ACADEMIA MILITAR DAS AGULHAS NEGRAS
ACADEMIA REAL MILITAR (1811) CURSO DE CIÊNCIAS MILITARES

Victor Hugo Diniz Taka

MEDIDAS DE PROTEÇÃO E SEGURANÇA FÍSICA NO CENTRO DE COMUNICAÇÕES

Resende
2023

TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA PROFISSIONAL

TÍTULO DO TRABALHO: MEDIDAS DE PROTEÇÃO E SEGURANÇA FÍSICA NO CENTRO DE COMUNICAÇÕES
AUTOR: VICTOR HUGO DINIZ TAKA

Este trabalho, nos termos da legislação que resguarda os direitos autorais, é considerado de minha propriedade.

Autorizo a Academia Militar das Agulhas Negras (AMAN) a utilizar meu trabalho para uso específico no aperfeiçoamento e evolução da Força Terrestre, bem como a divulgá-lo por publicação em periódico da Instituição ou outro veículo de comunicação do Exército.

A AMAN poderá fornecer cópia do trabalho mediante ressarcimento das despesas de postagem e reprodução. Caso seja de natureza sigilosa, a cópia somente será fornecida se o pedido for encaminhado por meio de uma organização militar, fazendo-se a necessária anotação do destino no Livro de Registro existente na Biblioteca.

É permitida a transcrição parcial de trechos do trabalho para comentários e citações desde que sejam transcritos os dados bibliográficos dos mesmos, de acordo com a legislação sobre direitos autorais.

A divulgação do trabalho, em outros meios não pertencentes ao Exército, somente pode ser feita com a autorização do autor ou do Diretor de Ensino da AMAN.

Resende, 11 de agosto de 2023

Cad Victor Hugo Diniz **Taka**

Dados internacionais de catalogação na fonte

T136m TAKA, Victor Hugo Diniz

Medidas de proteção e segurança física no centro de Comunicações / Victor Hugo Diniz Taka – Resende; 2023. 38 p. : il. color. ; 30 cm.

Orientador: Renan Viana Rocha

TCC (Graduação em Ciências Militares) - Academia Militar das Agulhas Negras, Resende, 2023.

1. Segurança. 2. Segurança Física. 3. Comunicações. 4. Centro de Comunicações. I. Título.

CDD**:** 355

Ficha catalográfica elaborada por Aline Viegas da Costa CRB-7/7409

Victor Hugo Diniz Taka

MEDIDAS DE PROTEÇÃO E SEGURANÇA FÍSICA NO CENTRO DE COMUNICAÇÕES

Monografia apresentado ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares** sob Orientação do 1º Tenente COM Renan Viana Rocha.

Orientador: 1º Ten COM Renan Viana Rocha

Resende
2023

Victor Hugo Diniz Taka

MEDIDAS DE PROTEÇÃO E SEGURANÇA FÍSICA NO CENTRO DE COMUNICAÇÕES

Monografia apresentado ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares** sob Orientação do 1º Tenente COM Renan Viana Rocha.

Aprovado em 19 de JUNHO de 2023

Banca examinadora:

Renan Viana Rocha, 1º Ten
(Presidente/Orientador)

Luiz Guilherme Ramos Vilas Boas, 1º Ten

Erickson Felippe de Azeredo Pereira, 1º Ten

Resende
2023

Dedico este trabalho primeiramente a Deus, que me guiou e protegeu ao longo destes 6 anos, me dando saúde e perseverança para vencer os desafios que me foram apresentados; e a minha família, pelos seus sacrifícios que possibilitaram eu estar aqui.

AGRADECIMENTOS

Agradeço a todos, que ao longo destes seis longos anos, permitiram tornar esta jornada mais leve, seja através de uma mão amiga, oferendo ajuda nos momentos difíceis; seja através da liderança, do exemplo, nutrindo e reforçando o meu ideal.

Agradeço minha namorada, Maria, por estar do meu lado, suportando a distância e a rotina da academia, e fazendo o possível para estar sempre presente.

Agradeço a equipe da 1ª Cia da EsPCEx de 2019, Maj Mariotoni, Maj Pires, Sub Barros, Sub Campos, Sgt Bessa e Sgt Gislaine; que me acolheram num momento difícil, me dando diversos ensinamentos e orientações, tanto na parte militar, tanto na parte pessoal, que levei para a AMAN e levarei para toda a vida.

Agradeço aos instrutores e monitores que encontrei ao longo da caminhada, os quais passaram seus conhecimentos visando contribuir na minha formação.

Agradeço aos amigos que fiz, os quais passamos por tantos obstáculos juntos, sempre buscando ajudar um ao outro para tornar este fardo mais leve.

Fé na missão pois ela é nobre!

RESUMO

MEDIDAS DE PROTEÇÃO E SEGURANÇA FÍSICA NO CENTRO DE COMUNICAÇÕES

AUTOR: Victor Hugo Diniz Taka
ORIENTADOR: Renan Viana Rocha

O uso de meios de comunicações no campo de batalha e em operações militares é amplamente utilizado, pois garantem a ligação entre as frações, permitindo o comando e controle pelo escalão superior. Para alcançar e garantir o funcionamento correto e ininterrupto das comunicações, é desdobrado um Centro de Comunicações, responsável por gerenciar as comunicações e serviços da operação. Por concentrar o tráfego de dados e informações, ele se torna um alvo de interesse de tropas inimigas, seja para negar as comunicações através de ataques que visem causar danos, seja para interceptar informações de interesse militar. Para se proteger de tais ataques, deve-se garantir, além da segurança da exploração, a segurança criptográfica e física, sendo essa última o enfoque deste trabalho, tendo em vista o estado de desatualização em que se encontra seu manual. Este trabalho destina-se analisar as normas em vigor no Exército Brasileiro e em outras instituições, buscando reunir procedimentos e medidas que possam ser utilizados no Centro de Comunicações e propor uma atualização do manual.

Palavras-Chave: Segurança, Segurança Física, Comunicações, Centro de Comunicações.

ABSTRACT

PROTECTION AND PHISICAL SECURITY POLICIES IN THE COMUNICATION CENTER

AUTHOR: Victor Hugo Diniz Taka
ADVISOR: Renan Viana Rocha

The use of communication means in the battlefield and military operations is widely employed as it ensures the connection between units, enabling command and control by the general staff. To achieve and guarantee the correct and uninterrupted functioning of communications, a Communications Center is deployed, responsible for managing the operation's communications and services. By concentrating data and information traffic, it becomes a target of interest for enemy troops, either to disrupt communications through attacks aimed at causing damage or to intercept information of military interest. To protect against such attacks, it is necessary to ensure not only exploitation security but also cryptographic and physical security, with the latter being the focus of this work, considering the outdated state of Brazilian Army manual. This work aims to analyze the rules in force in the Brazilian Army and in other institutions, seeking to gather procedures and measures that can be used in the Communications Center and propose an update of the manual.

Keywords: Security, Phisical Security, Comunication Center, Signals Corps

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

No cenário atual os conflitos não se restringem somente na linha de frente do campo de batalha através do poder de fogo maciço, como também no espaço aéreo, naval. Contudo, estas linhas de frente não são mais as únicas dimensões a serem consideradas durante uma batalha, haja vista a implementação do meio virtual. Logo, o meio virtual que se traduz na dimensão informacional é uma das três dimensões que compõem o ambiente operacional, ao lado da dimensão humana e dimensão física (BRASIL, 2019).

Com a grande evolução dos meios de comunicações no último século, bem como por meio do advento e da popularização dos dispositivos eletrônicos, além do barateamento do desenvolvimento de satélites (BRAGANÇA, 2009) tornou-se possível a incorporação da comunicação em tempo real e a longa distâncias por populares, não se restringindo somente através de grandes estruturas, como as detidas pelas emissoras de rádios e televisão. Pela primeira vez, era possível e acessível enviar grande quantidade de dados de forma rápida e eficaz.

Tais avanços tecnológicos foram logo observados pelas forças armadas, que viram grande ganho de poder para as tropas que possuíssem em sua organização meios eficazes e seguros de comunicação entre os escalões, sendo elencada como fator de destacada relevância na doutrina atual do Exército Brasileiro:

> "A dimensão informacional abrange os sistemas utilizados para obter, produzir, difundir e atuar sobre a informação. Reveste-se de destacada relevância em função dos avanços na área de Tecnologia da Informação e Comunicação (TIC), que proporcionaram elevada capacidade de transmissão, acesso e compartilhamento da informação" (BRASIL, 2019)

Tais informações auxiliam não somente o fluxo de mensagens em pequenas frações, mas também da tomada de todos os processos decisórios dos mais altos escalões, permitindo que o Comando tenha o máximo de dados possíveis para auxiliar suas tomadas de decisões. Todavia, para que isso ocorra, é necessário que a comunicação seja segura e eficiente, objetivando seu pleno funcionamento:

> "A superioridade de informações é traduzida por uma vantagem operativa derivada da habilidade de coletar, processar, disseminar, explorar e proteger um fluxo ininterrupto de informações em todos os níveis, ao mesmo tempo em que se busca tirar proveito das informações do oponente e/ou negar-lhe essas habilidades." (BRASIL, 2019)

Para melhor gerir o trânsito das informações no Exército Brasileiro, é utilizado um Centro de Comunicações (C Com) responsável pela transmissão de imagens de voz, texto,

vídeo e dados, aos escalões superiores, bem como enviar as ordens aos elementos subordinados. Tal instalação possui grande valor estratégico, visto que “o ataque com várias armas em diversos pontos requer planejamento que deve ser comunicado aos interessados” (BRASIL, 1978). Sabendo que o planejamento é essencial, por ser ponto de difusão para as tropas no terreno o C Com, é de grande interesse do inimigo impedir o correto funcionamento das comunicações, bem como interceptar tais mensagens para antever às açõesa serem realizadas. Cresce, portanto, a importância da segurança das comunicações, para que não somente ocorra o fluxo de mensagens, como também a garantia de sua privacidade,garantindo que não seja comprometida a informação em nenhum momento, desde sua emissão até recebimento e armazenamento.

