ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM ARTHUR CARVALHO MONTEMAGNI

O SISTEMA DE COMUNICAÇÕES DE ÁREA DE DIVISÃO DE EXÉRCITO: UMA ANÁLISE DA SEGURANÇA DA INFORMAÇÃO NO DESENVOLVIMENTO DA COMUNICAÇÃO

Rio de Janeiro
2021

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM ARTHUR CARVALHO MONTEMAGNI

O SISTEMA DE COMUNICAÇÕES DE ÁREA DE DIVISÃO DE EXÉRCITO: UMA ANÁLISE DA SEGURANÇA DA INFORMAÇÃO NO DESENVOLVIMENTO DA COMUNICAÇÃO

Trabalho acadêmico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Gestão Operacional.

Rio de Janeiro
2021

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DECEx - DESMil
ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS
(EsAO/1919)

DIVISÃO DE ENSINO / SEÇÃO DE PÓS-GRADUAÇÃO

FOLHA DE APROVAÇÃO

Autor: Cap Com **ARTHUR** CARVALHO MONTEMAGNI

Título: **O SISTEMA DE COMUNICAÇÕES DE ÁREA DE DIVISÃO DE EXÉRCITO: UMA ANÁLISE DA SEGURANÇA DA INFORMAÇÃO NO DESENVOLVIMENTO DA COMUNICAÇÃO.**

Trabalho Acadêmico, apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito parcial para a obtenção da especialização em Ciências Militares, com ênfase em Gestão Operacional, pós-graduação universitária lato sensu.

APROVADO EM _____/_____/_____ CONCEITO: _____

BANCA EXAMINADORA

Membro	Menção Atribuída
_____ Carlos André dos Santos **Meirelles** de Andrade – Maj Cmt Curso e Presidente da Comissão	
_____ Rodolfo de Azevedo **Maymone**– Cap 1º Membro e Orientador	
_____ **Glauco** Gonçalves da Silva– Cap 2º Membro	

_____
ARTHUR CARVALHO MONTEMAGNI **– Cap**
Aluno

AGRADECIMENTOS

Inicialmente, agradeço a Deus por ter-me feito instrumento da sua sabedoria, por ter-me permitido criar circunstâncias que me levaram a descobrir esta oportunidade e ter-me fornecido os elementos necessários para conseguir esta conquista;

A minha noiva Andréa, minha enteada, amigos e todos que, de alguma maneira, direta e indireta, contribuíram com este projeto, dando-me desde suporte, incentivo, ânimo, até uma simples palavra que se converteu em um sinal de motivação;

Ao Cap Maymone, meu orientador, por sua dedicação, compreensão, empatia, colaboração;

Ao Comando da EsAO, através de seu representante, ter facilitado as informações para a elaboração desta pesquisa; e

Finalmente, a todos que fizeram parte deste crescimento e concretização do presente trabalho.

RESUMO

O Sistema de Comunicações de Área (SCA) é um complexo conjunto de equipamentos de comunicação que tem como finalidade a transmissão segura das mensagens do comandante de uma Organização Militar para com os militares envolvidos em uma determinada operação dentro de um escalão, a fim de apoiar o Comando e Controle das tropas nas diversas operações. Este trabalho, entretanto, preocupa-se com a segurança da informação, principalmente no SCA, realizadas nas operações militares quanto ao seu sigilo, privacidade e manutenção desse sigilo; uma preocupação constante diante do bom gestor em manter a Instituição Exército Brasileiro em segurança, principalmente diante da atual pandemia de COVID-19, o qual impôs o uso, em larga escala, do trabalho em “home-office”, em que se tem acesso aos variados sistemas de comunicações, dando margem à invasões e uso de informações, pessoal e militar, que devem ser salvaguardada de terceiros. Assim, o Sistema de Comunicações de Área não deve apenas preocupar-se com o “falar, ouvir, responder e desligar”, deve também preocupar-se com a manutenção do sigilo durante todos os tipos de operações bem como no cotidiano de nossas Unidades.

PALAVRAS-CHAVE: Segurança nas Comunicações; Sigilo no Sistema de Comunicações de Área (SCA); Proteção de dados.

ABSTRACT

The Area Communications System (SCA) is a complex set of communication equipment, whose purpose is the secure transmission of messages, from the commander of the Military Organization and the military involved in a given operation, within a range, with the purpose of supporting o Command and Control troops in the various operations. This work, however, is concerned with the security of information, especially in the SCA and some other means of communications carried out in military operations, as to its secrecy, privacy and maintenance of this secrecy; a constant concern for the good manager to keep the Brazilian Army Institution safe, especially in the face of the COVID-19 pandemic, caused by the large scale of work in “home office”, in which one has access to various communication systems, giving room to invasions and use of information, personal and military, which must be safeguarded by third parties. Thus, the Area Communications System should not be only concerned with “talking, listening, responding and disconnecting”, it should also be concerned with this maintenance of the secrecy during all kinds of operations and in the daily life of our Units as well.

KEY WORD: Communications Security; Confidentiality in the Area Communications System (ACS); Data Protection.

SUMÁRIO

1. INTRODUÇÃO

O ato da comunicação, de comunicar-se em sociedade, é um dos pontos que tem a maior importância na união de um grupo. Afinal, uma equipe se torna eficaz quando que consegue entender o que um do grupo está fazendo, qual o objetivo de cada atitude. Num contexto de operações militares, entra em cena o Sistema de Comunicações Táticas, com segurança e sigilo, ainda mais quando o militar, bem como a operação, se encontra uma posição em que pode colocar a ele e outros em risco.

De acordo com o Manual EB70-MC-10.241: As Comunicações na Força Terrestre, o Sistema de Comunicações de Área (SCA) consiste no conjunto de meios de comunicações que se destinam a atender os elementos de determinada área geográfica sob a responsabilidade de um determinado escalão, os quais são dotados de grande funcionalidade de comutação a fim de assegurar a confiabilidade das informações transitadas. (Brasil, 2018, p. 3-4)

Ao passarmos pelo Sec. XXI, presenciamos uma forma revolucionária das comunicações em todo o mundo. Sejam por ondas eletromagnéticas ou por cabos que interligam o transmissor ao receptor, notamos a grande velocidade e praticidade de altas capacidades de transmissão, em tempo real; o que, no caso das operações militares, em especial as do Exército Brasileiro, dão uma maior segurança e conforto na decisão dos comandantes das frações que estão envolvidas na atividade.

