UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL DA LUSOFONIA AFRO-BRASILEIRA
INSTITUTO DE CIENCIAS SOCIAIS APLICADAS
CURSO DE PÓS-GRADUAÇÃO LATO SENSU EM GESTÃO PÚBLICA MUNICIPAL

FRANCISCO CHARLES SILVA

A INFORMAÇÃO E COMUNICAÇÃO NO SETOR PÚBLICO

Estudo de Caso Sobre a Gestão e Segurança da Informação e Comunicação no Setor Público da Saúde no Município de Caucaia

CAUCAIA
2018

FRANCISCO CHARLES SILVA

A INFORMAÇÃO E COMUNICAÇÃO NO SETOR PÚBLICO

Estudo de Caso Sobre a Gestão e Segurança da Informação e Comunicação no Setor Público da Saúde no Município de Caucaia

Trabalho de Conclusão de Curso apresentado ao Curso de Pós-Graduação Lato Sensu em Gestão Pública Municipal da Universidade da Integração Internacional da Lusofonia Afro-Brasileira como requisito parcial à obtenção do título de Especialista em Gestão Pública Municipal.

Orientador: Prof. Ms. Francisco Jose Aguiar Costa Junior.

.

CAUCAIA

2018

Dados Internacionais de Catalogação na Publicação

S58i Silva, Francisco Charles Silva.
A INFORMAÇÃO E COMUNICAÇÃO NO SETOR PÚBLICO : Estudo de Caso Sobre a Gestão e Segurança da Informação e Comunicação no Setor Público da Saúde no Município de Caucaia / Francisco Charles Silva. – 2018.
30 f. : il. color.

Trabalho de Conclusão de Curso (especialização) – Universidade Federal do Ceará, 2, Fortaleza, 2018.
Orientação: Prof. Ms. Francisco Jose Aguiar Costa Junior.

1. Segurança. 2. Informação. 3. Comunicação. I. Título

CDD

FRANCISCO CHARLES SILVA

A INFORMAÇÃO E COMUNICAÇÃO NO SETOR PÚBLICO

Estudo de Caso Sobre a Gestão e Segurança da Informação e Comunicação no Setor Público da Saúde no Município de Caucaia

,

Trabalho de Conclusão de Curso apresentado ao Curso de Pós-Graduação Lato Sensu em Gestão Pública Municipal da Universidade da Integração Internacional da Lusofonia Afro-Brasileira como requisito parcial à obtenção do título de Especialista em Gestão Pública Municipal.

Aprovada em: 07/07/2018.

BANCA EXAMINADORA

_____

Prof. Ms., Francisco Jose Aguiar Costa Junior
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

_____

Prof. Dr. Felipe Franklin De Lima Neto
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Carlos Augusto De Oliveira Azevedo Filho
Universidade Federal do Ceará (UFC)

Dedico este trabalho a todos que contribuíram direta ou indiretamente em minha formação acadêmica.

AGRADECIMENTOS

A Deus por ter me dado saúde e força para superar as dificuldades. A esta universidade, seu corpo docente, direção e administração que oportunizaram a janela que hoje vislumbro um horizonte superior, eivado pela acendrada confiança no mérito e ética aqui presentes.
Ao meu orientador Prof. Esp., Francisco Jose Aguiar Costa Junior, pelo suporte no pouco tempo que lhe coube, pelas suas correções e incentivos.
À minha família, pelo amor, incentivo e apoio incondicional.
E a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

.

RESUMO

O Presente trabalho é um estudo de caso sobre a gestão da segurança da informação e comunicação na Secretaria Municipal de Saúde de Caucaia. Um tema bastante atual e de grande importância. A informação em conjunto com os recursos tecnológicos passa a ser uma necessidade para o bom desenvolvimento de qualquer instituição, pois ela reduz as incertezas durante o processo de tomada de decisão. Assim deve-se considerar a necessidade de assegurar ações que possibilitem a segurança da informação e da comunicação como fundamentais para garantir a disponibilidade, a integridade, a confidencialidade e autenticidade da informação. A gestão da segurança da informação e comunicação enfoca principalmente os aspectos gerencias e tecnológicos, como planejamento estratégico, tomada de decisão e as diretrizes de acesso e manuseio dos dados. Quanto ao procedimento metodológico, será utilizada a pesquisa bibliográfica sobre as teorias referentes à informação e a comunicação e sua importância e para fundamentá-la será utilizado a pesquisa por levantamento e análise de dados que nos permite contato com o entrevistado utilizando como instrumento de coleta um questionário com perguntas fechadas.Promover uma política de segurança da informação e da comunicação é importantíssimo na gestão pública, pois com ela criam-se normas padronizadas a ser seguida por todos os integrantes da gestão, uma política que envolva uma série de boas práticas de segurança da informação e da comunicação, e que esteja ajustada às normas público-administrativas para que possam ser aplicadas.Com a aplicação do questionário foi possível observar a necessidade de elaborar com urgência, uma política de segurança da informação e da comunicação para a Secretaria Municipal de Saúde de Caucaia.

Palavras-chave: Segurança. Informação. Comunicação.

ABSTRACT

The present work is a case study on the management of information security and communication in the Municipal Health Department of Caucaia. A very current topic of great importance. Information in conjunction with technological resources becomes a necessity for the good development of any institution, since it reduces uncertainties during the decision-making process. Thus, we must consider the need to ensure actions that enable information and communication security as fundamental to guarantee the availability, integrity, confidentiality and authenticity of the information. Information and communication security management focuses mainly on management and technology aspects, such as strategic planning, decision making and data access and handling guidelines. As for the methodological procedure, we will use a bibliographical research about the theories related to information and communication and its importance and to base it will be used research by survey and data analysis that allows us to contact the interviewee using as an instrument of collection a questionnaire with closed questions. Promoting a policy of information and communication security is very important in public management, as it creates standardized standards to be followed by all members of management, a policy that involves a series of good practices of information and communication security , and that it is adjusted to the public-administrative standards so that they can be applied. With the application of the questionnaire, it was possible to observe the need to urgently elaborate an information and communication security policy for the Municipal Health Department of Caucaia.

Keywords: Security, Information, Communication.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

SUS - Sistema Único de Saúde

SMS – Secretaria Municipal de Saúde

UAPS - Unidades da Atenção Primária à Saúde

UPA – Unidades de Pronto Atendimento

CAPS - Centro de Atendimento Psicossocial

SAE - Serviço de Atendimento Especializado

CRSH - Centro de Referência de Saúde do Homem

CEO - Centro de Especialidades Odontológicas

TIC - Tecnologias de Informação e Comunicação

NBR - Norma Brasileira

ABNT - Associação Brasileira de Normas Técnicas

ISO - International Organization of Standardization

SIC - Segurança da Informação e da Comunicação

IEC - International Electrotechnical Commission

SICI - Segurança das Infraestruturas Críticas da Informação

SUMÁRIO

1. INTRODUÇÃO

O Presente trabalho é um estudo de caso sobre a gestão da segurança da informação e comunicação na Secretaria Municipalde Saúde de Caucaia. Um tema bastante atual e de grande importância principalmente no setor público. A informação em conjunto com os recursos tecnológicos passa a ser uma necessidade para o bom desenvolvimento operacional, tático e estratégico de qualquer instituição, pois ela reduz as incertezas durante o processo de tomada de decisão.

