CENTRO INTEGRADO DE COMUNICAÇÃO:
Gestão da segurança da informação na segurança pública na região de Paulo Afonso –BA

Thiago Fernando das Chagas Lima
Bacharel em Sistema de Informação. Especialista em Governança de TI. Policial Militar do Estado da Bahia
thiago_fernandopa@hotmail.com

Adailton Soares da Silva
Pedagogo. Assistente Social. Especialista em Pedagogia Social. Mestre em Educação
Professor Articulador da Universidade Tiradentes . Policial Militar do Estado da Bahia
Adailton.edusocial@gmail.com

RESUMO

Este trabalho justifica-se pela relevância que a informação e sua segurança têm para as organizações, principalmente no âmbito da segurança pública. Portanto, a pergunta formulada consiste em identificar a necessidade da implantação de uma política de segurança padrão na unidade do Centro Integrado de Comunicação - CICOM de Paulo Afonso-BA. Para isso, seu objetivo geral é identificar e analisar as principais vulnerabilidades quanto à segurança da informação evidenciando ou não a implantação de uma politica de segurança no CICOM. A metodologiautilizada na construção desta pesquisa foi a bibliográfica e um estudo de caso, com análise exploratória cujo principal instrumento de coleta de dados foi uma entrevistainformal. Constatou-se que a unidade do CICOM apesar de operar com alguns dos conceitos de segurança da informação não apresenta uma política de segurança padrão e concreta, evidenciando a necessidade de implantação de um política de segurança padronizada e capaz de garantir a gestão segura da informação da unidade contra eventuais ataques de agentes maliciosos e consequente perda de valiosas informações.

Palavra-chave: Gestão da Segurança da Informação. Política de Segurança. Segurança Pública. CICOM.

ABSTRACT

This work is justified by the relevance that information and its security have for the organizations, especially in the public security. Therefore, it aims to identify the needing of implementation of standard security policies in the Integrated Center of Communication – CICOM in Palo Afonso-BA. For this, the general objective is to identify and analyze the main vulnerabilities in information security, emphasizing the implementation or not of a security policy in CICOM. The methodology used in this research was bibliographical and case study, with an exploratory analysis that gathered data through an informal interview. It was found that this CICOM unit, although operating with some concepts of informa-

tion security, does not present a standardized security policy, making necessary the implementation of a policy that is capable of guaranteeing a safe management of the unit's information against eventual attacks by malicious agents and, consequently, the loss of valuable information.

Keywords: Management of information security. Security policy. Public security. CICOM.

INTRODUÇÃO

Na sociedade contemporânea o acesso à informação é condição essencial para a manutenção das relações sociais através das tecnologias da informação e comunicação com a propagação do acesso à internet aliados aos bens, serviços e entretenimento ofertados a população. Essa rede global requer dos seus usuários medidas e procedimentos na busca de uma circulação de informações seguras e autênticas no âmbito individual e principalmente das organizações públicas e privadas que detém o acesso restrito os dados de seus colaboradores.

Para Nakamura e Geus (2003) o valor da informática como parte do processo de negócios de qualquer organização pode ser evidenciada pelo aumento dos investimentos realizados na área de tecnologia da informação. A secretaria de segurança pública do Estado da Bahia apostando na tecnologia como meio de inovar os serviços públicos na segurança deu inicio a um projeto de integração da comunicação, um inovador centro integrado de comunicação – o CICOM. Este investimento tem como objetivo melhorar e tornar mais eficiente o serviço de chamadas de urgência e emergência e assim alimentar a base de dados dos órgãos a eles vinculados: Polícia Militar, Polícia Civil, Departamento de Polícia Técnica e Corpo de Bombeiros Militar.

Fazendo uso da integração entre tecnologias de radiocomunicação e sistemas de informação, busca prover dados de grande valor para as Corporações que a compõe combatendo o crime e auxiliando na promoção de segurança na região atuante. Diante do valor dessas informações geradas pelo CICOM justifica-se a necessidade de procedimentos formais para assegurar a sua segurança, evitando assim que dados e informações criticas possam ser usadas em prol da criminalidade, ou simplesmente serem perdidas por atos de vandalismo ou má uso delas. A segurança da informação, atualmente, é algo importantíssimo para os negócios das organizações, haja vista, que as informações estão expostas a uma enorme quantidade de ameaças, sendo estas, lógicas ou físicas.