Isto mostra uma dinâmica mais exigente a cada momento, obrigando os comandantes a contarem com sistemas de comunicação que os auxiliem na rapidez da transmissão das mensagens entre eles e seus subordinados.

Nesse pensar, a crescente dificuldade em se definir fronteiras e limites das situações nas quais se possam pôr em perigo a segurança no trâmite das informações, aumentam a necessidade de segurança de atuação das Operações Militares e a importância da função de combate Comando e Controle (C2). O Exército Brasileiro (EB) se mantém atualizado nesse processo de transformação, alinhando-se com a Estratégia Nacional de Defesa (END), buscando a modernização da Força Terrestre, uma vez que o atual combate requer militares mais qualificados, preparados para os diversos tipos de campos de batalha.

Nossa doutrina militar caracteriza de suma importância a dimensão informacional do nosso ambiente operacional terrestre, a qual abrange os sistemas utilizados para obter, produzir, difundir e atuar sobre a informação. Ela se reveste de destacada

relevância em função dos avanços na área da informação e comunicação, que proporcionam elevada capacidade de transmissão e acesso à informação. (BRASIL, 2019, p. 22).

Nesse viés, o pronto atendimento ao comando se torna mais eficaz e, por consequência, satisfatório à gestão, contribuindo para que tenhamos melhores resultados operacionais.

1.1 PROBLEMA

Vivemos em uma era em que a Tecnologia da Informação (TI), a análise de dados e as comunicações, em geral, evoluem de uma forma muito rápida e dinâmica. Assim, faz-se necessário o emprego de táticas e doutrinas militares as quais acompanhem esse rápido fluxo de mudanças no século XXI.

Justamente por essa velocidade da informação, com a quantidade de tantos dados sensíveis, de certa forma, podem estar suscetíveis a uma invasão de rede. A segurança das nossas informações se faz mais que do que necessárias. Afinal, dados sensíveis podem ser espalhados e modificar o ambiente operacional como um todo.

Desta forma, é saliente realizar as seguintes perguntas: 1ª) A forma atual como é realizado o desdobramento do Sistema Tático de Comunicações, no emprego das Operações, tem a segurança suficiente dos dados e informações por ele transitados? e 2ª) Como tornar o sistema de comunicações mais proveitoso funcionalmente?

1.1.1 Antecedentes do Problema

Atualmente, as redes usadas nos Sistemas de Comunicações de Área (SCA) apresentam um risco reduzido no que se trata à segurança da informação no emprego dos seus diversos meios desdobrados em campanha. Os elementos componentes que formam a malha de rede do SCA, são dotados de sistema de criptografia ponta a ponta, que asseguram comunicações confiáveis entre o transmissor e receptor dos dados e mensagens.

Entretanto, se numa operação militar específica a informação trafegada entre os meios do SCA for interceptado no meio do processo, seja por algum equipamento que possa decriptografar a mensagem, seja por falha humana na configuração e/ou no manuseio dos aparelhos, ou até mesmo pela captura de militares de nossa Força, o vazamento de informações militares é um risco real no tocante à segurança da informação do Exército Brasileiro.

1.1.2 Formulação do Problema

Em um mundo interconectado, a informação e os processos relacionados (sistemas, redes e pessoas envolvidas nas operações) são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos (ABNT, 2013, p. 10).

Em consequência desse mundo, um ritmo cada vez mais acelerado é exigido para a tomada de decisões, fato que influencia decisivamente, nos níveis tecnológicos alcançados, principalmente no campo das comunicações (BRASIL, 2020, p. 2-1).

A NBR ISO/IEC 27002, publicada no ano de 2013, trata sobre gestão de segurança da informação. No trecho abaixo, pode-se fazer um paralelo sobre a importância da mentalidade que todos os militares envolvidos em uma atividade ou operação devem possuir a fim de lograr êxito no sigilo do tráfego de informações:

> A segurança que pode ser alcançada através de meios técnicos é limitada e está apoiada por procedimentos e gerenciamentos apropriados. A identificação de quais controles devem ser implementados requer planejamento e atenção cuidadosa em nível de detalhes. Um sistema de gestão da segurança da informação bem sucedido requer apoio de todos funcionários da organização. Orientações de especialistas externos podem também ser necessárias. (NBR ISO/IEC 27002, 2013, p.10)

Nota-se que “segurança da informação” é um termo usado amplamente quando se faz necessária a proteção e defesa de dados, tendo como objetivo assegurar a integridade e sigilo daquelas informações, em um determinado sistema, as quais podem ter seu acesso apenas, e somente, pessoas que que sejam seus responsáveis, ou seja, os responsáveis de direito. Segundo Marcos Sêmola (2003, p. 1), a informação é “um

ativo cada vez mais valorizado", e no meio militar esse valor torna-se ainda mais crucial.

A segurança da informação deve proporcionar a circulação de dados confidenciais com segurança, principalmente, quando versam sobre informações de cunho militar, as quais podem possuir conteúdo sigiloso.

A fim de garantir essa privacidade de dados, faz-se imprescindível que tenhamos o devido cuidado para que não haja o vazamento dos mesmos, como informação, vindo a ser usada contra a Organização Militar ou até mesmo contra o Exército Brasileiro, expondo a imagem da Força. Tudo isso faz parte do cuidado com a proteção de dados, tais como a confidencialidade, autenticidade, integridade e legalidade.

1.2 OBJETIVOS

A fim de apresentar os objetivos principais deste trabalho, buscaram-se algumas preocupações que deveriam ser tomadas quando do uso do Sistema de Comunicação de Área (SCA), abaixo apontados nos Objetivos Geral e Específicos:

1.2.1 Objetivo Geral

A segurança da informação se faz uma grande aliada no ambiente militar, em especial no ambiente operacional, pois quando há a segurança de dados, evita-se o acesso, de forma indevida, por outros diferentes daquele grupo militar que se pertence.

No pensar de Gouveia (2016, p. 5), "a segurança da informação é a proteção de informação, dos sistemas e dos dispositivos (hardware) que usa, armazena e transmite informação."

Assim, o Sistema de Comunicações de Área (SCA) pode atuar de maneira mais segura, com uma menor chance de interferência, com a segurança e o devido sigilo necessário, permitindo que as operações saiam de acordo com a demanda do escalão superior.