Assim podemos considerar a necessidade de assegurar ações que possibilitem a segurança da informação e da comunicação como fundamentais para garantir a disponibilidade, a integridade, a confidencialidade e autenticidade da informação. A gestão da segurança da informação e comunicação enfoca principalmente os aspectos gerencias e tecnológicos, como **planejamento estratégico**, tomada de decisão **e as diretrizes de acesso e manuseio dos dados.**

Assim o problema que se expõe é como um ambiente que por natureza deveria apresentar políticas de segurança física e lógica mostra-se tão inseguro? A hipótese que levantamos é que a segurança neste ambiente não é levada a sério como deveria e porque a informação gerada e a forma como a comunicação é estabelecida não são compreendidas como ativos tão importantes como qualquer outro da instituição. Segurança é muito mais que estrutura hierárquica, ela envolve um aspecto gerencial.

Sabemos que a palavra comunicação vem do termo latino "communicare", que significa "partilhar, participar algo, tornar comum". Através da comunicação, nós partilhamos diferentes informações, tornando o ato de comunicar uma atividade essencial para a vida em sociedade. A comunicação possui um papel muito importante dentro da sociedade, ela é uma ferramenta necessária para o sucesso de qualquer organização. No entanto para que a comunicação aconteça de forma precisa e segura, é necessário o envolvimento de todos para que haja a troca de informações entre si.

Uma comunicação bem estabelecida e que realmente funcione de forma segura é um grande desafio para todos. Quando comunicamos partilhamos uma informação e a partir do momento que partilhamos essa informação ela precisa estar correta, ela precisa ser partilhada, comunicada em tempo hábil, com isso estaremos aumentando nossa capacidade de conhecimento, permitindo assim, que desempenhemos nossas atividades de forma mais segura, seja no âmbito operacional, tático ou estratégico.

Queremos estudar os processos de comunicação existentes na Secretaria de Saúde Municipal de Caucaia e de como os servidores se comportam frente ao problema da segurança das informações, buscando sempre aperfeiçoar esse fluxo, queremos também conceituar segurança da informação e comunicação e a partir daí entender quais as melhores diretrizes, além de verificar o processo de políticas de segurança da informação existentes na referida secretária.

Pois entendemos que falhas no processo de comunicação, sejam elas por falta de segurança ou por desconhecimento dos processos, geram conflitos entre as partes envolvidas e a gestão só tende a perder. Se as informações forem corrompidas ou extraviadas, produzirão sérias consequências. A informação partilhada reduz as incertezas durante o processo de tomada de decisão, por isso é de extrema importância a transparência nas informações, a confiabilidade e a segurança, para que os agentes que atuam possam acompanhar todo o processo de forma mais clara e mais precisa**.**

Entre as justificativas referentes à segurança da informação e da comunicação destacamos a crescente convergência tecnológica, a elevada interconexão de redes, por isso, faz-se necessário uma visão sobre segurança da informação mais abrangente, e que não seja voltada apenas aos recursos tecnológicos do que ao cliente final, seja ele interno,ou externo.

Quanto aos processos metodológicos e científicos utilizados para a realização da pesquisa serão evidenciados os tipos de pesquisa e o instrumento de coleta de dados. Em relação o tipo de pesquisa quanto aos procedimentos, será utilizada a pesquisa bibliográfica sobre as teorias referentes à Informação e a comunicação e sua importância. Para fundamentá-la utilizamos também o procedimento pesquisa por levantamento, pois é um método de levantamento e análise de dados que nos permite contato com o entrevistado utilizando como instrumento de coleta um questionário com perguntas fechadas.

2. INFORMAÇÃO E COMUNICAÇÃO

Com o advento das tecnologias de informação e comunicação – TIC´sjuntamente com a internet a administração pública vem enfrentando forte pressão por melhorias objetivando melhor atender àqueles que procuram por serviços de qualidade. Em compensação esse progresso fruto do aporte tecnológico trouxe grandes desafios referentes à segurança dos ativos concernente à informação e á comunicação, aumentando assim a demanda por maior nível de proteção das informações geradas e das técnicas de comunicação.

Segundo ABREU, (2003 p.60) “a informação é o resultado de um conjunto de dados que receberam algum tipo de tratamento e que assim podem ser visualizados pelos

usuários" é o registro ou a interpretação de dados vinculados a um contexto, pode ser distribuída sob diversas formas – oral, escrita, audiovisuais – de modo analógico ou digital. E quando a informação não é suficientemente precisa ou completa o profissional que trabalha dependendo dela pode tomar decisões equivocadas, podendo gerar grandes prejuízos. Por esse motivo devemos atentar para as diferenças que ela apresenta, dependendo do valor que é atribuído para cada uma de suas características, dentre as quais podemos destacar (Veja figura 01):

a) **Precisão:** A informação não deve conter erros, ela tem que ser precisa, uma informação imprecisa muitas vezes é originada por dados que foram coletados de forma imprecisa.
b) **Confiável:** A confiabilidade da informação depende muito do método de coleta, quanto mais precisa for a informação mais confiável ela será.
c) **Acessível:** A informação precisa está acessível a todos, que estejam devidamente autorizados, assegurando suas particularidades é claro.
d) **Segura:** A segurança da informação significa que nem todos devem ter os mesmos tipos de acesso, deve-se criar perfis de usuários com acessos diferentes.

