PLANO DE CONTINGÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO NO ÂMBITO DO CBMSC

Information And Communication Technology Contingency Plan Within The CBMSC

Carlos Alberto Sousa
Bacharel em Sistemas de Informação pela Universidade Federal de Santa Catarina (UFSC).
2º Sargento do Corpo de Bombeiros Militar de Santa Catarina (CBMSC).
E-mail: sousa@cbm.sc.gov.br

Paulo Cesar Souza
Mestre em Perícias Criminais Ambientais pela Universidade Federal de Santa Catarina (UFSC).
Subtenente da Polícia Militar de Santa Catarina (PMSC).
E-mail: pi4nane@gmail.com

RESUMO
As estruturas de Tecnologia da Informação e Comunicação (TIC) têm se mostrado parte do cotidiano coletivo e na esfera da segurança pública não poderia ser diferente. Com a crescente popularização das ferramentas informatizadas vêm os riscos associados à exploração das vulnerabilidades existentes, resultando em ataques cibernéticos cada dia mais frequentes. O objetivo geral deste trabalho é a proposição de um plano de contingência adequado à realidade de TIC do CBMSC. Para tanto, lançou-se mão de uma pesquisa aplicada, em face a sua implementação; qualitativa, dada sua relação dinâmica entre mundo real e os sujeitos envolvidos no processo que não pode ser traduzido em números; exploratória, já que envolve levantamento bibliográfico, explicitação do problema e análise de casos correlatos; uma pesquisa bibliográfica já que foi elaborada a partir de material já publicado. Como resultado, constatou-se que a necessidade de se estar preparado perante riscos e vulnerabilidades é essencial para uma resposta adequada às adversidades e que, apesar de se ter caracterizando um plano de contingência, é de suma importância detalhar os planos de ação, prever outros cenários de risco e conscientizar as lideranças.

Palavras-Chave: Plano de Contingência; Tecnologia da Informação e Comunicação; Corpo de Bombeiros Militar de Santa Catarina.

ABSTRACT

The structures of Information and Communication Technology - ICT - have been shown to be part of the collective daily life and in the sphere of public security it could not be different. With the increasing popularity of computerized tools, there are risks associated with the exploitation of existing vulnerabilities, resulting in cyber attacks that are more and more frequent. The general objective of this paper is to propose a contingency plan appropriate to the CBMSC's ICT reality. For this purpose, applied research was used in view of its implementation; qualitative, given its dynamic relationship between the real world and the subjects involved in the process, which cannot be translated into numbers; exploratory, as it involves a bibliographic survey, explanation of the problem and analysis of related cases; a bibliographical research since it was elaborated from material already published. As a result, it was found that the need to be prepared for risks and vulnerabilities is essential for an

adequate response to adversities and that, despite having characterized a contingency plan, it is of paramount importance to detail the action plans, foreseeing others risk scenarios and raise awareness among leaders.

Keywords: Contingency plan; Information and communication technology; Military Firefighters of Santa Catarina.

1 INTRODUÇÃO

A necessidade de prevenção direcionada às atividades de emergência e urgência demandadas pelo Corpo de Bombeiros Militar deve sempre ser motivo de estudo acadêmico e aplicabilidade prática no que tange a operacionalidade das ações preventivas. Masato (2006) alega que, a cada um real aplicado em prevenção, estes equivalem, em média para a época, entre vinte e cinco reais e trinta reais em obras de reconstrução após o evento. Em se tratando de Tecnologias aplicadas em estruturas e suportes emergenciais, devemos atentar para o prejuízo gerado com a perda de informações que este evento danoso possa causar, o que acaba interrompendo por dias serviços essenciais e de pronto atendimento a população, acarretando prejuízo não só material, mas acima de tudo social.

A prevenção aplicada aos Riscos Tecnológicos e de Comunicação são fundamentais em uma sociedade cada vez mais voltada para o meio digital, onde o acesso facilitado a informações é ferramenta essencial para o desenvolvimento da cidadania. Embora pareça paradoxal, devemos entender que o acesso facilitado nem sempre envolve ferramentas facilmente desenvolvidas. O contrário muitas vezes é verdadeiro, pois a simplicidade de acesso gerada ao usuário envolve uma infinidade de tarefas e permissões, validações de segurança e autorizações de usos, que demandam muito tempo em atividade laboral voltada para o desenvolvimento.