Entretanto, devido ao avanço tecnológico nos meios de comunicações, diversas novas ameaças foram criadas. Somente em 2021, de acordo com pesquisas de agências especializadas o Brasil, sofreu 9.7 milhões de ataques cibernéticos, estando em primeiro lugar sistemas de comunicação sem fio, e em terceiro sistema de armazenamento e processamento de dados (NETSCOUT, 2021).

No primeiro capítulo, “Documentações em vigor no Exército Brasileiro”, é analisado os manuais e documentos que tangem o tema de segurança física relacionado às comunicações, bem como as medidas neles descritas. Adiante, no capítulo “Documentações externas ao Exército Brasileiro”, a análise se concentra em dois documentos, sendo a primeira uma Norma Técnica Brasileira (NBR) e o segundo diretrizes do governo do Estados Unidos da América. Por fim, na conclusão, é feita a comparação entre ambos os tipos de documentações e avaliado a necessidade de atualização dos manuais vigentes.

Portanto, a pesquisa busca analisar as práticas de segurança e proteção física adotadas atualmente pelo Exército Brasileiro, e comparar com outras normas adotadas atualmente, levantando correções, melhorias e boas práticas que podem ser incorporadas à uma futura atualização dos atuais manuais, garantindo que sejam de melhor forma aplicadas às especificações da doutrina militar corrente.

1.1 OBJETIVOS

1.1.1 Objetivo geral

Analisar como a doutrina de proteção e segurança física do Centro de Comunicações pode ser atualizada para atender as necessidades do combate moderno.

1.1.2 Objetivos específicos

a) Analisar os manuais atuais em uso pelo Exército Brasileiro referente ao tema, C-24-17, C-24-50 e EB10-IG-01.011, e identificar práticas obsoletas e/ou incorretas;
b) Analisar a "NBR 17799: Tecnologia da informação - Código de prática para a gestão da segurança da informação" e *"Public Switched Network Security Assessment Guidelines",* observando medidas e boas práticas que podem ser adotadas;
c) Fundamentar a necessidade de atualização dos procedimentos de segurança física, mostrando como tal ação daria maior segurança as comunicações em operações militares e padronizaria os procedimentos de segurança física dos C Com no âmbito Exército Brasileiro.

2 REFERENCIAL TEÓRICO

2.1 DIMENSÃO INFORMACIONAL

A Dimensão Informacional consiste numa das 3 dimensões do ambiente operacional, que podem ser definidas como *"*conjunto de condições e circunstâncias que afetam o espaço onde atuam as forças militares e que interferem na forma como estas são empregadas*"* (BRASIL,2019), os quais são divididas em Dimensão Física, Humana e Informacional.

Fig. 1 - As dimensões do ambiente operacional terrestre.

Fonte: Brasil (2019)

Cabe a Dimensão Informacional obter, produzir, difundir e atuar sobre a informação, tal essa que é imprescindível para garantir a consciência situacional dos comandantes,

funcionamento correto de toda logística e serviços, e atuar como fator decisório para a tomada de decisões.

> "A superioridade de informações é traduzida por uma vantagem operativa derivada da habilidade de coletar, processar, disseminar, explorar e proteger um fluxo ininterrupto de informações em todos os níveis, ao mesmo tempo em que se busca tirar proveito das informações do oponente e/ou negar-lhe essas habilidades." (BRASIL, 2019)

O controle desta dimensão garante o funcionamento correto de toda a tropa, bem como a rápida coordenação e movimentação desta, através do fluxo ininterrupto de mensagens seguras, as quais o inimigo não terá acesso.

2.2 CENTRO DE COMUNICAÇÕES

O Centro de Comunicações (C Com) é uma instalação básica necessária para o emprego das comunicações em operações militares, tendo como definição:

> "O conjunto dos diferentes órgãos incumbidos da recepção, transmissão, criptografia, decriptografia e controle das mensagens, servindo a um comando ou a um escalão de comando[...]. O C Com é responsável pelo recebimento, manuseio, salvaguarda, criptografia, decriptografia, transmissão e entrega de mensagens oficiais" (BRASIL, 2001)

A responsabilidade da instalação das estruturas físicas é atribuída ao Grupo de Comando da Companhia de Comando e Apoio, o qual é responsável pela montagem da infraestrutura necessária para a disposição dos equipamentos utilizados no C Com (BRASIL, 2003).

Para melhor organização e divisão de tarefas, ele é dividido em Centro de Mensagens, Centro de Mensageiros, Centro de Transmissão e Recepção e Centro de Controle de Sistemas. Essa divisão permite o correto tratamento da mensagem, garantindo que o tempo entre o recebimento e a destinação dela seja o menor possível, garantindo que a mesma seja entregue em tempo oportuno a seu destinatário.

Nas últimas décadas, tem sido cada vez utilizado os meios informatizados nas atribuições do C Com, garantindo a ele novas possibilidades e recursos, como telefonia IP, videoconferência, e-mail, criptografia digital e aplicações da internet. Entretanto, isso se torna uma "via de mão dupla", abrindo novas frentes para ataques inimigos.

,

2.3 SEGURANÇA DAS COMUNICAÇÕES

A segurança das comunicações, segundo o Manual C-24-50 Segurança das Comunicações, é a garantia que a mensagem não será comprometida, echegará ao seu destino sem sofrer danos ou interceptações, de modo que somente pessoas autorizadas tenham acesso a ela. Tal segurança deve ser obtida de forma ativa, buscando medidas para ampliá-la

(BRASIL, 1978).

A segurança das comunicações é dividida em 3 subcategorias: segurança física, segurança da exploração e segurança criptográfica. A primeira aborda a segurança dos meios físicos e documentos, para que não caia em mãos inimigas, regulando o acesso a tais dados e realizando planos de destruição.

A segurança da exploração é focada em medidas para impedir a interceptação de mensagens pelo ar ou pelo fio, e boas práticas para reduzir tais riscos; e por último a segurança criptográfica aborda os processos de codificação e decodificação das mensagens.

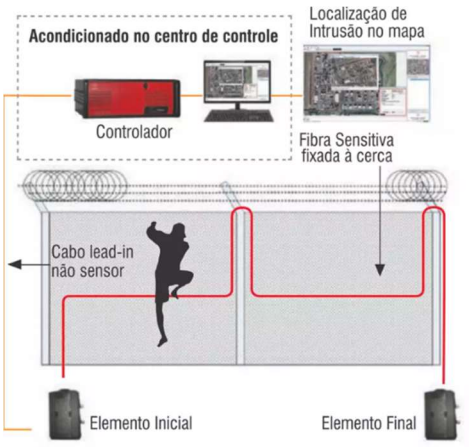
Apesar de sua grande importância, a segurança não pode comprometer a rapidez das mensagens, portanto *"*o mais alto grau de segurança a atingir depende de um equilíbrio perfeito entre a segurança e a rapidez necessária*"* (BRASIL, 1978), visto que as mensagens devem ser entregues em tempo oportuno para que as informações nela contidas não percam a validade.

2.4 SISTEMA DE DETECÇÃO DE INTRUSÃO

O Sistema de Detecção de Intrusão é constituído por um sensor de intrusão e um sistema de notificação, e tem como objetivo aumentar a segurança de uma área através da detecção de invasões ao ambiente o qual está instalado.

Seu funcionamento pode ocorrer ao detectar o movimento de indivíduos em um ambiente, ou detectando a abertura ao arrombamento de porta, janelas, muros e outros objetos de controle de acesso. Detectada a invasão, é acionado um sistema de notificação, que pode ocorrer o acionamento de um alarme sonoro, envio de mensagem à central de monitoramento (INTELBRAS, 2020), ou ainda, ambos.

Fig. 2 – Sistema de Detecção de Intrusão instalado em uma cerca.



Fonte: Terra (2017)

2.5 DISPOSITIVOS DE SEGURANÇA

Dispositivos de segurança são todos aqueles que através de tecnologia ou método específico, asseguram uma medida de proteção a mais a um sistema de segurança

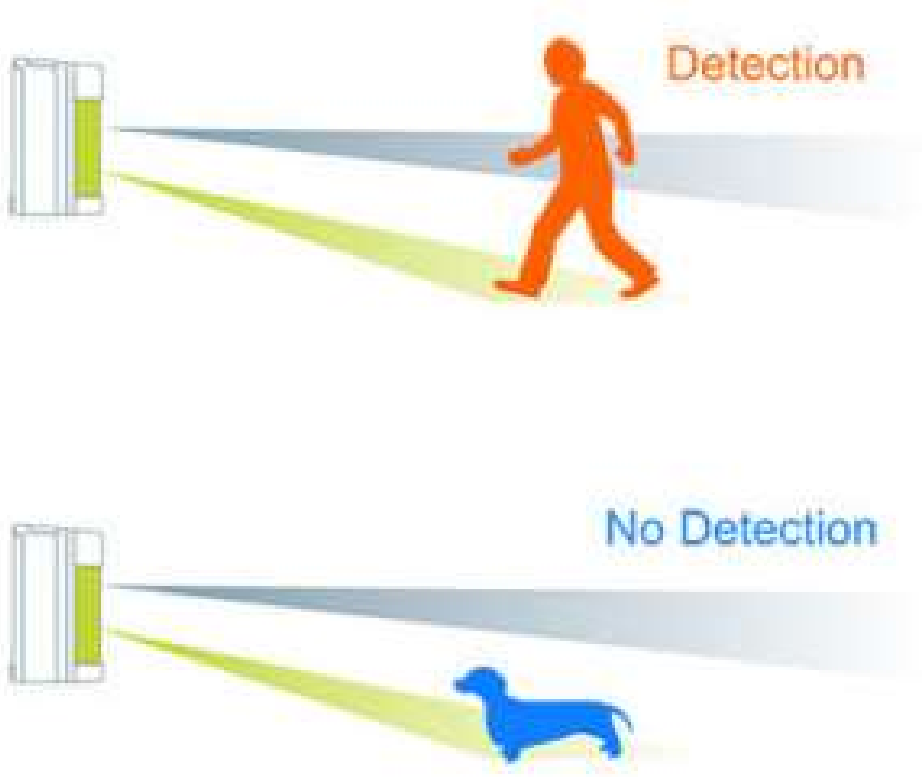
2.5.1 SENSOR INFRAVERMELHO

Os sensores infravermelhos funcionam através da utilização do espectro de luz infravermelha, invisível ao olho, e pode ser empregado de forma ativa ou passiva, na deteção de intrusões (INTELBRAS, 2022).

