



ESTADO DE SANTA CATARINA

**SECRETARIA DE ESTADO DA SEGURANÇA
PÚBLICA**

**COMANDO-GERAL DO CORPO DE BOMBEIROS
MILITAR**

SEPARATA AO BOLETIM Nº 20-2025

MANUAL DE REDES DE DADOS DO CBMSC



MANUAL DE REDES DE DADOS DO CBMSC

CORPO DE BOMBEIROS MILITAR DE SANTA CATARINA

EXPEDIENTE | MANUAL DE REDES DE DADOS DO CBMSC

(Edição instituída pela Resolução nº 7, de 19 de maio de 2025)

CORPO DE BOMBEIROS MILITAR DE SANTA CATARINA

COMANDANTE-GERAL

Coronel BM Fabiano de Souza

SUBCOMANDANTE-GERAL

Coronel BM Jefferson de Souza

CHEFE DO ESTADO-MAIOR GERAL

Coronel BM Vandervan Nivaldo da Silva Vidal

EQUIPE DE ELABORAÇÃO

COORDENADOR E ORGANIZADOR - Tenente Coronel BM Diego Felipe Marzarotto
e 3º Sargento BM Douglas de Oliveira Franco

AUTOR COLABORADOR e REVISÃO TÉCNICA - 3º Sargento BM Douglas de
Oliveira Franco, Cabo BM Crystian Schwinden da Silva e Soldado BM Murilo Bauer

PROJETO GRÁFICO E DIAGRAMAÇÃO - Soldado BM Eduardo Silva de Souza

REVISÃO ORTOGRÁFICA E GRAMATICAL - 3º Sargento BM Douglas de Oliveira
Franco, Cabo BM Crystian Schwinden da Silva e Soldado BM Murilo Bauer

@ 2025. Todos os direitos de reprodução são reservados ao Corpo de Bombeiros Militar de Santa Catarina. É permitida a reprodução parcial ou total desta publicação, desde que citada a fonte.

Edição, distribuição e informações:

Corpo de Bombeiros Militar de Santa Catarina

Centro de Comunicação Social

Florianópolis - SC

Disponível em: www.cbm.sc.gov.br

SUMÁRIO

1 APRESENTAÇÃO | 5

2 NORMAS REFERENCIAIS | 6

3 TIPOS DE LINK DE DADOS E INTERNET | 7

3.1 Rede do governo | 7

3.2 Rede SSP | 7

3.3 Rede privada | 7

4 CLASSIFICAÇÃO DAS UNIDADES BOMBEIRO MILITAR | 8

4.1 ALTA COMPLEXIDADE | 8

4.1.1 Unidades com Central de emergência; | 8

4.1.2 Unidades sede de Batalhões; | 8

4.1.3 Centro de Ensino; e | 8

4.1.4 Complexo administrativo do Comando Geral. | 8

4.2 MÉDIA COMPLEXIDADE | 8

4.2.1 Companhia e Pelotão Bombeiro Militar isoladas da sede do Batalhão; e | 8

4.2.2 Unidades administrativas isoladas do complexo administrativo do Comando Geral | 8

4.3 BAIXA COMPLEXIDADE | 8

4.3.1 Sede de RBM isolada de unidade operacional; | 8

4.3.2 Grupo de Bombeiro Militar; | 8

4.3.3 Sede SSCI isoladas; e | 8

4.3.4 Outros e locais de interesse Bombeiro Militar. | 8

4.4 Casos diversos | 8

5 LINKS DE REDE POR UNIDADES BOMBEIRO MILITAR | 9

6 INFRAESTRUTURA GERAL DE TELECOMUNICAÇÕES | 10

6.1 Pontos de rede | 10

6.2 Cabeamento | 11

6.3 Sala e *rack* de telecomunicações | 12

6.4 Área de trabalho | 13

6.5 Interferência eletromagnética em eletrocalhas e eletrodutos | 13

6.6 Projeto | 14

7 MEIOS DE ACESSO FÍSICO | 16

7.1 Cabeamento | 16

7.2 Cascadeamento | 17

7.3 Disposições gerais | 18

8 MEIOS DE ACESSO *WIRELESS* | 19

8.1 Tipos de redes | 19

8.1.1 Rede CBMSC-WiFi (*INTRANET*) | 19

8.1.2 Rede dispositivos (*INTRANET*) | 19

8.2 Rede visitantes | 20

9 PROCEDIMENTO PARA CONEXÃO REDE WIFI CBMSC-WIFI

(*INTRANET*) | 21

9.1 Ubuntu | 21

9.2 Android | 21

SUMÁRIO

10 CONFIGURAÇÃO DE IPV4 E DNS | 22

11 FORNECIMENTO DE EQUIPAMENTOS E MATERIAIS | 22

12 VPN (*VIRTUAL PRIVATE NETWORK*) | 23

13 OUTRAS DISPOSIÇÕES | 23

1 APRESENTAÇÃO

O Corpo de Bombeiros Militar de Santa Catarina (CBMSC) possui um setor de tecnologia da informação com a principal missão de definir e padronizar as tecnologias de sistema de informação e telecomunicações utilizadas pela corporação. Atuando também no gerenciamento, planejamento e execução das políticas de tais tecnologias. Além dessas funções a divisão ainda presta apoio a todas unidades bombeiro militar do Estado. Buscando sempre inovar, e desenvolver ferramentas e sistemas para a sua corporação, no intuito de acelerar os processos internos e melhorar o atendimento à população.

