COINTER PDVGT 2020
IV CONGRESSO INTERNACIONAL DE GESTÃO E TECNOLOGIAS
Edição 100% virtual | 02 a 05 de dezembro
ISSN:2596-0857 | PREFIXO DOI:10.31692/2596-0857

CAPTURA DE DADOS: AQUISIÇÃO NÃO AUTORIZADA POR MEIO DE APARELHOS DE VIGILÂNCIA ELETRÔNICA NO MUNICÍPIO DE PICOS-PI

CAPTURA DE DATOS: ADQUISICIÓN NO AUTORIZADA MEDIANTE DISPOSITIVOS DE VIGILANCIA ELECTRÓNICA EN EL MUNICIPIO DE PICOS-PI

DATA CAPTURE: UNAUTHORIZED ACQUISITION THROUGH ELECTRONIC SURVEILLANCE DEVICES IN THE MUNICIPALITY OF PICOS-PI

Apresentação: Comunicação Oral

Luis Henrique Carvalho Barros[1]; Éder Jânio Francisco Gomes[2]

DOI: https://doi.org/10.31692/2596-0857.IVCOINTERPDVGT.0031

RESUMO

A captura de dados aliado a segurança eletrônica é um modelo de proteção que vem em uma ascendência gigantesca, entretanto tudo que se torna mais visível produz aspectos positivos e negativos, em que a maior segurança física e residencial teve uma melhoria significativa, mas os crimes virtuais passaram a ser mais frequentes devido as falhas encontradas nos sistemas utilizados e na falta de propagação e instrução acerca do manuseio desses aparelhos de segurança. Diante disso, o presente trabalho busca analisar todas as falhas já ocorridas e registradas por utilitários do campo de vigilância eletrônica no município de Picos-PI, intensificando o aumento da proteção dos dados dos usuários por meio de medidas autossuficientes, definindo todas as possibilidades de melhorias na segurança da ingressão aos dados, especificando a forma de acesso ao sistema e descrevendo os mais variáveis processos existentes para dificultar a retirada dos dados através de chaves de acesso, além de fazer uma análise de forma satisfatória com clientes e empregadores do ramo de segurança eletrônica atrelada a segurança das informações. A pesquisa será feita de forma qualitativa e opinativa, por meio de questionários com os utilitários dos sistemas, os mesmos serão do tipo objetivo, explanando acerca da funcionalidade, do registro, dos processos incrementados e da utilização do sistema, em que será utilizado como análise, documentários, conteúdos históricos, falas de sujeitos, fatos comprovados e devidamente registrados, dentre outras técnicas, buscando então proporcionar um maior conforto e segurança para os utilitários desse meio, trazendo soluções claras e objetivas para os sistemas desenvolvidos e propagando um modelo de aprendizado para os aquisitores dessa area de atuação, produzindo assim maior confiabilidade e integridade aos requisitos desse modelo de segurança. Levando em conta que os resultados foram atribuidos a probabilidade de respostas identificadas por meio da analise dos questionários, obtendo-se um maior compreendimento acerca da influência do conhecimento sobre as ameaças existentes, as ferramentas de proteção de dados, o conhecimento e a confiabilidade acerca dos sistemas de segurança, adquirindo assim como conclusão que à existência de falhas em sistemas de segurança eletrônica e a falta de conhecimento dos utilitários a cerca dos mesmos, se tornam assim um campo de alto risco e instabilidade, podendo se manter exposto a diversos ataques tecnológicos.

[1] Bacharelado em Ciência da Computação, Instituto de Educação Superior Raimundo Sá, luishenriquepi@hotmail.com
[2] Especialista em Mídias na Educação, Instituto de Educação Superior Raimundo Sá, ederjanio@yahoo.com.br

Palavras-Chave: Captura de Dados, Segurança da Informação, Segurança Eletrônica.

RESUMEN
La captura de datos combinada con la seguridad electrónica es un modelo de protección que viene en una ascendencia gigantesca, sin embargo todo lo que se vuelve más visible produce aspectos positivos y negativos, en los que una mayor seguridad física y residencial ha mejorado significativamente, pero delitos virtuales se hicieron más frecuentes debido a las fallas encontradas en los sistemas utilizados y la falta de propagación e instrucción sobre el manejo de estos dispositivos de seguridad. Ante esto, el presente trabajo busca analizar todas las fallas que ya han ocurrido y registradas por las empresas eléctricas en el campo de la vigilancia electrónica en el municipio de Picos-PI, intensificando la mayor protección de los datos de los usuarios a través de medidas autosuficientes, definiendo todas las posibilidades de mejora. en la seguridad del ingreso de datos, especificando la forma de acceso al sistema y describiendo los procesos existentes más variables para dificultar la eliminación de datos mediante claves de acceso, además de realizar un análisis satisfactorio con clientes y empleadores en el campo de la seguridad electrónica vinculado a la seguridad de la información. La investigación se realizará de forma cualitativa y testaruda, a través de cuestionarios con las utilidades de los sistemas, serán del tipo objetivo, explicando sobre la funcionalidad, el registro, los procesos incrementales y el uso del sistema, en el cual se utilizará como análisis. , documentales, contenido histórico, discursos de temas, hechos comprobados y debidamente registrados, entre otras técnicas, buscando brindar mayor comodidad y seguridad a las utilidades de este medio, aportando soluciones claras y objetivas a los sistemas desarrollados y difundiendo un modelo de aprendizaje para adquirientes en esta área de actividad, produciendo así una mayor confiabilidad e integridad a los requerimientos de este modelo de seguridad. Teniendo en cuenta que los resultados se atribuyeron a la probabilidad de respuestas identificadas a través del análisis de los cuestionarios, obteniendo una mayor comprensión sobre la influencia del conocimiento sobre las amenazas existentes, herramientas de protección de datos, conocimiento y confiabilidad sobre el sistemas de seguridad, adquiriendo así como conclusión que la existencia de fallas en los sistemas electrónicos de seguridad y el desconocimiento de las utilidades que los rodean, se convierten así en un campo de alto riesgo e inestabilidad, pudiendo quedar expuesto a diversos ataques tecnológicos.
Palabras Clave: Captura de Datos, Seguridad de la Información, Seguridad Electrónica.

