramente são consultados e aguardam destinação final: eliminação ou guarda permanente.	Arquivo Intermediário
3ª idade Fase Permanente	Documentos que perderam a vigência administrativa, porém são providos de valor secundário ou histórico-cultural.	Arquivo Permanente ou Histórico

Fonte: BERNARDES; DELATORRE (2008)

Nesse sentido, Sá (2014, p.269) afirma que:

> A gestão de documentos e registros como prática empresarial proporciona ganhos significativos às organizações no que tange à rastreabilidade, manutenção e guarda de documentos necessários, bem como à tomada de decisão, redução de tempo na recuperação das informações para atendimento às partes interessadas (clientes, acionistas, colaboradores), agilidade nos processos de fiscalizações, perícias, auditorias, demandas jurídicas, atendimento à legislação e *compliance*, preservação da memória organizacional, suporte à transparência das atividades e controle do fluxo de documentos. (SÁ, 2014, p.269)

Ou seja, se a gestão de documentos for bem definida e aplicada de maneira correta, a organização pode tê-la como um diferencial competitivo.

2.4.1 Tabela de temporalidade

Em relação ao ciclo de vida dos documentos, o Manual de Gestão de Documentos do Estado do Paraná (2007, p. 4) afirma que a tabela de temporalidade é o “registro esquemático do ciclo de vida dos documentos, determinando os prazos de guarda no arquivo corrente ou setorial, sua transferência para o arquivo intermediário ou geral, a eliminação ou recolhimento”, sendo que mesma deve ser utilizada no momento de classificação e avaliação da documentação. E, ainda de acordo com o Manual de Gestão de Documentos do Estado do Paraná (2007, p.11), a tabela de temporalidade é: “um instrumento da gestão documental e passível de alterações na medida em que a produção de documentos se altera, devido a mudanças sociais, administrativas e jurídicas”.

Partindo da mesma ideia, o Conselho Nacional de Arquivos (2001, p.43) conceitua a tabela da temporalidade como:

> Um instrumento arquivístico resultante de avaliação, que tem por objetivos definir prazos de guarda e destinação de documentos, com vista a garantir o acesso à informação a quantos dela necessitem. Sua estrutura básica deve necessariamente contemplar os conjuntos documentais produzidos e recebidos por uma instituição no exercício de suas atividades, os prazos de guarda nas fases corrente e intermediária, a destinação final – eliminação ou guarda permanente –, além de um campo para observações necessárias à sua compreensão e aplicação. (CONSELHO NACIONAL DE ARQUIVOS, 2001, p.43).

O Manual de Gestão de Documentos do Estado do Paraná (2007, p.11) sugere que a tabela de temporalidade deve ser usada da seguinte forma:

> •Verificar se os documentos estão classificados de acordo com os assuntos do Código de Classificação de Documentos;
> •Documentos que se referem a dois ou mais assuntos, deverão ser classificados e agrupados ao conjunto documental (dossiê, processo ou pasta) que possui maior prazo de arquivamento ou que tenha sido destinado à guarda permanente;
> •O prazo de arquivamento deve se contar a partir do primeiro dia útil do exercício seguinte ao do arquivamento do documento, exceto aqueles que originam despesas, cujo prazo de arquivamento é contado a partir da aprovação das contas pelo Tribunal de Contas;
> •Eliminar as cópias e vias, quando o documento original estiver no conjunto documental (dossiê, processo ou pasta);
> •Proceder ao registro dos documentos a serem eliminados;
> •Elaborar listagem dos documentos destinados à transferência para o arquivo intermediário do órgão ou entidade, ou para a Divisão de Documentação Intermediária do Arquivo Público do Estado; (MANUAL DE GESTÃO DE DOCUMENTOS DO ESTADO DO PARANÁ, 2007, p.11).

Além disso, se usada de forma correta, a tabela de temporalidade pode trazer inúmeros benefícios, que segundo Badke (2004 *apud* Delgadillo *et al*, 2006, p. 82) são:

> Segurança no descarte, baseada na temporalidade do documento; garantia de expurgar documentos somente quando ocorrer uma análise prévia por profissional ou grupo que tenha investidura técnica mesmo hierárquica na tomada de decisão; redução do volume de documentos presentes nos setores, pelo correto gerenciamento do arquivamento; eliminação de multiplicidade de cópias presentes nos arquivos em todo o processo; eliminação de desperdício. (BADKE, 2004 *apud* DELGADILLO *et al*, 2006, p. 82)

2.5 A CLASSIFICAÇÃO DE INFORMAÇÕES E DOCUMENTOS SEGUNDO O GRAU DE SIGILO

Os documentos podem ser analisados com relação à sua segurança, podendo ser considerados ostensivos ou sigilosos. O Dicionário Brasileiro de Terminologia Arquivística (2005, p.79) define documento sigiloso como “documento que pela natureza de seu conteúdo sofre restrição de acesso”.

Existem legislações que se referem à classificação da informação, a Lei 12.527/2011 de Acesso à Informação, a qual obriga órgãos públicos federais, estaduais e municipais a oferecer informações relacionadas às suas atividades a qualquer pessoa que solicitar os dados, e também o Decreto n. 4553, que dispõe sobre

a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal.

A informação considerada sigilosa, segundo a Lei 12.527/2011 de Acesso a Informação, é “aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado”.

Quando os documentos são considerados sigilosos, a legislação estabelece quatro graus de sigilo a ser atribuído a cada um, o ultrassecreto, o secreto, o confidencial e o reservado, como apresentado pelo Decreto n. 79.099/1977 que classifica os documentos sigilosos da seguinte forma:

> § 1º O grau de sigilo ULTRA-SECRETO será atribuído aos assuntos que requeiram excepcionais medidas de segurança, cujo teor ou características só devam ser do conhecimento de pessoas intimamente ligadas ao seu estudo e ou manuseio.
> § 2º O grau de sigilo SECRETO será atribuído aos assuntos que requeiram elevadas medidas de segurança, cujo teor ou características possam ser do conhecimento de pessoas que, sem estarem intimamente ligadas ao seu estudo e ou manuseio, sejam autorizadas a deles tomarem conhecimento, funcionalmente.
> § 3º O grau de sigilo CONFIDENCIAL será atribuído aos assuntos cujo conhecimento por pessoa não autorizada possa ser prejudicial aos interesses nacionais, a indivíduos ou entidades ou criar embaraço administrativo.
> § 4º O grau de sigilo RESERVADO será atribuído aos assuntos que não devam ser do conhecimento do público em geral. (BRASIL, 1977).

De acordo com o Decreto n. 4553 de 27 de dezembro de 2002, cada classificação de grau de sigilo possui um prazo de guarda diferente a partir da sua produção: O ultra-secreto deve ser guardado pelo prazo de trinta anos; o secreto deve ser guardado por vinte anos; o confidencial deve ser guardado por dez anos; e o reservado deve ser guardado no período de cinco anos. O decreto n.4.553 também determina que esses prazos de guarda podem ser prorrogados por uma única vez, pelo mesmo período, desde que se tenha autorização do órgão competente.

Já a informação, de acordo com o Art. 24 da Lei 12.527/2011, pode ser classificada de três maneiras: ultrassecreta, secreta e reservada. Para a classificação da informação em grau de sigilo, segundo o Art. 27 do Decreto n. 7.724/2012 deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, devendo ser considerado: “a gravidade do risco ou

dano à segurança da sociedade e do Estado e o prazo máximo de classificação em grau de sigilo ou o evento que defina seu termo final". Vale ressaltar que a Lei 12.527/2011 aborda o direito do indivíduo à privacidade no Art. 31 afirmando que "o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais".

Os prazos máximos de restrição de acesso à informação vigoram a partir da data de sua produção e de acordo com sua classificação são os seguintes segundo o § 1º do Art. 24 da Lei 12.527/2011: "ultrassecreta: 25 (vinte e cinco) anos; secreta: 15 (quinze) anos; e reservada: 5 (cinco) anos"

Portanto, considerando os graus de sigilo, tanto da informação quanto dos documentos, é de responsabilidade da organização trabalhar com eles de maneira eficaz, visando coibir ações invasivas, ou seja, investindo em segurança da informação.