Quanto à fonte a informação apresenta algumas características que são:

a) **Formal e interna:** são os documentos internos;
b) **Formal e externa:** são as legislações, pesquisas, outros documentos externos;
c) **Informal e interna:** São as conversas informais;
d) **Informal e externa:** imprensa, congressos, feiras;

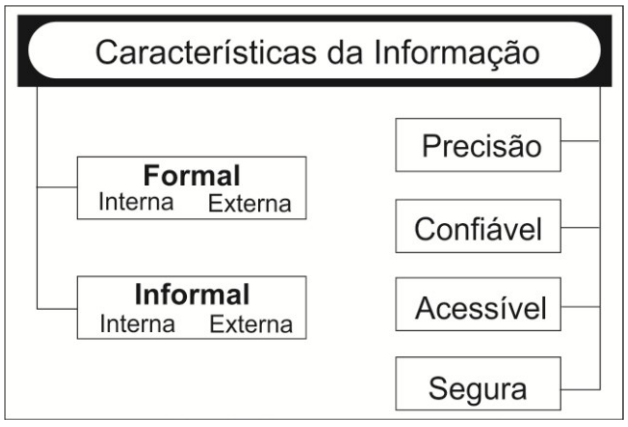

Figura 01 - Características da Informação
Fonte: Elaborado pelo autor

A Norma Brasileira - NBR 27002 de 2005 recomenda que, na classificação da informação, ela seja definida assegurando que a mesma esteja atualizada e no nível apropriado. Ela pode ser classificada como (Veja figura 02):

a) **Confidencial:** A informação que não podemos divulgar tornar público. Naquele devido momento ela é uma informação sigilosa, portanto restrita ao público em geral.
b) **Restrita:** O seu acesso é limitado é resumido.
c) **Pública**: Neste caso todos tem acesso, não restrições nem limites.

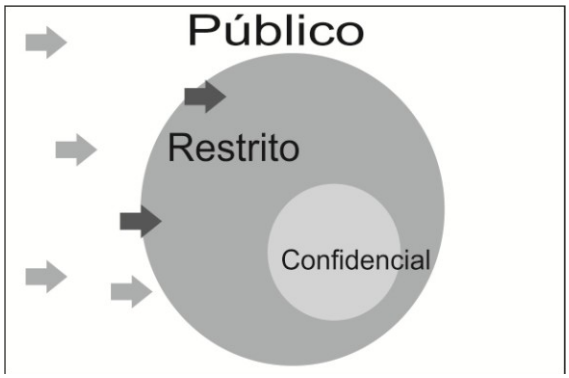

Figura 02 - Classificação da Informação
Fonte: Elaborado pelo autor

Um dos grandes desafios da gestão da informação pelo qual as administrações atualmente passam é a gestão da segurança de seus ativos de informaçãoe comunicação. Se estes não forem mantidos e controlados adequadamente, a instituição certamente sofrerá prejuízos tanto em sua gestão quanto em sua operação. A informação é um bem de valor intangível, mas isso não significa dizer que ela não tenha valor, ou que não possa ser mensurado.

Podemos afirmar que a informação possui um custo para ser gerada, para ser maturada, manuseada e estocada. Este é o seu valor direto, seu valor agregado. Portanto o valor da informação pode ser medido pelo esforço investido em obtê-la e em mantê-la. Ela é reconhecida como o recurso mais importante para a tomada de decisões, sendo necessário haver uma malha de informações abrangendo diversos aspectos técnico-científicos, administrativos, mercadológicos, econômicos, legais, ambientais e políticos.

Na realidade atual, a informação abarca uma série de aspectos, considerados imprescindíveis ao processo de gestão, e sua importância está fundamentada nos seguintes aspectos: a informação vem sendo considerada cada vez mais a base da competição; a informação é considerada como um dos principais recursos de qualquer gestão, devendo ser gerenciada com a mesma preocupação que os recursos tradicionais (finanças, materiais, pessoas, entre outros).

A obtenção de informações do ambiente e do desempenho e da realidade da organização são condições estratégicas para o tempo presente; a informação é a base do processo de tomada de decisões e o instrumento de comunicação e desdobramento de

objetivos. Com isso a segurança da informação tornou-se crucial para sobrevivência das instituições modernas e com isso faz-se necessário uma visão mais abrangente sobre segurança da informação com o desafio de, não apenas proteger um ativo das instituições, a informação, mas contribuir para a estratégia global dos projetos envolvidos.

A segurança da informação pode ser representada pela definição de cinco grandes assuntos que se inter-relacionam e que juntos garantem a proteção adequada ao conhecimento da instituição. É importante lembrar, que para se obter um nível adequado de proteção, esses assuntos não podem ser tratados isoladamente.

As dimensões identificadas são: **Governança** que mostra como a segurança da informação tem que estar alinhada com os interesses da instituição por meio dos controles internos; **Controles** e **Métricas** que trata dos controles internos, controles para tecnologia da informação, a administração de riscos de segurança da informação, esta dimensão se preocupa em verificar o estado atual da instituição;

Pessoas, onde é sobressaltado o papel decisório do capital humano, enfatizando que o sucesso dos controles internos, da proteção do conhecimento depende do nível de conscientização e responsabilidade de cada indivíduo na instituição; a **Tecnologia**, que trata dos assuntos referentes a decisões de aquisição, troca, atualização de equipamentos, programas, sistemas que disseminam a informação pela empresa, agilizam a tomada de decisão e protege a informação empresarial de ameaças externas; e finalmente, **Conformidade** com a legislação, seja ela nacional e internacional mostra a necessidade da preocupação com o cumprimento de normas e a sua legalidade. (Veja figura 03)

Figura 03 – As Dimensões da Segurança da Informação
Fonte: Adaptado de ISACA, 2009 p. 14

Assim a informação e os processos de comunicação começaram a desempenhar um papel predominante em todas as atividades consolidando-se como um dos principais ativos agregando valor às tomadas de decisões e direcionando as ações de forma mais adequada e ao alcance dos resultados esperados pela gestão. Para Mauro Wolf (1999) o

processo de comunicação ocorre quando o emissor emite uma mensagem ao receptor através de um canal. O receptor interpretará a mensagem que pode ter chegado até ele com algum tipo de barreira (ruído,bloqueio, filtragem) e, a partir daí, dará a resposta, completando o processo de comunicação.” (Veja figura 04)

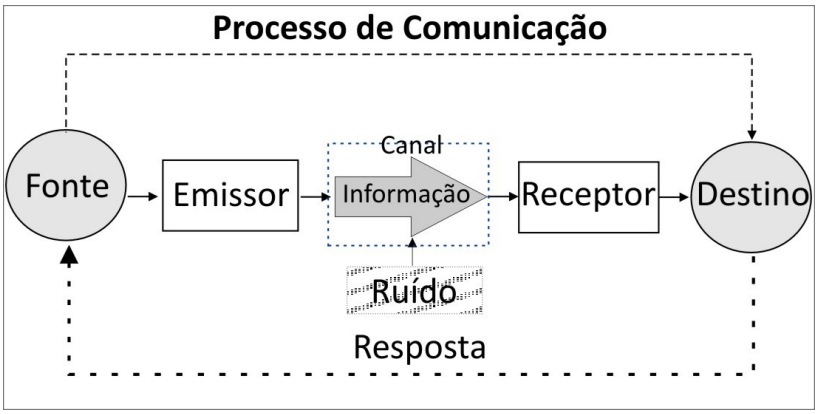

Figura 04 – Processo de Comunicação
Fonte: Adaptado de Francisco Rüdiger, 2011 p.20

Segundo Francisco Rüdiger (2011) no processo de comunicação a fonte simboliza aquele que executa a mensagem. O emissor é aquele que emite a mensagem, que a transforma em um sinal que será transportado pelo canal, meio pelo qual se passa o sinal da fonte para o receptor. O receptor é um tipo de transmissor invertido, que decodifica o sinal recebido, assegurando que ele chegue ao seu destino. A distorção da mensagem ou ruído é produzida por diversos fatores que, mesmo não desejado pela fonte, somam-se ao sinal durante o trabalho de envio. A resposta constitui, constitui um conjunto de procedimentos que facilita o controle, pela fonte emissora, de como o receptor está recebendo as informações.