Nesse sentido o objetivo geral desse estudo é identificar e analisar as principais vulnerabilidades no CICOM quanto à segurança de informação evidenciando a necessidade ou não da implantação de uma política de segurança. Especificamente será descrito na seção 2 os principais conceitos e análises quanto ao tema de segurança da informação enquanto que na seção 3 será descrito como se deu a criação do CICOM assim como seu objetivo e relacionar os procedimentos atualmente em prática nele com o tema de segurança da informação, analisando e evidenciando assim na conclusão deste trabalho a necessidade ou não de implantação de uma política de segurança com procedimentos formais. A metodologia usada será através de uma pesquisa exploratória assumindo a forma de pesquisabibliográfica e um estudo de caso, fazendo mão da observação e de uma entrevista informal como forma de coleta de dados com o gestor da unidade em Paulo Afonso-BA.

1 SEGURANÇA DA INFORMAÇÃO x CICOM: CONCEITOS E ANÁLISE

1.1 Gestão da segurança da informação

Quando se pensa em o que seria segurança de informação e para que se destine, primeiro é preciso entender oque significa informação e seu valor para as organizações. As informações são estruturas de valor, compostas por dados e a partir disso produzem conhecimentos para os usuários. Para Fontes (2006), a informação é independente do seu formato, e um dos ativos de grande valor para as organizações.

As informações só passaram a serem consideradas importantes para as empresas, organizações ou corporações em função do alto grau de dependência que hoje elas têm em tecnologias de informação. Atualmente estas informações possuem um valor inestimável não somente para as organizações que a geraram, como para seus concorrentes.(GHODDOSI, 2012).

1.1.1 Segurança da informação

É nesse contexto que a segurança da informação é considerada um item que tem ligação direta com a funcionalidade e a produtividade quando se fala em uso de tecnologia. Para Fontes (2006), a segurança da informação é o conjunto de orientações, técnicas, procedimentos e políticas que têm por finalidade proteger a informação possibilitando que a missão da organização seja cumprida com sucesso desejado.

De acordo com Ghoddosi (2012, p.17), "o principal objetivo da segurança da informação é minimizar os riscos do negocio em relação à dependência do uso dos recursos de informação para o funcionamento da organização". Sendo assim, existem os princípios que devem ser levando em conta pelos profissionais da área. Segundo Celso (2008, p. 47) São eles:

- Confidencialidade – propriedade que limita o acesso à informação (autorização do proprietário da informação);
- Integridade – propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação;
- Disponibilidade – propriedade que garante que a informação esteja sempre disponível para o seu uso legitimo.

Cabe aos gestores implementar uma política institucional onde promova e integração destes princípios e com o apoio dos colaboradores na perspectiva de manter um ambiente de trabalho seguro na transmissão e armazenamento de dados.

1.2 Política de segurança

A política de segurança reflete a preocupação de qualquer organização diante da importância da informação para sua missão. Dependendo da natureza do sistema, administrativo, militar, industrial, financeiro ou outros pode perceber que os riscos e ameaças mudam conforme estas naturezas.

Para Dias (2000) a política de segurança é um mecanismo preventivo de proteção de dados e processos valiosos para uma organização, que define um padrão de segurança a ser seguido pelo corpo técnico e gerencial e pelos usuários internos e externos.

Segundo Ghoddosi (2012), as medidas que decorrem da implantação bem sucedida de uma política de segurança podem ser destacadas em três categorias: redução da probabilidade de ocorrências danosas, redução dos danos provocados pelas eventuais ocorrências e a criação de procedimentos para se recuperar dos danos.

Conforme a NBR ISSO/IEC, o documento contendo as políticas de segurança de informação da organização, deve conter no mínimo a definição de segurança da informação com o seu foco

e a importância de segui-la para o cumprimento da missão da organização, declaração do alto escalão da diretoria apoiando as normas da política, uma explanação detalhada da mesma, com seus tópicos, princípios e padrões que devem ser respeitados por todos e suas consequências no caso de descumprimento da mesma.