2.6 A SEGURANÇA DA INFORMAÇÃO

Segundo Beal (2005, p.1), a segurança da informação pode ser entendida como "o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade". Porém além de se preocupar com esses três aspectos de segurança da informação é necessário ficar atento ao processo de comunicação da empresa, como Beal (2005, p.2) afirma:

> Problemas como a alteração fraudulenta de documentos em trânsito e disputas sobre a origem de uma comunicação ou o recebimento de uma informação transmitida precisam ser equacionados, levando à necessidade de estabelecer alguns objetivos adicionais relativos à segurança da comunicação. (BEAL, 2005, p.2)

Portanto, os profissionais envolvidos com a gestão de informações e de documentos sigilosos, além de preocupar-se com a guarda e com a preservação dos mesmos, também devem se preocupar com o controle e acesso aos mesmos, sempre buscando formas e procedimentos que garantam os princípios da autenticidade, confiabilidade, integridade e disponibilidade, além de prevenir

possíveis ameaças, independente do suporte do documento ser físico ou virtual. Esses princípios, segundo Sfreddo e Flores (2012, p.163) podem ser definidos da seguinte forma:

> A confidencialidade garante que as informações sejam acessíveis somente a pessoas que possuam permissão para acesso na instituição; a integridade proporciona a proteção das informações contra modificações, adulterações ou fraudes; e a disponibilidade assegura que os usuários autorizados tenham acesso às informações, quando requisitadas, e elas se mantenham protegidas e não se tornem indisponíveis. (SFREDDO; FLORES, 2012, p.163)

Nesse sentido, de acordo com Sfreddo e Flores (2012, p.164):

> As instituições devem ter a responsabilidade e o interesse pelo tratamento das informações, conscientes de que esses princípios que norteiam suas ações para a segurança ajudam a proteger as informações institucionais. (SFREDDO E FLORES, 2012, p.164).

Dessa forma, é importante não se preocupar apenas com as informações que estão armazenadas em meios eletrônicos, pois há razões para que seja feita a proteção de informações e documentos sigilosos que não estejam armazenados em computadores, como Beal (2005, p.9) afirma:

> Toda organização dispões de dados, informações e conhecimentos valiosos que não estão armazenados em sistemas informatizados ou meios eletrônicos, seja pela falta de tempo ou interesse do detentor da informação registrá-la, seja por estar temporariamente disponível apenas num documento em papel, microfilme ou outro tipo de mídia. Alguns documentos têm sua validade vinculada ao suporte físico em papel, precisando ser protegidos fisicamente mesmo quando existem cópias eletrônicas dos mesmos. Informações armazenadas em computadores podem ser impressas e ter sua confidencialidade comprometida pela falta de manuseio adequado de suas versões em papel. (BEAL, 2005, p.9)

Beal (2005, p.10) ainda afirma que:

> A fim de manter os ativos de informação protegidos contra perda, furto e alteração, divulgação ou destruição indevidas, além de outros problemas que podem alterá-los, as organizações precisam adotar controles de segurança – medidas de proteção que abrangem uma grande diversidade de iniciativas, indo dos cuidados com os processos de comunicação â segurança de pessoas, mídias e componentes de TI. (BEAL, 2005, p.10)

2.6.1 Melhores práticas

Em 1995, o *British Standard Institute* (BSI) criou a norma BS 7799, que trata da gestão da segurança da informação, sendo dividida em três partes: A primeira refere-se um código de prática para gestão da segurança da informação, a segunda discorre sobre as especificações e guia para uso, ou seja, fornece diretrizes para obter um eficiente sistema de gerenciamento em segurança da informação e, a terceira parte, concerne ao gerenciamento e análise de riscos. No ano de 2000 a parte 1 da BS 7799 tornou-se a norma oficial da *International Organization for Standardization* (ISO) como o seu padrão sob o código ISO/IEC 17799, e logo em seguida, em 2001, o Brasil adotou esta norma ISO como seu padrão através da Associação Brasileira de Normas Técnicas (ABNT) com a nomenclatura ABNT NBR ISO/IEC 17799. Em 2005 a ABNT NBR ISO/IEC 17799 foi revisada e então foram criadas as normas da família 27000.

A ABNT NBR ISO/IEC 27001:2006, que se refere à parte 2 da BS 7799, aborda técnicas de segurança para o Sistema de Gestão de Segurança da Informação (SGSI), tendo como objetivo principal “especificar os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização”. Essa norma descreve uma orientação para a existência de um SGSI considerando o modelo *Plan, Do, Check, Act* (PDCA), o qual é aplicado para estruturar todos os processos do SGSI, como mostra o quadro 3:

QUADRO 3 – ATIVIDADES DO PDCA

Plan (planejar) (estabelecer o SGSI)	Estabelecer política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
Do (fazer) (implementar e operar o SGSI)	Implementar e operar política, controles, processos e procedimentos do SGSI.
Check (checar) (monitorar e analisar criticamente o SGSI)	Avaliar e, quando aplicável, medir o desempenho de um processo frente a política, objetivos e experiência prática do SGSI e apresentar os resultados para análise crítica pela direção.
Act (agir) (manter e melhorar o SGSI)	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Fonte: ABNT NBR ISO/IEC 27001

Em relação aos princípios de segurança da informação, as organizações podem seguir a ABNT NBR ISO/IEC 27001 e a ABNT NBR ISO/IEC 17799/2005, que trata sobre a Tecnologia da Informação – Código de prática para a gestão da segurança da informação. Essa norma se divide em dez áreas de controle, ou seja, dez ações/práticas que, se adotadas, a organização pode alcançar melhor gestão da segurança da informação. As dez práticas podem ser listadas, conforme mostra o quadro a seguir:

QUADRO 4 – AS DEZ PRÁTICAS PARA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Prática	Descrição
Política de segurança	Orientações e apoio para a implementação e manutenção de uma política de segurança.
Segurança organizacional	Recomendações para prover o estabelecimento de uma infraestrutura para planejar e controlar a segurança da informação na organização.
Classificação e controle dos ativos de informação	Orientações sobre a realização de inventários dos ativos informacionais e atribuição de responsabilidades para manter a proteção adequada.
Segurança em pessoas	Orientações para a redução de riscos de erro humano, roubo fraude e uso indevido de instalações.
Segurança física e do ambiente	Orientações para prevenir acesso não autorizado, dano ou interferência dos recursos e instalações de processamento de informações.
Gerenciamento das operações e comunicações:	Orientações com vistas a garantir a operação correta e segura dos recursos de processamento da informação.
Controle de acesso	Orientações para o monitoramento e o controle de acesso à informação;
Desenvolvimento e manutenção de sistemas	Orientações para o uso de controles de segurança em todas as etapas do processo.
Gestão da continuidade do negócio	Orientações para que a organização neutralize as interrupções às atividades do negócio e proteção dos processos críticos contra falhas ou desastres.
Conformidade	Orientações para assegurar a conformidade dos sistemas com leis, regulamentações, políticas e normas internas de segurança.

Fonte: A autora (2015) com base na ABNT NBR ISO/IEC 17799:2005.

2.6.2 Política de segurança da informação

Uma forma da organização obter uma segurança da informação eficaz é criando uma política de segurança da informação (PSI), que segundo Beal (2005, p.43) é:

> O documento que registra os princípios e as diretrizes de segurança adotados pela organização, a serem observados por todos os seus integrantes e colaboradores e aplicados a todos os sistemas de informação e processos corporativos. (BEAL, 2005, p.43)

Do mesmo modo, Sêmola (2014, p. 105) aponta que:

> Com o propósito de fornecer orientação e apoio às ações de gestão de segurança, a política tem um papel fundamental e, guardadas as devidas proporções, tem importância similar à Constituição federal para um país. (SÊMOLA, 2014, p.105)

O autor ainda coloca que a política de informação:

> Estabelece padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a empresa; portanto, a política deve ser personalizada. (SÊMOLA, 2014, p.105)

.