A velocidade de transmissão de mensagens nos dias atuais é imperativa para o bom cumprimento da missão, antes, durante e após as fases das operações militares. A distância que separa as tropas desdobradas, sejam em campo ou em aquartelamento, sobrepondo-se as limitações do alcance dos equipamentos rádio,

podem exigir o emprego de postos de retransmissão de ondas de rádio, o que deve trazer uma preocupação quanto ao sigilo exigido nos dados da comunicação.

Para isto, nas diversas operações, é necessária uma preocupação constante dos militares de Comunicações, responsáveis pela manutenção do SCA, no que diz respeito ao sigilo e segurança das comunicações, a fim de que se evite ao máximo o vazamento de tais informações nos enlaces existentes no Teatro de Operações.

Assim, como Objetivo Geral, pretende-se apresentar o Sistema de Comunicações de Área de Divisão de Exército sob o ponto de vista da análise da segurança da informação.

1.2.2 Objetivos Específicos

Com a finalidade de delimitar e alcançar o desfecho esperado para o objetivo geral, foram levantados objetivos específicos que conduziram à consecução do objetivo deste estudo, os quais estão transcritos abaixo:

a) Caracterizar o Sistema de Comunicações de Área (SCA) quanto ao seu emprego no nível DE;

b) Apresentar algumas formas de segurança da informação no emprego do SCA;

c) Citar algumas formas de segurança que podem prevenir o vazamento de informações quanto ao planejamento de ações militares, buscando possíveis atos que venham a deixar os sistemas de comunicações mais seguro, sem vazamento das informações nas atividades operacionais.

1.3 QUESTÕES DE ESTUDO

O Sistema de Comunicações de Área (SCA), é empregado no nível Divisão de Exército (DE), é o sistema responsável por estabelecer ligações automatizadas e de grande capacidade aos elementos orgânicos de um escalão considerado dentro de determinada Zona de Ação (Z Aç), a fim de que se estabeleça a estrutura de comunicações necessária para o exercício do Comando e Controle (C2), e nesse estudo, questiona-se no decorrer deste Trabalho quanto ao grau de segurança das

informações e o seu grau de sigilo, um fator preponderante para as tomadas de decisões.

Para isso, como um dos objetivos específicos, apresentar-se-ão algumas formas de segurança da informação no emprego do SCA, para que essa estrutura de Comunicações no Teatro de Operações (TO) permita atender às necessidades do G Cmdo enquadrante, no tangente à estruturação do sistema de comunicações por área, garantindo aos G Cmdo/GU/U desdobrados na Z Aç do Elm apoiado, integração aos diversos sistemas instalados.

Os elementos do SCA são distribuídos com seus diversos meios desdobrados na Z Aç de modo a cobrir uma determinada área de operações, assegurando que o usuário, onde quer que se encontre, tenha sempre próximo a ele uma porta de entrada no sistema. É formada assim uma rede interconectada a qual é disposta no terreno de tal forma que os usuários fiquem livres para deslocar-se na Z Aç sem que haja a interrupção das comunicações nessa rede.

Os meios que o SCA emprega no nosso Teatro de Operações são dotados de equipamentos de comunicações que podem variar de acordo com a tecnologia disponível, que permitam, aos seus usuários, o estabelecimento de ligações automáticas, seguras e imediatas para qualquer parte da zona de ação.

Assim, diante do pensar do tema do presente trabalho, que busca uma “análise da segurança da informação no desenvolvimento da comunicação”, em termos de segurança da informação, é bom pensar-se em algumas formas de segurança que venham a prevenir o vazamento de informações, quanto ao planejamento de ações militares, buscando-se possíveis atos que venham a deixar os sistemas de comunicações mais seguros, sem vazamento das informações nas atividades operacionais, as questões postas tendem a verificar quanto à evasão das informações que devem ser coletadas dentro de um SCA e levadas a terceiros, estes de fora do meio militar; colocando em pontos diferentes de perigo às comunicações gravadas, copiadas ou repassadas dentro do SCA, pois de qualquer forma, qualquer falha às atividades rotineiras atinentes ao trabalho será afetada e algum prejuízo será tomado.

Cabe aqui ressaltar que deve haver uma preocupação constante de que isso não deva ser válido apenas para os sistemas já existentes, mas como também para os que estejam sendo previsto para serem adquiridos ou desenvolvidos.

1.4 METODOLOGIA

A presente pesquisa será de cunho bibliográfico, em torno de algumas publicações de manuais do próprio Exército Brasileiro, artigos acadêmicos publicados de forma *on line* e até mesmo informações de alguns *sites*.

No decorrer do presente trabalho, utilizar-se-á o método de pesquisa qualitativa descritiva, com ênfase na observação e estudos documentais.

1.4.1 Amostra

A amostra, normalmente, é feita com a prévia seleção de um universo (população), sendo definida como elementos que podem possuir determinadas características; em que se estabelecem ou estimam as características deste universo ou população. Este trabalho, para fins de amostra, não tende uma população, mas sim o sistema de Comunicação de Área (SCA) e seus aspectos de sigilo e segurança, dependendo unicamente de critérios bibliográficos.

Assim, apresente pesquisa será qualitativa, pois dará ênfase na análise dos diversos manuais de campanha do Ministério da Defesa e do Exército Brasileiro em que houver relatos do assunto atinente ao desdobramento do Sistema de Comunicações de Área (SCA).

1.4.2 Delineamento da pesquisa

Seguindo o Manual para apresentação de Trabalhos Acadêmicos (EsAO/2013), a metodologia a qual será empregada na confecção do presente trabalho de conclusão de curso será bibliográfica, qualitativa descritiva.

A pesquisa qualitativa privilegia o conhecimento de como os fenômenos ocorrem e suas possíveis explicações, onde, ao final dessa pesquisa, são expostas algumas análises de conceitos e ideias. Desta forma, o pesquisador tem um importante papel em juntar as fontes de dados, interpretar e tirar conclusões embasadas nas fontes.

Segundo Minayo (2004, p. 22), este tipo de pesquisa se preocupa com um nível de realidade que não pode ser quantificado, trabalhando com significados, motivos e atitudes dos processos dos fenômenos que não podem ser reduzidos à operacionalização de variáveis.