Problemas de indisponibilidade dos sistemas por fenômeno meteorológico, má utilização por parte do usuário, falta de documentação ou quebra da cadeia de suprimentos, quando não puderem ser evitados, precisam ao menos ser previstos. A fragilidade dos sistemas informatizados frente a essas adversidades precisa ser minimizada.

A Divisão de TI do Corpo de Bombeiros Militar de Santa Catarina não está livre destes problemas e, portanto, é fundamental buscar alternativas de prevenção, mitigação, preparação, resposta e recuperação a esses eventos.

Este artigo, então, busca estabelecer uma proposta de contingenciamento voltado às Tecnologias de Informação e Comunicação, com o intuito de reduzir significativamente os danos causados por desastres físicos (ditos naturais) como pelos desastres sociais causados (de forma intencional ou não), pelos usuários diretos e indiretos das infraestruturas de dados operados pelo CBMSC.

Para alcançar aquilo que se propõe, tem-se como objetivo geral a proposição de um plano de contingência adequado à realidade de TIC do CBMSC. Para atingir esse objetivo serão estabelecidos os seguintes objetivos específicos:

a. Caracterizar o que é um plano de contingência - PlanCon;
b. Organizar de forma clara e objetiva a estrutura de TIC de CBMSC enquanto serviços essenciais;
c. Propor a criação de um plano de contingência na área de TIC voltado aos serviços essenciais do CBMSC.

1.1 MATERIAIS E MÉTODOS

De acordo com Silva e Menezes (2001), as formas clássicas de classificação das pesquisas são de acordo com os pontos de vista da sua natureza, da forma de abordagem do problema, de seus objetivos e dos procedimentos técnicos. Este estudo, portanto, trata de pesquisa aplicada, em face a sua implementação; qualitativa, dada sua relação dinâmica entre mundo real e os sujeitos envolvidos no processo, um vínculo indissociável que não pode ser traduzido em números; exploratória, já que envolve levantamento bibliográfico, explicitação do problema e análise de exemplos de casos correlatos; pesquisa bibliográfica já que foi elaborada a partir de material já publicado.

2 CONCEITOS PRELIMINARES

A fim de facilitar a compreensão dos apontamentos que seguem, é importante relembrar alguns conceitos, a saber:

2.1 RISCO

De acordo com o SC Resiliente - guia conceitual (SANTA CATARINA; FAPESC; UFSC, 2019), *Risco* é a probabilidade de que a população e seus bens materiais sofram consequências prejudiciais ou perdas (mortes, lesões, danos em propriedades, interrupção de atividade econômica, etc.) diante do impacto de ameaças naturais ou antropogênicas (consequência das atividades humanas). Risco, então, é uma possibilidade de dano, não significa desastre. O desastre é um risco que se concretizou, sendo que sua intensidade depende de condições de vulnerabilidade em interação com as ameaças.

Dentre as categorias do risco, aquela relacionada ao risco tecnológico é o mais presente no que tange aos processos geradores produzidos pelas indústrias (SOUZA, 2019).

O risco tecnológico está relacionado principalmente com os processos produtivos e atividade industrial. A evolução na cadeia produtiva das indústrias na era da modernização não foi acompanhada pela evolução do controle dos riscos envolvidos nesse processo. Segundo Eagler (1996), a categoria de risco que envolve o risco tecnológico está relacionada à potencial ocorrência de eventos danosos a curto, médio e longo prazo, consequências das decisões de investimento do setor produtivo. Diz ainda que o critério metodológico de avaliação deste risco deve focar, entre outros, na gestão institucional e ambiental das empresas.

Ainda de acordo com Souza (2019), o controle se dá através de procedimentos/protocolos de ações, mão de obra especializada e plano de emergência desenvolvido especificamente para cada planta industrial.

2.2 CONTINGÊNCIA

De acordo com o SC Resiliente - Guia Conceitual (SANTA CATARINA; FAPESC; UFSC, 2019), *Contingência é* a incerteza sobre algo que poderá ou não vir a acontecer. O plano de contingência, portanto, é um planejamento visando a preparação de determinada organização em relação às medidas a serem tomadas para mitigar danos caso algum risco ou desastre específico aconteça. Em complemento, é uma situação de risco com potencial de ocorrer, inerente às atividades, os serviços e equipamentos, e que ocorrendo se transformará em uma situação de emergência. Diz respeito a uma eventualidade; possibilidade de ocorrer (IFRS, 2019).