Ainda no sentido da necessidade da política de segurança da informação Fontes (2012, p. 12) afirma que:

> É estrutural que a organização tenha uma política de segurança da informação para que o processo de proteção da informação possa ser elaborado, implementado e mantido. Essa política (ou conjunto de políticas) definirá as diretrizes, os limites e o direcionamento que a organização deseja para os controles que serão implantados na proteção da sua informação. (FONTES, 2012, p.12)

Segundo Araújo e Ferreira (2008, p. 37) a política de segurança da informação:

> Deve ser criada antes da ocorrência de problemas com a segurança, ou depois, para evitar reincidências. Ela é uma ferramenta tanto para prevenir problemas legais como para documentar a aderência ao processo de controle de qualidade. (ARAUJO; FERREIRA, 2008, p.37)

De acordo com Beal (2005, p.44) independente da organização existem alguns aspectos que devem ser levados em consideração na PSI, que são: Organização da segurança; Classificação e controle dos ativos de informação;

Aspectos humanos da segurança; Segurança do ambiente físico; Segurança do ambiente lógico; Segurança das comunicações; Prevenção e tratamento de incidentes; Desenvolvimento/aquisição, implantação e manutenção de sistemas; Gestão da continuidade do negócio; e, conformidade.

Nesse sentido, de acordo com a Norma Nacional de Segurança de Informações ABNT NBR ISO/IEC 17799/2005 (p.x), a segurança da informação é:

> Obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. (ABNT NBR ISO/IEC 17799, 2005, p.x)

E ainda segundo a norma, tais controles:

> Precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. (ABNT NBR/ISO/IEC 17799, 2005, p.x)

3 METODOLOGIA

A pesquisa em questão, quanto ao tipo, caracteriza-se como uma investigação exploratória, que segundo Gil (1988, p.45) ocorre quando o objetivo é proporcionar maior familiaridade com o problema com vistas a torná-lo explícito ou construir hipóteses. Ainda segundo Bertucci (2008, p.49) “quando se inicia esse tipo de trabalho, o pesquisador frequentemente parte de uma elaborada revisão de literatura (...)”.

Essa pesquisa não se enquadra exatamente em uma única técnica, ela fica entre o estudo de caso e a pesquisa-ação, pois estudo de caso segundo Godoy (1995, p.60) é “um tipo de pesquisa cujo objetivo é uma unidade que se analisa profundamente e visa ao exame detalhado de um ambiente, de um simples sujeito ou de uma situação em particular”. Bertucci (2008, p.53) complementa, afirmando que, em relação à natureza, os estudos de caso são:

> De natureza eminentemente qualitativa e valem-se preferencialmente de dados coletados pelo pesquisador por meio de consulta a fontes primárias e/ou secundárias, de entrevistas e da própria observação do fenômeno. Isso não significa, contudo, que não se possam utilizar dados quantitativos em estudos de caso. (BERTUCCI, 2008, p.53)

Já em contrapartida, segundo Thiollent (1997 *apud* Kraft *et al*, 2007, p.1) a pesquisa-ação é:

> Um tipo de pesquisa social com base empírica que é concebida e realizada em estreita associação com uma ação ou com a resolução de um problema coletivo e na qual pesquisadores e participantes representativos da situação ou do problema estão envolvidos de modo cooperativo ou participativo. (THIOLLENT, 1997 *apud* KRAFT *et a*l, 2007, p.1)

Ainda segundo Kraft *et al* (2007, p.1) a pesquisa-ação é “um método de condução de pesquisa aplicada, orientada para elaboração e diagnósticos, identificação de problemas e busca de soluções”.

A pesquisa é de natureza qualitativa, tendo como objetivo investigar como assegurar a qualidade da informação dos documentos sigilosos da empresa X, de forma a apontar as questões relevantes e propor alternativas que possam extinguir ou amenizar algum problema ou fragilidade identificados.

A coleta de dados foi realizada por meio de entrevistas com pessoas que estão diretamente envolvidas com a gestão de documentos sigilosos da empresa X. Segundo Bertucci (2008, p.63) a entrevista consiste em “uma indagação direta, realizada no mínimo entre duas pessoas, com o objetivo de conhecer a perspectiva do entrevistado sobre um ou diversos assuntos”. A entrevista foi de caráter estruturado, ou seja, com roteiro previamente estabelecido.

Sendo assim, pode-se definir as etapas da pesquisa na empresa X da seguinte maneira:

- Definição do problema;
- Revisão de literatura;
- Preparação da entrevista;
- Coleta de dados por meio da aplicação da entrevista;
- Análise dos dados coletados; e,
- Obtenção de melhorias que auxiliem a qualidade da informação por meio da segurança da informação.

3.1 ANÁLISE DOS DADOS COLETADOS

A entrevista foi estruturada com base na norma ABNT NBR ISO/IEC 17799:2005 e na literatura pertinente apresentada anteriormente. A mesma também foi aplicada de forma a abranger os dois níveis hierárquicos do departamento, o estratégico e o operacional, ou seja, foram entrevistas duas pessoas, das quais uma é do nível operacional e uma do nível estratégico, sendo que as duas estão envolvidas com a qualidade da informação/documento sigiloso e sua segurança. A escolha dos dois entrevistados se deu de forma metódica a fim de abordar as duas pessoas responsáveis pela estratégia e operacionalização dos processos informacionais do departamento.

As respostas obtidas durante as entrevistas juntamente com a política de segurança da informação que a empresa possui foram analisadas qualitativamente com base na norma ABNT NBR ISO/IEC 17799:2005 que se refere ao código de

prática para a gestão da segurança da informação. Os tópicos da norma que foram trabalhados na pesquisa são:

- Política de segurança da informação;
- Organizando a segurança da informação;
- Gestão de ativos;
- Segurança em recursos humanos;
- Segurança física e do ambiente;
- Gerenciamento das operações e comunicações; e,
- Controle de acessos; e,
- Continuidade de negócios.

Esses tópicos abordados na ABNT NBR ISO/IEC 17799/2005 foram comparados com as respostas obtidas nas entrevistas e então a partir dessa comparação foi verificado se há ou não a necessidade de melhorias na segurança da informação para que a qualidade das informações e documentos sigilosos seja mantida.

3.2 AMBIENTE DE ESTUDO

O estudo foi realizado na empresa X[1], a qual é de economia mista e se localiza no Brasil. Criada em 1954, é uma das maiores empresas do ramo de geração, transmissão e distribuição energia e telecomunicações do país, tendo como visão “Prover energia e soluções para o desenvolvimento com sustentabilidade”. A empresa, que contêm mais de oito mil funcionários, também apresenta um conjunto de valores que orientam todas as ações e decisões internas da empresa e de seus colaboradores, os quais são: Ética, respeito às pessoas, dedicação, transparência, segurança, responsabilidade e inovação.

O ambiente estudado é o Departamento de Gestão de Documentos e Informações Corporativas, o qual é subdividido em duas partes: biblioteca e arquivo. A unidade conta com 13 (treze) funcionários e faz aproximadamente 500 (quinhentos) atendimentos mensais, sendo a mesma responsável pela guarda e

[1] Nome fictício dado à empresa pesquisada devido a questões de sigilo impostas pela mesma.

armazenamento dos documentos da empresa, os quais devem estar dispostos de forma a servir aos seus colaboradores com precisão e rapidez, e da mesma forma, evitar acessos não autorizados ao capital intelectual da empresa.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

A análise de resultados é produto da entrevista (APÊNDICE A, p.56) realizada na empresa X e consequente comparação com as melhores práticas para a segurança da informação estabelecidas na ABNT NBR ISO/IEC 17799: 2005.

De acordo com a entrevista realizada, o objeto de informação do departamento pesquisado são todos os documentos produzidos pela empresa, independente de sua finalidade. Entre os documentos produzidos pela empresa, encontram-se informações pessoais de empregados, informações médicas, contábeis, de novos negócios, tais como documentos de extensão de linha, novos empreendimentos, transformadores, etc. Ou seja, o departamento armazena documentos de caráter sigiloso, e com isso é de extrema importância que se tenham cuidados especiais para que não ocorram episódios de vazamento, perda, alteração, ou qualquer ação que ameace a sua integridade, disponibilidade e confidencialidade.