Como parte atuante desse setor tem-se a equipe de gerência de redes do CBMSC, responsável por prover, manter e administrar a rede de dados dos data centers do CBMSC, disponibilizando acesso a todos os sistemas Web do CBMSC, como os sistemas utilizados para o atendimento e a geração de emergências, de forma ininterrupta. A equipe da Seção de Redes também é responsável por auxiliar na execução de manutenções por terceiros da infraestrutura e realizar as configurações dos equipamentos de rede em todos os quartéis do Estado para utilização dos sistemas de emergência, além de normatizar as estruturas física e lógica das redes seguindo os padrões nacionais e internacionais vigentes buscando sempre a melhoria no serviço de trafegabilidade de dados.

É ainda atribuição da referida equipe regular e administrar as redes de dados, mantendo a segurança da informação trafegada nos meios físicos ou sem fio no âmbito da corporação e em acordo com as políticas e leis de segurança de dados vigentes. Buscando de forma constante novas tecnologias e alternativas, bem como realizar treinamentos e cursos para a melhoria da rede de dados de toda a instituição.



2 NORMAS REFERENCIAIS

A instalação do cabeamento estruturado bem como o projeto para a rede lógica deverá, no que couber, seguir os padrões estipulados pelas seguintes normas e práticas:

I. Normativas nacionais:

- a. **ABNT – NBR 14565:2013** – Cabeamento estruturado para edifícios comerciais e data centers;
- b. **ABNT – NBR 16415:2015** – Caminhos e Espaços para cabeamento estruturado;
- c. **ABNT – NBR 5410:2004** Versão CORRIGIDA: 2008 – Instalações elétricas de baixa tensão;
- d. **ABNT – NBR IEC 60065:2009** – Aparelhos de áudio, vídeo e aparelhos eletrônicos similares – Requisitos de segurança
- e. **ABNT NBR IEC 60839-1-1:2010** – Sistemas de segurança eletrônica e alarme
- f. **ABNT NBR IEC 60839-1-2:2010** – Parte 1: Requisitos gerais Seção 2: Unidades de alimentação, métodos de ensaio e critérios de desempenho;
- g. **Normas da Anatel;**
- h. **RDC ANVISA no 50**, de 21 de fevereiro de 2002 – Dispões sobre o Regulamento Técnico para planejamento, programação e avaliação de projetos físicos;
- i. **Caderno de Encargos e Projetos em BIM e CAD de Santa Catarina** (p.101 a 106).

II. Normativas internacionais:

- a. **ANSI/TIA/EIA 568** – Sistema de cabeamento genérico de telecomunicações para edifícios comerciais;
- b. **ANSI/TIA/EIA 569A** – Especificações de infraestrutura de cabeamento estruturado;
- c. **ANSI/TIA/EIA 606** – Especificações da administração e identificação dos sistemas de cabeamento estruturado;
- d. **ANSI/TIA/EIA 607** – Aterramento e Requisitos de Telecomunicações em Edifícios Comerciais.

3 TIPOS DE LINK DE DADOS E INTERNET

O CBMSC, em suas unidades administrativas e operacionais atualmente utilizam os seguintes modelos de links de dados e internet:

3.1 Rede do governo

Disponibilizado para as unidades através de recursos financeiros do Estado para utilização de acesso à rede mundial de computadores além de acesso a sistemas e serviços internos do Estado e do CBMSC (E193, ESCI, e-mail, VOIP, ROIP);

3.2 Rede SSP

Disponibilizado para algumas unidades em comum acordo com a Secretaria de Segurança Pública do Estado. Essa rede não possibilita acesso a rede mundial de computadores, somente acesso a rede de governo, sistemas e serviços internos do Estado e do CBMSC, mas poderá ter provimento de acesso de rede mundial de computadores em situações prioritárias e emergências;

3.3 Rede privada

Contratada pelas unidades através de recursos financeiros do município para utilização de acesso à rede mundial de computadores mas possibilitando acesso aos sistemas e serviços internos do Estado e do CBMSC (E193, ESCI, e-mail, VOIP, ROIP) através de tunelamento (VPN) com o equipamento roteador/concentrador especificado pelo setor de tecnologia da informação do CBMSC;

OBSERVAÇÃO: As especificações e termo de referência dos links citados estão disponíveis <https://documentoscblmsc.cbm.sc.gov.br/>.

4 CLASSIFICAÇÃO DAS UNIDADES BOMBEIRO MILITAR

As unidades de bombeiro militar, para regulamentação deste manual, são classificadas em 3 (três) tipos: Alta Complexidade, Média Complexidade e Baixa Complexidade.

4.1 ALTA COMPLEXIDADE

4.1.1 Unidades com Central de emergência;

4.1.2 Unidades sede de Batalhões;

4.1.3 Centro de Ensino; e

4.1.4 Complexo administrativo do Comando Geral.

4.2 MÉDIA COMPLEXIDADE

4.2.1 Companhia e Pelotão Bombeiro Militar isoladas da sede do Batalhão; e

4.2.2 Unidades administrativas isoladas do complexo administrativo do Comando Geral

4.3 BAIXA COMPLEXIDADE

4.3.1 Sede de RBM isolada de unidade operacional;

4.3.2 Grupo de Bombeiro Militar;

4.3.3 Sede SSCI isoladas; e

4.3.4 Outros e locais de interesse Bombeiro Militar.

4.4 Casos diversos

Cabe ao setor de tecnologia da informação do CBMSC julgar exceções das classificações acima e determinar ações e tipos de links inerentes à atividade. Essa classificação serve para determinar o tipo e quantidade de links de rede de dados para as unidades, além de servir de base para estipular as normas a serem seguidas para a implantação da infraestrutura de rede interna.