Portanto não podemos esquecer que assim como a informação, a comunicação também é um ativo imprescindível para qualquer organização, pois ela produz, registra todas as relações com os clientes da instituição. Por isso estabelecer metas que garantam a segurança desses ativos passa a ser uma tarefa indispensável para o alcance da qualidade nos serviços oferecidos. Segundo a ABNT NBR-ISO/IEC 17799:2005 (Associação Brasileira de Normas Técnicas, 2005, p.9),

> “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.” 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.”

A Segurança da Informação e da Comunicação – SIC é o ponto principal para a preservação das atividades nas instituições e para a qualidade dos serviços prestados. Diversos

são os problemas envolvidos, ao mesmo tempo em que as instituições dependem das informações arquivadas nos sistemas computacionais para a tomada de decisão. Portanto podemos dizer que a SIC compreende um pacote de medidas formadas basicamente de controles e de políticas de segurança, tendo como objetivo a preservação das informações e dos processos de comunicação, através da gerência das ameaças ou adulteração por indivíduos não autorizados. De acordo com as boas práticas em segurança da informação do Tribunal de Contas da União, p.10,

> "Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações."

Podemos ver que as políticas que envolvem a SIC tem a função de criar diretrizes estratégicas, e desenvolver habilidades, buscando garantir a integridade, confidencialidade, disponibilidade e autenticidade das informações (NBR 17799, 2005, p.1). Assim entendemos que as políticas que garantem a SIC são normas que apontam formalmente as regras e os direitos para todos os colaboradores, buscando sempre a preservação apropriada dos que compartilham a informação e praticam os processos de comunicação. Segundo o portal Governo Digital do Ministério do Planejamento,

> "Disponibilidade, Integridade, confidencialidade e Autenticidade - problemas decorrentes da falta desses atributos nos ativos de informação levam à necessidade de desenvolver ações permanentes de segurança nas organizações governamentais"

A garantia da segurança da informação e a comunicação pode ser mantida com a elaboração e implementação de diretrizes de segurança que mantenham esses ativos seguros de qualquer vulnerabilidade ou ameaças. É primordial que seja identificado os requisitos de segurança da informação e comunicação. Segundo a Norma Técnica ABNT NBR ISO/IEC 17799:2005 no item 04,

> "Os requisitos de segurança da informação são identificados por meio de uma análise/avaliação sistemática dos riscos de segurança da informação. Os gastos com os controles precisam ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança da informação."

É imprescindível que se determine controles que possibilitem o monitoramento e diagnóstico crítico dos serviços de comunicação de dados contratados de terceiros para suprir às deficiências e carências do setor púbico. A finalidade desse controle é o de garantir a execução das decisões referentes ao serviço contratado por parte da empresa, observando as recomendações do item 10.2 e 10.2.2 da Norma Técnica ABNT NBR ISO/IEC 17799:2005.

> "Convém que a organização verifique a implementação dos acordos, monitore a conformidade com tais acordos e gerencie as mudanças para garantir que os serviços

> entregues atendem a todos os requisitos acordados com os terceiros. E que os serviços, relatórios e registros fornecidos por terceiro sejam regularmente monitorados e analisados criticamente, e que auditorias sejam executadas regularmente."

Para melhorar a gestão da SIC é necessário focar também nas pessoas envolvidas no processo e não apenas nas tecnologias. O agente humano também é responsável pela integridade dos ativos da instituição, seu comportamento deve observar fatores culturais, educacionais e principalmente a conscientização da maneira correta e segura do uso das tecnologias (ver figura 04). Segundo a Norma Técnica ABNT NBR ISO/IEC 17799:2005 no item 11,

> "Convém que o acesso à informação, recursos de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação,... e que todos os usuários tenham um identificador único (ID de usuário) para uso pessoal e exclusivo, e convém que uma técnica adequada de autenticação seja escolhida para validar a identidade alegada por um usuário."

Todos aqueles que usam o sistema fazem parte do chamado elemento humano, essencialmente os que têm acesso aos recursos tecnológicos. A segurança não é um empecilho para a tecnologia, e sim para as pessoas que a manipulam, por isso se tornam o elemento mais difícil de coordenar e avaliar. Por ser um dos fatores na SIC, o elemento humano precisa de controle continuo, é preciso também investir na organização e na capacitação das equipes internas, que é o ponto mais frágil de toda a ação, sempre objetivando atingir a perfeição nos serviços públicos. Segundo a Norma Técnica ABNT NBR ISO/IEC 17799:2005 no item 15.1.5,

> "Convém que todos os usuários estejam conscientes do escopo preciso de suas permissões de acesso e da monitoração realizada para detectar o uso não autorizado. Isto pode ser alcançado pelo registro das autorizações dos usuários por escrito, convém que a cópia seja assinada pelo usuário e armazenada de forma segura pela organização. Convém que os funcionários de uma organização, fornecedores e terceiros sejam informados de que nenhum acesso é permitido com exceção daqueles que foram autorizados."

Com isso precisamos entender que a segurança deve ser abordada como parte da instituição e não apenas como mais uma necessidade do setor de tecnologia. Para que possamos prevenir as ameaças de maneira mais decisiva e eficaz é necessário que saibamos como coletar os dados para assim compreendermos melhor os procedimentos, desta forma poderemos garantir as atividades que assegurem a segurança da informação e comunicação como essenciais.

Entendemos por ameaça tudo aquilo que diz respeito ao risco ou a possível situação de perigo que pode causar possíveis danos a quem estar envolvido. É um

acontecimento ou uma conduta indesejável que é capaz de desabilitar ou destruir um ativo. As ameaças geralmente tiram proveito das falhas de segurança da instituição, elas normalmente não podem ser controladas. De acordo com Flávia Estélia em Gestão da Segurança da Informação NBR 27001 e NBR 27002 p. 87

> "Ameaças são eventos que exploram vulnerabilidades (fragilidades) e podem causar danos. O impacto é a consequência de uma vulnerabilidade ter sido explorada por uma ameaça."