Em seu modo passivo, realiza a detecção através da variação de calor gerada pelo deslocamento de um corpo, podendo ter sensibilidade variada, para detectar qualquer movimentação ou ignorar corpos pequenos, como de animais de pequeno porte, evitando que seja acionado desnecessariamente (MOBEYSTORE, 2023).

O seu modo ativo, por sua vez, ocorre com a instalação de um emissor e receptor de feixe infravermelho, criando uma barreira no ambiente, e devido ao fato de ser invisível ao olho humano, age como uma cerca virtual (INTELBRAS, 2022), que, ao ser atravessada por um corpo, o feixe de luz deixa de chegar no receptor, e é detectada a invasão.

Fig. 3 – Distinção de animais de pequeno porte.



Fonte: Mobeye Store (2023)

2.5.2 SENSOR MAGNÉTICO

Os sensores magnéticos funcionam através da utilização do campo magnético de imãs e de contato elétrico, que, ao serem separados, aciona o sistema de detecção de intrusão (INTELBRAS, 2022). Sua instalação ocorre em portas, janelas, armários e demais objetos que possam ser abertos, onde são instalados os contatos e imãs. Seu funcionamento pode ser por fio, que envia um sinal elétrico informando a invasão, ou sem fio, onde é enviado um sinal de radiofrequência.

Fig. 4 – Sensor magnético em porta.

. Fonte: Swann.

2.5.3 SENSOR DE VIBRAÇÃO

Os sensores de vibração funcionam através de um captador de vibração, que pode ou não ser ajustável, tornando-o mais ou menos tolerável a vibrações, que detecta tentativas de invasão através de alguma barreira física, acionando ao detectar golpes, tentativas de arrombamentos, tentativas de perfuração, quebra de vidros, uso de explosivos e qualquer outra atividade que gere impacto (MARCONDES, 2016).

Fig. 5 – Sensor de vibração ajustável.

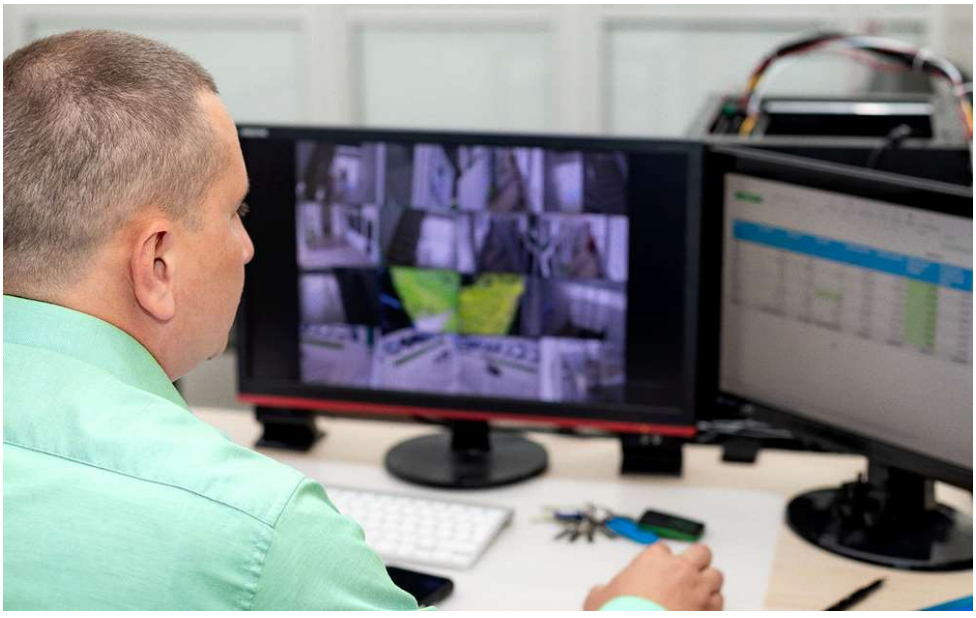
Fonte: Blog Gestão de Segurança Privada

Sua principal característica é permitir a deteção antes que a invasão ocorra, ainda na sua tentativa pelo indivíduo, ao detectar impactos gerados no sistema de barreira físicos da instalação.

2.5.4 CIRCUITO FECHADO DE TELEVISÃO (CFTV)

O Circuito Fechado de Televisão é um sistema de monitoramento por câmeras de um determinado perímetro, que captura as imagens e as envia para uma central, onde são gravadas e transmitidas (INTELBRAS, 2023).

Fig. 6 – Central de monitoramento.



Fonte: Intelbras, 2023

Seu uso permite o monitoramento do perímetro em tempo real e à distância, bem como registro de gravação de imagens (INTELBRAS, 2023), possibilitando a análise posterior de fatos ocorridos, essenciais para esclarecer situações que ocorreram em determinado local.

2.5.5 EXTINTOR DE INCÊNDIO

Extintor de Incêndio são equipamentos móveis, de acionamento manual, portátil ou sobre rodas, destinado a combater princípios de incêndio" (CBMES, 2020). Possuem em seu interior, um agente extintor, que tem por finalidade intervir na combustão, agindo visando diminuir, controlar e extinguir o fogo.

Fig. 7 –Demonstração do uso do extintor de incêndio -

Fonte: 1º Centro de Geoinformação, 2022.

São classificados em sua eficácia em 4 classes de fogos, A, B, C e D, sendo respectivamente fogos oriundos de combustível sólido (madeira, plástico, papeis, tecidos, etc), líquidos e gases inflamáveis (gasolina, álcool, GNV), instalações elétricas, e metais (magnésio, sódio, potássio, etc), (CBMES – 2020) podendo um mesmo extintor ser apto a combater mais de uma classe.

Seu uso de destaca na resposta imediata à visualização de focos de incêndio, permitindo ao individuo prover pronta resposta de combate, e para isso, devem estar próximos a locais com risco de incêndio, em locais de fácil acesso, sinalizados e desobstruídos.

2.5.6 SPRINKLER

Sprinklers são dispositivos de combate a incêndio, constituídos de chuveiros

automáticos distribuídos em uma área, conectados a um sistema hidráulico, que são acionados em caso de princípio de fogo (ABNT, 2020).

Seu funcionamento ocorre através de um dispositivo detector, sendo o mais utilizado o bulbo de vidro, que ao atingir determinada temperatura, se rompe e libera a passagem de água pela tubulação, combatendo o incêndio (MI FIRE, 2021).

Fig. 8 – Rompimento do bulbo e vazão da água -

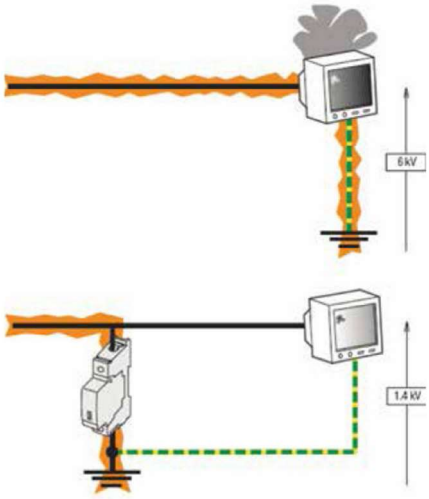
Fonte: Mi Fire, 2021.

Sua principal característica é o acionamento automático (SKOP, 2021) e analógico do sistema, independente de ação humana e energia elétrica, garantindo sua confiabilidade e funcionamento.

2.5.7 DISPOSITIVO DE PROTEÇÃO CONTRA SURTOS (DPS)

Os Dispositivos de Proteção contra Surtos (DPS) são equipamentos cuja finalidade é “detectar a presença de sobretensões transitórias e neutralizá-las por meio do aterramento, antes de danificarem qualquer dispositivo” (INTELBRAS, 2022).

Fig. 9 – Proteção realizada pelo DPS -



Fonte: Valeman, (2020)

Seu funcionamento varia de acordo com o modelo, sendo os principais através de fusível ou chave inteligente, ambos associados a um varistor, que possuí função de absorver os picos de energia, protegendo os equipamentos conectados ao DPS. Nos dispositivos com fusível, em caso de sobrecarga, ele é rompido, protegendo o circuito, e, devendo ser trocado posteriormente (INTELBRAS, 2022). Os dispositivos de chave inteligente, por sua vez, em caso de sobrecarga desarmam, interrompendo o circuito, e, resolvido o problema, basta religá-lo, permitindo assim maior vida útil do DPS.

2.5.8 FONTE DE ENERGIA ININTERRUPTA (UPS)

As Fontes de Energia Ininterrupta (Uninterruptible Power Supply – UPS), popularmente chamadas de *Nobreak* são dispositivos projetados e dimensionados para permitir o funcionamento de equipamentos elétricos em situações de ausência ou instabilidade de energia elétrica devido à alguma pane na rede elétrica (INTELBRAS, 2020).

Possuem em seu conjunto, baterias para suprir a demanda elétrica no caso de queda de energia ou instabilidade da rede, na qual é acionado através de um DPS, que ativa as baterias, protegendo assim, os equipamentos eletrônicos a ele conectados.

Fig. 10 – Capacidades de um UPS.