Um dos cuidados que se deve ter com as informações e documentos sigilosos é o prazo de guarda. Para tal, o departamento criou uma tabela de temporalidade interna nos anos 80, a qual foi definida com base nas atividades de cada área e normas do Estado. Tal tabela é atualizada constantemente à medida que há algum diálogo com as demais áreas ou quando é feita alguma solicitação de alteração. Com estas ações o departamento atende a boa prática adotada na ABNT NBR ISO/IEC 17799 (2005, p.108):

> Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e sobre o uso de produtos de software proprietários. (ABNT NBR ISO/IEC 17799, 2005, p.108).

Porém, essas ações não são formalizadas, e, portanto seria interessante que fosse elaborada e divulgada uma política de conformidade com os direitos de propriedade intelectual que definisse o uso legal das informações, além de notificar a possibilidade de se tomar medidas disciplinares contra os indivíduos que violarem essa política.

Os entrevistados do Departamento de Gestão de Documentos e Informações Corporativas informaram que as informações estão registradas em

suporte tanto físico quanto digital. Em suporte físico estão as informações em forma de livros, relatórios, folhetos, normas técnicas, etc., já as digitais estão acondicionadas em um banco de dados. Vale ressaltar que também existem informações armazenadas em microfilme, e para que esse tipo de informação seja tratado de forma correta existe uma fitoteca no departamento, a qual armazena essas mídias específicas com códigos numéricos em uma sala separada que é monitorada por câmeras vinte e quatro horas por dia, além de possuir climatização adequada. O acesso a esta sala só é permitido para funcionários do departamento responsável pela custódia da informação, os quais só podem acessar a fitoteca quando há alguma solicitação. Para acessar a fitoteca é utilizada uma chave comum que fica sob-responsabilidade da gerência da unidade, porém seria conveniente que houvesse uma porta com leitor biométrico para maior segurança. O departamento também possui equipamentos de leitura desses microfilmes conservados, garantindo o acesso aos dados, conforme a norma ABNT NBR ISO/IEC 17799 (2005, p.109) orienta:

> Onde mídias eletrônicas armazenadas forem escolhidas, convém que sejam incluídos procedimentos para assegurar a capacidade de acesso aos dados (leitura tanto na mídia como no formato utilizado) durante o período de retenção, para proteger contra perdas ocasionadas pelas futuras mudanças na tecnologia. (ABNT NBR ISO/IEC 17799, 2005, p.109).

Este aspecto também é atendido pelo departamento tendo em vista que oferece um conversor de fita VHS(*Vídeo Home System*, que pode ser traduzido para Sistema Doméstico de Vídeo) para DVD (*Digital Versatile Disc*, que pode ser traduzido para Disco Digital Versátil*)*, o que demonstra a preocupação em manter o acesso às informações mesmo com as mudanças tecnológicas verificados nos últimos anos.

Ainda segundo a ABNT NBR ISO/IEC 17799 (2005, p.x):

> A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.(ABNT NBR ISO/IEC 17799 (2005, p.x)

Para que a informação seja protegida adequadamente é necessário que a empresa mantenha um conjunto de controles que visem garantir a segurança da informação e sua qualidade. No que diz respeito a esse conjunto de controles a norma inclui “políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*”. Além disso, a norma ainda ressalta que esses controles “precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos”. Porém isso não ocorre atualmente na empresa e, consequentemente, essas seriam ações que a empresa deveria realizar.

Em relação à informação como ativo estratégico, com os resultados obtidos na entrevista, é possível observar que a informação é vista de forma especial somente quando há alguma auditoria ou fiscalização, quando na verdade deveria ser vista como um ativo imprescindível na empresa, pois a informação é um diferencial estratégico e deve ser sempre bem protegida, pois de acordo com a norma, garantir a segurança das informações pode assegurar a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre investimentos e as oportunidades de negócio. Ou seja, a empresa deveria dar mais atenção à proteção da informação e de sua qualidade colocando em prática o conjunto de controles citado ainda há pouco, que envolve políticas, processos, procedimentos, etc., pois assim a empresa aumentaria as chances de obter um diferencial de mercado.

A preocupação da empresa com a proteção da qualidade da informação é a existência de uma política de segurança da informação (ANEXO A, p.62), sendo que a mesma possui apenas diretrizes do que seria a segurança da informação na empresa, porém a mesma não possui procedimentos de como garantir a segurança e nem cita punições para quem descumpri-la, sendo que deveria fazê-los. A política também está disponível na intranet da empresa plenamente acessível aos colaboradores, permitindo-lhes acessá-la. Entretanto, em todos tem conhecimento da mesma. Para resolver esse problema, recomenda-se que a empresa campanhas de divulgação, que poderiam ser através de uma nota no portal corporativo, envio de e-mail pela comunicação corporativa, inserção de papel de parede automático convidando os colaboradores a conhecê-la, além de colocar cartazes em locais

estratégicos da empresa em que fosse mais fácil à visualização, tais como corredores, pontos-eletrônicos, elevadores, etc.

Em relação à estrutura da política de segurança da informação, seria importante a empresa revisá-la de forma a abranger procedimentos que demonstrassem como garantir a segurança de informação e, como a norma ABNT NBR ISO/IEC 17799 (2005, p. 8) sugere, o documento deveria possuir declarações relativas 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;
> • uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhada com os objetivos e estratégias do negócio;
> • uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco;
> • breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo:
> - conformidade com a legislação e com requisitos regulamentares e contratuais;
> - requisitos de conscientização, treinamento e educação em segurança da informação;
> - gestão da continuidade do negócio;
> - consequências das violações na política de segurança da informação;
> • definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança da informação;
> • 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. (ABNT NBR ISO/IEC 17799, 2005, p. 8).

Vale ressaltar que a política também deve ser revisada e analisada criticamente em intervalos planejados, de modo a garantir sua eficácia, além de que os funcionários devem ser motivados a entender e cumprir a política de segurança da informação. Essa motivação dos colaboradores pode ser feita por meio de algumas ações, tais como: Somente o departamento que cumprir a política ganha a Participação de Lucros e Resultados (PLR); os departamentos que cumprirem todas as políticas podem concorrer algum prêmio uma vez ao ano, como por exemplo, uma viagem ou um jantar; a comunicação corporativa pode enviar e-mails de motivação; além de que o gestor de cada área pode fazer um monitoramento para verificar se a política está sendo cumprida dentro de seu departamento.

Atualmente o departamento não conta com nenhum mecanismo formal de classificação da criticidade da informação, e a gerência afirmou que não precisa de um mecanismo, pois há confiança nas pessoas na unidade. Com isso, percebe-se que as pessoas que trabalham com as informações sigilosas estão despreparadas para tal, pois deve-se haver uma proteção contra perda de confidencialidade, uso impróprio e perda de integridade das informações, e para que isso ocorra é necessário que se tenha graus da criticidade da informação, para tratar adequadamente cada ativo informacional. Já em relação à gerência possuir confiança nas pessoas que trabalham no departamento é algo a se preocupar, pois caso ocorra algum vazamento ou perda de informação, não há como saber quem foi o responsável, por isso é relevante que haja um comprometimento da diretoria em um trabalho de conscientização com as hierarquias superiores mostrando exemplos de casos que já ocorreram de vazamento/perda/alteração da informação e suas consequências, para que dessa forma os gestores saibam lidar com seus subordinados e a não confiar plenamente neles a fim de reduzir o risco de furto ou roubo, fraude ou mau uso de informações.

Nesse mesmo sentido, na unidade pesquisada existem informações sigilosas, tais como documentos pessoais de empregados, informações médicas, contábeis, sobre novos negócios (documentos de extensão de linha, novos empreendimentos, transformadores, etc.), mas não existem definições de graus de sigilo e nem um controle de acessos formais dessas informações, o único mecanismo de controle que existe informalmente é de que somente o departamento que enviou o documento para a unidade de documentação é que pode retirar ou consultar o documento. Caso algum colaborador queira ter acesso a algum documento enviado por outro departamento, esse deve ter autorização do departamento “proprietário” do documento para poder acessá-lo. Para que a qualidade da informação desses documentos seja preservada se faz necessária a definição de graus de sigilo e a identificação de alguns requisitos de confidencialidade, como identifica a ABNT NBR ISO/IEC 17799 (2005, p.12):

> Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados e analisados criticamente. (ABNT NBR ISO/IEC 17799, 2005, p.12).