ABSTRACT
Data capture combined with electronic security is a protection model that comes in a gigantic ancestry, however everything that becomes more visible produces positive and negative aspects, in which greater physical and residential security has significantly improved, but virtual crimes they became more frequent due to the flaws found in the systems used and the lack of propagation and instruction about the handling of these safety devices. In view of this, the present work seeks to analyze all the failures that have already occurred and registered by utilities in the field of electronic surveillance in the municipality of Picos-PI, intensifying the increased protection of user data through self-sufficient measures, defining all possibilities for improvements. in the security of data entry, specifying the form of access to the system and describing the most variable existing processes to hinder the removal of data through access keys, in addition to making a satisfactory analysis with customers and employers in the field of electronic security linked to information security. The research will be done in a qualitative and opinionated way, through questionnaires with the systems utilities, they will be of the objective type, explaining about the functionality, the registration, the incremented processes and the use of the system, in which it will be used as analysis , documentaries, historical content, speeches of subjects, proven and properly recorded facts, among other techniques, seeking to provide greater comfort and safety for the utilities of this medium, bringing clear and objective solutions to the systems developed and propagating a learning model for acquirers in this area of activity, thus producing greater reliability and integrity to the requirements of this security model. Taking into account that the results were attributed to the probability of responses identified through the analysis of the questionnaires, obtaining a greater understanding about the influence of knowledge on existing threats, data protection tools, knowledge and reliability about the security systems, thus acquiring as a conclusion that the existence of flaws in electronic security systems and the lack of knowledge of the utilities around them, thus become a field of high risk and instability, and can remain exposed to various technological attacks.

Keywords: Data Capture, Electronic Security, Information Security.

INTRODUÇÃO

Praticamente de forma obrigatória as empresas e a sociedade tiveram que buscar um modelo de proteção físico e virtual para o seu meio, em busca de melhorias na qualidade de vida, na privacidade e na proteção individual, o uso da tecnologia atrelada a segurança eletrônica traria um maior suporte e qualidade ao longo do tempo que fosse sendo aperfeiçoado e melhor utilizado.

> A tecnologia da informação alterou o mundo dos negócios de forma irreversível. Desde que a tecnologia da informação foi introduzida sistematicamente em meados da década de 50, a forma pela qual as organizações operam, o modelo de seus produtos e a comercialização destes produtos mudaram radicalmente. (MCGEE, 1994, p 5).

Assim como a evolução pode ajudar todo o âmbito mundial, surgem também as falhas, em que é nelas que os seres humanos por diversas vezes se aproveitam, necessitando assim de uma excelente estratégia em qualquer empresa e em ambientes residenciais. Portanto, a segurança dos dados implementada na vigilância eletrônica tem a finalidade primordial ser uma dessas estratégias, fornecendo assim maior proteção e comodidade a sociedade.

Em diversos casos observados as falhas não estão nos sistemas em si ou nas interfaces ou até no processamento das informações, mas sim em quesitos básicos, tais quais podem ser falhas além de técnicas, falhas humanas, passando assim a destinar possíveis erros no processamento dos dados. Segundo a análise de (SILVA, 2008), os grandes problemas que surgem na segurança em organizações é devido a inúmeras falhas desde a implantação dos sistemas, passando pelo desenvolvimento do processo, até chegar ao produto final.

Segundo (CELSO, 2011), nos tempos atuais, as empresa criam hábitos de armazenamento computacional de informações, podendo ser por um ponto de vista da administração ou por exigência do governo. Diante disso, o objetivo de nosso estudo é demonstrar os métodos de segurança utilizados para explanar o quanto seguro é o sistema utilizado e a importância que é composto e que mesmo com toda segurança pode fornecer melhorias evitando assim possíveis perda de informações que são de âmbitos pessoais dos usuários.

Desse modo, a segurança eletrônica usa parte da segurança, que por intermédio de sistemas eletrônicos, são projetados para monitorar, detectar e alarmar eventos previamente programados, busca promover a proteção de pessoas, bens e valores. Baseando-se na ideia de (BLUEPHOENIX, 2008), qualquer emprega de pequeno porte até chegar a uma multinacional que garantem a continuação do negócio e a confiabilidade da mesma, por meio da estabilidade

demonstrada na sua segurança, permitindo assim os investimentos das pessoas, sem que esteja propícios a nenhuma ameaça ou perigo. Os sistemas de segurança eletrônica têm como objetivo detectar e inibir eventos indesejáveis, prevenir ocorrências por intermédio do efeito dissuasivo, detectar automaticamente o início de um evento indesejado e comunicar, remotamente, que algo está em desacordo ao previsto. Refere-se também ao emprego de equipamentos eletrônicos, de forma integrada e sistematizada com o objetivo de certificar a segurança e a integridade. É um grupo de sistemas que alia tecnologia ao serviço de profissionais qualificados para inibir ações criminosas.

Explorando os dados referentes às ocorrências registradas por as diversas empresas existentes no município de Picos-PI, será analisado quais as relações entre os fatores humanos e os fatores computacionais, para melhor entender o lugar em que está a disseminação das falhas ocorridas na proteção dos dados existentes. A partir disso, extrair a melhor solução feito por meio de um estudo detalhado e fornecer maior informação aos usuários destes sistemas de segurança eletrônica, podendo assim evitar futuros acontecimentos na cidade.

FUNDAMENTAÇÃO TEÓRICA

Segundo a GSCSegurança (2019), o embasamento da segurança eletrônica vem sendo conceituado como a utilização de equipamentos e sistemas de segurança para monitorar e proteger locais, bens e principalmente pessoas. Essa segurança ela serve para monitorar e vigiar por meio de equipamentos, tais como: sensores, câmeras, sistemas e softwares.