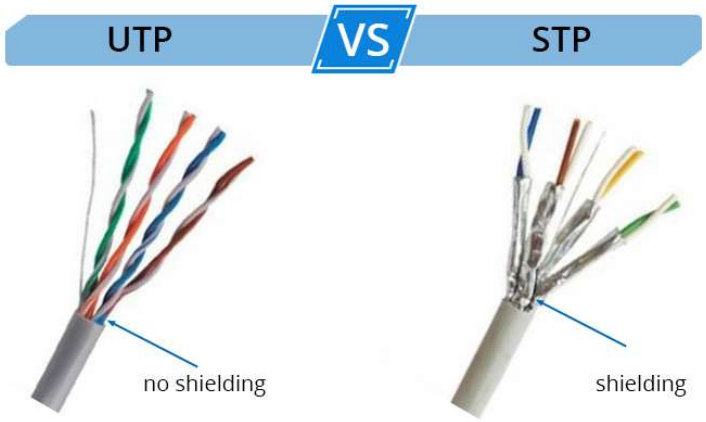
Fonte: Intelbras, (2020)

2.5.9 CABO DE PAR TRANÇADO

Os Cabos de Par Trançado são um tipo de cabeamento utilizado em arquiteturas de rede, para transmissão de dados em distâncias de até 100 metros, com a velocidade entre 100Mbps e 1000Mbps. Sua principal característica é ser constituído de 4 pares de fios de cobres, trançados entre si, de modo a cancelar o campo magnético gerado pela energia que é transmitida (CISCO, 2003).

Os principais tipos utilizados em sistemas de redes são os Cabos de Par Trançado Não Blindados (Unshielded Twisted Pair - UTP) e os Cabos de Par Trançado Blindados (Shielded Twisted Pair – STP). Os cabos UTP são cobertos por uma capa plástica simples, que oferece apenas proteção física ao cabeamento interno, e os cabos STP possuem em cada par uma cobertura metálica, que protege os sinais de campos magnéticos externos (CISCO, 2003), tais como cabos de energia e outros dispositivos que gerem campo eletromagnético.

Fig. 11 – Interior de um cabo de par trançado blindado e não blindado.



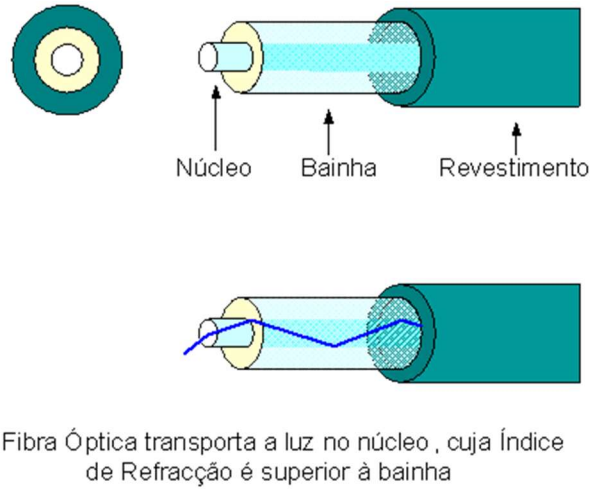
Fonte: QSFPTEK, (2021)

2.5.10 CABO DE FIBRA ÓPTICA

Os Cabos de Fibra Óptica são um tipo de cabeamento para transmissão de dados, que, ao invés de sinais elétricos, utiliza pulsos de luz para transmitir, tornando-o assim, imune a interferências eletromagnéticas (CISCO, 2005).

Sua estrutura é constituída de um núcleo, com fator N1 de refração, e um revestimento, com fator N2 de refração (CISCO, 2005). Tal diferença, permite, ao sinal luminoso ir refletindo ao longo do núcleo da fibra óptica, percorrendo grandes distâncias em um curtíssimo espaço de tempo, garantindo velocidades de transmissão de dados de até 40Gbps, e podendo alcançar distâncias de até 100Km (CISCO, 2005).

Fig. 12 – Interior de um cabo de fibra óptica.



Fonte: QUORA, (2021)

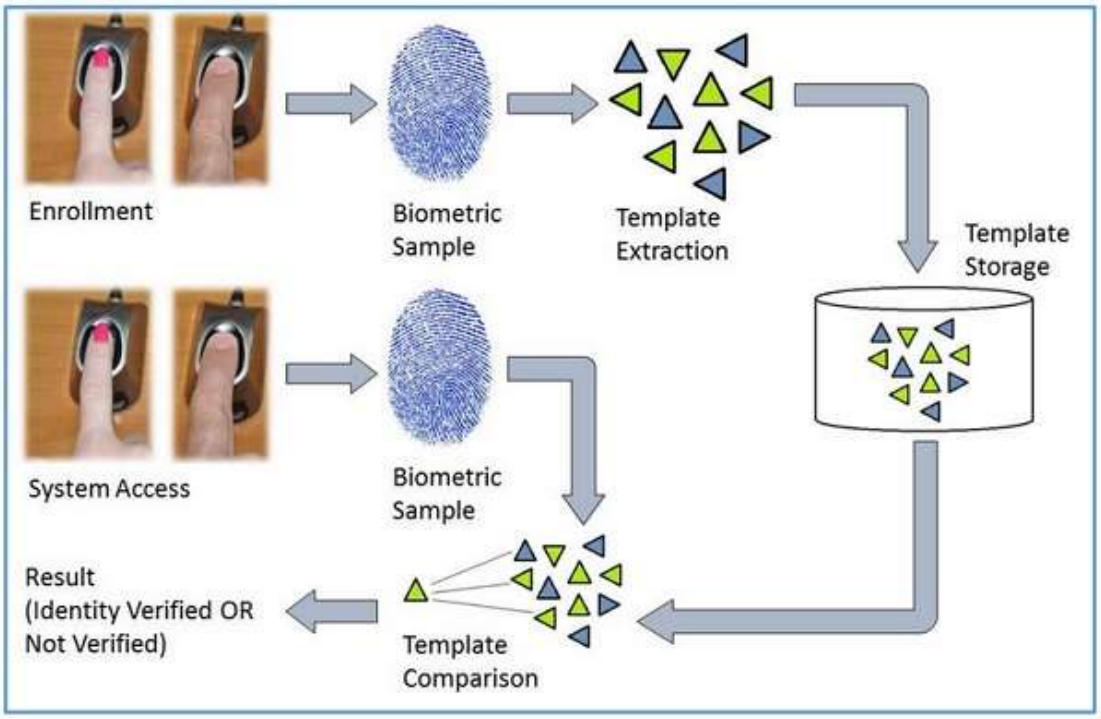
2.5.11 BIOMETRIA

Biometria é a medição e análise de características corporais humanas (KASPERSKY,

2023), tais como impressões digitais, íris, retina, rosto, veias, voz, entre outros. Tais dados tem seu principal uso em sistemas de identificação de indivíduos, devido a confiabilidade e instransferidade do objeto de verificação utilizado.

Seu funcionamento ocorre por 3 fases, registro, armazenamento e comparação (QAMAR, MUSTAFA, 2017). Num primeiro momento, é feito o registro do usuário, capturando uma característica pré-definida do usuário. Após isso, é feito o armazenamento em um sistema atrelando determinado indivíduo a característica que acabara de ser registrada. Por fim, toda vez que for solicitada a autenticação por biometria, o indivíduo irá utilizar um leitor que irá verificar determinada característica com a que o sistema possui em seus bancos de dados, comparando se quem realizou a requisição é o mesmo usuário que está cadastrado.

Fig. 13 – Fluxograma do processo de registro, armazenamento e comparação de identificação biométrica digital.

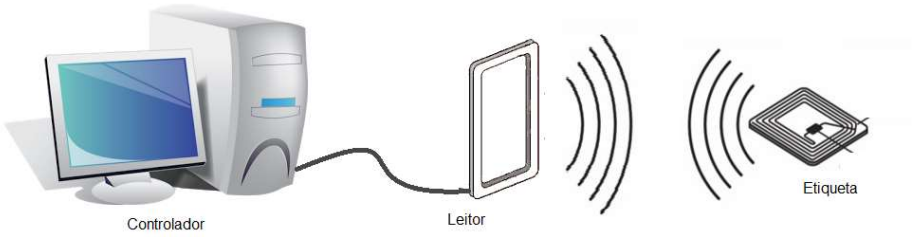


Fonte: Tutorials Point.

2.5.12 RFID

Identificação por Radiofrequência, do inglês Radio Frequency Identification (RFID), são sistemas inteligentes no qual é feita a comunicação entre um dispositivo transmissor e um leitor, através de ondas de rádio (COUTO; MALAFAIA, 2019).

Fig. 14 – Esquematização do sistema RFID -



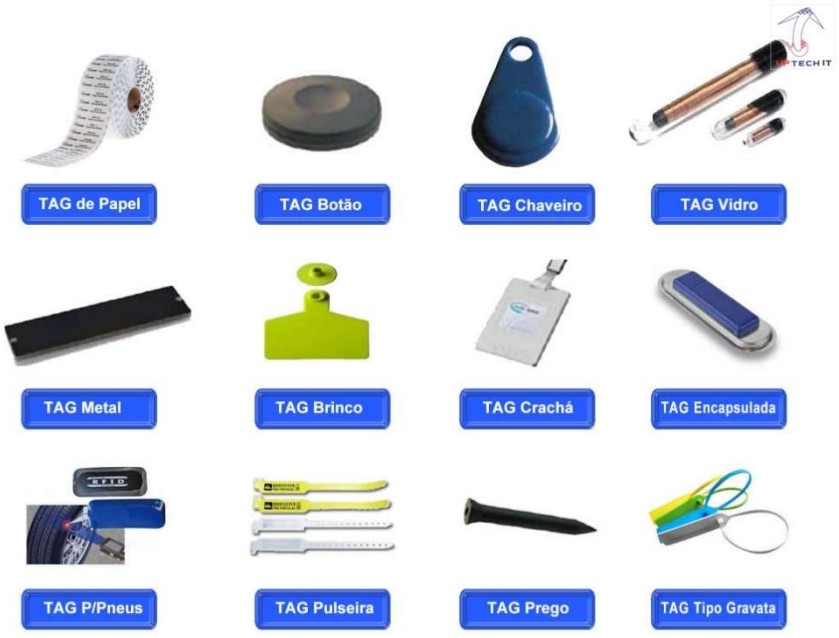
Fonte: UFRJ, (2015)

Nesta comunicação, o dispositivo transmissor, também chamado de transponder, possui armazenado em seu interior dados, tais como número de série, nome do usuário, validade do acesso, etc; que, ao entrar no campo eletromagnético do leitor, também chamado de transceptor, decodifica os dados e os envia para um computador, no qual é feito o seu processamento (SANTANA, 2005).