Para identificá-los, a norma considera os seguintes elementos:

> •uma definição da informação a ser protegida;
> •tempo de duração esperado de um acordo, incluindo situações onde a confidencialidade tenha que ser mantida indefinidamente;
> •ações requeridas quando um acordo está encerrado;
> •responsabilidades e ações dos signatários para evitar a divulgação não autorizada da informação;
> •proprietário da informação, segredos comerciais e de propriedade intelectual, e como isto se relaciona com a proteção da informação confidencial;
> •uso permitido da informação confidencial e os direitos do signatário para usar a informação;
> •direito de auditar e monitorar as atividades que envolvem as informações confidenciais;
> •processo para notificação e relato de divulgação não autorizada ou violação das informações confidenciais;
> •termos para a informação ser retornada ou destruída quando do término do acordo; e
> •ações esperadas a serem tomadas no caso de uma violação desse acordo. (ABNT NBR ISO/IEC 17799, 2005, p.12).

Vale ressaltar que esse controle de acesso deve estar presente na política de segurança da informação, onde todos os colaboradores da empresa devem ter acesso.

Além disso, também foi constatado que as pessoas que trabalham no departamento e lidam com os documentos sigilosos não assinam nenhum termo de responsabilidade, o que deveria ser feito no momento da contratação dos colaboradores nos termos e condições de contratação, como afirma a ABNT NBR ISO/IEC 17799 (2005, p.25):

> Convém que as responsabilidades pela segurança da informação sejam atribuídas antes da contratação, de forma adequada, nas descrições de cargos e nos termos e condições de contratação. (ABNT NBR ISO/IEC 17799, 2005, p.25).

Bem como a norma também afirma que “convém que todos os candidatos ao emprego, fornecedores e terceiros sejam adequadamente analisados, especialmente em cargos com acesso a informações sensíveis”. E para finalizar, a norma afirma que “convém que todos os funcionários, fornecedores e terceiros,

usuários dos recursos de processamento da informação, assinem acordos sobre seus papéis e responsabilidades pela segurança da informação".

Ou seja, não só os colaboradores, mas todo e qualquer indivíduo que tiver acesso liberado para uso de informações de caráter sigiloso deve assinar um acordo ou termo de responsabilidade para que seja assegurada a segurança das informações. Assim sendo, deve-se instaurar um processo disciplinar para quem cometer alguma violação em relação a segurança da informação da empresa, conforme a ABNT NBR ISO/IEC 17799 (2005, p.29) afirma:

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

Portanto, o termo de responsabilidade deve estar vinculado ao contrato de trabalho, para que se o mesmo for violado, possam-se executar as punições cabíveis, inclusive justa causa, pois de acordo com o Artigo 482 do Decreto n.5.452 de 01 de maio de 1943 que trata a Consolidação das Leis de Trabalho, constitui justa causa para rescisão do contrato de trabalho casos de ato de improbidade; incontinência de conduta ou mau procedimento; e, violação de segredo da empresa.

O departamento não possui nenhum plano de contingenciamento em caso de desastre ou catástrofe que possa ocasionar a perda das informações, para que os danos causados fosse o menor possível uma sugestão seria a implantação de GED (Gerenciamento Eletrônico de Documentos), pois caso ocorra uma catástrofe no ambiente em que os documentos físicos estão armazenados, haveria cópias eletrônicas em servidores e locais distintos para que se pudesse fazer uma restauração imediata de todos os documentos, além de que para os documentos que necessitam de validade jurídica poderia ser usada a autenticação digital, a qual é realizada em cartório e valida o documento eletronicamente. Outra sugestão seria que essas informações possuíssem cópias de segurança armazenadas em nuvem,

a qual dispensaria a instalação de equipamentos físicos, porém para que isso fosse feito, seria necessária uma política de segurança da informação com a empresa contratada, a qual fornece o armazenamento em nuvem, que envolvesse um contrato de prestação de serviço com clausulas bem definidas sobre a garantia de inviabilidade de confidencialidade, integridade e disponibilidade. Vale ressaltar que para o plano de contingência seja eficaz, também é necessário um conjunto de documentos sobre adequações de infraestrutura e dos procedimentos do dia a dia da empresa.

Assim, ainda com o objetivo de proteger a informação, a norma sugere que seja feito um inventário de ativos, o qual deve incluir todas as informações necessárias que permitam recuperá-los, tais como: tipo do ativo, formato, localização, informações sobre cópias de segurança, informações sobre licenças e a importância do ativo para o negócio. E, adicionalmente, é importante que o proprietário e a classificação da informação sejam acordados e documentados para cada um dos ativos. Além disso, de acordo com a ABNT NBR ISO/IEC 17799 (2005, p. 34) convém que algumas medidas preventivas sejam adotadas:

> •os materiais perigosos ou combustíveis sejam armazenados a uma distância segura da área de segurança. Suprimentos em grande volume, como materiais de papelaria, não devem ser armazenados dentro de uma área segura;
> •os equipamentos para contingência e mídia de *backup* fiquem a uma distância segura, para que não sejam danificados por um desastre que afete o local principal;
> •os equipamentos apropriados de detecção e combate a incêndios sejam providenciados e posicionados corretamente. (ABNT NBR ISO/IEC 17799, 2005, p. 34).

Ao encontro disso, a segurança do ambiente físico também deve ser levada em consideração, e para isso a empresa possui câmeras de segurança, vigilância armada e controle na recepção, no qual a recepcionista anota o nome do visitante e horário de entrada e saída. Contudo, a empresa poderia adotar mais controles na segurança física, visto que já ocorreu um episódio de invasão ao departamento que detêm as informações sigilosas, para isto poderiam ser colocadas paredes robustas, as portas poderiam possuir barras, alarmes e fechaduras com leitor biométrico, além de serem trancadas quando não houvesse monitoramento. Também seria conveniente possuir portas corta-fogo, que os visitantes fossem supervisionados e

todas as pessoas que circulassem pelo ambiente usassem uma forma visível de identificação.

O departamento de gestão de documentos e informações corporativas não realiza auditoria de segurança da informação, porém deveria fazê-lo, pois com as auditorias é possível proteger a integridade e prevenir o uso indevido de informações. Mas é importante ressaltar que quando houver auditoria é preciso tomar algumas ações para que haja maior proteção às informações, que segundo a norma são:

> •requisitos de auditoria sejam acordados com o nível apropriado da administração;
>
> •escopo da verificação seja acordado e controlado;
>
> •a verificação esteja limitada ao acesso somente para leitura de *softwares* e dados;
>
> •outros acessos diferentes de apenas leitura sejam permitidos somente através de cópias isoladas dos arquivos do sistema, e sejam apagados ao final da auditoria, ou dada proteção apropriada quando existir uma obrigação para guardar tais arquivos como requisitos da documentação da auditoria;
>
> •recursos para execução da verificação sejam identificados explicitamente e tomados disponíveis;
>
> •requisitos para processamento adicional ou especial sejam identificados e acordados;
>
> •todo acesso seja monitorado e registrado de forma a produzir uma trilha de referência[2]; convém que o uso de trilhas de referência (*time stamped*) seja considerado para os sistemas ou dados críticos;
>
> •todos os procedimentos, requisitos e responsabilidades sejam documentados;
>
> •as pessoas que executam a auditoria sejam independentes das atividades auditadas.(ABNT NBR NBR ISO/IEC 17799, 2005, p. 113).

Também é conveniente que a empresa realize auditoria no sistema que armazena as informações sigilosas, pois de acordo com Schmidt *apud* Lyra (2008, p.105) a auditoria de sistemas visa:

> Promover adequação, revisão, avaliação e recomendações para o aprimoramento dos controles internos nos sistemas de informação da empresa, bem como avaliar a utilização dos recursos humanos, materiais e tecnológicos envolvidos no processamento dos mesmos. (SCHMIDT *apud* LYRA, 2008, p.105).