1.4.3 Procedimentos para revisão da literatura

Como fontes para a revisão de literatura desta pesquisa acerca da “Análise da segurança da informação no desenvolvimento da comunicação”, tema do presente Trabalho, foram pesquisadas obras correlacionadas, em publicações que tenham abrangência acerca do assunto da pesquisa; em especial, as que sejam voltadas para segurança da informação e que venham a impactar diretamente as atividades do Sistema de Comunicações de Área (SCA).

Considerando que o enfoque do presente estudo será qualitativo, o procedimento para a revisão da literatura será, mormente, a pesquisas bibliográficas e documentais, a fim de proporcionar um suporte satisfatório para os resultados das conclusões obtidas.

1.4.4 Análise dos Dados

Os dados analisados no presente trabalho, além de toda coleta bibliográfica citada nas referências, se resumem aos materiais componentes do Sistema Tático de Comunicações (atual SCA) existentes no 1º Batalhão de Comunicações (1º B Com) em Santo Ângelo – RS, o qual fora visitado durante o estágio realizado pelos Cap Alunos da Escola de Aperfeiçoamento de Oficiais na semana de 16 a 20 de agosto do corrente ano.

1.5 JUSTIFICATIVA

No atual mundo globalizado, no qual tarefas diversificadas são realizadas, de

simultaneamente, uma troca bastante consideráveis de *e-mails* confidenciais, em que mensagens são e podem ser trocadas, em apenas um clique, fazendo-se fundamental que haja uma proteção para evitar-se evasão de informações por sistemas e até por usuários.

Assim, o presente Trabalho se justifica pela importância de manter-se em segurança as informações de atividades militares realizadas, dentro do campo das informações trafegadas pelo SCA, dentro da OM responsável pela operação do sistema.

Há um dever tanto profissional quanto funcional nesta preocupação que deve ser constante: a segurança do sistema de informações, considerando que as operações, bem como as suas informações, sejam de interesse de serem mantidas, no mínimo, protegidas de quem não seja do meio militar, ou que participem daquela operação, sendo relevante pensarmos, conjuntamente, sobre a manutenção e segurança das informações.

Assim, nesse pensar específico, a segurança da Informação nos permite e nos exige que pensemos e construamos formas e métodos que visem evitar a livre circulação de dados, estes de caráter sigiloso ou confidencial, devendo restringir ao máximo a quantidade de pessoas que tenham manipulação direta a esses dados, a essas informações.

Nesse viés, sabe-se que o Sistema de Comunicações de Área (SCA) tem como sua missão principal apoiar o comando e controle no nível tático de uma operação com o trâmite das informações do escalão superior para com o escalão considerado. Tal exigência é fruto da profundidade de uma operação, bem como da necessidade de comunicar-se com os diversos escalões, em que não devem ter seu sigilo e seguridade quebrados, isto é, devendo ser apenas de confidencialidade dos militares pertencentes ao Comando para com seus escalões considerados.

O Comando e Controle em combate sobre as diversas frações é, indubitavelmente, essencial para obter-se o sucesso ou fracassar nas operações. Cabe aqui inferir que a transferência de informação do SCA para o comando, de forma fluida, eficiente e atualizada nos embates atuais, é um fator chave para auxiliar nas decisões do comando.

O benefício deixado, bem como buscado por essa pesquisa, é o dever de um olhar mais atento quanto ao sistema de vigilância da informação pelos integrantes da Força Terrestre, visando unicamente a segurança que deve ser proporcionada pelo

estabelecimento de uma rede segura; se possível, mitigando ao máximo os riscos de invasão, complementada por instrumentos e sensores eletrônicos, evitando que tais informações das comunicações trafegadas possam ser vazadas por e repassadas a terceiros que não tenham afeto à Instituição.

2. REFERENCIAL TEÓRICO

2.1 O SISTEMA DE COMUNICAÇÕES DE ÁREA

Segundo consta no C 11-30 (Brasil, 1998, p. 4-1), o Sistema de Comunicações de Área (SCA) é composto por vários meios de comunicações cujos sistemas de enlace devem ser utilizados de forma a atender, simultaneamente, ao maior número possível de princípios de emprego de comunicações.

O SCA, quando apoia o escalão Divisão de Exército (DE), como este é considerado um grande comando operacional da força terrestre, deve estar propício a atuar em áreas de grandes dimensões e com elevado grau de confiabilidade. (BRASIL, 2018, p. 3-4).

Os diversos meios componentes do SCA são distribuídos de modo a cobrir, de forma celular, uma determinada Zona de Ação (Z Aç) na área de operações da DE, assegurando que o usuário, onde quer que se encontre, tenha sempre próximo a ele uma porta de entrada a qual dá acesso ao sistema.

De acordo com o Manual de Campanha – Comunicações na Divisão de Exército (C 11-61), as finalidades dos meios componentes do Sistema de Comunicações de Área são (BRASIL, 1995, p. 3-4):

> a. Abranger toda a zona de ação atribuída à DE;
> b. Interligar os postos de comando divisionários a todas as GU operacionais (até 5 Brigadas) e as GU e U da Base Divisionária, inclusive ao comando logístico da DE, quando ativado;
> c. Interligar-se aos sistemas dos escalões superiores e vizinhos;
> d. Ter acesso às estações do Sec existentes na Z Aç, ampliando as possibilidades de ligação;
> e. Ter acesso ao SNT e às estações fixas ou móveis do SISCOMIS desdobradas na sua Z Aç, permitindo o estabelecimento de ligações com outros elementos, inclusive fora do Teatro de Operações (TO) e aumentando consideravelmente as rotas alternativas;

> f. Permitir as ligações através de transmissão automática de dados, aumentando a capacidade de tráfego e possibilitando a utilização da informação, de forma simultânea;
> g. Acompanhar os deslocamentos dos Postos de Comando (PC) da DE e de elementos subordinados;
> h. Permitir a integração com o SIGELEX
> i. Permitir a conexão, ao sistema, de postos rádio móveis (sistema do assinante móvel), dos postos rádio das redes rádio em campanha e dos terminais de telefonia (assinantes fixos);
> j. Estabelecer a sua própria proteção através do gerenciamento automático de acesso, do emprego de códigos preestabelecidos, da comutação entre assinantes com a designação automática de rotas aleatórias e da intensiva utilização de Medidas de Proteção Eletrônica (MPE);
> k. Acompanhar a grande mobilidade das unidades de combate; e
> l. Comutar automaticamente os assinantes através de rotas aleatórias.