Existem três imperativos para a adoção de um sistema de gerenciamento de segurança em um negócio, são eles: ética, legislação e finanças. A segurança do local de trabalho e da conformidade da execução de cada atividade é preestabelecida como uma responsabilidade do empregador, o sucesso dessa segurança está orientada de acordo com determinações regulamentadas que descrevem como deve ser efetuada essa supremacia e há um ambiente de estudo capaz de demonstrar que gerência da proteção é eficaz, que é a diminuição das ameaças no âmbito de responsabilidade trabalhista, podendo restringir a exibição monetária, ou seja, os perigos recorrentes em uma corporação, amenizando de forma direta ou indireta as despesas ligada à acidentes.

Constatando a grande relevância de todos os itens, um conjunto de segurança eficaz deveria ter para administrar os riscos uma corporação preparada para tal ação, detectar as prováveis fragilidades, propor ações para evitar ou atenuar as fragilidades existentes, elaborar uma conexão eficaz em quaisquer estágios da organização, estabelecer um procedimento para detectar e resolver todas as não-conformidades e também concretizar um método de

aperfeiçoamento ininterrupto.

Tratando-se de um aprofundamento histórico sobre esses sistemas de segurança, a iCasa (2018) especifica que os mesmos surgiram inicialmente em Nova Iorque, sendo utilizados pela polícia para fazer o uso dos aparelhos para melhorar as ações policiais por meio desses sistemas, as imagens utilizadas eram de qualidade extremamente baixa, preto e branco e não existia a expectativa de armazenamento ou de gravação, mas que durante essa época foi bastante produtiva no âmbito policial. Eram desse modo porque o sistema que surgiu e se popularizou foi o CFTV (Circuito Fechado de TV) que consiste apenas na captura e exibição das imagens no circuito interno por meio de um monitor. Como o CFTV eram câmeras que não permitiam a gravação ou armazenamento, esses sistemas precisavam ser monitorados vinte e quatro horas por dia, assim eles tinham vários pontos de visualização que, para manter o maior sigilo, poucas pessoas poderiam ter acesso a essas imagens. Atualmente os parâmetros de sistemas são muito modernos: a principal evolução foi que o sistema se tornou integrado e digital garantindo assim a maior segurança e confiabilidade na utilização desses métodos de segurança.

Levando em conta a autenticidade da iCasa (2018), ele aponta que o inicio da utilização de gravação de imagens surgiu na década de 70, a partir das fitas cassetes que começaram a ser utilizadas pela câmera de segurança principalmente residenciais, porque devido ao baixo custo das fitas esse sistema de segurança poderia passar a ser bastante utilizado, só que a partir disso mostrou-se que poderia surgir um evolução maior, Ao chegar a década de 80 e percorrer até a década de 90 teve uma evolução exorbitante com relação a utilização do sistema de segurança eletrônica, pois as câmeras foram ganhando bastante incidência para população e para os governos, passando assim a serem utilizadas em vários aspectos como tráfego aéreo, sistemas de bancos, entre outros, fazendo com que essas câmeras chegassem ao mercado e passassem a evoluir podendo capturar imagens durante o dia ou ainda assim durante a noite, podendo aplicar zoom as imagens, podendo fazer com que essas câmeras gravassem as imagens sem a obrigatoriedade de alguém monitorando 24 horas, fazendo essa captação por meio de microchip e fitas.

Foi quando com a evolução surgiu a chegada dos computadores, transformando os sistemas de segurança eletrônica ainda mais práticos e fortes no mercado, porque chegou a inovação de não ser preciso mais gravar imagens e sons em microchip ou fitas e começar a serem guardadas em discos rígidos, o que facilitou muito o armazenamento principalmente por causa da capacidade e sem falar a evolução das câmeras que continuaram trazendo ainda mais nitidez, possuindo mais modelos para o âmbito comercial, em que a população pôde buscar alcançar uma maior privacidade e maior proteção diante das ameaças e da criminalidade.

Tratando ainda do projeto de surgimento na legislação, Sabará e Alves (2015, p.21) afirmam que:

> Dado então o contexto de reconhecimento legal e difusão dos serviços de segurança pela iniciativa privada, a partir de 1996, [...] percebeu-se uma grande movimentação legislativa no sentido de uma maior expansão da vigilância pelo monitoramento visual, destacando-se várias iniciativas em forma de projetos de lei que intencionaram tornar obrigatório à instalação de câmeras em estabelecimentos como hospitais, casas lotéricas, postos de gasolina, estádios desportivos, rodovias, escolas e, ademais, o monitoramento visual de presos em liberdade condicional, trabalhadores em seus exercícios profissionais e pontos turísticos e/ou de grande fluxo de movimento.

Segundo Sabará e Alves (2015, p21), "no Brasil o surgimento das câmeras de vigilância eletrônica ocorreu com a aparição da Lei 1.034 de 21 de outubro de 1969" que proporcionava a utilização pelo serviço privado, em função do enorme crescimento dos assaltos a bancos, a lojas e residências. Neste período, somente às instituições fiscalizadas pela Secretária de Segurança Pública poderiam exercer e oferecer esse atividade, até que chegou a um ponto tão extremo que os aspectos que a lei disponibilizava já não comportava mais as atividade que estava sendo exercidas sendo necessárias novas determinações, então com o surgimento da Lei 7.102 de 20 de junho de 1983, o exercício de proteção particular passou a ter medidas estáveis e responsabilidades, colocando sobre segurança para departamentos monetários e determinando normas para a carta constitucional e andamento das empresas privadas que dispõem atividades de vigilância. Então com a Lei 8.863/94 as empresas particulares passaram a operar em todo e qualquer estabelecimento comercial público ou privado, sob condição de atender os contratos locais e capacitar constantemente seus vigilantes de forma apropriada.

Desse modo, a segurança eletrônica, segundo Henrique Portugal (2019) pode fornecer recursos e facilitar a proteção tanto dos dados, quanto de pessoas físicas e de empresas trazendo principalmente três benefícios essenciais: a vigilância em tempo integral, o controle do fluxo de entrada e saída e também da economia.

A vigilância de tempo integral é baseada em câmeras de segurança de alta qualidade que podem ver e avisar em tempo real tudo que está ocorrendo por meio de sistemas eletrônicos, softwares que são programados para essas necessidades, inibindo possíveis ações ou intenções questionáveis de pessoas que estejam buscando fazer com que ocorra alguma perda ou prejuízo a algum meio.