[2]Detalhes informacionais do registro de um evento

Portanto, é essencial que a empresa realize auditorias periodicamente com o propósito de verificar o cumprimento das políticas e investigar a utilização das informações, bem como realizar e a elaboração de sugestões de aprimoramento para proteger os documentos sigilosos da empresa e tornar mais eficiente os seus controles, vale ressaltar que há necessidade de se formalizar o processo e a utilização de alguma metodologia para o processo é altamente desejável.

A unidade de informação também não possui certificação em segurança da informação, a qual pode ser dada através da norma ABNT NBR ISO/IEC 27001 (2006, p.1) que trata sobre requisitos para sistemas de gestão da segurança da informação e tem como objetivo:

> Especificar os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização. Ela especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes. (ABNT NBR ISO/IEC 27001, 2006, p. 1).

Ou seja, a organização deveria seguir os requisitos solicitados pela norma a fim de assegurar a seleção de controles adequados para proteger os ativos de informação e propiciar confiança para as partes interessadas.

4.1 SÍNTESE DAS AÇÕES SUGERIDAS

Em resumo, seguem sugestões de ações a serem tomadas pela empresa para que ocorram melhorias visando assegurar a qualidade da informação por meio da segurança da informação:

QUADRO 5 – SÍNTESE DE AÇÕES SUGERIDAS

Problema	**Ações sugeridas**
Informação não protegida	-Implementar, monitorar, analisar criticamente e melhorar onde necessário um conjunto de controles de segurança (políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware)*
Ações realizadas informalmente sobre o acúmulo de documentos/descarte de informações	-Criar uma política de conformidade que defina o uso legal das informações, formalizando as práticas já adotadas pelo departamento.

	-Notificar a possibilidade de se tomar medidas disciplinares contra os indivíduos que violarem a formalização de procedimentos para descarte de informações.
Segurança na fitoteca	-Instalar mecanismo de controle de acesso baseado em sistema biométrico.
Política de segurança da informação sucinta	-Incluir os procedimentos na política. -Incluir consequências das violações da política. -Criar uma definição de segurança da informação, suas metas globais, escopo e importância da SI como um mecanismo que habilita o compartilhamento da informação. -Formalizar o comprometimento da direção em relação à Política de Segurança da informação, apoiando as metas e princípios da segurança da informação alinhada com os objetivos e estratégias do negócio. -Definir as responsabilidades gerais e específicas da segurança da informação. -Fazer referência às documentações que possam apoiar a política. -Revisar a política periodicamente.
Desconhecimento da política de segurança da informação	-Realizar campanhas de divulgação -Colocar uma nota no portal corporativo -Envio de e-mails pela comunicação corporativa ou pelo presidente da empresa -Inserção de papel de parede automático convidando os colaboradores a conhecê-la -Colocar cartazes em locais estratégicos divulgando-a. -Inserir no contrato de trabalho clausula de ciência da existência da PSI
Falta de incentivo/monitoramento para o cumprimento da PSI	-Criar ações de motivação: Somente o departamento que cumprir a política ganhará Participação nos Lucros e Resultados; As áreas que cumprirem todas as políticas podem concorrer a prêmios como jantares e viagens; Podem ser enviados e-mails de motivação; e, o gestor de cada área deve fazer um monitoramento para averiguar se a Política de Segurança da Informação está sendo cumprida pelos seus subordinados.
Caracterização da informação	-Identificar os graus de criticidade da informação.
Confiança nas pessoas	-Fazer um trabalho de conscientização com as hierarquias mostrando casos que

	já ocorreram de vazamento/perda/alteração da informação e suas consequências.
Perda/Roubo/Vazamento de informação	-Definir graus de sigilo e um controle de acesso formal.
Divulgação/Uso de informação indevida	-Criar um acordo de confidencialidade. -Criar punições para quem descumprir o acordo. -Vincular clausulas contratuais ao processo de contratação de colaboradores.
Não há responsabilização por informações vazadas por colaboradores, fornecedores, terceiros e demais usuários	-Criar um termo de responsabilidade e também processos disciplinares para quem não o respeitar, tal deve estar vinculado ao contrato de trabalho.
Ocorrência de catástrofe	-Implantação de GED. -Armazenar cópias de segurança em nuvem. -Adequar os equipamentos de infraestrutura. -Criar um inventário de ativos. -Armazenar materiais perigosos a uma distância segura das informações. -Posicionar corretamente equipamentos de detecção e combate de incêndio -Formalizar um plano de continuidade de negócios consistente e adequado à criticidade dos ativos de informação.
Invasão ao departamento informacional	-Construção de paredes robustas. -Instalar portas com barras, alarmes e fechaduras com leitor biométrico. -Trancar a porta quando não houver monitoramento. -Inserir portas corta-fogo. -Supervisionar os visitantes. -Visitantes devem usar uma forma visível de identificação.
Não há investigação do cumprimento das políticas e utilização das informações	-Realizar auditoria periodicamente. -Requisitos de auditoria sejam acordados com o nível apropriado da administração. -Escopo de verificação deve ser bem definido. -Sejam criados níveis de acessos. - Monitorar e registrar todos os acessos. -Todos os procedimentos, requisitos e responsabilidades sejam documentados. -Os auditores não devem estar ligados com as atividades auditadas. -Auditar o sistema que armazena as informações sigilosas.
Não há certificação em segurança da informação (27001)	-Especificar, implementar, monitorar, analisar, manter e melhorar um Sistema de Gestão de Segurança da Informação.

Fonte: A autora (2015)

5 CONSIDERAÇÕES FINAIS

A pesquisa a que se refere o presente relatório objetiva investigar como assegurar a qualidade da informação dos documentos sigilosos em uma unidade da empresa X na perspectiva da segurança da informação. Para obter sucesso no propósito estabeleceram-se algumas metas, quais sejam: Identificar os cuidados, quanto ao acesso e a guarda, que a organização possui em relação aos documentos e informações sigilosas; Identificar as boas práticas e os procedimentos adotados para garantir a segurança da informação; Identificar possíveis fragilidades de segurança da informação na organização; e, identificar procedimentos a serem adotados para objetivar a melhoria da segurança da informação.

Em relação à metodologia caracterizada como exploratória e qualitativa, é importante deixar claro o uso de duas técnicas: Estudo de caso e pesquisa-ação. Estudo de caso devido analisar detalhadamente um único ambiente e, pesquisa-ação por não apenas analisar, mas sugerir mudanças no departamento da empresa X e de certa forma, interferir no ambiente de pesquisa. Seria interessante que houvesse um estudo futuro para verificar se as ações sugeridas foram postas em prática corretamente e analisar quais foram os resultados, analisá-los e propor novos procedimentos num ciclo contínuo de mudanças na busca do modelo de gestão da informação mais indicado à realidade do ambiente de informação objeto de estudo.

Após a aplicação da entrevista identificou-se através deste estudo na empresa X, a existência de uma preocupação com a qualidade e segurança da informação, entretanto existem muitas ações a serem adquiridas e praticadas pela empresa para que se possam obter melhores controles das informações sigilosas assegurando-se uma segurança da informação mais eficaz. Algumas dessas ações a serem obtidas pelo departamento de gestão de documentos e informações corporativas e pela empresa como um todo foram propostas e cabe a empresa avalia-las e decidir quais são passíveis de implementação.

Durante esta pesquisa também foi possível notar que o gestor da informação possui condições técnicas para contribuir com a segurança da informação, pois com a análise de resultados pode-se compreender que é necessário conhecer diversos fatores que influenciam a segurança da informação,

tais como os recursos humanos, tecnológicos e organizacionais, dos quais o curso de Gestão da Informação da Universidade Federal do Paraná oferece conhecimentos por meio de disciplinas como: Gestão da Informação, Gestão de Documentos, Segurança da Informação e Políticas de Informação, as quais dão suporte para que o gestor da informação trabalhe com o problema objeto de estudo abordado no presente relatório de pesquisa.

REFERÊNCIAS

ALMEIDA, F. C. de; LESCA, H.. **Administração estratégica da informação**. Disponível em: <http://www.rausp.usp.br/download.asp?file=2903066.pdf>. Acesso em: 17 mai 2014.