Quando falamos em ameaça percebemos que ela poder ser qualquer coisa que venha atuar sobre um ativo da instituição por meio da vulnerabilidade produzindo assim consequências desastrosas (ver figura 05). A existência dela é decorrente da presença de vulnerabilidades, portanto, as informações importantes devem ter a proteção necessária contra tudo o que for ameaça. Segundo Flávia Estélia,

> "As pessoas devem conhecer as possíveis ameaças e riscos de segurança, de forma que entendam seu papel quanto à segurança da informação na organização. De modo especial, todos devem efetuar suas ações em conformidade com a política de segurança vigente, reduzindo, assim, a ocorrência de erros humanos e, consequentemente, os riscos. (Gestão da Segurança da Informação NBR 27001 e NBR 27002 p. 100)"

	INFORMAÇÕES		
ATIVOS	**Físicos** Agenda Sala Arquivo	**Tecnológicas** Sistemas Email Servidor (PC)	**Humanos** Servidores Fornecedores Terceiros
	VULNERABILIDADE		
AMEAÇAS	**Físicas** Incêndio Inundação Curto circuito	**Tecnológicas** Vírus Falha técnica Invasão	**Humanas** Sabotagem Fraude Descuido

Figura 05 – Ativos e Ameaças
Fonte: Elaborado pelo autor

Quando a ameaça ocorre é sinal de que houve falha na manutenção de dados confidenciais fazendo com que informações sigilosas se tornem expostas a todos, ou quando ela fica visível à manipulação não permitida, efetuando assim qualquer alteração sem autorização e sem o conhecimento do responsável pela mesma. Outro caso seria quando a perda no processo de comunicação seja por falhas na rede, nos equipamentos ou até mesmo conduta desautorizada fazendo com que a informação deixe de estar disponível ao acesso de todos. Segundo Marcos Aurelio Laureano,

> "A vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações, etc. Todos os ambientes são vulneráveis, partindo do principio de que não existem ambientes totalmente seguros. Muitas vezes encontramos vulnerabilidades nas medidas implementadas pela empresa." (Gestão da Segurança da Informação p.17)

Para que possamos nos proteger de qualquer risco precisamos saber identificar as vulnerabilidades, fazendo-se necessário um diagnóstico e avaliação dos controles que foram ou serão instalados, com o intuito de reduzir a hipótese de uma ameaça encontrar vulnerabilidade presentes. O reconhecimento de possíveis ameaças e vulnerabilidades envolve a etapa de estudo e observação e avaliação dos riscos. Para encontrar e analisar falhas em um universo informatizado utilizamos a técnica de avaliação de vulnerabilidade. Quando é realizado o reconhecimento e avaliação dos riscos, teremos uma panorâmica do cenário atual, este é um procedimento de identificação constante dos resultados para que medidas possam ser tomadas.

A análise de vulnerabilidade constitui uma técnica conhecida como gerenciamento de risco, é uma metodologia bem mais ampla que nos permite ter uma visão geral do gerenciamento de riscos. Os processos de gerenciamento de risco englobam qualquer situação que pode gerar danos patrimoniais à instituição. A figura 06 nos apresenta algumas das etapas que compõe o gerenciamento de riscos.

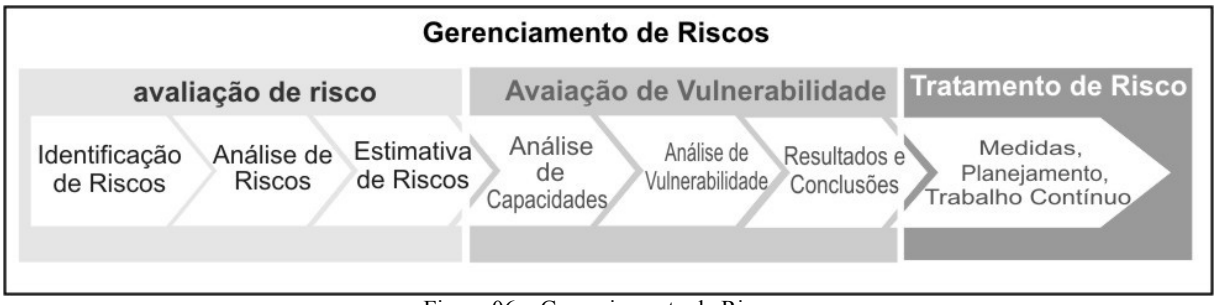

Figura 06 – Gerenciamento de Riscos
Fonte: Elaborado pelo autor

O processo de avaliação de risco é a técnica usada para descobrir o verdadeiro potencial da ameaça com métodos que definam e analisem de uma forma ordenada os riscos de segurança, descobrindo e averiguando falhas em um determinado ambiente, ela é a parte central do Gerenciamento de Riscos.Com a avaliação de risco realizada poderemos determinar se o risco é ou não aceitável para a instituição.

A análise de vulnerabilidade vai alimentar a instituição sobre informações, muitas vezes desconhecidas, sobre sua rede com relação ao que pode acontecer, com que frequência e a quão crítica é a consequência, somada a um relatório técnico detalhando de quais serviços e sistemas estão sujeitos a quais tipos de ameaça. De pose dessas informações a gestão será

capaz de tirar conclusões sobre seu estado atual de exposição a ameaças.Assim você terá em mãos o conhecimento mais que necessário para traçar um plano de ação. Em seguida, basta colocar a mão na massa e partir para o próximo passo!

> "São três os fatores considerados na formulação de estratégias para atender os requisitos mínimos necessários à Segurança das Infraestruturas Críticas da Informação: segurança, resiliência e capacitação. (Guia SICI p 84")

Uma das ações que seria essencial para qualificar a SIC seria assumir procedimentos simples, contudo eficientes, treinar os servidores quanto às táticas de segurança para impedir ataques, implementar diretrizes quanto ao emprego de senhas complexas para acesso a e-mails e sistemas. Existem incontáveis formas e tecnologias que possam melhorar a SIC no setor público.

3. A Secretaria Municipal de Saúde de Caucaia

A Secretaria Municipal de Saúde de Caucaia - SMS é um órgão da administração direta do Governo Municipal de Caucaia, ela é responsável porgerenciar no Município o Sistema Único de Saúde (SUS). A SMS Possui 46 Unidades da Atenção Primária à Saúde – UAPS, seis destas possuem residência médica, 02 Unidades de Pronto Atendimento – UPAS, 01 Hospital e 01 Maternidade, 03 Centro de Atendimento Psicossocial – CAPS, 01 S.O.S., 01 Serviço de Atendimento Especializado – SAE, 01 Centro de Referência de Saúde do Homem – CRSH, além de 01 Centro de Especialidades Odontológicas – CEO, com isso a SMS deseja alcançar sua missão que é garantir um serviço de saúde de qualidade à população, com acesso integral eresolutivo em todos os níveis de atenção, assegurando uma gestão eficiente das políticas públicas de saúde, fazendo uma gestão eficiente e humanizada para toda a população. O questionário que foi aplicado na pesquisa foi elaborado com 37 perguntas objetivas e por questão de logística o mesmo foi aplicado somente na sede da SMS, entre os 13 setores existentes. Os dados obtidos através do questionário foram analisados e serão mostrados na seção seguinte.