O controle do fluxo de entrada e saída, além de possuir o monitoramento por meio dessas imagens, é possível controlar as ações de quem entra e quem sai fazendo uma identificação dessas pessoas que circulam nas dependências da residência ou da empresa por meio de sensores de movimento ou ainda assim com identificação facial, fazendo com que os dispositivos integrados tenham a visão sobre possíveis invasões ou sobre suspeitas que

poderiam chegar a prejudicar a proteção do local.

Por último, levando para parte econômica, explana-se que esses aparelhos de segurança eletrônica não só servem para proteger as economias de muitas empresas, mas também de pessoas físicas em bancos ou em outras instituições, como também em casa por meio desse monitoramento, mostrando que o investimento de segurança eletrônica pode sair barato, principalmente se é visto no passar do tempo, tornando-se uma lógica exatamente oposta as que são expostas, tais como que esse investimento é bastante caro, mas a realidade é que eles reduzem os custos de funcionários físicos e poderão obter até melhor produtividade, citando também o melhor acompanhamento deles por seus donos, monitorando-os por meio de aparelhos de celular, tablet, equipamentos de fácil acesso.

É essencial o investimento em segurança, por ser um ponto fundamental para qualidade de vida das pessoas, assim, Lordello (2016, p.59), explica:

> É importante frisar que as chamadas câmeras de segurança apresentam diversos benefícios: a) Fator psicológico de dissuasão, pois o marginal sabe que está sendo vigiado e suas imagens armazenadas. b) inibe a ação de invasores, depredadores, pichadores e pessoas mal-intencionadas. c) facilita o trabalho de pronta reposta (polícia e vigilância particular) fornecendo pormenores do crime que está ocorrendo. d) Integração com sistemas de alarmes. e) Acesso às imagens pela internet.

Na segurança eletrônica existem quatro tipos principais de proteção que é o monitoramento eletrônico, as cercas elétricas, os alarmes de segurança e os vídeos porteiros eletrônicos, tratando separadamente de cada um deles (MARCONDES, 2016).

O monitoramento eletrônico é feito por meio da utilização de câmeras portando uma tecnologia muito elevada, fazendo com que elas tenham uma resolução de alta qualidade, sendo tão eficaz que a partir de certa distância consegue identificar o rosto de qualquer ser humano sem nenhuma dificuldade, mostrando assim que é possível ter o domínio de entrada a qualquer ambiente. As câmeras possuem uma conexão de rede de informações por meio de um aparelho que armazena todas essas imagens e faz com que o monitoramento seja vinte e quatro horas, sem necessidade que tenha um assistente analisando o monitoramento, pois elas podem efetuar a gravação e serem reproduzidas novamente em outro período.

As cercas elétricas, que são mais comumente utilizados em residências, para que haja uma proteção pelo lado externo da casa, o seu funcionamento é feito por meio de arames galvanizados ligados a eletrificadores de alta tensão que causam descargas elétricas suficientes para atordoar, mas não levar à morte, fazendo com o que utilitário deste equipamento tenha tempo para entrar em contato com a polícia e autuar em flagrante o invasor. Levando em conta um dos mais eficientes sistemas de segurança eletrônica que é o alarme, principalmente por causa do seu grande poder de inibir a presença de qualquer intruso a residência ou a empresa

fazendo com que a partir do momento que o indivíduo adentre ao local indevido o sistema de alarme dispare, emitindo alertas sonoros ou ainda assim acionando uma equipe física de segurança vinte e quatro horas fazendo com que ocorra o frustamento do ato ilícito.

O vídeo porteiro tem sido bastante eficaz, principalmente depois do surgimento dos interfones. Nesse momento que a segurança tem obtido investimentos altos, o sistema de vídeo porteiro proporciona a população um tipo de comunicação visual, de áudio ou áudio visual, podendo fazer com que o proprietário ou responsável saiba quem está querendo adentrar a sua residência ou a sua empresa antes mesmo da pessoa fazer um primeiro contato, trazendo assim um ambiente de conforto e um controle de tudo que está a sua volta, além de um limite estável de segurança.

A proteção da sociedade embora bastante evoluída, tem sido um dos termos mais preocupantes atualmente, pois cada vez fica mais claro que os elevados índices de criminalidade e violência chegam até as pessoas, suas casas, empresas ou aos patrimônios, das mais variadas formas. Temos que partir de um pressuposto que essa responsabilidade inicialmente é do Estado, mas também temos que lembrar que os cidadãos devem sempre buscar colaborar com a segurança local e residencial, incentivar e até mesmo adotar medidas iniciais que acomodem a sua proteção.

Gradativamente se observa indivíduos tendo facilidade de acesso a computadores, rede sociais, internet, dispositivos móveis, fazendo com que a sua voz chegue a lugares que jamais eram imaginados. Essa é uma boa maneira de fazer benefícios a todos os indivíduos, adotando medidas de incentivos locais, adquirindo aparelhos de vigilância eletrônica e expondo que o crescimento da segurança disponibiliza meios eficazes para essa proteção.

Sendo assim, a partir dessas ações uma segurança colaborativa que é a maneira que a sociedade pode se ajudar, expondo para outras pessoas algo que facilite com o que medidas de vigilância se tornando comuns, levando assim prevenção e redução de índices de violência e criminalidade. Assim, o valor da segurança eletrônica por meio dessa vigilância tornando mais ininterrupta, mas eficaz e mais punitiva pode trazer uma maior comodidade para toda sociedade levando com que os riscos possam ser reduzidos ao mínimo.

Para Foulcalut (1987, p.98):

> Métodos de vigilância mais rigorosos, um policiamento mais estreito da população, técnicas mais bem ajustadas de descoberta, de captura, de informação: o deslocamento das práticas ilegais é correlato de uma extensão e de um afinamento das práticas punitivas.