ALVARENGA NETO, R. C. D.. **Gestão do conhecimento em organizações**: proposta de mapeamento conceitual interativo. São Paulo: Saraiva, 2008.

ARAÚJO, M. T.; FERREIRA, F.N.F.. **Política de segurança da informação:** guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006.

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: tecnologia da informação – técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro, 2006.

Arquivo Nacional (Brasil). Conselho Nacional de Arquivos. **Classificação, temporalidade e destinação de documentos de arquivo**; relativos às atividades-meio da administração pública/Arquivo Nacional. Rio de Janeiro: Arquivo Nacional, 2001.

BEAL, A.. **Gestão estratégica da informação**: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações. São Paulo: Atlas, 2004.

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

BERNARDES, I. P.; DELATORRE, H.. **Gestão documental aplicada**. São Paulo: Arquivo Público do Estado de São Paulo, 2008. Disponível em:<http://200.144.6.120/saesp/GESTAO_DOCUMENTAL_APLICADA_Ieda.pdf>. Acesso em 18 mai 2014.

BERTUCCI, J. L. O.. **Metodologia básica para elaboração de trabalhos de conclusão de cursos (TCC)**. São Paulo: Atlas, 2008.

BELLOTTO, H. L.. **Arquivos Permanentes:** tratamento documental. 2.ed. Rio de Janeiro: Editora FGV, 2004.

BEUREN, I. M. **Gerenciamento da informação**: um recurso estratégico no processo de gestão empresarial. 2. ed. São Paulo: Atlas, 2000.

BLUE P.. **Boas práticas de segurança**. Disponível em: <www.bluephoenix.pt>. Acesso em: 11 mar 2015.

BRASIL. **Decreto n. 4553**, de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/D4553.htm>. Acesso em: 4jun 2014.

BRASIL. **Decreto n. 5452**, de 01 de maio de 1943. Aprova a Consolidação das Leis do Trabalho. Disponível em: <http://www.jusbrasil.com.br/topicos/10709394/artigo-482-do-decreto-lei-n-5452-de-01-de-maio-de-1943>. Acesso em: 12 jun 2015.

BRASIL. **Decreto n. 7724**, de 16 de maio de 2012. Dispõe sobreo acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm>. Acesso em: 5 mar 2015.

BRASIL. **Lei 8159**, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8159.htm>. Acesso em: 18 mai 2014.

BRASIL. **Lei 12527**, de 18 de novembro de 2011. Dispõe sobreos procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 05 mar 2015.

CONSELHO NACIONAL DE ARQUIVOS. **Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos.** E-Arq Brasil**.** Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/earqbrasilv1.pdf>.Acesso em: 20 mar 2014.

DAVENPORT, T. H.. **Ecologia da informação**: por que só a tecnologia nãobasta para o sucesso na era da informação. São Paulo: Futura, 1998.

DELLGADILLO, S. M. L. T et al. Repensando o método 5S para arquivos. **Ciência e Informação**. Espírito Santo, n.22, p.57-63, 2006.

DEPARTAMENTO ESTADUAL DE ARQUIVO PÚBLICO**. Manual de gestão de documentos do Estado do Paraná**. Disponível em: < http://www.arquivopublico.pr.gov.br/arquivos/File/pdf/gestao.pdf>. Acesso em 09 out 2014.

DICIONÁRIO BRASILEIRO DE TERMINOLOGIA ARQUIVÍSTICA. Rio de Janeiro: Arquivo Nacional, 2005. Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/dicionrio_de_terminologia_arquivstica.pdf>. Acesso em: 18 mai 2014.

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

GIL, A. C.. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 1988.

GODOY, A. S.. Introdução à pesquisa qualitativa e suas possibilidades. **RAE**, São Paulo, v.35, n.2, p.57-63, mar./abr. 1995.

GOVERNO DO ESTADO DO RIO DE JANEIRO. **Manual de gestão de documentos**. Disponível em: <http://download.rj.gov.br/documentos/10112/1711903/DLFE-71375.pdf/ManualdeGestaodeDocumentos_2012.pdf>. Acesso em: 15 set 2014

JARDIM, J. M.. **O conceito e a prática de gestão de documentos**. Acervo. Rio de Janeiro, v.2, n.2,p. 35-42, jul./dez. 1987. Disponível em:<http://arquivoememoria.files.wordpress.com/2009/05/o-conceito-e-pratica-gestao-documentos.pdf>. Acesso em: 18 mai 2014.

LYRA, M. R.. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

MCGARRY, K. **O contexto dinâmico da informação.** Brasília: Briquet de Lemos, 1999.

PAES, M. L.. **Arquivo:** teoria e prática. Rio de Janeiro: Editora FGV, 2007.

PAIM, I.; NEHMY, R. M. Q.; GUIMARÃES, C. G. Problematização do conceito “qualidade” da informação. **Perspectivas em Ciência da Informação**, Belo Horizonte, v.1, n.1, p.111-119, jan/jun 1996.

ROCHA, C. L. et. al. **Gestão arquivística de documentos eletrônicos.** Disponível em: <http://arquivonacional.gov.br/conarq/cam_tec_doc_ele/download/GT%20gestao%20arquivistica.pdf>. Acesso em: 08 mar 2014.

RODRIGUES. A. C.. **Gestão de documentos:** uma abordagem conceitual. Disponível em: <http://www.ejef.tjmg.jus.br/home/files/publicacoes/gest_arqui/palestra_ana_celia_rodrigues.pdf>. Acesso em: 4 jun 2014.

SÁ, E. P.. Gestão de documentos: uma visão empresarial. In: SOUTO, Leonardo Fernandes (Org.).**Gestão da informação e do conhecimento**: práticas e reflexões.Rio de Janeiro: Interciência, 2014.

SANTO, A. F. S. E.. **Segurança da informação**. Disponível em: <http://www.ice.edu.br/TNX/encontrocomputacao/artigos-internos/aluno_adrielle_fernanda_seguranca_da_informacao.pdf> Acesso em: 12 mar 2015.

SCHELLENBERG, T. R.. **Arquivos modernos:** princípios e técnicas. 2.ed. Rio de Janeiro: Editora FGV, 2002.

SÊMOLA, M.. **Gestão da segurança da informação:** uma visão executiva. 2.ed. Rio de Janeiro: Elsevier, 2014.

SILVA, A. B. M. **A Gestão da Informação Arquivistica e suas repercussões na produção do conhecimento científico.** Seminário Internacional de Arquivos de Tradição Ibérica. Conselho Nacional de Arquivos – Conferências. Disponível em: <http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?sid=74> Acesso em: 23 mar 2014.

SFREDDO, J. A.; FLORES, D.. Segurança da informação arquivística: o controle de acesso em arquivos públicos estaduais. **Perspect. ciênc. inf.**, Belo Horizonte , v. 17, n. 2, Jun 2012 . Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-99362012000200011&lang=pt>. Acesso em: 23 mai 2014.

SORDI, J. O. **Administração da Informação**: fundamentos e práticas para uma nova gestão do conhecimento. São Paulo: Saraiva, 2008.

THIOLLENT, M. **Pesquisa-Ação nas Organizações**. São Paulo: Atlas, 1997.

VALENTIM, M. L. P. (Org.). **Gestão da informação e do conhecimento no âmbito da Ciência da Informação**. São Paulo: Cultura Acadêmica, 2008.

APÊNDICE A - Entrevista

1. Qual é o objeto de informação da área?

Entrevistado 1: Existem documentos relacionados a recursos humanos, financeiro, jurídico, contábil, comercial, ou seja, todos os documentos que são resultados da empresa.

Entrevistado 2: Toda e qualquer informação gerada pela empresa, que tem como finalidade gerar, transmitir e distribuir energia.

2. Qual o suporte da informação?

Entrevistado 1: Físico e digital, sendo o digital uma base de dados.

Entrevistado 2: Existem documentos em forma de mídias, papel, microfilme (existe uma fitoteca), etc.

3. Qual papel que a informação representa para a empresa? Ela é vista como um ativo estratégico?

Entrevistado 1: Sim, é estratégico, principalmente quando há auditoria ou fiscalização.