1.3 Controle de acesso: segurança lógica e segurança física

O objetivo do controle de acesso lógico e físico é de proteger os equipamentos, aplicativos e *softwares* contra danos ou qualquer violação. Os dados e informações digitais não podem somente ser protegidos por dispositivos físicos, como alarmes e travas, sendo assim se faz necessários procedimentos específicos para seu controle.

1.3.1 Controle de acesso lógico

É um conjunto de procedimentos e métodos que podem ser manuais ou automatizados com o objetivo de proteger os recursos tecnológicos (condigo fonte do software, arquivos de senhas, arquivos de log, sistemas operacionais e utilitários) e os recursos intangíveis (dados e informações) contra: a quebra de integridade, modificações não autorizadas e acesso e uso indevido. O controle lógico e um processo que o usuário deseja acessar um arquivo ou outro recurso. Mesmo com toda a tecnologia atual merece destacar que não existe segurança 100% (cem por cento) completa, e que o maior ponto fraco de um processo de controle de acesso lógico é o próprio usuário. (GHODDOSI, 2012).

Os elementos de controle de acesso logico vão desde o processo de logon, identificação e autenticação com o uso de senhas com uma política de senhas (histórico de senhas, tempo de vida máx. e mín., comprimento mín., complexidade de senhas) até o uso da inovadora biometria. O monitoramento através de logs (registros) do sistema também é de grande importância para a eficiência do processo.

O compartilhamento de senhas, usuários mal treinados, escolha de senhas simples e descuido em relação às informações sigilosas são exemplos que prejudicam a eficiência do controle de acesso logico. Destacando assim que a conscientização do usuário é muito importante para a estratégia de qualquer política de segurança.

1.3.2 Controle de acesso físico

Corresponde a segurança física das condições operacionais e da integridade dos componentes dos ambientes, recursos materiais e recursos computacionais. Os recursos a serem protegidos são os insumos (papel, fitas magnéticas, cartuchos de impressora e CD's), hardware (UCP, terminais, estações de trabalho, impressoras, servidores e monitores) e componentes de informática (estabilizadores, *no-brakes*, cabos de redes) e etc. De acordo com Ghoddosi (2012), O controle de acesso físico tem como principal objetivo assegurar a proteção dos equipamentos e informações contra os usuários não autorizados, prevenindo o acesso a esses recursos.

Os elementos de controle de acesso nos casos de estrutura física podem ser os sistemas manuais ou visuais (porteiros, guardas e recepcionistas verificando crachás, método muito utilizado), semiautomáticos (porteiro eletrônico que se utiliza de interfones) e automáticos (senhas de acesso, cartões magnéticos e a biometria). Depende do tipo de organização e do valor de suas informações geradas, há o controle explicito, que é implementado por meio de cadeados, fechaduras automáticas, biométricas e câmeras de vídeo com a finalidade de restringir acesso físico a lugares restritos.

Cuidados contra incêndios, descargas elétricas naturais e acidentais, enchentes, umidade e temperatura são controles físicos ambientais e também merecem a devida atenção, pois estão relacionados diretamente com a disponibilidade e integridade dos sistemas computacionais.

1.4 Riscos envolvendo informações

Nos últimos anos observa-se um crescimento sem limites dos meios de comunicação em especial a internet. (SANTOS JUNIOR, 2008) explica que com a crescente demanda por serviços Web e o aumento da quantidade de pessoas com acesso a internet (inclusão digital), todos os dias centenas de vulnerabilidades são reportadas em aplicações web comerciais ou de condigo aberto. Diante disso Ghoddosi (2012, p. 54), pontua que "cada serviço na internet tem seus próprios riscos associados. Uma política de segurança deve definir quais os serviços a serem disponibilizados na rede interna.".

Como base em cada serviço autorizado pela política de segurança para atuar na rede interna é que se devem definir os dispositivos de proteção para a segurança da informação da organização.

1.4.1 E-mail e transferência de arquivos

De acordo com (GHODDOSI , 2012, p. 55) o "e-mail é a principal porta de entrada para vírus na sua rede interna". Em um e-mail despretensioso um hacker pode enviar uma mensagem, por exemplo, com um cavalo de Tróia, que é um vírus de ataque cujo objetivo é de roubar as senhas digitadas na máquina e enviá-las para o atacante.