Quando se leva em consideração a relevância da segurança da informação, passa a se

analisar toda a proteção dos dados perante ameaças ou modificação de informações não autorizados, roubo ou a destruição deles. Entretanto, à preservação de informações e dados é de grande valor para pessoas físicas ou empresariais, lembrando que em alto ou baixo nível, todas as informações têm significativo valor. "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." (BLUEPHOENIX, 2008, p.28).

As ameaças as informações são extremamente perigosas, mas essas fraquezas podem ser controladas, até porque elas sempre irão existir. Tratando-se de pessoas, pode-se levar em conta que a principal preocupação está nos responsáveis técnicos do campo de inteligência, necessitando assim da consciência dos mesmos.

Para Sêmola (2003, p.47):

> Agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio de exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade, disponibilidade, autenticidade e legalidade, consequentemente, causando impacto aos negócios de uma organização.

Desse modo, atributos básicos da segurança da informação são:

• Confidencialidade: É a garantia que a informação estará segura, sob supervisão apenas das entidades responsáveis, fazendo assim com que somente o proprietário tenha autorização para acesso dos dados.

• Integridade: É a garantia de que a informação esteja totalmente ilesa, sem sofrer qualquer alteração do formato original, a não ser que a mudança tenha sido estabelecida pelo proprietário dela.

• Disponibilidade: É a garantia que a informação esteja sempre a pronta utilização do seu proprietário, ou seja, a informação esteja pronta pra uso.

• Autenticidade: É a garantia que a informação é de particularidade absoluta, sem sofrer qualquer alteração no processamento dela.

Como em qualquer empresa, existem as políticas de segurança e principalmente no campo de segurança da informação os funcionários sabem o que se espera deles. Eles têm a consciência da importância da sua função e do cuidado que possuem quanto a responsabilidade. Precisam sempre atender aos requisitos mínimos de organização, manutenção, revisão, proteção e segurança. Precisam também que todas essas conformidades sejam aceitas tanto pela direção quanto por todos os funcionários. (SANTANDER, 2009)

A segurança eletrônica relacionada a segurança da informação tem uma ascensão tão significativa de atuação no mercado comercial que chegou ao âmbito dessa tecnologia ser um

ponto extremo na evolução de todo o processo de crescimento financeiro e profissional, levando em conta como poderia se analisar que essas duas crescentes poderiam se aliar e formar uma conexão tão significativa e a iniciação disso tudo está no ambiente teórico.

Essa inter-relação é possível devido os fundamentos e concepções das duas áreas de se complementarem bem ativamente, levando em conta os requisitos de autenticidade, para disponibilizar os acessórios de controle de admissão corporativa e residencial, sendo também requisito fundamental para os sistemas fechados de televisão, que além da autenticidade, carregam consigo a disponibilidade da vigilância e a confidencialidade, no modelo de quem e quando podem ter acesso as imagens restritas e confidenciais.

Todavia, isso é só o início de toda essa relação entre a área de segurança da informação e segurança eletrônica, já que tendo em vista que o futuro é o principal influenciador desses dois campos, que só tendem a crescer e a conexão se tornar mais impactante, levando em conta que em qualquer âmbito estarão todos se relacionando no ambiente de propagação de respostas baseadas na internet das coisas, do mesmo modo que as informações serão guardadas e protegidas na computação em nuvem.

Além disso, as informações deverão ser analisadas como dados significativos para os crimes ocorridos por meio da conexão entre redes de computadores. Por causa desse fato, pode-se notar uma crescente ainda mais exponencial da plenitude baseada na segurança da informação com os acessórios eletrônicos, assegurando que as ligações desses equipamentos sejam cada vez mais desenvolvidos e resistentes e cada vez menos fragilizados.

Como base para o campo de pesquisa, a SS Seguritech é um empreendimento de segurança e vigilância eletrônica, que engloba a área de informática e tecnologia, devido à necessidade dos equipamentos destas áreas, na utilização durante os processos de instalação e manutenção, conta com cerca de 200 clientes que colabora de forma fixa e mais outros 200 clientes de forma rotativa, atendendo ao âmbito de sua localidade e demais regiões em seu entorno, fica localizada na Rua Projetada 201, número 75, bairro Aerolândia, no município de Picos no Piauí, município este que conta com uma das maiores economias do estado, por agregar o seu comércio as demais macrorregiões, além da sua vasta extensão correspondente a 577,304 km² (quinhentos e setenta e sete trezentos e quatro mil quilômetros quadrados), pertencente ao bioma Caatinga, consta com uma população estimada em 78222 pessoas, sendo registradas pelo último senso de 2019 (IBGE, 2020).

METODOLOGIA

O presente trabalho é um estudo bibliográfico e de campo acerca da dogmática sobre a

aquisição de dados não autorizados por meio de aparelhos de vigilância eletrônica, em especial a realidade da município de Picos. Foram estudadas obras doutrinadoras de autores renomados no campo de atuação da segurança eletrônica e segurança de informação, bem procedimentos de processos de evolução, instrumentos como informativos e artigos. Além disso, será realizada uma pesquisa normativa, composta de requisitos, fundamentos e pautas aplicáveis as melhorias da segurança, tendo como métodos principais a consulta de livros, análise documental, análise de leis que se encaixam na aplicabilidade, artigos, instrumentos legais, obedecendo ao que se busca evidenciar e constatar nesta obra acadêmica.

Essa pesquisa é classificada também como descritiva em que se exige do investigador uma série de informações sobre o que deseja pesquisar. Esse tipo de estudo pretende descrever os fatos e fenômenos de determinada realidade (TRIVIÑOS, 1987). Assim, analisar a aquisição de dados de forma ilegal através dos sistemas de vigilância eletrônica disponibilizados aos clientes colaboradores da empresa Seguritec Segurança no município de Picos em relação ao seu direito mínimo de proteção de dados, observando a realidade oferecida pelo poder público, sendo importante ressaltar que a segurança público é bastante ineficiente quando vem a se tratar de ocorrências tecnológicas e computacionais.