5 LINKS DE REDE POR UNIDADES BOMBEIRO MILITAR

A unidade classificada como **ALTA COMPLEXIDADE** devido sua atividade exercida, necessita de alta disponibilidade, segurança e confiabilidade na rede de dados. É obrigatório que esta unidade possua pelo menos 3 (três) links de rede de dados e internet de operadoras diferentes, possibilitando redundância para que os serviços digitais não sejam afetados por falhas e interrupções da operadora. O objetivo é justamente garantir que o atendimento emergencial na forma digital (193, 192) bem como o acionamento das unidades (radiocomunicação, acionamento remoto, VoIP, RoIP) estejam sempre disponíveis.

Essas Unidades devem possuir 3 (três) links de dados integrados de forma redundante dos tipos:

- A. Rede GOVLINK;
- B. Rede PRIVADA, contratada via fundo municipal e de operadora diferente da Rede de GOVLINK; e
- C. Rede SSP.

A unidade classificada como **MÉDIA COMPLEXIDADE** devido à sua atividade exercida, também necessita de disponibilidade, segurança e confiabilidade na rede de dados. Esta unidade necessita possuir pelo menos 2 (dois) links de rede de dados e internet de operadoras diferentes, possibilitando redundância para que os serviços digitais da Unidade não sejam afetados por falhas e interrupções provenientes da operadora. O objetivo é justamente garantir que o acionamento da unidade (radiocomunicação, acionamento remoto, VoIP, RoIP) esteja sempre disponível, assim como os seus serviços administrativos essenciais (SSCI).

Essas Unidades devem possuir 2 links de dados integrados de forma redundante dos tipos:

- A. Rede de GOVLINK ou Rede SSP;
- B. Rede PRIVADA, contratada via fundo municipal e de operadora diferente da Rede GOVLINK ou Rede SSP.

A unidade classificada como **BAIXA COMPLEXIDADE** devido sua atividade exercida, necessita de disponibilidade, segurança, confiabilidade na rede de dados, **mas não de redundância ativa**. Essa classificação determina que a unidade contrate um link de dados por operadora privada com recursos exclusivos dos fundos municipais, cabendo ainda a critério e disponibilidade financeira do setor de tecnologia da informação do CBMSC determinar outro tipo de link de dados.

É dispensada a contratação de link Rede PRIVADA para as unidades Bombeiro Militar classificadas como **BAIXA COMPLEXIDADE** que possuírem ou vierem a ter link de dados cedidos de forma gratuita por qualquer órgão, como prefeituras, ou empresas privadas.

OBSERVAÇÃO: O link de dados e internet cedido de forma gratuita para as unidades Bombeiro Militar classificadas como **MÉDIA e ALTA COMPLEXIDADE** deve ser somado a integração com os demais links descritos nesta seção do manual. Pode-se eximir o link cedido dessa soma desde que seja aprovado previamente pelo setor de tecnologia da informação do CBMSC.

6 INFRAESTRUTURA GERAL DE TELECOMUNICAÇÕES

6.1 Pontos de rede

As unidades de bombeiro militar, para regulamentação deste manual, deverão dispor de infraestrutura de acordo com o número de pontos de acesso e sistemas a serem instalados, e deverá seguir o estipulado no item 5 (CLASSIFICAÇÃO DAS UNIDADES BOMBEIRO MILITAR), quanto ao nível de complexidade:

Para a infraestrutura da rede lógica atender toda a demanda da edificação é necessário contabilizar os pontos de acesso à rede, o número de pavimentos e tamanho total do edifício:

- I. Reservar obrigatoriamente no mínimo 2 (dois) pontos de rede por usuário em sua bancada, sendo 1 (um) para conectar um computador de mesa; 1 (um) para conectar um telefone IP ou outro equipamento, como impressora/scanner;
- II. Nas Centrais de Operações Bombeiro Militar(COBOM), fica obrigatório o mínimo de 3(três) pontos de rede por estação de trabalho, possibilitando assim a redundância de pontos em caso de falha;
- III. Ainda é essencial a contabilização dos pontos para interconexão a periféricos distintos, fora das bancadas, como Impressoras, televisores, roteadores WiFi, pontos eletrônicos, aparelhos de multimídia, etc;
- IV. É recomendado a utilização de pontos de distribuição separados por pisos, ou seja, de modo que cada piso possua um equipamento de rede

concentrador, facilitando assim a manutenção e as futuras ampliações da rede; e

- V. Cada pavimento deverá possuir a quantidade e dimensionamento de *rack* necessárias para a perfeita distribuição no interior da edificação.

Nas unidades onde pretende-se instalar ou já existir instalado sistema de CFTV (monitoramento por câmeras) este deve-se levar em conta quando do dimensionamento do *Rack*, independente do Tipo de classificação em que a OBM se enquadrar.

Deverá ser previsto passagem para o cabeamento externo (a ser utilizado pela provedora de internet) até o *rack* central, sendo esta, realizada com dutos de diâmetro de no mínimo 2" (duas polegadas) e construída em material rígido de forma que não haja descontinuidade do conduíte, devendo ainda possuir caixas de passagem e inspeção.

- I. O conduíte de entrada deverá terminar na parede mais próxima do *rack* principal, em caixa de passagem de telefonia de 40cm X 40cm (quarenta centímetros por quarenta centímetros) a ser instalada a meia parede em altura padrão.