4. ANÁLISE DOS DADOS

Foram distribuídos 30 questionários dentro da Secretaria Municipal de Saúde, apenas 22 responderam os demais relataram falta de tempo, destes 22 mostrou-se que o quadro funcional dos servidores é composto por um perfil mais maduro, ou seja 32% estão com idade entre 40 e 50 anos, e 23% dos servidores com idade entre 30 e 40 anos, e apenas 22% entre os 50 a 70 anos. Indicando um público relativamente maduro e experiente.(ver gráfico 01)

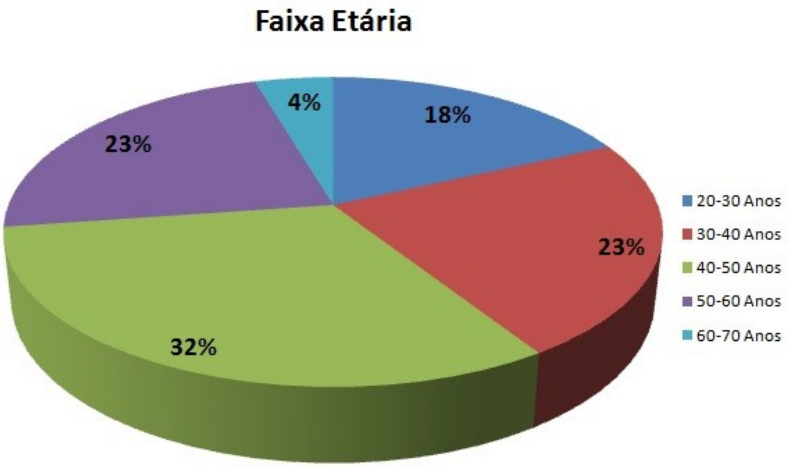

Gráfico 01 – Faixa Etária

Quanto à formação acadêmica destes servidores de acordo com a pesquisa podemos constatar que 37% possuem apenas graduação, 21% possuem título de especialista, 10% não concluíram a graduação e 32% não informou. (ver gráfico 02)

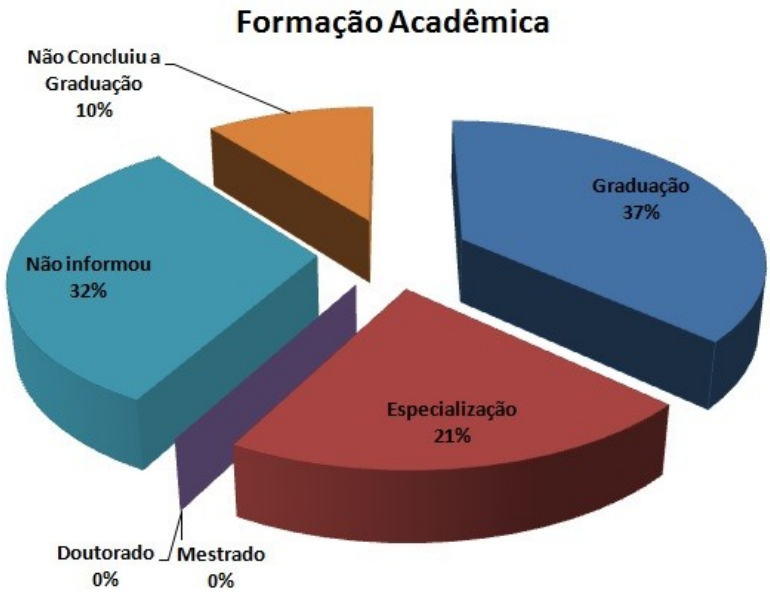

Gráfico 02 – Formação Acadêmica

Em relação ao tipo de vínculo apenas 36% são servidores efetivos, 41% possuem outro tipo de vínculo e 23% não informou (ver gráfico 03). Essa realidade é um tanto... no que diz respeito à continuidade dos trabalhos em cada gestão dificultando assm uma continuidade nos planos de segurança.

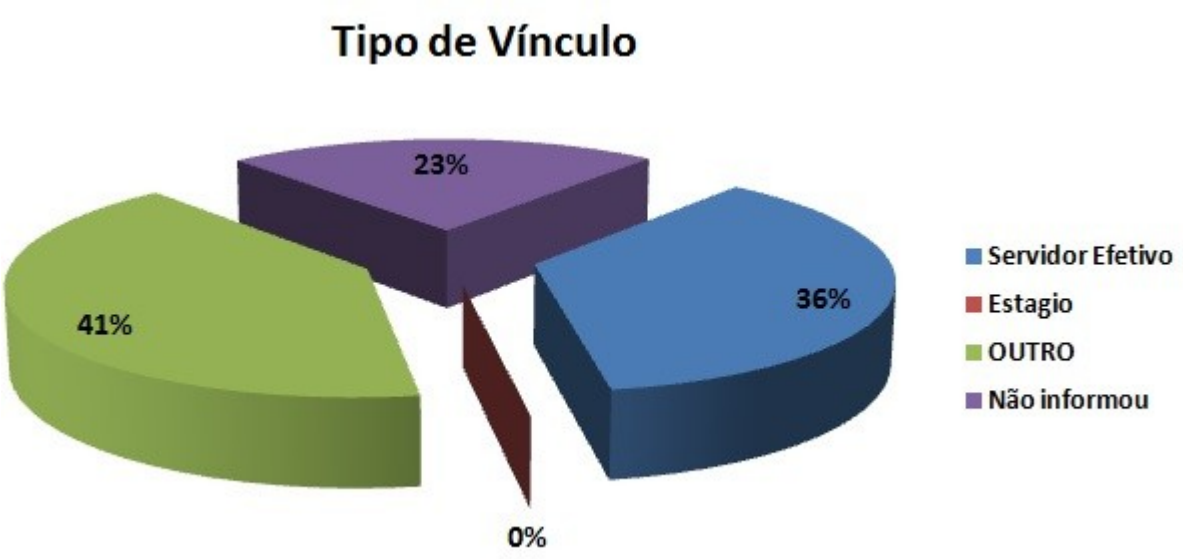

Gráfico 03 – Tipo de Vinculo

Em relação ao sexo 59% são do sexo feminino e 41% do sexo masculino (ver gráfico 04). Esses dados nos mostram como é o perfil dos servidores lotados na Secretaria Municipal de Saúde de Caucaia, onde a maioria do sexo feminino não concursado e com idade entre 30e 60 anos. (ver gráfico 04)