A coleta de dados será realizada pela aplicação do instrumento de questionários aos utilitários dos sistemas, os questionários serão do tipo objetivo, explanando acerca da funcionalidade, do registro, dos processos incrementados, da utilização do sistema e com um espaço aberto para demais observações constatadas pro os entrevistados, será usado gravador no momento da entrevista, se autorizado por os entrevistados, para melhor proteção dos dados. O questionário será aplicado pessoalmente, para possíveis duvidas que possam vir a existir pela complexidade das perguntas, anotando possivelmente outras informações complementares pelo decorrer da entrevista.

A pesquisa será realizada com clientes e utilitários do equipamentos de vigilância eletrônica da empresa Seguritec Segurança na cidade de Picos – PI, para melhor compreender como estão ocorrendo as possíveis falhas dos sistemas de segurança, serão abrangidas na pesquisa todos os clientes e colaboradores da empresa, tais como funcionários e proprietário. Sendo assim, em um breve esclarecimento de como será decorrido, após o conhecimento dos objetivos de pesquisa, todos os participantes irão participar de forma livre e consciente.

Após o tratamento dos dados coletados por meio da análise dos percentuais encontrados nas respostas dos respondentes será feita uma análise aprofundada dos mesmos, recorrendo a gráficos ou outros modelos e recursos visuais que permitem o maior detalhamento da pesquisa elaborada, filtrando e classificando os dados em diferentes modelos tornando-a mais dinâmica,

à medida que os dados são analisados e disponibilizados através dos gráficos, ocorre por mais uma vez a revisão dos mesmos, para dar mais confiança e veracidade a pesquisa.

RESULTADOS E DISCUSSÃO

Todo e qualquer sistema possui vulnerabilidades que se torna sujeito a constantes ameaças que podem ser do tipo natural, intencional e involuntária. As ameaças devem ser estudadas de fato antes de seu acontecimento, porque podem chegar a interromper o funcionamento do sistema ou causar perda de dados. Tratando dessas ameaças, descrevem-se as que ocorrem de forma natural, devido a incêndios, aquecimento, entre outros; as ameaças intencionais, aquelas propositais, causadas por seres humano, como hacker, ladrões e vírus;... e as ameaças involuntárias, como acidentes, erros, falta de energia, causada pelo desconhecimento. Essas ameaças podem ser vistas no gráfico 01.

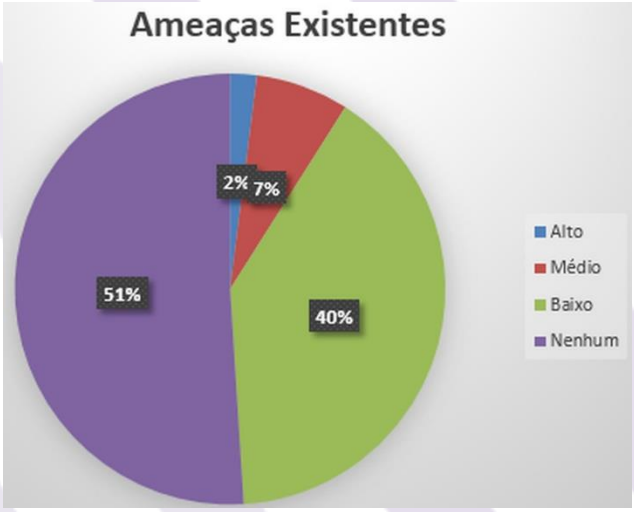

Gráfico 01: Grau de conhecimento dos utilitários acerca das ameaças existentes em porcentagem

Fonte: Elaborado pelos autores (2020).

O gráfico 01 demonstra que o conhecimento acerca de todas as ameaças existentes na utilização desses sistemas é de caráter crítico, levando em conta que 51% dos entrevistados não possuim nenhum tipo de conhecimento acerca das ameaças que estão ao seu redor e 40% possuem um peqeuno conhecimento, deixndo apenas a quantidade minima de usuarios com consciencia acerca das ameaças. Por mais que ameaças nem sempre são sejam combatidas, são usadas técnicas básicas para assegurar a disponibilidade dos recursos do sistema, mesmo na presença de defeitos, entretanto o gráfico expõe que é necessário uma maior propagação de todas as ameaças existentes, prevenindo os utilitários sobre aquilo que os mesmos estão expostos.

Alguns aspectos importantes podem auxiliar para evitar a usurpação de dados, entre eles se encaixam o controle de acesso, a monitoração do ambiente e condições técnicas, em que se todos eles estiverem em perfeita sincronia os sistemas tendem a funcionar regularmente, mas cada caso é característico ao ambiente escolhido, onde muitas vezes não terão as condições ideais, abrindo assim cada vez mais portas para os roubos de dados. Mesmo que nas piores condições poderá ainda assim ter uma boa monitoração e demonstrar os riscos que a empresa ou a sociedade podem vir a sofrer. Claramente algumas seções possuem maior sensibilidade quando comparada a outras, principalmente envolvendo a segurança da informação. No presente momento toda a sociedade e as organizações estão cada vez mais sujeitos a utilização de computadores proporcionando assim maior exposição a ataques e roubos as informações guardadas.

Uma ferramenta de proteção como um sistema de vigilância eletrônica desenvolvida para atender a sociedade, requer suporte e acompanhamento quanto a sua segurança, devido possuírem equipamentos que garantem o arquivamento, o processamento e a disponibilidade de dados que necessitam ser monitorados e supervisionados continuamente como uma forma de prevenir falhas e minimizar os erros, podendo ser cada vez mais aprimorados e desenvolvidos contribuindo assim para a modernização e a eficácia desses sistemas, segundo o gráfico 02.

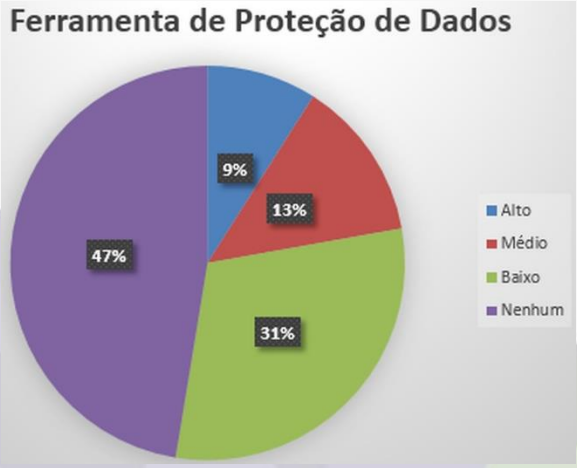

Gráfico 02: Grau de conhecimento dos utilitários acerca das ferramentas de proteção de dados em porcentagem
Fonte: Elaborado pelos autores (2020).