Ainda em relação ao manual citado anteriormente, podemos inferir que existem vários fatores de decisão os quais influem no emprego dos meios e dos sistemas de comunicações:

> Fatores diversos influem no emprego dos meios e no estabelecimento do sistema de comunicações. A Dispersão tática e as operações em largas frentes acarretam um desdobramento correspondente das comunicações ao longo dos eixos de progressão e dificultam as ligações laterais. Uma área despovoada priva a DE de possíveis recursos locais que possam ser aproveitados para o sistema. (BRASIL, 1995, p. 3-1)

2.2 OS SISTEMAS DE INFORMAÇÕES

Pode-se afirmar que as informações são uma das principais vantagens que temos na atualidade, estas que tem de ser protegidas em todos os processos da Organização Militar.

Todos os sistemas de informações têm falhas, vulnerabilidades estas que cedo ou tarde acabam sendo descobertas por usuários ou até pelo fabricante. Estas podendo ser falhas eletrônicas ou causadas por operadores, quando da utilização do sistema de forma ampla, há de se ter uma preocupação com esses acessos, que pode gerar um risco à segurança das informações trafegadas dentro do SCA.

Para que isto venha a ser evitado, descobertas essas vulnerabilidades que podem trazer problemas para o sistema, pode-se ser feito um inventário do sistema, completo, e, que deve ser sempre atualizado com os ativos de informação (tais como fabricantes, versões e seus usuários internos).

Com isso, passa-se a ter uma noção se as informações que trafegam pelo SCA poderiam estar expostas ou não, podendo analisar suas vulnerabilidades, estas que, caso existam, devem ser mitigadas ou eliminadas, com a alteração de novas rotinas operacionais, ou, se for o caso, mudanças nos sistemas de segurança da informação.

Com a permanente evolução das ameaças, gerenciar e conhecer bem os riscos de segurança da informação se torna uma das maiores, senão a maior, preocupações dos comandantes. As organizações devem agir, de forma que adotem, cada vez mais, tecnologias inovadoras, como a segurança analítica e a proteção cibernética baseada em nuvem, para reduzir estes riscos e melhorar os programas destinados à segurança.

A segurança analítica, resumidamente, se consiste na análise de imagens geradas em tempo real que podem vir a identificar padrões suspeitos e realizar alertas sem a necessidade de um monitoramento humano por 24 horas do dia.

A proteção cibernética, algo que desde 2008 o Exército Brasileiro foi responsável via o plano da Estratégia Nacional de Defesa (END) e vem aprimorando anualmente, poderia ser aplicada no SCA em conjunto com a segurança analítica, através de câmeras a serem instaladas nas cabines existentes, de modo que os dados de filmagem fossem criptografados e constantemente enviados a um escalão superior para análise caso houvesse algum risco existente.

Tais ações provavelmente contribuiriam para o aumento da mentalidade no tocante à segurança das informações de todos militares envolvidos numa determinada operação.

Ou seja, evitar ou minimizar a possibilidade de captura de dados que trafegam no SCA e, em caso de sucesso na coleta de informações, que sejam o menos inteligível possível.

2.3 AVALIAÇÕES DE SEGURANÇA

O SCA é um canal que trafega uma massa grande de informações, pois por ele se passa as mais variadas informações acerca de uma operação, de suas atividades, quantidade de militares empregado nela entre outras. Cuidar destas Informações significa o dever de proteger os dados existentes, bem como os sistemas de informação de acessos, juntamente com seu uso não autorizados.

Com isso, no tangente a essas informações trafegadas pelo Sistema de Comunicações de Área (SCA), precisa-se evitar ao máximo sua divulgação, bem como a modificação, releitura, gravação, a fim de prezar pela segurança da informação nas organizações além de introduzir conceitos associados a esse fim.

Assim, cabe aos Cmt imediatos das frações do pessoal que operam os meios do SCA, bem como aos militares que servem em OM que possuem esse sistema, militares capacitados na operação do SCA, para a defesa e proteção dos dados gerados pelo SCA, com o conhecimento necessário, as possíveis fragilidades apresentadas pelos sistemas; visando, exclusivamente, a segurança das comunicações, num viés de sigilo da informação, indo ao encontro da segurança e do sigilo das ações do comando.

Acredita-se que se faz necessário comentar o quão é importante o especial cuidado quanto a não divulgação das senhas, bem como os códigos de acesso (formas eletrônicas de acesso e identificação nos meios componentes do SCA) a ninguém, pois alguém mal-intencionado pode gerar e produzir verdadeiros danos ao comando da Unidade, bem como a Força Terrestre.

Coadunando nesse pensar, Serafim *et al*, p. 46, destaca que as

> Preocupações desse tipo já devem começar no processo de recrutamento de pessoal. É muito importante que exista uma política de seleção e contratação

> de recursos humanos e que, nessa fase, sejam incluídas em contratos as responsabilidades de segurança e os possíveis acordos de confidencialidade atribuídos a cada cargo.

Assim, faz-se necessário, ao pensar em segurança da informação, pensar em formas de proteção de dados de comunicação, em especial as enviadas via ondas de rádio.

Como toda a informação se faz importante, para assegurar essas informações, a seguir abordar-se-ão algumas formas para diminuir esses riscos que podem ser prejudiciais ao bom andamento do trabalho do Sistema de Comunicações de Área (SCA), sob a responsabilidade dos Oficiais de Comunicações e os comandantes de fração imediata dos operadores do Sistema.

2.3.1 Falhas na segurança de um Sistema de Comunicações

Falar em segurança, ainda mais em se tratando da informação, torna-se um sistema muito complexo, uma forma difícil para implantar um sistema, principalmente nos devidos ambientes com atividades computacionais. Assim, a ideia de implantar um sistema que vislumbre a segurança, significa analisar um complexo conjunto de situações diversificadas, em que se devem elaborar estratégias completamente independentes.

No que tange aos aspectos de segurança requeridas pelo Sistema de Comunicações de Área (SCA), que podem ser analisados, deve se ter uma plena preocupação, ainda mais em relação ao tema do assunto abordado nesta pesquisa, é a segurança lógica dos dados, que buscam garantir:

-a privacidade: alguns dados devem ser acessíveis somente por pessoas que sejam autorizadas;

- a autenticidade de dados: estes são autenticados (desde que gerados pelos militares autorizados);

- a integridade: estes mesmos dados deverão estar protegidos contra algumas modificações (sejam totais ou parciais); e

- a disponibilidade: estes mesmos dados têm de estar disponíveis para consulta sempre que forem necessários.