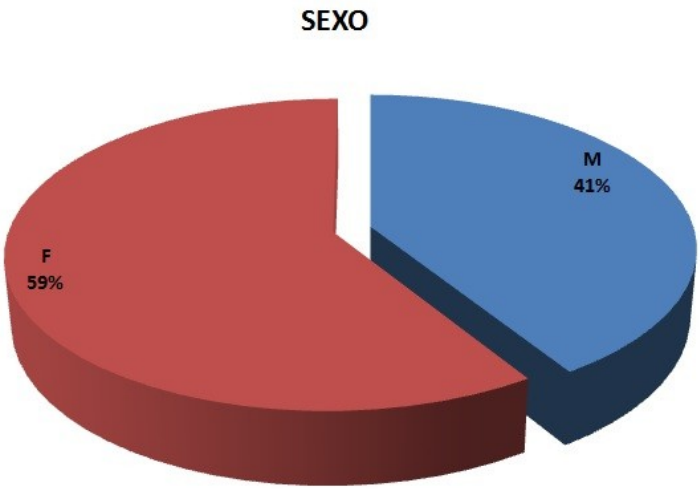

Gráfico 04 - Sexo

Quanto aos itens relativos à segurança dividimos em dois: segurança física reativa aos equipamentos e a segurança lógica concernente aos softwares utilizados. Quanto à segurança física esse é um dos itens que mais preocupa, pois na secretaria não existe nenhum tipo de

política de segurança, pessoas sem credenciais circulam livremente pelos corredores da secretaria, os equipamentos não são protegidos por nenhum tipo de proteção seja capa plástica ou contra queda de tensão da rede elétrica, os documentos que não serão mais utilizados são usados para rascunho e não destruídos.

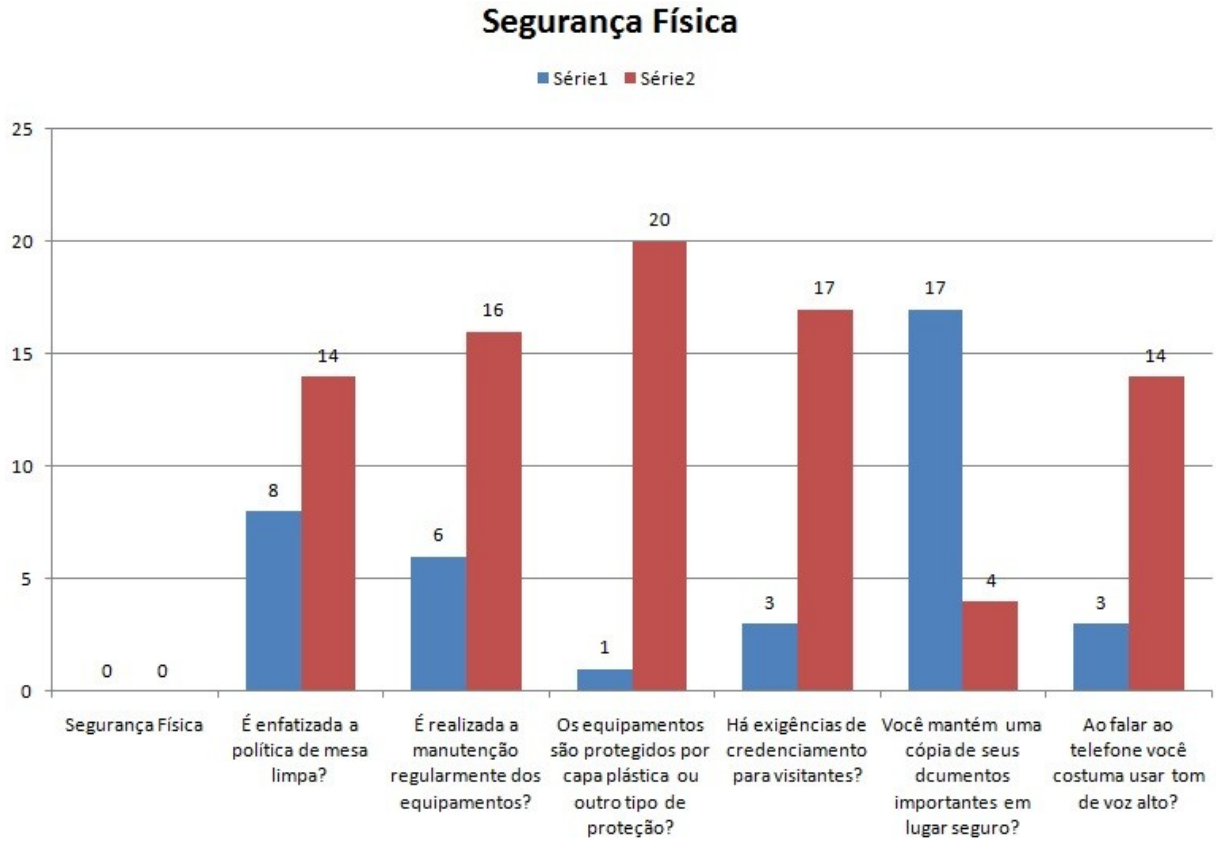

Gráfico 05 – Segurança Física

Quanto à segurança lógica não é realizado nenhum tipo de treinamento sobre segurança, não é feito nenhum tipo de cópia de segurança, e a maioria dos servidores ao se ausentarem da sala não bloqueiam a sua estação de trabalho, deixando e-mails conectados além de não utilizarem nenhum antivírus ao plugarem as unidades móveis (pen drives, HD externos) por considerarem perda de tempo.