Cabe ao chefe do setor de tecnologia da informação do CBMSC julgar exceções das classificações acima e determinar as ações;

6.2 Cabeamento

Para que o conjunto de cabos utilizados na rede interna possa ser considerado estruturado, são indispensáveis a este uma série de medidas para que o mesmo disponha de previsão adequada dos recursos necessários para atender a quaisquer exigências de expansão ou movimentação dos pontos de rede na infraestrutura física das edificações, possibilitando entregar um serviço de maior confiabilidade e velocidade no que diz respeito às taxas de dados trafegantes pelo sistema. Desta forma, para a operacionalização correta de um cabeamento estruturado alguns pontos devem ser seguidos:

- I. Deverá ser contratada empresa especializada para realização das instalações de cabeamento horizontal e vertical(cabeamento de *backbone*), através de projeto e execução obedecendo às normas estipuladas no Capítulo 2 Normas para o Projeto de Rede Lógica deste manual, que especificam sistemas de cabeamento estruturado para edifícios comerciais e trazem os procedimentos básicos para a elaboração de projetos de cabeamento estruturado em redes de telecomunicações.
- II. O Cabeamento estruturado deverá seguir o padrão estipulado pela norma tendo todos os seus componentes adequados de forma que não existam incongruências entre os equipamentos podendo-se admitir os seguintes padrões:
 - A. No mínimo, cabeamento de categoria 5e (Cat5e) para as Unidades enquadradas como Baixa Complexidade;
 - B. No mínimo, cabeamento de categoria 6 (cat6) para as unidades enquadradas como Média e Alta Complexidades;
 1. As unidades que já possuem rede estruturada de acordo com a norma em categoria 5 estão dispensadas da exigência de categoria superior, as demais, deverão ao regularizar sua infraestrutura de rede, seguir o exigido.
 - C. Para os elementos de CFTV e alarme se admitirá cabeamento e componentes de categoria 3 (Cat3) para qualquer complexidades;
 1. Este cabeamento deverá estar identificado conforme as normas para evitar equívocos em relação ao cabeamento de rede.
 2. Sempre que possível deverá chegar em *rack* separado utilizado unicamente para o sistema de CFTV e alarme.
 - D. A interligação entre *racks* deverá preferencialmente ser com cabeamento óptico, podendo, em algumas exceções ser admitido o cabeamento de par trançado com categoria 6 ou superior.
 1. As exceções de que trata esse inciso deverão passar por análise da equipe técnica do setor de tecnologia da informação do CBMSC.
 - E. Em nenhuma hipótese admitir-se-á a conexão direta do cabeamento horizontal ao equipamento de rede, devendo sempre este ser espelhado em *patch panel* de mesma categoria conforme as normas exigidas;
 - F. A conexão entre o *patch panel* e o equipamento de rede deverá ser sempre através de *patch cord* certificados e de mesma categoria que os demais componentes da rede.

G. Não será admitido a conexão direta do cabeamento horizontal aos periféricos, tendo este sempre que ser espelhado a um RJ45 fêmea;

H. A identificação do cabeamento deve ser executada de acordo com o estipulado nas normas constantes no capítulo 2 de NORMAS REFERENCIAIS deste manual de forma que conste se é Lógico ou de Telefonia, o número do *Rack*, do *Patch Panel* dentro do *Rack* e da posição do cabo no *Patch Panel*, sempre a ser fixada no espelho da tomada de rede de forma a facilitar na resolução de problemas.

O cabeamento horizontal (cabos Utps) deverão obrigatoriamente terminar (serem conectados) em pontos de Telecomunicações (PTR) ou tomadas de estação, que nada mais é do que um subsistema composto de espelho com previsão para instalação de uma, duas ou mais tomadas RJ45 fêmeas de 8 vias, de categoria igual ou superior à do cabeamento estruturado e com previsão para instalação de etiqueta de identificação.

6.3 Sala e *rack* de telecomunicações

A Sala de telecomunicações, é o nome dado ao ambiente destinado em uma edificação para acomodar o *rack* central, bem como a chegada do cabeamento externo vindo da operadora de internet e do cabeamento estruturado (em geral os cabos de *backbone*) além dos servidores, roteadores, distribuidores e demais componentes necessários. Sua estrutura deverá ser adequada às premissas abaixo.

Para as unidades enquadradas como alta complexidade deste manual, será exigida uma sala de uso exclusivo para os equipamentos de telecomunicações com espaço mínimo de 3m x 3m (três metros por três metros) com sistema de resfriamento e rede de energia separada no quadro de disjuntores (quando

não atendido por gerador) e dispor de *rack* de Piso, desmontável de 19" (dezenove polegadas, padrão EIA 310-D), com tamanho entre 32 a 44 U's (*Units*) de modo a acomodar toda a estrutura de cabeamento e equipamentos necessários.

De preferência a sala deverá estar localizada ao centro geográfico da edificação e deverá ter utilização exclusiva, livre de infiltrações e com porta de acesso restrito.

O sistema de resfriamento deverá ter potência suficiente para manter a temperatura da sala entre 18°C e 24°C com umidade relativa entre 30% e 55%.

A alimentação elétrica do *rack* deverá ser com circuito dedicado direto do distribuidor principal com instalação de quadro de proteção no local por disjuntor de no mínimo 20A.

O piso deverá ser composto por material antiestático.

Em hipótese alguma será admitido a utilização da sala como depósito de materiais ou para outros fins que não sejam única e exclusivamente os destinados a acomodação de cabeamento e equipamentos de telecomunicações.

O *rack* deverá conter no mínimo: 2 (duas) bandejas fixas ventiladas padrão 19" (dezenove polegadas); 2 (duas) guias de cabo 19" (dezenove polegadas) de 1U; 2 (duas) réguas de tomadas padrão de 19" (dezenove polegadas) com 12 (doze) posições.

Para as Organizações Bombeiro Militar de média e baixa complexidade admite-se a instalação de *rack* de parede (mini *rack*) padrão 19" (dezenove polegadas) a ser instalado em ambiente climatizado com temperatura ambiente não superior a 24°C e com umidade entre 30% e 55%, para evitar superaquecimento dos equipamentos.