Entrevistado 2: Ela é bem vista, mas não tem como mensurar até que nível ela vai.

4. **Qual a preocupação da organização com a proteção da qualidade da informação? (integridade, acessibilidade, confidencialidade)**

Entrevistado 1: Existe a política de segurança da informação na empresa.

Entrevistado 2: Existem normas internas para proteção da qualidade, e também há uma preocupação por parte de quem detém a informação.

5. **Existe algum mecanismo de classificação da criticidade da informação?**

Entrevistado 1: Formalmente não.

Entrevistado 2: Não existe atualmente, o departamento confia nas pessoas.

6. **Existe informação ou documento sigiloso na área? Se sim, o que é considerado informação/documento sigiloso?**

Entrevistado 1: No arquivo tudo tem um nível de sigilo e só acessa o documento quem mandou ele para o departamento.

Entrevistado 2: Sim, existem documentos pessoais de empregados, informações médicas, contábeis, novos negócios (Documentos de extensão de linha, novos empreendimentos, transformadores, etc.).

7. **São delimitados graus de sigilo nos documentos na empresa?**

Entrevistado 1: Oficialmente não.

Entrevistado 2: Não, porque os documentos não são publicados, há apenas as normas da empresa.

8. Existe algum mecanismo formal de controle de acesso a informações sigilosas?

Entrevistado 1: Formalmente não, apenas informal que somente o departamento que mandou o documento para a nossa área pode acessá-lo.

Entrevistado 2: Tem, pois uma área não pode acessar o que é de outra área e pessoas que não são da empresa não possuem acesso.

9. Existe uma política/norma de proteção a essas informações? Se sim, todos tem acesso à mesma?

Entrevistado 1: Existe uma política da segurança da informação em que todos os colaboradores têm acesso.

Entrevistado 2: Sim, todos tem acesso, ela fica na intranet da empresa.

10. Onde na política o controle de acessos está sendo tratado o controle de acesso?

Entrevistado 1: Não sei informar.

Entrevistado 2: Não fala sobre o controle de acessos.

11. Quais cuidados a empresa/departamento tem em relação à segurança desses documentos?

Entrevistado 1: Disponibilização dos documentos dentro de um sistema da empresa; o documento é integro pois ninguém altera os documentos; as caixas não são identificadas, é apenas colocado um número que só quem trabalha na área consegue identificá-lo.

Entrevistado 2: Existe a política de segurança da informação; para ter acesso aos sistemas existem senhas; existem câmeras de segurança e vigilância armada.

12. As pessoas responsáveis pelos documentos sigilosos assinam algum termo de responsabilidade de sigilo quando são contratadas?

Entrevistado 1: Na nossa área não, o que existe é o código de conduta que todos os funcionários assinam.

Entrevistado 2: Não.

13. Esse termo está vinculado de alguma forma com o contrato de trabalho?

Entrevistado 1: O código de conduta sim.

Entrevistado 2: Não existe termo de responsabilidade.

14. As pessoas que emprestam os documentos sigilosos assinam algum termo de responsabilidade quando realizam o empréstimo? (remoção de propriedade)

Entrevistado 1: Assinado não, é só registrado no sistema.

Entrevistado 2: Não, quem deposita no arquivo é quem pode retirar, e quem é de outra área só retira com autorização da área que depositou.

15. Existe uma tabela de temporalidade implementada e operacional? Como funciona?

Entrevistado 1: Sim, foi criada com base nas atividades de cada área, nos processos da empresa e também é feito um diálogo entre as áreas para identificar o prazo de guarda, juntamente com as leis vigentes e normas do estado.

Entrevistado 2: Existe, é da década de 80 e é atualizada constantemente à medida que se visitam as áreas ou que se é solicitado. Também existe a documentação histórica, permanente e intermediária, a qual é destruída com frequência quando expira o prazo, porém pede-se autorização da área para então serem eliminadas.

16. Já ocorreu algum episódio de vazamento de documento/informação?

Entrevistado 1: Que eu saiba não.

Entrevistado 2: Já, o arquivo foi arrombado uma vez há muitos anos atrás, mas não conseguiram identificar os códigos, e consequentemente não sabiam o que tinham de documentos dentro das caixas.

17. Qual a proporcionalidade entre os documentos sigilosos que são físicos e digitais?

Entrevistado 1: Existem digitais e também existem os físicos, não sei dizer qual seria a proporcionalidade, mas o único 100% digital é o cartão ponto.

Entrevistado 2: Não sei estimar, mas a maior parte do que existe digitalmente existe o físico também.

18. Existe algum plano de contingenciamento em caso de ocorrência de catástrofe, como incêndio ou enchente? (recuperação de serviços)?

Entrevistado 1: Que eu saiba não.

Entrevistado 2: Existe o PPRA - Programa de Prevenção dos riscos ambientais, o qual cuida do tipo de piso, iluminação, ventilação, acabamentos/forração e divisórias, além dos riscos químicos, biológicos e ergonômicos. O PPRA é mais voltado para os funcionários, mas acaba ajudando nos cuidados com os documentos. Porém o local em que os documentos estão armazenados não é o mais adequado, pois é um prédio muito antigo.

19. É feito periodicamente auditoria da segurança da informação?

Entrevistado 1: Não.

Entrevistado 2: Tinha antigamente, hoje não mais.

20. Como a empresa trata a qualidade da informação?

Entrevistado 1: As áreas técnicas têm registros de evidência, mas trabalham de forma independente.

Entrevistado 2: A área não é certificada, mas existe a certificação em outras áreas, única coisa que é feita pela nossa área é o preenchimento do arquivo da fundação nacional da qualidade.

ANEXO A – Política de segurança da informação da empresa X

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
Versão 04 de 20/01/2015

1. FINALIDADE

Estabelecer diretrizes relativas à Segurança da Informação na empresa.

2. CONCEITOS

2.1 - INFORMAÇÃO
Ativo, expresso de forma impressa, escrito em papel, armazenado digitalmente, transmitido por correio ou meios eletrônicos, mostrado em filmes, dialogado em palestras, postado em redes sociais, mídias sociais ou em reuniões formais ou informais, que necessita, por sua importância, ser adequadamente protegido, manuseado e gerenciado.

2.2 - SEGURANÇA DA INFORMAÇÃO
Conjunto de diretrizes, instrumentos e ações que garantem adequado grau de confidencialidade, integridade, disponibilidade e rastreabilidade à informação na empresa.

2.3 - CONFIDENCIALIDADE
Característica da informação que a torna reservada, com acesso por pessoas autorizadas.

2.4 - INTEGRIDADE
Característica da informação que a torna exata e completa.

2.5 - DISPONIBILIDADE
Característica da informação que a torna acessível quando necessária em prazo compatível com o processo de negócio.

2.6 - RASTREABILIDADE

Característica da informação que possibilita acompanhar ou identificar algo durante um processo: saber "o quê", "quem", “quando”, de “onde" e "para onde".

2.7 - DEVER DE DILIGÊNCIA

Obrigação de ter o cuidado necessário na execução de ato ou procedimento num negócio, para que tudo se cumpra com regularidade.

3. PRINCÍPIOS

3.1 - DIREITOS MÍNIMOS

As pessoas, os sistemas de informação e os processos devem acessar apenas as informações que garantam a execução de suas atividades.

3.2 - EXPOSIÇÃO MÍNIMA

A informação deve ser mantida protegida, sendo exposta apenas quando necessária.

4. DIRETRIZES

4.1 - Toda informação produzida ou incorporada pela empresa é de sua propriedade, sendo parte de seu patrimônio como ativo intangível.

4.2 - A informação será protegida pelos níveis de autoridade formal estabelecidos pela empresa, sendo exposta de acordo com a necessidade.

4.3 - Todas as características de segurança da informação devem ser preservadas na empresa.

4.4 - Os processos e sistemas de informação devem atender às exigências de transparência e rastreabilidade para alterações e acessos às informações.

4.5 - Todo acesso e uso da informação deve ser realizado com dever de diligência.

Atualiza a política de 01.10.2013 e substitui quaisquer outros instrumentos normativos relativos ao assunto.