Observa-se no no gráfico 02 que o conhecimento dos consumidores sobre as ferramentas de proteção dos seus dados é mínima, ou seja, cerca de 78% dos utilitários não tem conhecimemto ou só por o básico acerca do serviço de suporte, o mapeamento do fluxo de dados, os testes de vulnerabilidade, entre outras formas de segurança dos seus dados são

praticamente desconhecidos pelos usuários, apenas utilitários técnicos do sistema possuem conhecimento acerca dos mesmos, somente cerca de 22% deles, causando assim uma enorme instabilidade no modelo de garantia de segurança.

Os sistemas de segurança são de equivalência gigantesca, sendo composto por amplos pontos a serem conhecidos, afim de se possuir um ponto fundamental para evitar possíveis falhas de caráter ocasional, levando em conta que qaunto maior o poder de entendimento acerca do funcionamento, maior a forma de proteção a ser conhecida e aplicada, tratando-se desse conhecimneto no grafico 03.

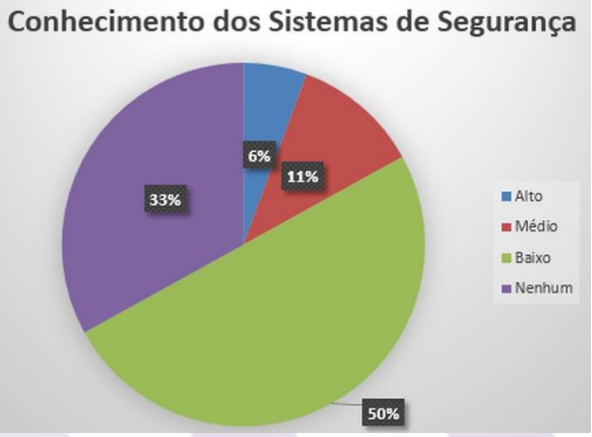

Gráfico 03: Grau de conhecimento dos utilitários acerca dos sistemas de segurança em porcentagem

Fonte: Elaborado pelos autores (2020).

Nota-se no gráfico 03 acima trata-se a questão do conhecimento acerca dos sistemas utilizados na segurança eletrônica, em que mais de 80% dos utilitários, não possuem conhecimento necessários acerca dos sitemas utlizados, causando uma falta de equilíbrio entre o propósito dos sistemas e os utilitários, onde o resultado final que são as medidas de segurança por inúmeras vezes ficam de lado, não fornecendo assim a garantia de total preservação, integridade e autenticidades dos dados armazenados.

Os utilitários dos sistemas de segurança aliados a segurança da informação devem compreender que o processo de confiabilidade é trabalhada de forma a manter as informações em privacidade e sem desvios dessas informações. É um processo que mantém o controle e a segurança desses dados, e que vai além do conhecimento sobre os sitsemas, sendo atribuidos a maioria das vezes a empresa fornecedora, exposto com mais detalhes no gráfico 04.

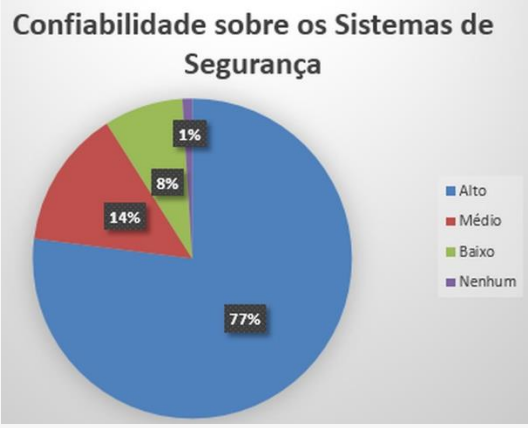

Gráfico 04: Grau de confiabilidade acerca dos sistemas de segurança em porcentagem

Fonte: Elaborado pelos autores (2020).

O gráfico 04 demonstra que o padrão de confiabilidade desse tipo de sistema de segurança é altíssimo, sendo assim mais de 90% dos utilitários confiam nesses sistemas mesmo não possuindo tanto conhecimento técnico acerca do funcionamento deles, do modelo de proteção, das possíveis formas de evitar, querendo ou não sendo obrigados a se adaptar ao padrão lógico de segurança, permitindo ser vítima de ataques externos em redundância.

É visto então que a segurança das informações está completamente aliada a dedicação e conhecimento dos utilitários acerca das ferramentas do sistemas de segurança, levando em conta que os consumidores que possuem maior conhecimento no assunto em questão estão menos expostos ao roubo dos seus dados e os consumidores que não possuem conhecimento necessitam de uma instrução em relação a como proteger melhor seus dados, além de que nenhum sistema se torna totalmente imbatível devido ao requisito fundamental que é o fator humano e que vem a se torna algo sem consistência, então somente uma melhor fundamentação dos usuários pode fornecer maior segurança e confiabilidade.

CONSIDERAÇÕES FINAIS

Essa pesquisa tem a finalidade de contribuir para debater um tema muito importante e para esse debate foi realizado o levantamento de dados referentes à existência de falhas em sistemas de segurança eletrônica e a falta de conhecimento dos utilitários a cerca dos mesmos, produzindo assim um campo de alto risco e instabilidade, podendo se manter exposto a diversos ataques tecnológicos.

Um dos principais objetivos deste presente trabalho foi explanar os padrões de aplicabilidade da segurança da informação, com o intuito de tratar que a execução de medidas de segurança possuem eficiência para melhoria do funcionamento. Como tratado na contextualização investigada desta pesquisa conclui-se que cerca de 90% dos sistemas de

segurança que executam planejamentos e funcionalidades contra riscos necessitam da combinação básica das competências de performance em tecnologia e a atenção às regras, para obter a confiabilidade nas execuções.