- I. O *rack* deverá possuir sistema de circulação de ar e ter tamanho entre 12 e 16 U, sendo este último o mais recomendado.
- II. O *rack* deverá conter no mínimo: 1 (uma) bandeja fixa ventilada padrão 19" (dezenove polegadas); 1 (uma) guia de cabo 19" (dezenove polegadas) de 1U; 1 (uma) régua de tomadas padrão de 19" (dezenove polegadas) com 12 (doze) posições.
- III. Para edificações verticais com dois ou mais pisos deverá haver uma estrutura de mini *rack* nos pisos superiores para abrigar os dispositivos ativos de rede, sendo facultada a aquisição da bandeja fixa para este caso.

6.4 Área de trabalho

Área de trabalho ou estação de trabalho é o local onde se localizam os equipamentos de uso pessoal como *desktops*, telefones VoIP ou qualquer outro dispositivo operado pelo usuário que demanda de uma conexão de rede.

Fica definido que, para os ambientes de uso habitual mas que de início não serão povoados, como almoxarifados, depósitos, e salas de

assepsia, considerar-se-á uma estação de trabalho a cada unidade de área correspondente a 10m² ou a cada ambiente, se este possuir uma metragem menor, e que em cada unidade deverá ser previsto o mínimo de 2 pontos de rede, sendo o ideal a instalação de 3 pontos ou tomadas de telecomunicações, desconsiderando banheiros e áreas de circulação.

- I. Nas áreas de circulação a instalação de pontos de rede dependerá da necessidade de conexão de equipamentos e/ou roteadores Wi-Fi.

Os conectores RJ45 fêmeas bem como a conectorização do *patch* painel deverão seguir o padrão EIA/TIA T658A, não sendo admitido qualquer outro padrão para confecção das tomadas.

Para os locais onde houver demanda maior, considerar-se-á sempre um mínimo de dois pontos de telecomunicações por estação, sendo recomendada a instalação de 3 pontos. Este caso se refere a salas onde duas ou mais pessoas trabalham juntas, sendo uma estação de trabalho para cada pessoa.

6.5 Interferência eletromagnética em eletrocalhas e eletrodutos

Para evitar problemas oriundos de interferências eletromagnéticas originadas de circuitos e componentes elétricos com potências inferiores a 5KVA, necessita-se de uma separação mínima entre estes e o cabeamento estruturado, conforme segue:

- I. O cabeamento deverá estar distante a pelo menos 1,20 metro de grandes motores elétricos ou transformadores.
- II. O cabeamento deverá estar distante a pelo menos 30 cm de condutores e cabos de distribuição elétricas..
- III. O cabeamento deverá estar distante a pelo menos 15 cm de lâmpadas fluorescentes.

As eletrocalhas devem ser do tipo lisas com tampa para se evitar acúmulos de poeira sendo construídas em aço-carbono preferencialmente pré-zincado a fogo ou com galvanização eletrolítica, sendo que sua instalação preferencialmente deverá seguir a mesma estrutura lógica das edificações.

Os eletrodutos devem ser utilizados em locais com baixa densidade de cabos, quando no sentido horizontal os segmentos contínuos não poderão exceder 30m e a fim de facilitar futuras manutenções esse intervalo não poderá ter mais que duas curvas de 90°. Os mesmos são recomendados somente em derivações da eletrocalha para encaminhamento dentro de salas ou em prumadas verticais, nunca sendo de bitola menor que 3/4 (2,10 mm).

6.6 Projeto

O projeto da rede lógica deverá ser elaborado por pessoa com capacitação técnica para tal e deverá conter os dados do responsável técnico.

Todos os projetos deverão passar por análise da equipe técnica do setor de tecnologia da informação do CBMSC antes de sua execução para fins de adequação, devendo conter os seguintes produtos:

- I. Peças Gráficas, representadas por: Plantas; Cortes; Fachadas; Detalhes; Diagramas; Ampliações e Detalhamentos executivos;
- II. Memorial descritivo;
- III. Memorial de Cálculo;
- IV. Especificações técnicas completas;
- V. Memorial Quantitativo / Lista de Materiais
- VI. Orçamento

Admitir-se-á para os casos que se enquadram como baixa complexidade, a inexigibilidade da responsabilidade técnica, no entanto o projeto ainda deverá seguir as normas constantes no Capítulo 2 Normas para o Projeto de Rede Lógica deste manual assim como dispor de meios para que seja possível a análise do projeto por parte da equipe técnica do setor de tecnologia da informação do CBMSC.

Para unidades de média e alta complexidade somente será dispensada a responsabilidade técnica do projeto mediante autorização do setor de tecnologia da informação do CBMSC após prévia justificativa.

Para os quartéis novos ou que passarem por reforma, deverá ser previsto e dimensionado no projeto de telecomunicações a construção de uma estrutura na cobertura da edificação que permita a instalação e retirada de antenas sem perfuração da laje de cobertura, com passagem para o cabeamento até o *rack* central tendo o dimensionamento mínimo de 2" (duas polegadas).

A instalação do sistema de monitoramento e alarme não poderá utilizar a infraestrutura de rede (cabeamento, conectores, *patch panels* e *switches*) sendo imperativo a utilização de meio físico próprio para tal, instalado visando sempre o mesmo padrão do cabeamento de rede e de forma a não atrapalhar sua manutenção.

7 MEIOS DE ACESSO FÍSICO

O meio físico de acesso a rede é todo método de conexão dos dispositivos a rede externa através de algum tipo de cabeamento, coaxial, par trançado ou fibra óptica, para permitir o transporte de sequências de bits entre dois pontos distintos, da melhor forma possível, evitando erros de conflito com outros dispositivos já conectados à rede e atrasos (*delay*) ou latência dos pacotes trafegados.

Os únicos meios físicos aprovados para utilização de acesso a rede no âmbito do CBMSC são: cabo de par trançado tipo UTP, podendo este ser de categoria 5 (Cat5E) ou superior, e fibra óptica, onde couber sua utilização.