2.3 TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - TIC

Já no tocante a Tecnologia da Informação e Comunicação (TIC), Oliveira, 2015 conceitua da seguinte forma:

> TIC consistem em TI bem como quaisquer formas de transmissão de informações e correspondem a todas as tecnologias que interferem e mediam os processos informacionais e comunicativos dos seres. Ainda, podem ser entendidas como um conjunto de recursos tecnológicos integrados entre si, que proporcionam por meio das funções de software e telecomunicações, a automação e comunicação dos processos de negócios, da pesquisa científica e de ensino e aprendizagem. (OLIVEIRA, 2015)

Marcondes (2020), por sua vez, afirma que a TI refere também ao departamento da empresa responsável pela gestão das tecnologias utilizadas

para transmitir, receber, armazenar, compartilhar ou processar dados e informações da organização.

No cenário em que está inserido o CBMSC, as atividades de tecnologia da informação e comunicação estão concentradas na Divisão de Tecnologia da Informação - DiTI, uma das frações da Diretoria de Logística e Finanças - DLF.

2.4 PLANO DE CONTINGÊNCIA

A referência estadual para Planos de Contingência é a Defesa Civil do Estado de Santa Catarina, que defende que

> [...] o Plano de Contingência pode ser definido como o documento que registra o planejamento elaborado a partir do estudo de um ou mais cenários de risco de desastre e estabelece os procedimentos para ações de monitoramento, de alerta e alarme, assim como ações de preparação e resposta ao evento adverso" (BRASIL, 2018).

De acordo com o site da Defesa Civil de Santa Catarina (2013), a estrutura do Plano de Contingência é composta por Introdução, Finalidade, Situação e Pressupostos, Operações, Atribuição de Responsabilidades, Administração e Logística, Relacionamento com outros Planos, Instruções para Uso do Plano.

A elaboração de um plano com antecedência ao evento adverso facilita as atividades de preparação e também otimiza as atividades de resposta ao desastre. Pode ele ser genérico, abordando a estrutura de resposta a qualquer desastre em uma área, ou específico, focalizando um cenário em especial.

No trabalho em tela será tratado de forma específica, para evento adverso sobre a área de TIC do Corpo de Bombeiros Militar de Santa Catarina.

3 TIC NO CBMSC

Segundo a LEI Nº 7.783, de 28 de junho de 1989, em seu Art. 10 , são considerados serviços ou atividades essenciais, dentre outros, telecomunicações (VII) e processamento de dados ligados a serviços essenciais (IX). No âmbito do CBMSC esses serviços são mantidos pela já mencionada Divisão de Tecnologia da Informação e pulverizados ao longo Estado na forma de Telefonia Analógica e Digital (VoIP); Rádio Analógico e Digital (RoIP); Redes de Internet em suas modalidades (Cabeada, Wireless e VPN); e servidores de processamento de dados.