Nesse mesmo contexto, a importação descontrolada de arquivos facilita a entrada de softwares piratas, ou qualquer outro arquivo indesejado para o proposito da organização e a exportação de arquivos é um problema ainda maior, pois alguns softwares de transferência não garantem de quem esta recebendo o arquivo seja à pessoa autorizada.

1.4.2 Acesso remoto por terminais e a *word wide web* (www)

Alguns *softwares* que permitem o acesso remoto a rede através de um terminal, Muitas vezes estas informações estão transitando sem nenhuma forma de criptografia. Da mesma forma que a *word wide* web facilita a vida de seus usuários, é uma bela porta de entrada para um eventual atacante. Devido a sua imensa flexibilidade qualquer tipo de controle de acesso se torna ineficaz. Além disto, existe um grande desperdício de temo útil dos funcionários em função de acesso a sites com conteúdos que difere do objetivo da organização.

1.4.3 Usuários

Os usuários é o ponto chave dentro de uma política de segurança da informação, pois mesmo com os mais eficientes sistemas de controle, o usuário interno ou externo pode colocar tudo a perder, seja com a motivação de realmente fazer o mal (divertimento, vandalismo, competição, espionagem) ou apenas com o uso indevido dos recursos tecnológicos. Posto isso, é de extrema importância que exista na organização políticas de treinamento e conscientização do usuário, requisitos mínimos de conhecimento e comprometimento para admissão de seus funcionários, principalmente em organizações onde o acesso à informação é restrito.

1.5 Medidas de proteção

Medidas de proteção nada mais são do que ter políticas e procedimentos formais de segurança.

É de extrema importância manter em uma organização um sistema antivírus atualizado, de preferência que tenha procedência comprovada no mercado, usar criptografia para armazenamento e transporte de arquivos críticos, instalar e manter sistemas de *firewall* que segundo Chapman (2000), "O *Firewall* é um componente ou conjunto decomponentes que restringe o acesso entre uma rede protegida e a internet, ou entreoutros conjuntos de rede.", ou seja, ele reforça a comunicação entre redes.

Além disso, instalar e manter sistemas de detecção de intrusão (IDS – *Intrusion Detection Systems*), que são ferramentas complementares ao firewall, é um conjunto de meios técnicos para descobrir em uma rede de computadores acesso não autorizado. Nakamura; Geus (2007) definem que IDS tem como objetivo detectaratividades suspeitas, impróprias, incorretas ou anômalas. Trata-se um elementoimportante dentro do arsenal de defesa da organização.

2 CICOM

De acordo com a Secretaria de Segurança pública do Estado da Bahia (2017), foi criada em março de 2004 a Superintendência de Telecomunicações (STELECOM) que tem por objetivo impulsionar a integração dos diversos órgãos que compõem o Sistema Estadual de Segurança Pública na Bahia, no que diz respeito ao processamento das telecomunicações.

Sediada no Centro Administrativo da Bahia, no complexo administrativo da Polícia Militar, a STELECOM agrega ainda seu mais novo projeto: o Centro Integrado de Comunicação (CICOM), que tem como objetivo fornecer um atendimento eficaz para as chamadas de urgência e emergência, bem como alimentar o sistema de telecomunicações dos órgãos a eles vinculados: Polícia Militar, Polícia Civil, Departamento de Polícia Técnica e Corpo de Bombeiros Militar.

Fazendo usoda integração entre tecnologias de radiocomunicação e sistemas de informação, busca prover dados de grande valor para as Corporações que a compõe combatendo o crime e auxiliando na promoção de segurança na região atuante.

2.1 Análise da existência de vulnerabilidades quanto à segurança da informação no CICOM de Paulo Afonso - BA

Diante dos vários aspectos vistos anteriormente referentes à segurança da informação constatou-se através de uma entrevista com o gestor do CICOM, Cap. PM Nery, assim como observação da unidade em Paulo Afonso – BA vulnerabilidades quanto à segurança da informação. Para um melhor entendimento a análise dos questionamentos foi estruturada em camadas (logica, física e humana) seguidas das considerações e apresentados resumidamente em um quadro de vulnerabilidades abaixo.

Quadro 1 – Vulnerabilidades quanto à segurança da informação da unidade do CICOM da cidade de Paulo Afonso- BA.