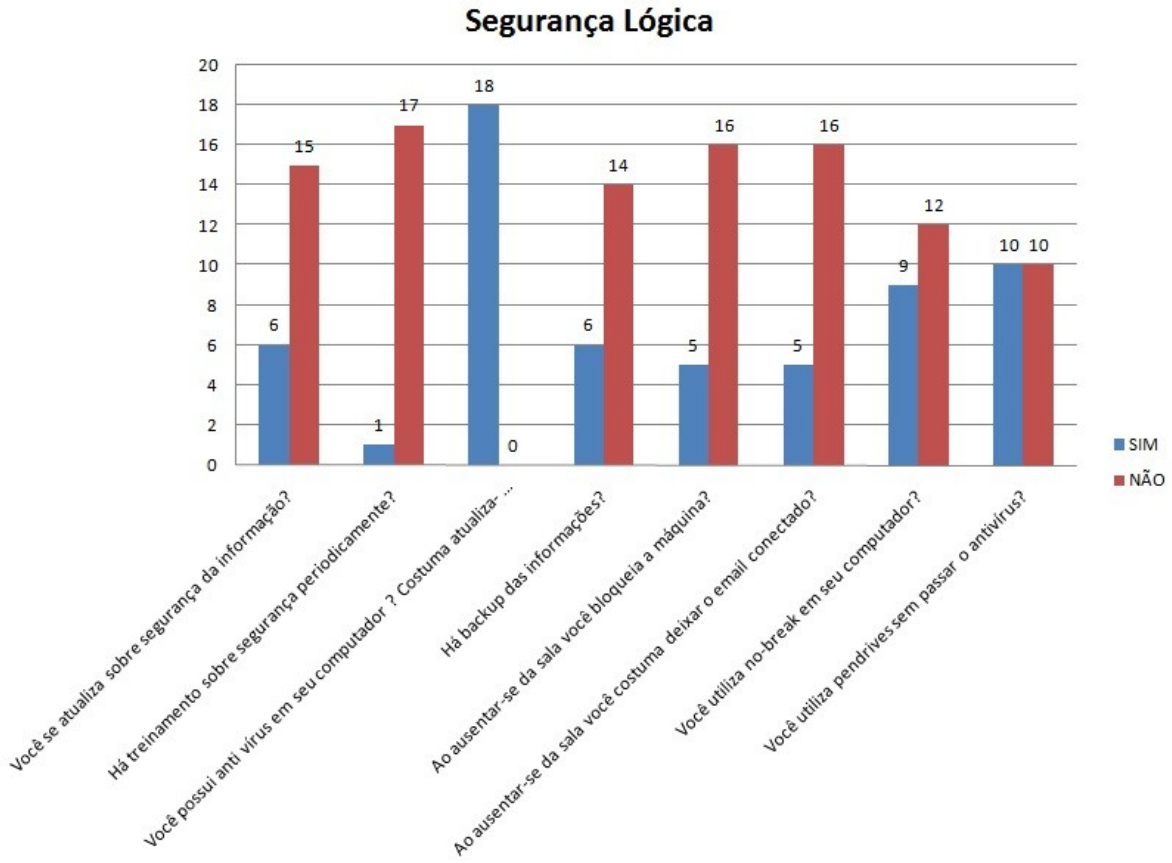

Gráfico 06 – Segurança Lógica

5. CONCLUSÃO

Promover uma política de segurança da informação e da comunicação é importantíssimo na gestão pública, pois com ela criam-se normas padronizadas a ser seguida por todos os integrantes da gestão, uma política que envolva uma série de boas práticas de segurança da informação e da comunicação, e que esteja ajustada às normas público-administrativas para que possam ser aplicadas.

Com a aplicação do questionário pudemos observar a necessidade de elaborar com urgência, uma política de segurança da informação e da comunicação para a Secretaria Municipal de Saúde de Caucaia, essa análise está baseada no resultado obtido pela pesquisa onde constatamos um público de perfil maduro, ou seja 32% dos servidores estão com idade entre 40 e 50 anos, e que 41% não possuem vínculo estatutário com a instituição, sendo contratos temporários ou comissionados e 51% dos servidores entrevistados são do sexo feminino.

Durante o processo de entrevista e anterior à pesquisa encontrou-se a dificuldade por parte dos servidores entrevistados no manuseio e no entendimento das tecnologias

utilizadas na instituição além da falta de padronização nos documentos e no atendimento à população, criando dificuldades e obstrução nos canais de comunicação.

Essas dificuldades tornam mais frágeis o manuseio das informações criando um ambiente instável e inseguro, principalmente quando se permite o acesso de todos ao interior da instituição sem qualquer tipo de credenciamento e quanto à segurança lógica, ou seja dos dados informatizados foi visto que não é feito nenhum tipo de cópia de segurança.

Também não é realizado nenhum tipo de treinamento sobre segurança, sobre proteção dos ativos da instituição, foi diagnosticado também que a maioria dos servidores ao se ausentarem da sala não bloqueiam a sua estação de trabalho, deixando e-mails conectados além de não utilizarem nenhum antivírus ao plugarem as unidades móveis (pen drives, HD externos) por considerarem perda de tempo.

Para que possamos resolver tal situação precisamos elaborar uma política de segurança bem estruturada e isso requer bastante tempo e dedicação, e deve ser elaborada com a cooperação de todos os gestores, liderados por especialistas em segurança da informação e da comunicação.

A preparação, construção e estudo dos termos incluídos na política de segurança da informação e da comunicação deverá ser de responsabilidade de pessoal qualificado e certificado, no entanto sua aprovação deverá ser feita pelo gestor.

Com a aprovação das políticas de segurança da informação e da comunicação e sua total divulgação junto aos servidores não haverá a menor dúvida de que muitas das prováveis complicações envolvendo a confidencialidade, disponibilidade e integridade das informações serão evitadas.

Por isso é necessário, para que as políticas de segurança da informação e da comunicação se tornem mais efetiva, mais confiável, o avanço nas propostas e orientações estabelecidas. E só alcançaremos essa realidade por meio do compromisso dos atores envolvidos no processo.

O aspecto humano foi o que apresentou o menor índice de proteção por isso precisa de uma atenção redobrada para que possamos reduzir o número de incidentes quanto à segurança da informação e da comunicação. Não devemos esquecer que o fator humano é dos maiores responsáveis pelas falhas ocorridas na segurança da informação e da comunicação.

6. BIBLIOGRAFIA

Associação Brasileira de Normas Técnicas (ABNT). ABNT NBR ISO/IEC17799.
Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

Boas práticas em segurança da informação / Tribunal de Contas da União. – 4. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

_____. Tribunal de Contas da União. Acórdão nº. 1137/2012-2ª Câmara. Levantamento de Governança de TI 2014. Brasília, 20125. Disponível em: <https://contas.tcu.gov.br/etcu/ObterDocumentoSisdoc?seAbrirDocNoBrowser=true&codArqCatalogado=4210319>. Acesso em: 08mai 2018

_____.Governo Digital - Ministério do Planejamento, Desenvolvimento e Gestão. Disponível em: <http://www.digix.com.br/governanca-de-ti-no-setor-publico/>. Acesso em: 10 mai 2018

Guia de referência para a segurança das infraestruturas críticas da informação / Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações – Brasília: GSIPR/SE/DSIC, 2010.

Demo, Pedro. Metodologia científica em ciências sociais. São Paulo: Atlas, 1995

Demo, Pedro. Pesquisa e construção de conhecimento. Rio de janeiro: Tempo Brasileiro, 1997.

Rüdiger, Francisco. As teorias da comunicação / Francisco Rüdiger. – Porto Alegre : Penso, 2011

Mauro Wolf (1999) **TEORIAS DA COMUNICAÇAO,** Editorial Presença 5.'edição, Lisboa, Setembro, 1999

ISACA, 2009, An Introduction to the Business Model for Information Security

ABREU, Aline França de. Tecnologia da informação aplicada a sistemas de informa- ção empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas. 4. ed. São Paulo: Atlas, 2006.