O uso destes dados, como atributos ativos em uma comunicação, deve ser com a proteção como ferramentas de segurança de dados, como a criptografia ou outras técnicas, desde que visando sempre evitas falhas, mas aconselha-se sempre dedicar uma atenção especial à prevenção contra falhas ocasionadas por terceiros, ou seja, intencionais.

2.3.2 Análise de vulnerabilidades

Uma análise de vulnerabilidades quanto ao funcionamento do SCA pode ser definido por uma fraqueza que pode vir a colocar em risco o Sistema de Comunicações de Área.

É um ato para poder analisar as vulnerabilidades de uma rede. Torna-se necessário conduzir uma análise de risco da segurança da informação, de modo a determinar as ameaças e as vulnerabilidades para a informação e as contramedidas necessárias para serem aplicadas de modo a reduzir (mitigar) o efeito destes riscos (impacto) para um nível aceitável.

Para Gouveia (2016, p. 7)

> É da análise de risco que a informação que é necessária para a gestão tomar decisões acertadas relativas à segurança da informação de uma organização, é obtida. Essa obtenção por esta via, devesse ao facto da análise de risco identificar os controlos de segurança no local, calcular as suas vulnerabilidades e avaliar o efeito das ameaças, em cada área ou situação de vulnerabilidade.

Esta verificação de segurança visa identificar possíveis brechas, bem como falhas que podem deixar o SCA vulnerável às ameaças, como interceptação dos dados. Isto pode ocorrer por falha humana, pela ocorrência de interceptação de tráfego ou até por força bruta, ou seja, ação truculenta, físicas, de terceiros para com militares.

Gouveia (2016, p. 21), ainda defende que

> (...) deve ser especificado quais as pessoas que são responsáveis por implementar os requisitos de segurança. Esta documentação suporta quem tem a tarefa de coordenar as responsabilidades individuais em conjunto com os especialistas em segurança. Ao mesmo tempo, o plano torna explícito quem é (ou pode ser) responsável, se existem requisites que não possam ser cumpridos e vulnerabilidades a que não foi dada resposta.

Para evitar estes tipos de problemas de vazamento de informações do SCA, devem-se identificar os sistemas de dados que integram a estrutura da usada na rede, bem como os militares que trabalham na respectiva rede. Assim, os militares que estão diretamente operando o SCA não devem deixar de acompanhar as medidas de segurança já existentes.

2.3.3 Teste de invasão

Qualquer forma ou tentativa, bem ou malsucedida, o acesso ou uso não autorizado do SCA ou de seu respectivo serviço, pode ser denominado como uma invasão.

Assim, pode-se aplicar testes de invasão, com simulações de invasão à rede rádio do Sistema de Comunicações de Área (SCA), simulando um ataque real àquela rede, com a finalidade de avaliar a segurança existente, com uma análise de possíveis vulnerabilidades, deficiências técnicas e fraquezas da estrutura física da rede rádio, por exemplo.

Atualmente, uma sugestão de uma possível maneira de contribuir para o aumento da segurança e monitoramento caso uma invasão no sistema seja identificada, já que o SCA em operações costumam distar de 40 a 50 Km umas das outras, é a aquisição de Veículos Aéreos não Tripulados (VANTs) ou Sistemas Aéreos remotamente pilotados (SARPs) para melhor visualização da localização da ameaça.

O VANT, por exemplo, auxiliaria na vigilância aérea da área onde se encontram as cabines, a fim de dar um alerta antecipado para sua desmontagem e saída de posição, caso alguma ameaça estivesse muito próxima.

Já que não é possível garantir a proteção total às informações das ameaças, torna-se necessário conduzir uma análise de risco da segurança da informação, que seja possível determinar as ameaças, as vulnerabilidades para a informação; bem como as contramedidas necessárias para serem aplicadas de modo a reduzir (mitigar) o efeito destes riscos (impacto) para um nível aceitável.

2.3.4 Plano de segurança

Faz-se imperioso que exista um plano de segurança para o SCA. Deve ser previsto um canal técnico onde trafeguem informações especificas da operação do Sistema, inclusive em caso de acionamento (simulado ou não) do Plano de Segurança. Assim, a OM deve ter em seus quadros de pessoal efetivos especialistas que possam vir a desenvolver planejamentos de segurança, formalmente definidos.

2.3.5 Avaliação de riscos

Serafim *et al (*p. 55), defende que,

> [...] quando a avaliação apontar para um nível de risco médio, ações e planos corretivos são necessários em um período de tempo razoável, durante o qual o sistema pode continuar em operação. Por outro lado, quando níveis de risco baixos forem obtidos, medidas corretivas podem ser adotadas ou pode-se optar por correr esses riscos.

Esta operação avaliativa de risco do SCA tem como finalidade gerar informações para uma possível tomada de decisão nas atividades de controle às informações que trafegam pelo Sistema e que estejam em risco, devendo esta avaliação ser adequada e suficiente. Considerando que “da mesma forma, como a abordagem correta é enfocar riscos e a sua consequente minimização, fica evidente a dificuldade em mensurar quantitativamente o quão protegido um sistema está.” (Serafim *et al*, p. 46)

Em relação à avaliação de riscos do Sistema de Comunicação de Área (SCA), tratando-se da política de segurança, deve existir sempre latente essa preocupação por parte do responsável pelo sistema. Deve presumir-se que:

> O plano de segurança é um documento dinâmico e que acompanha a evolução da própria organização, pelo que precisa de revisto e melhorado, de forma periódica. A alteração do plano de segurança depende essencialmente das necessidades da organização, das suas necessidades de segurança e dos resultados da gestão de risco. Um bom plano de segurança é um registro oficial da prática de segurança corrente, na organização. (GOUVEIA, 2016, p. 15)

Assim, os requisitos de segurança devem ser desenvolvidos a fim de especificar as políticas relacionadas à segurança do sistema e devem mapear os riscos do sistema de segurança que já foram identificados, as vulnerabilidades e as ameaças. Os requisitos devem também suportar a implementação de um plano de segurança. Este plano deve ser revisto periodicamente.