Realizado este processo, o sistema irá concluir a identificação, e a partir dela, será desencadeado ações pré-definidas, seja a abertura ou não de portas, acesso a terminais eletrônicos como computadores, autorização de pagamentos, etc.

O transponder pode se apresentar na forma de cartões, crachás, chaveiros, etiquetas, etc, devido ao seu tamanho reduzido, garantindo portabilidade e versatilidade (COUTO; MALAFAIA, 2019).

Fig. 15 – Exemplos de transponder RFID

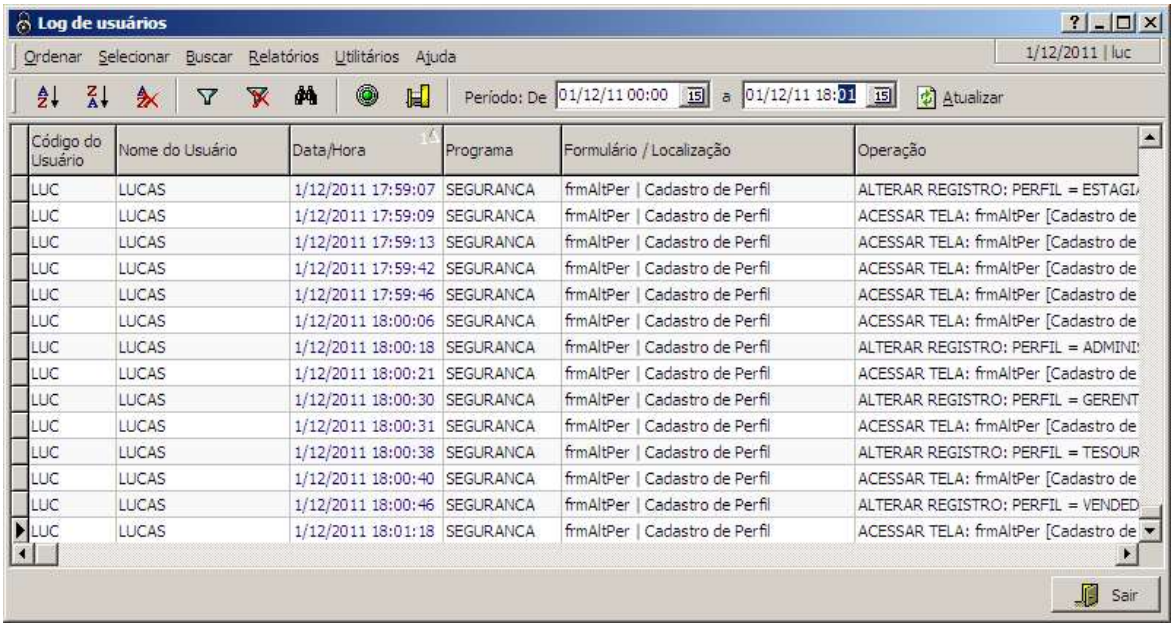


Fonte: UFRJ, (2019)

2.5.13 LOG

Log é um registro escrito de eventos com data e hora, que ocorre de forma ininterrupta (OLIVEIRA, 2021), podendo ocorrer de forma digital, através de softwares, ou analógica, em um livro de registros. Sua principal função é servir de ferramenta para o apuramento de falhas e invasões, entretanto também pode ser utilizado para registro de acesso de usuário, modificações realizadas em sistemas, e análise de atividade suspeita.

Fig. 16 – Log de acesso digital.



Código do Usuário	Nome do Usuário	Data/Hora	Programa	Formulário / Localização	Operação
LUC	LUCAS	1/12/2011 17:59:07	SEGURANCA	frmAltPer | Cadastro de Perfil	ALTERAR REGISTRO: PERFIL = ESTAGI
LUC	LUCAS	1/12/2011 17:59:09	SEGURANCA	frmAltPer | Cadastro de Perfil	ACESSAR TELA: frmAltPer [Cadastro de
LUC	LUCAS	1/12/2011 17:59:13	SEGURANCA	frmAltPer | Cadastro de Perfil	ACESSAR TELA: frmAltPer [Cadastro de
LUC	LUCAS	1/12/2011 17:59:42	SEGURANCA	frmAltPer | Cadastro de Perfil	ACESSAR TELA: frmAltPer [Cadastro de
LUC	LUCAS	1/12/2011 17:59:46	SEGURANCA	frmAltPer | Cadastro de Perfil	ACESSAR TELA: frmAltPer [Cadastro de
LUC	LUCAS	1/12/2011 18:00:06	SEGURANCA	frmAltPer | Cadastro de Perfil	ACESSAR TELA: frmAltPer [Cadastro de
LUC	LUCAS	1/12/2011 18:00:18	SEGURANCA	frmAltPer | Cadastro de Perfil	ALTERAR REGISTRO: PERFIL = ADMINI
LUC	LUCAS	1/12/2011 18:00:21	SEGURANCA	frmAltPer | Cadastro de Perfil	ACESSAR TELA: frmAltPer [Cadastro de
LUC	LUCAS	1/12/2011 18:00:30	SEGURANCA	frmAltPer | Cadastro de Perfil	ALTERAR REGISTRO: PERFIL = GERENT
LUC	LUCAS	1/12/2011 18:00:31	SEGURANCA	frmAltPer | Cadastro de Perfil	ACESSAR TELA: frmAltPer [Cadastro de
LUC	LUCAS	1/12/2011 18:00:38	SEGURANCA	frmAltPer | Cadastro de Perfil	ALTERAR REGISTRO: PERFIL = TESOUR
LUC	LUCAS	1/12/2011 18:00:40	SEGURANCA	frmAltPer | Cadastro de Perfil	ACESSAR TELA: frmAltPer [Cadastro de
LUC	LUCAS	1/12/2011 18:00:46	SEGURANCA	frmAltPer | Cadastro de Perfil	ALTERAR REGISTRO: PERFIL = VENDED
LUC	LUCAS	1/12/2011 18:01:18	SEGURANCA	frmAltPer | Cadastro de Perfil	ACESSAR TELA: frmAltPer [Cadastro de

Fonte: Thotau.

Devido a sensibilidade dos dados que possui, os logs não podem ser alterados, nem acessado por qualquer usuário, tendo seu acesso restrito (MACHADO, 2012). Também devem ser protegidos de destruição, através da existência de cópias e backups dos registros.

3 MATERIAIS E MÉTODOS

3.1 TIPO DE PESQUISA

A pesquisa tem método indutivo, com abordagem qualitativa, do tipo exploratório (MERRIAM, TISDEL, 2016), sendo um estudo secundário, haja vista que, por meio de revisão bibliográfica assistemática e análise dos manuais militares em uso e em publicações civis que abordam o tema de segurança das comunicações, bem como pela observação da estrutura de um C Com ao longo do último ano durante exercícios no terreno na Academia Militar das Agulhas Negras, conclui-se a necessidade de aprimoramento desse setor de segurança. Os dados

estudados se atêm somente a segurança física das comunicações.

Este estudo visa, portanto, responder se:

a) Há a necessidade de atualizar os manuais do Exército Brasileiro existentes no tocante a segurança física das comunicações?

b) Houve uma mudança tecnológica suficiente para atualizar as técnicas implementadas pelo Exército Brasileiro na segurança das comunicações?

3.2 MÉTODOS

3.2.1 Avaliação dos manuais atuais

Foi realizado o estudo dos manuais C-24-17 e C-24-50, reunindo os princípios de segurança das comunicações, com ênfase na segurança física, objetivando analisar as medidas ali presentes.

3.2.2 Avaliação de publicações civis

Foi feito uma pesquisa bibliográfica sobre medidas de segurança das comunicações, com ênfase na segurança física, que abordam os aspectos atuais das comunicações, buscando boas práticas que atendam as necessidades do C Com e do Exército Brasileiro.

3.2.3 Avaliação da aplicabilidade de medidas no C COM

Foi realizada um estudo exploratório, através da Teoria Fundamentada (STRAUSS, GLASER, 1999), observando o funcionamento do C Com nos exercícios de terreno realizados no ano de 2022 no Curso de Comunicações da Academia Militar das Agulhas Negras, focando nas medidas e boas práticas de segurança física realizadas pelos Cadetes e as encontradas nos manuais do Exército, hipotetizando a viabilidade da adoção de medidas já existentes em instituições externas. Também foi observado se tais medidas estão alinhadas com a doutrina militar corrente, e quais delas serão de maior eficácia e facilidade de emprego pela tropa.

4 ANÁLISE E DISCUSSÃO

4.1 DOCUMENTAÇÕES EM VIGOR NO EXÉRCITO BRASILEIRO

Atualmente, é utilizado pelo Exército Brasileiro para normatizar as medidas de segurança das comunicações o manual “C-24-50 SEGURANÇA DAS COMUNICAÇÕES”, publicado em 1978, o qual aborda noções básicas de segurança, segurança física, segurança da

exploração, segurança criptográfica e sistema de autenticação utilizado pelo Exército Brasileiro. A seção de segurança física, enfoque deste trabalho, ocupa, todavia, apenas pouco mais de 2 páginas deste manual.