A prática mestre da sociedade é estar um passo à frente de qualquer tipo de pessoa mal intencionada e se prevenir de uma maneira em que suas informações, seus dados não estejam expostos ao perigo. A segurança da informação deve ser utilizada como um ponto estratégico para toda e qualquer organização, permitindo assim reduzir bastante os riscos de perda ou roubo de informações, pois é o meio capaz de manter as informações de forma sigilosa e segura.

Tolerância a falhas compreende muitas das técnicas que deixam aumentar a qualidade de sistemas de segurança, além de que existe o fator humano que é uma das circustancias primordiais a serem tratadas, pois podem influenciar em diversos requisitos para proteção dos dados e apesar da tolerância a falhas não garantir a conduta correta na presença de todo, ela permite alcançar a confiabilidade e a disponibilidade.

Tratando do propósito do questionário realizado no estudo de caso foi plausível analisar que a base utilizada dos sistemas de segurança e o alto comprometimento com às regras, proporcionou uma crescente na credibilidade, no que se apresenta a otimização e desempenho dos mecanismos envolvidos para transmissão dos dados.

A principal cooperação deste estudo é evidenciar mecanismos de segurança para a proteção dos dados que são expostos nesses sitemas, e a constatação de que é possível e totalmente viável o desenvolvimento de um ambiente seguro e robusto. A solução apresentada neste trabalho evidencia políticas que asseguram um ambiente seguro para tratamentos de dados. Ou seja, é uma estrutura informatizada de alta segurança e de alta confiança.

REFERÊNCIAS

BLUE PHOENIX. **Boas práticas de segurança**. Disponível em: www.bluephoenix.org. Acesso em: 15 maio 2020.

CELSO ANDERSON. **SEGURANÇA DA INFORMAÇÃO EM REDES CORPORATIVAS [Online]**. Disponível em: http://www.administradores.com.br/mobile/artigos/carreira/seguranca-da-informacao-emempresas/58918/. Acesso em: 13 jul. 2020.

FINK, Arlene. How to sample in surveys. Thousand Oaks, Sage, 1995d. [**The Survey Kit, v.6**]. Acesso em: 23 jun. 2020.

FOUCAULT, Michel. **Vigiar e punir.** Petrópolis: Editora Vozes. 1987. Disponível em: https://www.ufsj.edu.br/portal2- repositorio/File/centrocultural/foucault_vigiar_punir.pdf,

Acesso em: 01 jun. 2020.

GIGA SECURITY. **“Tudo o que você precisa saber sobre segurança da informação”**. Disponível em: https://blog.gigasecurity.com.br/seguranca-da-informacao/. Acesso em: 01 jun. 2020.

GSC SEGURANÇA ELETRÔNICA. “**Qual o conceito de segurança eletrônica?**”. Disponível em: https://gscseguranca.com.br/seguranca-eletronica/conceito-de-seguranca-eletronica/. Acesso em: 30 maio 2020.

HISTÓRICO DE SEGURANÇA. “HISTÓRICO DA SEGURANÇA PRIVADA”. Disponível em: https://sesvesp.com.br/institucional/historico-seguranca/. Acesso em: 30 maio 2020.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA **(IBGE).** Cidades: Picos, Piauí, 2018. Disponível em <https://cidades.ibge.gov.br/brasil/pi/picos/panorama>. Acesso em: 23 jun. 2020.

LORDELLO, J. **Câmeras de Segurança Benefícios e Proibições.** Disponível em:<http://tudosobreseguranca.com.br/portal/index.php?option=com_content&task=view&id=753&Itemid=168 > Acesso em: 15 jul. 2020.

MARCONDES, J. S. **Sistemas de alarme da segurança eletrônica: conceitos, equipamentos.** Disponível em: https://gestaodesegurancaprivada.com.br/sistemas-de-alarme-da-seguranca-eletronica/. Acesso em: 15 jul. 2020.

MCGEE, J.; PRUSAK, L.; **Gerenciamento Estratégico da Informação**; Editora Campus, 1994; ISBN 85-7001-924-6; p. 5, 23-24.

PORTUGAL, Henrique. **Segurança eletrônica para empresas: benefícios e principais equipamentos.** Disponível em: https://www.em.com.br/app/noticia/patrocinado/ortep/2019/12/16/noticia-patrocinado-ortep,1108154/seguranca-eletronica-para-empresas-beneficios-e-principais-equipament.shtml. Acesso em: 15 jul. 2020.

SABARA, M. T. Ribas; ALVES, Daniela Alves de. **Disciplina e Controle: análise de uma rede de monitoramento visual.** Disponível em: < https://revistas.utfpr.edu.br/rts/article/view/2861>. Acesso em: 15 jul. 2020.

SANTANDER. “**Principais itens em segurança da informação**”. Disponível em: http://www.santander.com.br/document/gsb/seguranca_parceiros_principais_itens.pdf. Acesso em: 30 maio 2020.

SEGURANÇA ELETRÔNICA. “**A evolução da segurança eletrônica**”. Disponível em: https://ser-tel.com.br/a-evolucao-da-seguranca-eletronica/ Acesso em: 30 maio 2020.

SEGURANÇA ELETRÔNICA. “**Entenda o que é segurança colaborativa e qual sua importância na sociedade**”. Disponível em: https://revistasegurancaeletronica.com.br/entenda-o-que-e-seguranca-colaborativa-e-qual-sua-importancia-na-sociedade/. Acesso em: 01 jun. 2020.

SÊMOLA, M. **Gestão da segurança da informação**. Rio de Janeiro: Campus, 2003.

SILVA, Alexandro. "**Dez falhas em segurança da informação**". Disponível em: http://softwarelivre.org/alexos/blog/dez-falhas-em-seguranca-da-informacao. Acesso em: 20 maio 2020.

TRIVIÑOS, A. N. S. **Introdução à pesquisa em ciências sociais**: a pesquisa qualitativa em educação. São Paulo: Atlas, 1987. Acesso em: 24 jun. 2020.