7.1 Cabeamento

Os cabos de par trançados para uso são do tipo UTP (*unshielded twisted pair*), estes além de outras classificações são divididos entre: cabo rígido e cabo flexível:

- I. Cabo rígido: é o cabo que devido a suas propriedades construtivas não dispõe de resistência considerável quando submetido a tração ou torção, sendo o mais indicado para emprego apenas em cabeamentos horizontais estruturados, ou seja, são utilizados em locais onde o cabeamento não sofre constantes mudanças nem lhe é empregado algum tipo de entorse.

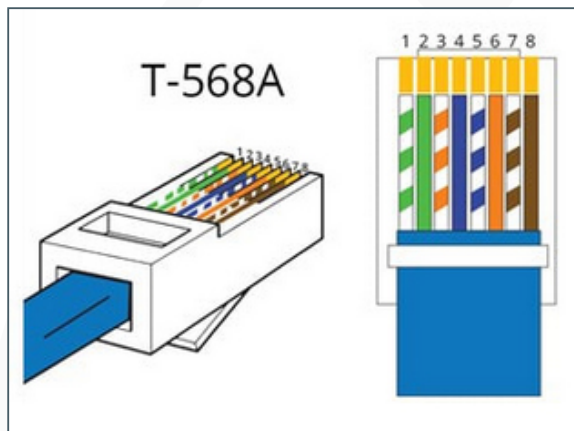
- II. Cabo flexível: é o tipo de cabo recomendado para a utilização na conexão dos equipamentos à rede, ou conexão dos dispositivos a tomada de rede ou tomada de telecomunicações (TO), pois possui alta resistência ao manuseio contínuo, e por ser mais maleável sofre menos deformações no decorrer do tempo.

Desta forma, em conformidade com as normas vigentes fica estabelecido que, a conexão de qualquer dispositivo de rede às tomadas de telecomunicações (TO) deverá ser efetuada com *patch cords*, ou cordões de rede, construídos a partir de cabos flexíveis. Os cabos a serem utilizados, além de flexíveis deverão possuir classificação de categoria igual ou superior a categoria utilizada para o cabeamento horizontal.



Patch Cord

Os *patch cords* devem conter certificação da ANATEL de modo a comprovar que estão dentro dos padrões de resistência, inflamabilidade e flexibilidade. O padrão de conectorização a ser utilizado na infraestrutura de redes do CBMSC será obrigatoriamente o padrão T658A, para qualquer aplicação ou dispositivo a ser conectado. Casos onde a utilização de cabos certificados não seja possível, devem ser remetidos ao setor de tecnologia da informação do CBMSC para análise e posterior deferimento.



Padrão T658A

OBSERVAÇÃO: É proibida a utilização de um mesmo ponto de rede para conexão de dois dispositivos através de qualquer técnica não autorizada com velocidades de conexão abaixo do padrão 100Base T (como exemplo, padrão 10Base T onde cada dispositivo utiliza apenas 2 pares de fios para a navegação), devendo, cada dispositivo de rede ser conectado em um cabeamento separado e identificado conforme as normas vigentes. Cabe ressaltar que esta técnica além de deixar o acesso à rede lento ainda cria um problema adicional para a identificação e manutenção em casos de defeito, sendo proibida a sua utilização no âmbito do CBMSC.

7.2 Cascadeamento

O cascadeamento de equipamentos acontece quando se conectam múltiplos *Switches* ou HUBs em sequência na rede, ou seja, quando o usuário por não ter a disposição tomadas de telecomunicações em número suficiente para a conexão dos seus dispositivos conecta a saída de rede existente em um dispositivo multiplicador de pontos.

Para estes casos deve ser contratada empresa especializada para que seja efetuada a instalação de novo cabeamento vindo do ponto de distribuição mais próximo. Sendo que este cabeamento a ser lançado deverá seguir o recomendado no Capítulo 6 de Infraestrutura Geral de Telecomunicações.

No caso da impossibilidade técnica para instalação de novo cabeamento, deverá ser instalado no local em questão nova estrutura de rede horizontal utilizando-se do cabo existente como cabo de *backbone* ou até mesmo prevendo a substituição deste por fibra óptica ou cabo de categoria 6 (CAT6), caso já não seja.

É proibida a utilização de qualquer ativo de rede que não seja gerenciável, ou seja, é proibida a instalação de HUBs e *Switches* na rede que não possuam, no mínimo Controle de *Looping*, *spanning tree*, envio de dados através de SNMP e acesso via GUI (*Graphical user interface*) ou CLI (*Command line interface*).

Esta medida se deve ao fato de que:

- I. A grande maioria desses equipamentos deixa a rede lenta, pois todos os pacotes de rede são distribuídos em modo de *broadcast* o que também gera uma falha de segurança, já que qualquer dispositivo na rede pode

subtrair informações sensíveis destinadas a outros dispositivos na rede.

- II. Estes equipamentos não permitem que o administrador da rede ou o técnico local possa localizar erros em caso de problemas de conexão.
- III. Eles não permitem o gerenciamento de problemas de forma autônoma.

Da mesma forma que os HUBs, a utilização das portas de rede LAN presente em roteadores *wireless* não deve acontecer, pois o seu comportamento é similar. Existe o fator agravante de que os roteadores *wireless* estejam configurados de forma errônea, por exemplo, com o serviço de DHCP Server ativo em suas portas LAN. Desta forma, o equipamento fornece endereço de rede diferente do padrão estabelecido, impossibilitando o uso dos sistemas internos do CBMSC.