No início do capítulo, somos apresentados de imediato à finalidade da segurança física nas comunicações:

> "A segurança do material compreende todas as medidas destinadas a impedir que o material de comunicações, o material criptográfico, as mensagens e todos os documentos sigilosos caíam intactos em poder do inimigo, ou sejam extraviados ou mesmo manuseados ou fotografados por pessoas inidôneas." (BRASIL, 1978)

Em seguida, é apresentado no subcapítulo "Medidas de Segurança", 4 medidas para serem adotadas, a primeira versa acerca da importância do recrutamento do pessoal a trabalhar com criptografia e documentos sigilosos, medida a qual se mantém atualizada e verdadeira.

Prosseguindo, é tratado que o material e documentos "devem ser guardados em locais que ofereçam a maior segurança possível" (BRASIL, 1978), contudo, não é especificado ou exemplificado nenhum procedimento para garantir a maior segurança possível, apenas que somente pessoas autorizadas podem ter acesso e o material em carga deve ser registrado em protocolo (Log).

A terceira medida trata acerca do uso mínimo de documentação sigilosa em postos avançados, e a quarta trata acerca da necessidade de um plano de destruição de material em cada Posto de Comando e Centro de Comunicações em caso de perigo imediato, ambos não relevantes para este trabalho por não tratar de segurança física, e sim de medidas de contrainteligência. Findo este subcapítulo, é abordado a classificação sigilosa dos documentos e se encerra o capítulo existente de segurança física do manual.

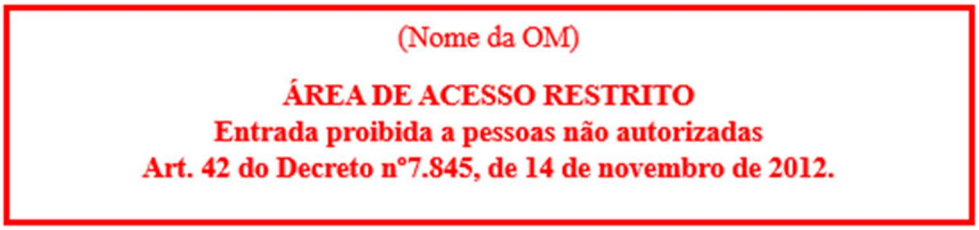
Abordando especificamente o C Com, existe o manual "C-24-17 CENTRO DE COMUNICAÇÕES", publicado em 2001, o qual aborda a elaboração e processamento de mensagens físicas e por meio eletrônico, a organização, planejamento e funcionamento de um C Com, e as atribuições relativas aos elementos que o compõe. Ao contrário do manual anterior, o qual possuía uma seção dedicada à segurança física, o C-24-17 apenas cita em alguns trechos deveres que são atribuídos ao C Com relativo à segurança, sem especificar novamente, nenhuma medida que deve ser empregada.

No primeiro capítulo, o qual aborda as generalidades do C Com, é informado que é responsabilidade do C Com fiscalizar "aspectos relativos à adequada [...]segurança e outros fatores ligados ao fluxo de informações pelos meios de comunicações" (BRASIL, 2001). No terceiro capítulo, o qual aborda as atribuições do C Com, é reforçado a responsabilidade da segurança, "O C Com é responsável pela coordenação e emprego dos meios de comunicações

e pela sua segurança" (BRASIL, 2001). Logo, fica claro que cabe ao C Com realizar e fiscalizar a sua segurança, incluindo a segurança física das comunicações.

Prosseguindo, é abordado no subcapítulo Planejamento, o qual enumera aspectos que devem ser observados no planejamento de um C Com, fatores de planejamento, o qual, para este estudo, se destaca a "necessidades relativas à segurança das comunicações" (BRASIL, 2001) e a "proteção adequada para o equipamento de comunicações classificado como sigiloso" (BRASIL, 2001). Entretanto, novamente não é informado quais ações devem ou podem ser tomadas, tampouco o que seria uma proteção adequada, tornando as medidas de segurança a serem adotadas subjetivas ao Oficial responsável, cabendo a ele tecer um julgamento se a proteção existente é adequada ou não.

Um terceiro documento, o "EB10-IG-01.011 Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (IGSAS)", publicado em 2014, que apesar de não tratar diretamente do Comunicações, tampouco do Centro de Comunicações, aborda aspectos que devem ser adotados no C Com, tendo em vista que o mesmo trata do manuseio de documentação sigilosa, atividade recorrente em um C Com.



No capítulo 3, é conceituado uma área de acesso restrito como "área ou instalação que contenha documento classificado ou sob restrição de acesso ou material que, por sua utilização ou finalidade, demandar proteção" (BRASIL, 2014), e que tais áreas devem possuir sinalização conforme modelo (Fig. 16) indicando que o seu acesso é restrito a pessoas autorizadas, de modo a alertar indivíduos desatentos adentrem no recinto.

Fig. 17 – Modelo de placa de sinalização de área de acesso restrito.
Fonte: BRASIL, (2014)

Adiante, no capítulo 5 – Segurança da Informação, é abordado medidas de segurança a serem adotadas, havendo entre elas, medidas referentes a procedimentos a serem adotadas para garantir a segurança física, e que podem e devem ser utilizadas no C Com.

A subseção Segurança do Arquivamento, versa sobre como deve ser guardado documentos sigilosos, discriminando os níveis de segurança para cada classificação, reservado, secreto e ultrassecreto. Os documentos ultrassecretos e secretos devem ser guardados em cofre,

sempre o primeiro em um com segredo de no mínimo 3 combinações, e os documentos reservados e demais de acesso restrito, em armário com chave. Caso não seja possível adotar o cofre de segredo de 3 combinações para os documentos ultrassecretos, deve ser empregado guarda armada no perímetro de acesso.

Seguindo até a subseção Segurança das Áreas e Instalações, é encontrado recomendações sobre a rede elétrica, "As instalações das OM, particularmente [...] as de Comunicações, deverão utilizar rede elétrica dimensionada ao número de equipamentos a ela ligados, visando à sua proteção contra sobrecargas." (BRASIL, 2014), tendo em vista o constante emprego de meios eletrônicos e elétricos em instalações de comunicações, incluindo o C Com.

Por fim, encontra-se também a subseção Segurança Física, que semelhantemente ao manual C-24-50, é escassa, possuindo apenas 4 linhas, as quais tratam que os arquivos digitais sigilosos devem possuir cópia de segurança, e esta deve estar em cofre fora da seção de informática (podendo ser lido C Com, para fins deste estudo); e que "deverá utilizar, sempre que possível, gerador ou outro equipamento que garanta a continuidade no fornecimento de energia elétrica aos equipamentos de informática" (BRASIL, 2014).

No tangente a segurança da área externa do C Com, segundo o "MANUAL C-11-20 BATALHÃO DE COMUNICAÇÕES", é atribuída ao Pelotão C Com a responsabilidade de "realizar a defesa imediata de suas instalações" (BRASIL, 2003), entretanto, ao se tratar de um Posto de Comando de Corpo de Exército, recai sobre o Pelotão de Segurança de um Batalhão de Polícia do Exército:

> "A segurança interna das instalações do PCP é provida pelo BPE, normalmente, através do seu Pel Seg. [...] Deve ser dada atenção especial aos pontos-chave da instalação, tais como: o centro de comunicações (C Com), o centro de operações e o alojamento do Cmt do C Ex." (BRASIL, 2022)

4.2 DOCUMENTAÇÕES EXTERNAS AO EXÉRCITO BRASILEIRO

Embora não haja um C Com propriamente dito em um ambiente civil, há estruturas similares que funcionam em empresas e demais órgãos públicos, as quais possuem necessidades de segurança física similar às do C Com. Para nortear tal planejamento de segurança, é utilizado como principalmente o guia "Norma Brasileira 17999 - Código de prática para a gestão da segurança da informação (NBR ISO/IEC 17799)", publicada em 2001.

Tal NBR, tem por finalidade "prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança" (ABNT, 2001), abordando segurança organizacional, controle de informação, gerenciamento das

comunicações, controle de acesso, manutenção de sistemas, e o enfoque deste trabalho, segurança física e do ambiente.

O capítulo 7 da NBR supracitada “Segurança Física e do Ambiente”, é subdivido em 3 subcapítulos, Áreas de Segurança, Segurança do Equipamento e Controles Gerais, os quais abordam conceitos de segurança e medidas a serem adotadas. Iniciando em Áreas de Segurança, são descritos procedimentos para “Prevenir acesso não autorizado, dano e interferência às informações e instalações físicas da organização (ABNT, 2001), que são apresentados de forma progressiva, sendo o primeiro passo a ser adotado é a definição do perímetro de segurança, para, a partir dele, ser tomadas demais medidas de segurança física a fim de atingir o resultado desejado.

> “Um perímetro de segurança é qualquer coisa que estabeleça uma barreira, por exemplo, uma parede, uma porta com controle de entrada baseado em cartão ou mesmo um balcão de controle de acesso com registro manual. A localização e a resistência de cada barreira dependem dos resultados da avaliação de risco.” (ABNT, 2001)

Entretanto, para uma instalação como um C Com, onde há fluxo de dados e mensagens sensíveis, a norma recomenda que tal perímetro receba uma atenção maior:

> “Convém que o perímetro de um prédio ou local que contenha recursos de processamento de dados seja fisicamente consistente (isto é, não podem existir brechas onde uma invasão possa ocorrer facilmente). Convém que as paredes externas do local possuam construção sólida e todas as portas externas sejam protegidas de forma apropriada contra acessos não autorizados, como, por exemplo, mecanismos de controle, travas, alarmes, grades etc...” (ABNT, 2001)

Definido o perímetro de segurança da instalação, a norma aborda sobre o controle de entrada e saída de indivíduos de tais ambientes, os quais apenas pessoas autorizadas devem ter acesso, e para garantir isso, deve existir o Log de entrada e saída, bem como o propósito de estarem adentrando o ambiente. Novamente, é recomendado que para o “acesso às [..] instalações e recursos de processamento de informações” (ABNT, 2001), o qual se encaixa o C Com, seja feito o controle com cartões de acesso ou método de identificação individual eletrônico semelhante, e o controle de direito de acesso sejam revistos e atualizados constantemente.