O aparato tecnológico citado pode ser percebido no cotidiano

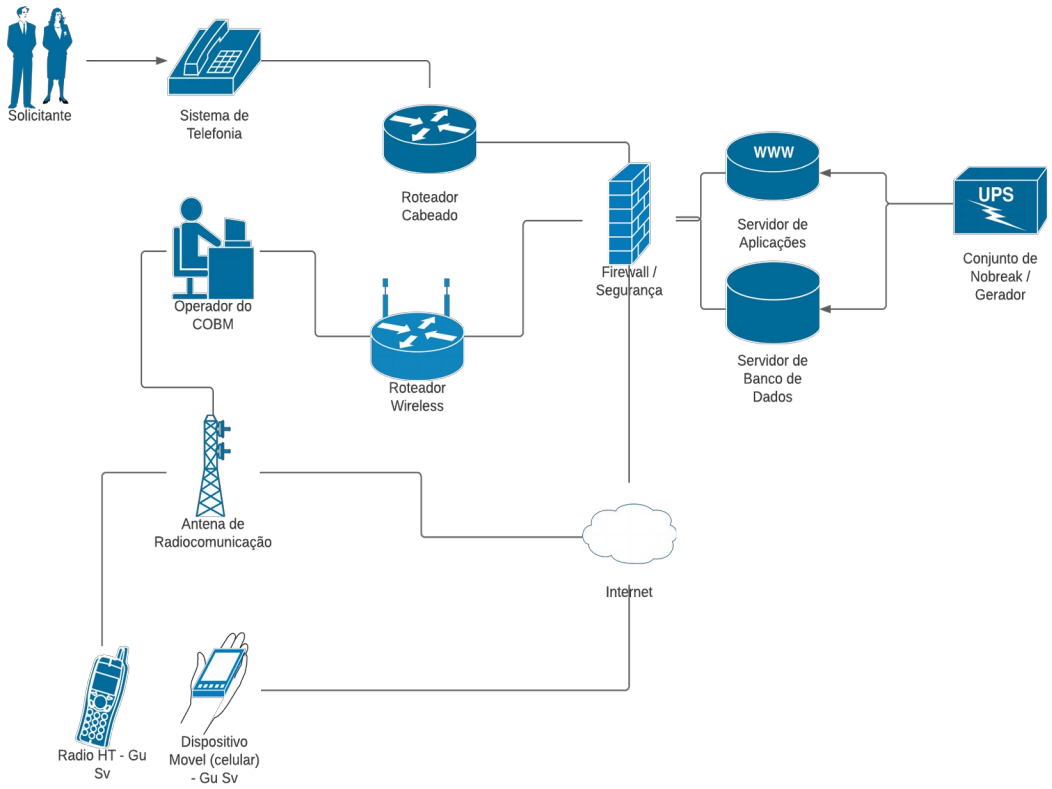
administrativo em vários níveis, desde o contato telefônico entre duas Unidades com telefonia VoIP até a complexa gestão de recursos, quer seja pessoal ou financeiro, através dos Sistemas Gerenciador de Recursos Humanos ou Sistema de Apoio a Gestão (SAG) ou ainda no compartilhamento de documentos de forma segura totalmente em meio digital reduzindo o consumo de papel.

Da mesma forma, todo o ciclo operacional (CBMSC, 2017) está contemplado, pois quando as fases preventiva e estrutural, efetuadas através dos sistemas de segurança contra incêndio (e-SCI), por exemplo, foram vencidas e inicia-se o atendimento da chamada do cidadão, a integração entre software de atendimento de emergências (*e193*) e telefonia já inicia o preenchimento das informações que serão encaminhadas via dispositivo móvel (celular ou tablet) para o trem de socorro. Durante o atendimento, a comunicação via rádio é viabilizada não só pelos equipamentos nas mãos do bombeiro combatente, mas também pelas repetidoras de rádio e servidores de gravação que resguardam a instituição juridicamente. Se essa mesma linha for seguida, os relatórios de atendimento, certidões de ocorrência, atividades periciais e estatísticas para suporte à tomada de decisão serão encontrados vinculando tecnologia e atividade fim em prol da sociedade.

Para o cumprimento da missão de suportar toda a atividade administrativa e operacional do corpo de bombeiros, esses serviços são providos por uma infraestrutura robusta composta por ativos de rede elétrica, rede de dados, climatização e servidores de processamento de dados.

Na Figura 1 são representados os principais serviços de competência da Divisão de TI do CBMSC, essenciais ao funcionamento do serviço administrativo e operacional da instituição.

Figura 1- Serviços de Telefonia, Rádio, Transmissão e Processamento de Dados



Fonte: do autor (2021).

Percebe-se aqui o envolvimento de diversas áreas especializadas, tais como telefonia digital e analógica, rede física de comunicação, rede lógica de comunicação, rede de energia elétrica, mecânica, infraestrutura de servidores e desenvolvimento de software.

4 MATERIAIS E MÉTODOS

De acordo com Silva e Menezes (2001), as formas clássicas de classificação das pesquisas são de acordo com os pontos de vista da sua natureza, da forma de abordagem do problema, de seus objetivos e dos procedimentos técnicos. Para obter os resultados e respostas acerca da problematização apresentada, este estudo, portanto, trata de pesquisa aplicada, em face a sua implementação; qualitativa, dada sua relação dinâmica entre mundo real e os sujeitos envolvidos no processo, um vínculo indissociável que não pode ser traduzido em números; exploratória, já que envolve levantamento bibliográfico, explicitação do problema e análise de exemplos de casos correlatos; pesquisa bibliográfica já que foi elaborada a partir de material já publicado.