HUB



Roteador WI-FI

A utilização da saída de rede presente nos equipamentos de Telefonia (telefones IP e/ou ATAs) poderá ser utilizada, desde que seja como **último**

recurso e os aparelhos sejam devidamente configurados de modo que as portas estejam em modo Bridge e não forneçam serviço de DHCP Server. É importante ressaltar que esta técnica limita a velocidade de navegação do computador uma vez que as interfaces LAN dos telefones possuem limite de 100 Mbps o que em muitos casos gera lentidão de navegação.

7.3 Disposições gerais

Fica **proibida** a utilização de cabeamento coaxial ou cabeamento de par trançado de categoria inferior à categoria 5 (Cat5) para a conexão de dispositivos de rede, sendo permitida a utilização destes somente em sistemas de alarme e vídeo monitoramento (CFTV) e desde que seja de forma separada da estrutura de cabeamento de rede.

O emprego de dispositivos de rede que utilizam alimentação de energia via *Power over Ethernet* (PoE), padrão 802.3bt, é permitida atendendo os seguintes pontos:

- I. A alimentação dos dispositivos e *switch* de acesso instalados no *rack*
- II. A tomada de telecomunicações com identificação da posição no *Patch Panel*, conforme as normas vigentes e a identificação de alimentação via PoE para evitar eventuais equívocos com queima de equipamentos.

Fica permitido, para casos onde seja possível a aplicação de tal tecnologia, a utilização de Transmissores *Power Line Communication* (PLC), desde que eventuais serviços de DHCP presentes nos dispositivos sejam desativados e que tudo seja bem documentado e etiquetado para facilitar manutenções futuras.

8 MEIOS DE ACESSO WIRELESS

Com a crescente tendência no avanço da tecnologia aliada a demanda por conexão a redes móveis, tornou-se fundamental ao CBMSC empenhar esforços nesta área objetivando a preservação da rede de ataques cibernéticos, além de estabelecer níveis de segurança capazes de proteger dados pessoais e manter, de certa forma, a privacidade das pessoas.

Deste modo, para proteger usuários e os dados institucionais, o setor de tecnologia da informação estabeleceu que todas as unidades administrativas e operacionais do CBMSC devem contar com redes padronizadas, possuindo diferentes métodos de autenticação e navegação, de acordo com a necessidade de utilização da rede de cada usuário.

Desta forma, fica padronizado que o acesso se dará através de 3 (três) diferentes redes sem fio, de modo que cada pessoa e/ou dispositivo possa conectar de acordo com seu perfil de utilização.

Uma vez configurada no equipamento estas redes permitem conexão automática em diferentes OBMs, desde que possuam a rede padronizada, evitando assim que o utilizador necessite efetuar diversos cadastros de rede para cada local que estiver.

Estas redes bem como suas diretrizes estão elencadas nos itens abaixo:

8.1 Tipos de redes

8.1.1 Rede CBMSC-WiFi (INTRANET)

Esta rede está representada com nome ou SSID (*Service Set Identifier*)

“**CBMSC-WIFI**”, e está destinada a utilização de usuários que possuam login e senha próprios do CBMSC, ou seja, todo militar ou civil que possua cadastro no LDAP (*Lightweight Directory Access Protocol*) e consiga acesso aos sistemas como Ebombeiro e ESCI, poderá/deverá conectar-se a essa rede.

Conectado a ela, o usuário possui acesso à intranet do CBMSC, aos sistemas de governo, às impressoras locais da edificação, além de navegação na internet.

Em OBMs que possuem internet privada, toda a navegação diferente dos serviços de governo é automaticamente encaminhada para a rede privada possibilitando assim maior qualidade de acesso.

Esta rede possui controle de segurança, prioridade de navegação em relação a rede visitantes (CBMSC-WIFI-VISITANTES) e deve seguir na íntegra a INSTRUÇÕES REGULADORAS PARA O USO DE PROGRAMAS ABERTOS NO CORPO DE BOMBEIROS MILITAR - IR 30-11-BM.

8.1.2 Rede dispositivos (INTRANET)

Esta rede é apresentada com o SSID “**CBMSC-WIFI-DISPOSITIVO**” ficando destinada a utilização de equipamentos (câmeras ip, impressoras, televisores, *chromecast*, *firestick*) que não possuem os protocolos de autenticação da rede CBMSC-WIFI ou que sejam de utilização coletiva e que precisam de acesso a intranet da corporação, rede do governo e navegação externa.

Esta rede é protegida pela senha “cbmsc#dispositivos”, e a sua utilização depende de liberação por parte do setor de tecnologia da informação do

CBMSC. Esta liberação do acesso se dará por solicitação dos interessados através do sistema sau.cbm.sc.gov.br, onde o usuário deverá informar o tipo de equipamento, sua utilização e o endereço MAC (endereço de interface física) do equipamento. Todo dispositivo conectado a esta rede terá as mesmas prerrogativas de navegação que a rede CBMSC-WIFI.

8.2 Rede visitantes

Esta rede é apresentada através do SSID “**CBMSC-WIFI-VISITANTES**”, estando esta reservada à utilização de pessoas que estejam de passagem pela OBM e para instruções em salas de aula onde os alunos não possuam login e senha próprios do CBMSC, já que esta rede é protegida apenas por senha definida pelo Setor de Redes”.

Conectado a essa rede o utilizador estará isolado da rede interna, tendo apenas acesso a rede mundial de computadores com uma certa limitação e com prioridades inferiores às redes CBMSC-WIFI e CBMSC-WIFI-DISPOSITIVOS. Essa medida faz-se necessária para o incremento da segurança evitando assim que dispositivos de terceiros que por ventura estejam infectados venham a causar prejuízos à corporação.

Vale ressaltar ainda que o corpo orgânico deverá evitar a disseminação das credenciais de acesso a essa rede de modo a impedir que vizinhos ou estranhos venham a utilizar a rede de forma indiscriminada.