Após o acesso, a norma trata sobre a segurança interna nas instalações, que devem possuir “indicações mínimas do seu propósito, sem sinais óbvios, tanto fora quanto dentro do prédio, da presença de atividades de processamento de informação” (ABNT, 2001), portanto, aplicando ao C Com, dificultar a identificação da existência de um C Com através da

observação externa. A norma recomenda também quanto ao trancamento de portas e janelas que não estão em uso, e a instalação de sistemas de detecção de intrusão, os quais devem estar sempre com seus sistemas de alarme ativados em ambientes vazios.

Findo o subcapítulo, é feita a recomendação da proibição de uso de equipamentos de gravação de imagens e/ou áudio, de modo a evitar o vazamento de dados e informações.

Prosseguindo, no subcapítulo Segurança dos Equipamentos, são abordados procedimentos para "Prevenir perda, dano ou comprometimento dos ativos, e a interrupção das atividades do negócio" (ABNT, 2001). Sabendo que a Norma é Civil, poderíamos modificar o termo "negócio", para "operação", no contexto militar. O capítulo inicia tratando da instalação e proteção do equipamento em si, que devem ser alocados de forma a minimizar riscos físicos, como roubo, fogo, água, poeira, vibração, etc; bem como a proibição de comida, bebidas e fumo no ambiente, para evitar possíveis danos aos equipamentos.

Após isso, a norma trata do fornecimento de energia aos equipamentos elétricos, que devem possuir meios para garantir a continuidade do serviço em casa de falha elétrica, e é sugerido o uso de mais de um ponto de fornecimento elétrico, uso de UPS e/ou existência de gerador reserva. Entretanto, para garantir que em caso de falha tais medidas funcionem, a norma recomenda a verificação periódica de tais meios; e que o sistema não se baseie em apenas um método, de modo que caso haja falha, existe uma redundância e não ocorra a interrupção do fornecimento.

O próximo tópico a ser abordado é a segurança do cabeamento, tanto o elétrico, quanto o de redes, que devem estar protegidos contra interceptação e dano. Para obter isso, a norma recomenda que sejam instalados de forma subterrânea, e quando não possível, em conduítes, e que haja separação entre os cabos de energia e os de redes. Para os sistemas mais críticos e sensíveis, é recomendado adotar medidas extras, como cabo de redes blindados, terminais trancados por chave, redundância de rotas de transmissão, uso de fibra ótica e varredura periódica para identificar dispositivos não autorizados conectados aos cabos (ABNT, 2001),

Terminado os 2 primeiros subcapítulos, o terceiro, Controle Gerais, lista medidas que devem ser adotadas para "Evitar exposição ou roubo de informação e de recursos de processamento da informação" (ABNT, 2001), e é apresentado a política de "mesa limpa e tela limpa", cuja ideia força é manter uma área de trabalho organizado, evitando que o material seja roubado ou danificado (mesa limpa) e que estejam abertos somente os arquivos e programas que estejam em uso nos terminais de computador (tela limpa), para evitar que seja facilitado o acesso de dados por indivíduos não autorizados.

Para isso, a norma recomenda que sejam padronizados procedimentos como manter

guardado em armário ou gaveta com chave, papéis e mídias digitais quando não estiverem em uso, e documentos sensíveis devem ser guardados preferencialmente em cofre ou arquivo resistente a fogo. A utilização de impressoras e copiadoras devem ser ter uso controlado, e quando utilizadas, devem ter a impressão retirada imediatamente, para evitar extravio (ABNT, 2001). Para a política de tela limpa, os usuários devem sempre utilizar senhas de acesso nos computadores, e ao se ausentarem, bloquearem a tela para evitar uso não autorizado.

Por fim, este subcapítulo encerra reforçando o controle de acesso e saída de material e informação do ambiente, bem como a necessidade de inspeções pontuais para verificar a possível ausência de algum material.

Outro documento a ser analisado é "Public Switched Network Security Assessment Guidelines", elaborado pelo Sistema de Comunicação Nacional (*National Comunication Stystem - NCS*), uma agência do Departamento de Segurança Interna dos Estados Unidos (*United States Department of Homeland Security - DHS*). Este documento foi criado com o objetivo de nortear a elaboração de procedimentos, diretrizes e metodologias padronizadas para identificar, avaliar e mitigar riscos de centrais de rede de comunicações do governo americano (NCS, 2000). O documento aborda sobre segurança pessoal, segurança física, segurança da rede, gerenciamento de rede, suporte de operações e segurança de acesso.

Nele, é definido como políticas de segurança física, medidas que visam proteger instalações de furtos, arrombamentos, vandalismo, destruição, desastres naturais, ameaças internas, e demais situações que podem causar perda de dados, capacidade de operação, reputação e imagem, e perigo aos funcionários (NCS, 2000). Para atender a tais demandas, os procedimentos a serem adotados devem incluir medidas de controle de acesso, segurança interna, segurança estrutural, segurança ambiental e segurança de computadores e dados.

O documento aborda que apesar das portas serem o principal ponto de acesso, outras vias como janelas, tubulações, dutos de ventilações, etc, também devem ser avaliados e avaliado o nível de risco que apresenta (NCS, 2000). Acerca das portas, deve-se primeiro garantir que foram instaladas corretamente, de modo que não possam ser desparafusadas pelo lado de fora, portas de pouco usadas, como saídas de emergências, devem possuir alarme em caso de uso. Todas devem estar sempre trancadas ou guardadas, devendo sempre durante períodos que haja grande entrada e saída de pessoas, estarem guarnecidas. As portas quando não guarnecidas, devem possuir métodos de identificação, bem como métodos de garantir que entre e saia somente um indivíduo por vez, como uma porta giratória, evitando que entre acompanhantes não autorizados juntos (NCS, 2000).

As chaves, sejam elas físicas ou RFID, devem ser itens controlados e numerados, tendo

registro de quantas cópias existem e de quem as possuem (NCS, 2000). Também deve ser feito conferências periódicas se alguém perdeu uma cópia, bem como deve ser realizado o recolhimento de chaves dos indivíduos que tiveram seu acesso às instalações revogado ou modificado. As chaves RFID, por sua vez, possuem a vantagem de terem seu controle facilitado visto que podem ser desabilitadas em caso de perca ou extravio (NCS, 2000). Ainda é recomendado que cadeados com combinação numérica devem ser trocados periodicamente para evitar que o seu desgaste facilite a identificação da senha de acesso (NCS, 2000).

Prosseguindo, é abordado medidas para a segurança interna das instalações, e é recomendado acha o registro de acesso de todos os indivíduos, os quais devem portar crachá com sua foto colorida, de tamanho suficiente para que seja possível realizar a identificação, e se possível, com chip RFID. Os visitantes devem também portar crachá específicos, com data de validade referente ao tempo que permanecerão no ambiente (NCS, 2000).

Os armários devam estar sempre trancados, e quando não estejam em uso, os documentos e demais papéis estejam em seus respectivos lugares. Dispositivos de armazenamento devem estar criptografados ou trancados em áreas de acesso limitado, e a localização de sistemas e equipamentos críticos devem ser restrito apenas aos indivíduos que necessitem saber (NCS, 2000).

Quanto a segurança estrutural, o documento aborda a importância de recursos como energia, água e lixo funcionarem corretamente para que seja possível operar de forma efetiva. (NCS, 2000). Para isso, é considerado essencial a existência de alternativas para caso de falta de energia elétrica, garantindo a redundância da rede elétrica através de geradores. Deve haver também água para consumo e resfriamento de equipamentos, através de reservatórios ou possibilidade de acionar caminhões pipas (NCS, 2000). É orientado também que o lixo para documentos e papéis seja trancado e com triturador, bem como seu descarte acompanhado para evitar que informações sejam recuperadas do lixo (NCS, 2000).

Ademais, deve existir no ambiente, dispositivos de detecção e supressão de incêndio, de proteção contra surtos elétricos e ar-condicionado para resfriamento de equipamentos sensíveis como servidores (NCS, 2000).

Acerca da segurança ambiental, o principal aspecto que o documento orienta a ser observado é a identificar se a área que está ou irá ser instalada a unidade é provável de sofrer desastres naturais (terremotos, vulcões, furacões, enchentes, raios, etc), desastres humanos (estouro de represa, explosão de gasoduto, vazamentos químicos) (NCS, 2000). Deve ser observado ainda as considerações civis, analisando riscos de atos de hostilidades que possam ser gerados por problemas políticos, religiosos, sociais, entre outros (NCS, 2000).

5. CONCLUSÃO

Analisado os manuais vigentes do Exército Brasileiro que abordam da segurança física do Centro de Comunicações, e ainda se valendo da Instrução Geral de Salvaguarda de Documentos Sigilosos, que, apesar de não tratar diretamente do Centro de Comunicações, podem ter suas orientações seguidas devido ao C Com lidar com documentos sigilosos, é notável ao compararmos tanto com a NBR, quanto com a documentação do DHS, que os manuais em uso no Exército Brasileira não aprofundam, tampouco exemplificam questões relativas a segurança física, principalmente de um setor considerado de importância crítica como o C Com.

Delimitando-se ao manual "Segurança das Comunicações", não houve acompanhamento da evolução tecnológica, tendo em vista que sua publicação ocorreu em 1978, época esta que que ainda não havia ocorrido a informatização do C Com, e, por conseguinte, vasta parte do material outrora utilizado não é mais empregado e foi somado tantos outros ao C Com.

Diversas medidas como o registro de acesso, utilização de crachás, mesa limpa, tela limpa, trancamento de gavetas e portas, entre outras, podem ser aplicadas de imediato e com custo próximo a zero, visto que são em sua grande maioria, exclusivamente procedimentais, sendo necessário apenas treinamento e instrução aos militares integrantes do C Com. Outras medidas como instalação de alarmes, sensores, sistema de monitoramento como o CFTV, log, extintores de incêndio, geradores, nobreaks, UPS e DPS, podem ser adquiridos e integrados ao sistema atual do C Com sem ocasionar alteração grande na sua estrutura física, organizacional e doutrinária. Contudo, para utilização de tecnologias mais complexas, como identificação biométrica, cabeamento por fibra ótica, cartões RFID e sistema de combate a incêndio mais complexo, como os Sprinklers, podem apresentar maior dificuldade de serem implementados em um C Com, devido ao seu custo elevado e serem de complexa integração com os demais sistemas e equipamentos utilizados pelo Exército Brasileiro.