Camadas	Vulnerabilidades detectadas	Procedimentos atuais	Propostas de implementação
Humana	Políticas de Segurança	- Há uma norma de conduta não padronizada	- Política de segurança padrão
	Política de treinamento	- Há treinamento inicial para operação do sistema - Não há treinamento técnico em informática	- Uma política de treinamento e reciclagens apropriadas para cada função desempenhada
Lógica	Senhas	- Utilização de senhas simples e compartilhamento das mesmas	- Política para geração de senhas - Uso da Biometria
	Medidas de proteção (antivírus e IDS)	- Ausência de conhecimento	- Utilização de um sistema de antivírus e IDS de procedência -Contratação de um técnico local qualificado
	Monitoramento de rede (registro de sistemas, internet e e-mails)	- Administrador de rede remoto	- Contratação de um técnico local qualificado
	Criptografia	- Base de dados compartilhada e sem criptografia	- Utilização de *softwares* criptografados
Física	Controle de acesso simples	- Fechaduras - Acesso de forma visual controlada pelos próprios operadores de sistema	- Controles automáticos - Uso da biometria - Contratação de funcionários para a função específica

Fonte: O autor, 2017.

Fica evidente uma constante relação entre o agente, a lógica e estrutura física disponível no ambiente de trabalho na unidade do CICON, na ´perspectiva de reduzir as vulnerabilidades de-

tectadas. Medidas importantes já foram adotadas, porém é preciso uma qualificação dos agentes para a manutenção da segurança dos dados com os quais trabalham no cotidiano da instituição. Para Levy (2015, p 26), "é uma inteligência por toda parte, incessantemente valorizada, coordenada em tempo real, que resulta em uma mobilização efetiva das competências".

2.1.1 Camada Humana

O gestor da unidade foi questionado no que diz respeito à existência de uma norma ou política de segurança no CICOM e como era composto o quadro de funcionários da unidade. Foi dito que há utilização de uma norma de conduta onde todos os prepostos estão sujeitos, inclusive cientes das sansões pertinentes no caso de quebra de sigilo.Quanto à contratação dos funcionários foi dito que há uma pré-seleção com requisitos mínimos de perfil psicológico e habilidades técnicas para compor o quadro do CICOM tanto dos militares selecionados para a função quanto dos civis contratados.

A conscientização da responsabilidade da função é de vital importância para um plano de segurança eficaz, porém como na unidade há civis e militares como funcionários e com regimentos disciplinares diferentes abre um leque de preocupações neste sentido já que não existe uma política de segurança padrão.

Foi questionado também sobre a existência de uma política de treinamento dos militares selecionados e dos civis contratados. Diante disto foi dito que o sistema de chamadas de urgência e emergência é exclusivo de uso do CICOM e foi projetado especificamente para este serviço, seus operadores passam por treinamento inicial apenas para aprenderem a utiliza-lo de forma correta, não havendo de nenhuma forma um treinamento técnico especifico em informática e tão pouco nos riscos envolvendo informações.

O usuário é o ponto chave de qualquer política de segurança, e ter uma política de treinamento e reciclagem é essencial para que o ataque não seja facilitado por uma má utilização dos equipamentos tecnológicos. Há a ausência de uma política de treinamento padronizada é um ponto fraco constatado na unidade.

2.1.2 Camada lógica

Diante do questionamento quanto aos elementos de controle lógico, ficou claro que se utiliza basicamente de senhas e estas sem a presença de uma política de senhas. Foi dito que há o compartilhamento destas e a não utilização de técnicas como tempo mínimo e máximo de vida e complexidade de elaboração das senhas, podendo com isso ser prejudicial para a segurança e facilitar um eventual ataque ao sistema.

Foi dito que o monitoramento de rede é feito por um administrador remoto, que faz o monitoramento de rede e registro de eventos. Também foi colocado que o banco de dados é compartilhado e não há utilização de criptografia assim como a utilização da internet e de e-mails são restritos ao gestor da unidade e seus auxiliares.Quando questionado quanto à utilização de sistemas antivírus e sistemas de detecção de intrusão (IDS), foi exposto à ausência do conhecimento sobre a utilização de tais dispositivos.