A senha, QRcode, arte para publicação nas OBMs, assim como orientações de acesso estarão disponíveis em manuais no endereço <https://documentoscblmsc.cbm.sc.gov.br/>;

A rede estará disponível apenas onde a OBM contar com link de internet privado diferente do link de internet da rede de governo, pois a navegação na internet é exclusivamente pela internet privada da OBM e sem acesso a rede interna da corporação.

9 PROCEDIMENTO PARA CONEXÃO REDE WIFI CBMSC-WIFI (INTRANET)

9.1 Ubuntu

Autenticação necessária na rede Wi-Fi

Senhas ou chaves de criptografia são necessárias para acessar a rede Wi-Fi "CBMSC-WIFI".

Segurança Wi-Fi: WPA & WPA2 empresas

Autenticação: TLS encapsulado

Identidade anônima:

Domínio:

Certificado de CA: (Nenhum)

Senha de certificado de CA:

☐ Mostrar senhas

☒ Nenhum certificado CA é necessário

Autenticação interna: GTC

Nome de usuário: Seu Usuário LDAP

Senha:

☐ Mostrar senha

Cancelar Conectar

9.2 Android

CBMSC-WIFI

Método EAP: PEAP

Autenticação da Fase 2: GTC

Certificado CA: Não validar

Privacidade: Usar MAC aleatório

Seu Usuário LDAP:

Identidade anônima:

Senha:

☐ Exibir senha

Opções avançadas

Opções simples Conectar

OBSERVAÇÃO: Inserir o seu usuário e a sua senha utilizados para acesso aos demais sistemas do CBMSC. Ativar a opção: "Nenhum Certificado de CA é necessário" e na opção "autenticação interna:" colocar o modo "GTC"

10 CONFIGURAÇÃO DE IPV4 E DNS

Fica estabelecido que todos os computadores, notebooks, celulares, *tablets* e demais dispositivos de uso pessoal ao se conectarem à rede, independente do meio de acesso, deverão utilizar o serviço de DHCP de forma integral e automática para receber IP e DNS do roteador *gateway* desta rede, ficando proibida a fixação de qualquer dessas configurações de forma manual pelo usuário sem a prévia autorização por parte do gestor da rede.

A utilização de configuração de IP de forma fixa no dispositivo é exclusiva apenas para equipamentos de uso coletivo como, por exemplo, impressoras, *smart* TVs e gravadores de imagens de segurança. Devendo sempre ser remetida ao gestor local ou em últimos casos a equipe de redes do setor de tecnologia da informação do CBMSC para que seja efetuado o devido cadastro, evitando duplicidade de IP na rede e futuros problemas.

Com exceção da rede *Wifi* para Visitantes, sempre que por algum motivo, ao se conectar a rede do CBMSC o dispositivo receber endereço de rede IP diverso do padrão adotado pela corporação (tem-se como padrão de endereçamento da rede interna as faixas 10.193.0.0/16 e 10.194.0.0/16) o usuário primeiramente deve procurar o técnico responsável pela TI da OBM e caso necessário apoio, abrir uma solicitação via SAU (sau.cbm.sc.gov.br) para que os administradores do setor de redes do CBMSC possam auxiliar na correção do problema.

11 FORNECIMENTO DE EQUIPAMENTOS E MATERIAIS

As unidades administrativas e operacionais do CBMSC devem prever em seus fundos a compra de todos os equipamentos de rede, tais como *Switches*, roteadores, *Access Point*, com as especificações técnicas elaboradas pelo setor de tecnologia da informação do CBMSC, seguindo o que preconiza a Diretriz Nº33 de 02/02/2022 que diz respeito às atribuições da DiTI e das demais Organizações de Bombeiro Militar quanto a coordenação e execução administrativa da rede de dados institucional.

OBSERVAÇÃO: Todas as especificações técnicas dos equipamentos bem como a diretriz de redes estarão disponíveis no endereço <https://documentoscblmsc.cbm.sc.gov.br/> e deverão ser seguidas pelas OBMs para aquisição dos equipamentos compatíveis com o padrão CBMSC.

12 VPN (VIRTUAL PRIVATE NETWORK)

Atualmente o CBMSC conta com o serviço de VPN, onde o usuário através de seu celular ou computador consegue acessar os sistemas do Bombeiro através de sua própria internet. Estão liberados a instalar e acessar a VPN os usuários que possuem dispositivos com Android, MacOS, Linux Ubuntu e Iphone.

A VPN trata-se de um túnel direto entre o dispositivo do usuário e a rede interna do bombeiro, dessa forma, não está autorizada a utilização da mesma no Sistema Operacional Windows devido aos riscos com segurança. Vale ressaltar que uma vez conectado a VPN do CBMSC, para os sistemas, é como se o usuário estivesse dentro de um quartel, desta forma deve se atentar quanto a utilização da rede e evitar configurar a VPN em máquinas suspeitas de estarem infectadas.

O serviço de VPN pode ser instalado e configurado através do link <https://minhavpn.cbm.sc.gov.br/>. O passo a passo de instalação para cada Sistema Operacional está disponível também através do link.

OBSERVAÇÃO: Cabe ao Chefe do Setor de tecnologia da informação do CBMSC julgar exceções para utilização de VPN em Sistemas Operacionais diversos dos disponíveis no link <https://minhavpn.cbm.sc.gov.br/>. O solicitante deverá enviar uma solicitação formal para o email ditich@cbm.sc.gov.br informando a necessidade de utilização de outro Sistema Operacional, nome completo, lotação, conforme PAP do Windows.

13 OUTRAS DISPOSIÇÕES

Casos não previstos neste manual devem ser remetidos à Chefia da DiTI para análise.