Portanto, é necessário que seja feito uma atualização dos atuais manuais, buscando atualizar os procedimentos adotados com as novas tecnologias e equipamentos, podendo alinhar com as diretrizes já seguidas e consolidadas por organizações civis e outros órgãos públicos internacionais.

REFERÊNCIAS

ADÃO, Manoel. Como a fibra óptica transmite dados? Por que ela é mais rápida? **Quora**. Disponível em: <https://pt.quora.com/Como-a-fibra-%C3%B3ptica-transmite-dados-Por-que-ela-%C3%A9-mais-r%C3%A1pida> Acesso em: 08 de maio 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 16400: Chuveiros automáticos para controle e supressão de incêndios - Requisitos e métodos de ensaio**. Rio de Janeiro. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 17799: Tecnologia da informação - Código de prática para a gestão da segurança da informação**. Rio de Janeiro. 2001.

Biometrics – Quick Guide. **Tutorials Point**. Disponível em: <https://www.tutorialspoint.com/biometrics/biometrics_quick_guide.htm> Acesso em: 08 de maio 2023.

BRAGANÇA, Isabel. **Evolução da Comunicação Humana Podemos Explicar A História da Existência Humana Através das Etapas do Desenvolvimento da Comunicação**.Maio 2009.

BRASIL. Exército Brasileiro. Estado-Maior Do Exército. **Instruções Gerais para a Salvaguarda de Assuntos Sigilosos.** EB10-IG-01.011. 1ª Edição, 2014.

BRASIL. Exército Brasileiro. Estado-Maior Do Exército. **Manual de Campanha Batalhão de Comunicações**. C11-20. 1ª Edição, 2003.

BRASIL. Exército Brasileiro. Estado-Maior Do Exército. **Manual de Campanha Batalhão de Polícia do Exército**. EB70-MC-10.326. 1ª Edição, 2022.

BRASIL. Exército Brasileiro. Estado-Maior Do Exército. **Manual de Fundamentos Doutrina Militar Terrestre**. EB20-MF-10.102. 2ª Edição, 2019.

BRASIL. Exército Brasileiro. Estado-Maior Do Exército. **Manual de Campanha Segurança das Comunicações**. C24-50. 1ª Edição,1978.

BRASIL. Exército Brasileiro. Estado-Maior Do Exército. **Manual de Campanha Centro de Comunicações.** C 24-17. 1ª Parte. 2ª Edição, 2001.

CBMES - Corpo De Bombeiros Militar Do Espírito Santo. **Norma Técnica nº 12/2020**. Vitória. 2020.

CCNA: Network Media Types. **CISCO**. 14 mar. 2003. Disponível em: <https://www.ciscopress.com/articles/article.asp?p=31276/> Acesso em: 08 de maio 2023.

CFTV: saiba tudo sobre esse sistema. **Intelbras**. 19 jan. 2023 Disponível em: <https://blog.intelbras.com.br/cftv-saiba-tudo-sobre-esse-sistema/> Acesso em: 08 de maio 2023.

COUTO, Guilherme; MALAFAIA, Tarsius. **Identificação por Radiofrequência**. 2019.

Universidade Federal do Rio de Janeiro, Rio de Janeiro. 2019.

Dispositivos contra surto elétrico: saiba como proteger seus equipamentos. **Intelbras**. 17 out. 2022. Disponível em: <https://blog.intelbras.com.br/dispositivos-contra-surto-eletrico/> Acesso em: 08 de maio 2023.

DPS: o que é Dispositivo de Proteção contra Surtos e por que você precisa de um na sua empresa? **Valemam**. 27 mar. 2020. Disponível em: <https://valemam.com.br/dps-o-que-e-dispositivo-de-protecao-contra-surtos-e-por-que-voce-precisa-de-um-na-sua-empresa/> Acesso em: 08 de maio 2023.

Entenda o funcionamento do alarme de intrusão. **Intelbras**. 29 out. 2022 Disponível em: <https://blog.intelbras.com.br/alarme-de-intrusao/> Acesso em: 08 de maio 2023.

Instrução de Combate a Incêndio. **1º Centro de Geoinformação**. 17 out. 2022. Disponível em: <https://1cgeo.eb.mil.br/publicacoes-2/816-instrucao-de-combate-a-incendio/> Acesso em: 08 de maio 2023.

Introdução a fibras ópticas, dB, atenuação e medições. **CISCO**. 20 abr. 2005 Disponível em: <https://www.cisco.com/c/pt_br/support/docs/optical/synchronous-digital-hierarchy-sdh/29000-db-29000.html#topic1> Acesso em: 08 de maio 2023.

Log de usuários. **Thotau**. Disponível em: <http://www.thotau.com.br/help/2.3/Seguranca/frmLogUsr.html/> Acesso em: 08 de maio 2023.

LOUREIRO, Gabriel; SOUZA, Isabella; LOPES, Marcelle. **Identificação por Radiofrequência**. 2015. Universidade Federal do Rio de Janeiro, Rio de Janeiro. 2015.

MACHADO, Marcel. **Segurança da Informação: uma Visão Geral sobre as Soluções Adotadas em Ambientes Organizacionais**. 2012. Trabalho de Graduação – Bacharelado em Ciência da Computação, Universidade Federal do Paraná, Curitiba, 2012.

MARCONDES, José. Sensores de Vibração Utilizados Nos Sistema de Alarme. **Blog Gestão de Segurança Privada**. 22 nov. 2016. Disponível em: <https://gestaodesegurancaprivada.com.br/sensores-de-vibracao-detectores-sismicos/> Acesso em: 08 de maio 2023.

MERRIAN, Sharan; TISDELL, Elizabeth. **Qualitative Research A Guide To Design And Implementation.** 4. ed. São Francisco: Jossey-Bass, 2016.

NCS - NATIONAL COMMUNICATIONS SYSTEM. **Public Switched Network Security Assessment Guidelines**. Arlington. 2000.

O que é biometria? **Kaspersky**. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/biometrics> Acesso em: 08 de maio 2023.

OLIVEIRA, Paulo. Sistema de gerenciamento de logs: Como funciona? **Linux Solutions**. 18 mar. 2019. Disponível em: <https://www.linuxsolutions.com.br/sistema-de-gerenciamento-de-logs-como-funciona/> Acesso em: 08 de maio 2023.

QAMAR, Noor; MUSTAFA, Kamran. **Biometric covert acquisition protection by enhancing sweat glands and cryptography.** 2017. Lahore Garrison University, Lahore. 2017.

SÁ, Brian. Você sabe o que é um Sprinkler? **Mi Fire**. 16 mar. 2021. Disponível em: <https://www.mifire.com.br/2021/03/16/voce-sabe-o-que-e-um-sprinkler/> Acesso em: 08 de maio 2023.

SANTANA, Sandra. **RFID - Identificação Por Radiofreqüência**. 2005. Trabalho de Graduação – Tecnólogo em Informática com Ênfase em Gestão de Negócios, Faculdade de Tecnologia da Baixada Santista, Praia Grande, 2005.

Sensor de intrusão: quais as tecnologias ideais para cada ambiente. **Intelbras**. 11 maio 2020 Disponível em: <https://blog.intelbras.com.br/sensor-de-intrusao-quais-as-tecnologias-ideais-para-cada-ambiente/> Acesso em: 08 de maio 2023.

Sprinklers em áreas de data center: como funciona? **SKOP**. 22 abr. 21. Disponível em: <http://www.skop.com.br/2021/04/22/sprinklers-em-areas-de-data-center/> Acesso em: 08 de maio 2023.

STRAUSS, Anselm; GLASER, Barney. **The Discovery of Grounded Theory: Strategies for Qualitative Research.** São Francisco: Aldine, 1999.

THREAT INTELLIGENCE REPORT. **NETSCOUT**. 2021. Disponível em: <https://www.netscout.com/threatreport/> Acesso em: 24 de jul. 2022.

Tipos de sensores de alarme: funcionamento e exemplos de aplicação. **Intelbras**. 28 set. 2022. Disponível em: <https://blog.intelbras.com.br/saiba-como-funcionam-os-tipos-de-sensores-de-alarme/> Acesso em: 08 de maio 2023.

Tudo sobre Nobreak: o que é, tipos e muito mais! **Intelbras**. 21 dez. 20. Disponível em: <https://blog.intelbras.com.br/tudo-sobre-nobreak/> Acesso em: 08 de maio 2023.

UTP vs STP Cable Wiki and Guide. **QSFPTEK**. 23 dez. 2021. Disponível em: <https://www.qsfptek.com/article/utp-vs-stp-cable-wiki-and-guide> Acesso em: 08 de maio 2023.

Veja a diferença entre protetor eletrônico, filtro de linha e régua de tomada. **Intelbras**. 15 fev. 2022. Disponível em: < https://blog.intelbras.com.br/o-que-difere-a-regua-de-tomada-do-protetor-eletronico/> Acesso em: 08 de maio 2023.

Vianet implanta solução de segurança perimetral inédita. **Terra**. 08 ago. 2017. Disponível em: <https://www.linuxsolutions.com.br/sistema-de-gerenciamento-de-logs-como-funciona/> Acesso em: 08 de maio 2023.

What is PIR? **Mobeye Store**. Disponível em: <https://www.mobeyestore.com/faq/what-is-pir/> Acesso em: 08 de maio 2023.

Wi-Fi Window & Door Alarm Sensor. **Swann**. Disponível em: <https://us.swann.com/swifi-wdoor/> Acesso em: 08 de maio 2023.