Monitorar o plano se faz um papel importante para qualquer sistema de gestão de segurança da informação. Desta forma, para avaliar as soluções de segurança, bem como suas práticas, como as políticas de segurança. O Plano e seus requisitos são importantes, agindo como referenciais para todo o processo.

2.3.6 Controle de acesso

Um fator que deve ser levado em conta deve ser os acessos ao complexo Sistema de Comunicação de Área (SCA), ou seja, as pessoas quem têm esses acessos.

Todos os usuários devem ser monitorados, a fim de que sejam inspecionadas as ações de envio de dados/mensagens, evitando quaisquer “ruídos” diferentes do que deveria ser transmitido, que venham a causar danos diretamente na eficiência da comunicação.

> Uma pessoa não autorizada que tem acesso a alguns dos elementos acima é denominada de um atacante. Um atacante passivo somente consegue obter cópias destes elementos, enquanto um atacante ativo consegue não somente obter cópias como também modificar os elementos. (SERAFIM *et al*, pag.16 e 19)

Os controles de acesso do sistema de segurança do SCA, são medidas operacionais recomendadas para os sistemas de informação, que visam proteger a confidencialidade, a integridade, a disponibilidade de um sistema, bem com suas informações. Estes controles, quando utilizados de uma forma adequada, podem prevenir, limitar ou até deter uma ameaça aos ativos que trafegam no sistema.

2.3.7 Formas de segurança nas Comunicações

O problema maior, atualmente observado, é um enfoque excessivo nos vários mecanismos que visam dar a segurança que, em vários casos, gera uma falsa sensação de estar seguro para os dados.

Tais sistemas que visam unicamente a segurança do SCA deverão ser selecionados criteriosamente seguindo as características comerciais, com a indicação de militares que tenham o devido conhecimento para evitar que sejam mal configurados, ou até instalados em locais que venham a se tornarem pouco eficazes; em especial, por pessoas que não possuem o conhecimento necessário.

Desta forma, não se faz necessário apenas possuir conhecimentos nos respectivos mecanismos em segurança, faz-se expressamente necessário conhecer e aplicar na prática a política de segurança.

Essa política é quem dita todos os princípios, bem como as regras que regulam o quesito complexo da segurança da informação. Para isso, ao implantar tal norma de segurança, faz-se importante conhecer seus mecanismos e a adoção de todos os procedimentos relacionados ao tema.

Sem esta devida e imperiosa preocupação, qualquer estratégia usada na segurança da rede do Sistema de Comunicações de Área (SCA), tornar-se-á ineficaz pelo fato de estar suscetível.

Devem ser pensadas as soluções com a definição de uma política de segurança, podendo-se escolher os primeiros passos para implementar mecanismos de proteção, passando a considerar tais questões:

- qual a probabilidade de um ataque?
- o que é preciso para proteger?
- o que se está querendo proteger?
- qual o prejuízo se o ataque for bem sucedido?

Preocupações simples, mas que visam expressamente à segurança da Rede de Comunicação, devendo ter como finalidade principal o fiel cumprimento do que fora traçado na política de segurança e devendo estar alinhados às suas exigências.

2.4 DELIMITAÇÃO DO ESTUDO

A fim de buscar uma possível solução para o problema apresentado, o presente trabalho pretende limitar-se pesquisa sobre uma análise da segurança da informação no desenvolvimento da comunicação em torno do Sistema de Comunicações de Área(SCA) de uma Divisão de Exército, em algumas de suas especificidades de sigilo e segurança.

O presente estudo, desta forma, direciona-se ao Sistema Tático de Comunicações do Exército Brasileiro em apoio às operações, utilizando todos seus meios orgânicos de pessoal e material.

2.5. ANÁLISE E RESULTADOS

Assim, considerando-se a revisão conduzida, cabe salientar que não se busca resolver todos os fatores, mas aportar cuidados que se devem tomar ao expor as informações militares.

O mundo globalizado é um emaranhado de teias de informação. Segundo o pensador Beloti[1], “Quem tem informação, tem poder! Quem tem conhecimento, tem sabedoria para mantê-lo!”. Assim, a segurança da informação se torna um dos objetivos que se pode julgar ser um dos mais importantes no seio de uma instituição, sobretudo, na instituição do Exército Brasileiro.

Nesse pensar, o Exército Brasileiro deve manter sempre em sigilo suas informações.

Desta forma, pode-se afirmar que o tema da segurança da informação, cada vez mais, está se tornando por demais complexa e, cada vez mais, importante para a proteção e salvaguarda do EB, aumentando de importância esta proteção de dados como um ativo, de uma forma mal-intencionada, devendo sempre prezar pela segurança da informação, sem olvidar da confidencialidade, da disponibilidade e da integridade.

---

[1] Emerson Beloti. Disponível em: <https://www.pensador.com/frase/MjEyNTgyMg/#:~:text=Quem...-,Quem%20tem%20informa%C3%A7%C3%A3o%2C%20tem%20poder!,sabedoria%20para%20mant%C3%AA%2Dlo!!! >. Aceso em 17 Set 2021.

Nesse pensar, Gouveia (2016, p. 11) mostra um fator como preocupação quanto ao sigilo de dados.

> Deste modo, as preocupações com a segurança são importantes e a norma ISO 27000 constitui a principal família de normas para a segurança da informação, em que é apresentada a classificação de informação de acordo com a sua confidencialidade e a norma está apoiada nos princípios da integridade, disponibilidade e confidencialidade da informação.

Assim sendo, o simples ato de operar uma rede simples de comunicação se torna primordial pensar sobre o assunto da segurança da informação, vazamento das comunicações, em especial nas operações e atividades militares.

Assim, cabe a esse trabalho de conclusão de curso (TCC) apontar para a análise da segurança do canal, frente a esta realidade de manter seguro os dados produzidos pelo SCA, sobremaneira, o papel primordial da proteção do tráfego de informações.

Faz-se claro, no aspecto da segurança, como ainda, a preocupação na segurança das informações, que com as boas e eficazes práticas devem sempre ser estimuladas, buscando a segurança operacional no tangente a proteção das informações.

3. CONSIDERAÇÕES FINAIS E SUGESTÕES

A presente pesquisa buscou abordar de algumas maneiras que podem trazer mais segurança ao Sistema de Comunicações de Área (SCA) durante as suas atividades. O SCA se integra às operações, sendo o elo de comunicação entre o comando e parte operacional. No que diz respeito aos níveis de segurança das comunicações, via rede, é uma maneira que necessita ser rápida e eficaz, para se obter sucesso em apoiar o Comando e Controle dos elementos subordinados e em apoio.