A Biometria aparece atualmente como uma alternativa viável de segurança e não explorada pela unidade assim como também seguir uma política de geração de senhas. A utilização da rede por terminais remotos tem por recomendação ser feito por softwares criptografados o que dificulta o acesso às informações que estão transitando pela rede, a não utilização de criptografia no envio de informações e uma porta de entrada para atacantes. Há ausência dos sistemas auxiliares de segurança como (antivírus, IDS, *firewall*), pode dificultar consideravelmente a proteção da rede para atacantes maliciosos. Porém foi dito que o sistema de *firewall* é operante na rede, inclusive restringindo acessos não autorizados. Por ter um administrador de rede apenas remoto, aumenta sem sombra de dúvidas as chances de problemas quanto a uma eventual perda de informação, sendo recomendável manter alguém capacitado para suprir esta necessidade na unidade local.

2.1.3 Camada física

Foi observado que a unidade do CICOM em Paulo Afonso- BA é situada ao lado do departamento de policia civil e tem seu acesso restrito aos seus funcionários, o acesso é feito de forma visual apenas e com utilização de simples fechaduras, há um sistema de vídeo monitoramento como elemento de controle explícito e cuidados básicos quanto aos controles físicos ambientais, que é a utilização de extintores para eventuais incêndios e aterramento para evitar danos por descargas elétricas. A unidade e climatizada o que favorece ao controle de temperatura e umidade.

Por se tratar de uma unidade Militar controles automáticos e biométricos poderiam ser mais bem explorados, dificultando o acesso de pessoas não autorizadas.

CONSIDERAÇÕES FINAIS

Este estudo procurou explicar os principais pontos referentes ao tema de segurança da informação e o valor que a informação tem atualmente para todas as organizações. Diante disso, foi colocada a necessidade de uma organização se ater a preocupação de possuir uma norma que garanta a proteção de seus recursos tanto tangíveis quanto intangíveis.

Na análise desenvolvida, foram identificados que os recursos tecnológicos têm promovido um grande avanço na melhoria dos serviços prestados pelas organizações principalmente os serviços públicos como o de segurança. Tais tecnologias são facilmente exploradas pela rapidez,facilidade e economia que elas provêm porem, certos riscos são inerentes do seu uso, justificando a necessidade de utilização de uma política de segurança que proteja as informações geradas.

O presente trabalho tinha como objetivo geral identificar e analisar as principais vulnerabilidades na unidade do CICOM de Paulo Afonso – BA quanto à segurança da informação evidenciando a necessidade ou não da implantação de uma política de segurança.

Um gestor de segurança da Informação deve estar atento a itens como ambiente, tecnologia, processos e pessoas. Em cada uma dessas vertentes surgem diversas iniciativas como políticas, normas e procedimentos, controle de acesso (físico e lógico), criptografia, segurança da Rede, conscientização dos usuários, dentre outros.

Constatou-se que a unidade do CICOM apesar de operar com algumas destas iniciativas não apresenta uma política de segurança padrão e concreta, muitas vezes constatada pela ausência de tecnologias mais atuais e eficientes como a biometria e uso de criptografia, ate mesmo a utilização de procedimentos simples como elementos de controle lógicos e físicos.

Desta forma ficou evidenciada a necessidade de implantação de umapolítica de segurança padronizada, mais completa e eficiente que seja capaz de garantir a gestão segura da informação da unidade contra eventuais ataques de agentes maliciosos e consequente perda de valiosas informações.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. NBR ISO/IEC: **Tecnologia da informação** - código de prática para a gestão da segurança da informação, 2005.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da informação**. Rio de Janeiro: Excel Books, 2000.

FONTES, Edison. **Segurança da Informação**. São Paulo: Saraiva,2006.

GHODDOSI, Nader. **Segurança da Informação**. Indaial: Uniasselvi, 2012.

NAKAMURA, Emilio Tissato; GEUS, Paulo L.**Segurança de redes**. São Paulo:Editora Futura, 2003.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes emambientes cooperativos**. São Paulo: Novatec Editora, 2007.

LÉVY, Pierre. **A inteligência coletiva**. São Paulo; Loyola, 1998.

SANTOS JUNIOR, Alfredo Luiz dos. **Quem mexeu no meu sistema?**: segurança em sistemas de informação. Rio de Janeiro: Brasport, 2008.

Secretaria de Segurança Publica do Estado da Bahia. **CICOM**. Disponível em: <http://www.ssp.ba.gov.br>. Acesso em: 10 de jan. 2017.