Nesse pensar, as forças de defesa empregadas devem estar aptas a combinarem atitudes, simultâneas ou sucessivamente, em operações defensivas ou ofensivas, de pacificação e de apoio a órgãos governamentais (operações de cooperação e coordenação com agências), observado sempre que as medidas de confidencialidade e salvaguarda devam estar e ser persistentes, devendo prevalecer durante e enquanto os dados que sejam elaborados pelos sistemas da rede da OM, na transmissão de todos os dados e comunicação, de origem e de destino.

Assim, qualquer processo para a tomada de decisão envolve, nesse complexo processo de comunicação, no envio e recebimento de dados, da posse deles; a obtenção e a manutenção da consciência situacional, até a decisão propriamente dita. Nesse sentido, a atividade do Oficial de Comunicações encarregado pelo desdobramento do SCA em uma determinada operação, apoiado por um administrador de rede, é fundamental para o êxito das operações militares.

Estima-se que a guerra do futuro será em um ambiente de rede, uma guerra eletrônica e cibernética. Quanto aos dados, localização, comunicação, invasão de redes de comunicações e software, deve-se ter sempre em mente as medidas para as proteções eletrônicas; na segurança e sigilo de pacotes de comunicações, não apenas de voz, mas também de dados.

Por isso, a importância deste trabalho em apresentar questões acerca do Sistema de Comunicações de Área (SCA), sobre segurança às transmissões do sistema.

É imprescindível garantir o sigilo e manutenção nas atividades do SCA, uma vez que um simples *bug* ou *malware* pode colocar em perigo as informações.

Considerado que o C 11-30 - As Comunicações na Brigada (Brasil, 1998, pg. 2-3), cita: “a importância representada para o comando e controle tornam o posto de comando das operações militares um alvo extremamente compensador para o inimigo, o que obriga a implantação de medidas efetivas para a sua segurança”, que recomendo a adoção das observações abaixo, estas necessárias ao funcionamento de um SCA, pra manter a “(...) estabilidade para o comandante e seu estado-maior conduzirem as operações:”

- busca da segurança física dos órgãos de Com, mantendo-se distâncias de segurança entre os diversos postos de Com (Brasil, 1998, p. 4-2);

- confidencialidade: a devida informação só poderá ser acessada por pessoas que possuam autorização, “devendo ser previstas medidas de proteção, ativas e passivas, no uso do espectro eletromagnético e das redes computacionais, visando à segurança e à confiabilidade das informações e Comunicações, negando dados aos eventuais elementos adversos”; (Brasil, 2020, 1-3)

- confiabilidade: é o ato de demonstrar a que há fidelidade e uma boa qualidade na informação com a qual o sistema estará trabalhando (Brasil, 1998, p. 4-7);

- integridade: é a garantia que a informação corrente estará protegida, completa,

da mesma maneira como fora arquivada, evitando-se, desta forma, quaisquer problemas, como alterações de má fé ou indevidas (Brasil, 2020, p. 5-12);

- disponibilidade: é possuir a certeza que aquela informação estará sempre disponível, acessível em qualquer lugar e hora, para aquele usuário que fora autorizado para acessá-las (Brasil, 1998, p. 4-7);

- autenticidade: é saber que, através de registros apropriados, as pessoas que tiveram acesso as informações, quem fez as alterações/exclusões e, acima de tudo, se esta pessoa possui autorização para essas execuções; de forma que todos os usuários do grupo vejam que a segurança daquelas informações estão sendo tratadas com a devida responsabilidade e cuidado para que, dessa forma, sejam beneficiados (Brasil, 2020, p. 4-15).

As atividades acima descritas são exigidas em Manual para o Sistema Tático de Comunicações de uma Divisão de Exército, com a finalidade unicamente de apoiar as necessidades do Comando e Controle, com comunicações rápidas e eficazes. (Brasil, 1995, p. 3-1)

Em concluso, faz-se necessário perceber que os sistemas de comunicações são de importância extrema. E, a fim de contribuir com a otimização de uma melhor comunicação, é bom pensar nesses quesitos no tangente à segurança da informação.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 27002. **Tecnologia da Informação – Técnicas de Segurança Código de prática para a gestão de segurança da informação**. Rio de Janeiro, 2013.

BRASIL. Exército. Estado Maior do Exército. EB20-MF-10.102: **Doutrina Militar Terrestre**, 2. ed. 2019.

BRASIL. Exército Brasileiro. Estado Maior do Exército. C11-30: **As Comunicações na Brigada**, 2. ed. 1998.

BRASIL. Exército Brasileiro. Estado Maior do Exército. C11-61: **Comunicações na Divisão de Exército**, 1. ed. 1995.

BRASIL. Exército Brasileiro. Comando de Operações Terrestres. EB70-MC-10.246: **As Comunicações nas Operações**, 1.ed. 2020.

BRASIL. Exército Brasileiro. Comando de Operações Terrestres. EB70-MC-10.241: **As Comunicações na Força Terrestre**, 1. ed. 2018.

GOUVEIA, Luís Borges. **Gestão da Segurança da Informação.** Conceitos básicos e introdução ao tema. v. 1.1, mar 2016. Disponível em: <https://bdigital.ufp.pt/bitstream/10284/5954/1/securv1_1_mar2016.pdf>. Acesso em: 12 Set 2021.

MINAYO, Maria Cecília de Souza (Org.). **Pesquisa Social**: teoria, método e criatividade. 23. 1. ed. Petrópolis: Vozes, 2004.

SÊMOLA, M. **Gestão da Segurança da Informação: Uma visão executiva.** Rio de Janeiro: Campus, 2003.

Técnicas de Segurança da Informação: da Teoria à Prática(Cap 4). SERAFIM, Vinícius da Silveira; WEBER, Raul Fernando; CAMPELLO, Rafael Saldanha. Disponível em: <https://www.segurancalegal.com/wp-content/uploads/2017/09/T%C3%A9cnicas-de-Seguran%C3%A7a-da-Informa%C3%A7%C3%A3o-da-Teoria-%C3%A0-Pr%C3%A1tica.pdf>. Acesso em: 12 Set 2021.