5 PLANO DE CONTINGÊNCIA DE TIC/CBMSC

Conforme visto, a estrutura do Plano de Contingência é composta por Introdução, Finalidade, Situação e Pressupostos, Operações, Atribuição de Responsabilidades, Administração e Logística, Relacionamento com Outros Planos e Instruções para Uso do Plano. No caso da área de tecnologia, desdobrar-se-á da forma que se segue.

5.1 INTRODUÇÃO

O Plano de Contingência de Tecnologia da Informação (PlanCon/TI) - para suspensão de serviços de TIC da Divisão de Tecnologia da Informação (DiTI) do CBMSC estabelece os procedimentos a serem adotados pelos centros envolvidos direta ou indiretamente na resposta a eventos desta natureza.

5.2 FINALIDADE

Preparar os Centros envolvidos para dar uma resposta mais efetiva quando da ocorrência de eventos que comprometam o correto funcionamento das áreas de TIC.

5.3 SITUAÇÃO E PRESSUPOSTOS

O perfeito funcionamento das partes é essencial para que o todo o sistema seja efetivo e, portanto, os riscos precisam ser gerenciados de modo a mitigar os danos produzidos por quaisquer situações adversas que representem riscos ao sistema.

5.3.1 Cenário de Risco

O Cenário de Risco ao funcionamento das atividades consiste na indisponibilidade ou inacessibilidade dos sistemas.

Os pontos sensíveis que representam maior vulnerabilidade ao sistema estão descritos na Tabela 1.

Quadro 1 - Vulnerabilidades e Risco às Operações de TIC/CBMSC

Vulnerabilidade	Risco
Dependência de Energia Elétrica da Concessionária	Falta de energia para manter os equipamentos funcionando

Dependência de rede de dados da Rede Governo	Indisponibilidade dos sistemas
Climatizadores de conforto	Mau funcionamento por uso inadequado
Sensibilidade de Hardware	Baixa de equipamentos e, por conseguinte, indisponibilidade dos sistemas
Sistemas acessíveis pela rede alheia a Rede de Governo (internet)	Ataques cibernéticos

Fonte: do autor (2021).

5.4 OPERAÇÕES

O PlanCon/TI será ativado sempre que forem constatadas as condições e pressupostos que caracterizam um dos cenários de risco previstos, seja pela evolução das informações monitoradas, pela ocorrência do evento ou pela dimensão do impacto, em especial:

- Quando os sistemas de monitoramento[1] reportarem interrupção do fornecimento de energia elétrica pela concessionária local (CELESC) conforme definido pelo Centro de Infraestrutura;
- Quando os sistemas de monitoramento reportarem falha de comunicação com o link de dados principal (rede CIASC), conforme definido pelo Centro de Processamento de Dados e Redes;
- Quando os sistemas de monitoramento reportarem temperatura do(s) data center(s) for superior ao limite aceitável, conforme definido pelo Centro de Processamento de Dados e Redes;
- Quando os sistemas de monitoramento reportarem falha de comunicação com algum dos equipamentos ou serviços essenciais, conforme definido pelo Centro de Desenvolvimento de Software.

5.4.1 Procedimentos Para Ativação

Após a decisão formal de ativar o Plano, as seguintes medidas serão desencadeadas:

- A autoridade responsável acionará o Chefe da DiTI e o(s) Chefe(s) do(s) Centro(s) afetado(s) pelo incidente com a compilação das informações que possuir (evento, início, evolução e situação);
- Os Centros mobilizados ativarão os protocolos internos definidos de

1 Sistemas utilizados pelo efetivo da DiTI tais como Nágios (https://www.nagios.org/) e Zabbix (https://www.zabbix.com/)

acordo com os respectivos planos de ação.

5.4.2 Desmobilização

A desmobilização será feita de forma organizada e planejada, priorizando os recursos externos e mais impactados nas primeiras operações. Deverá ordenar a transição da reabilitação de cenários para a restabelecimento dos sistemas sem que haja interrupção no acesso do usuário sempre que possível.

O PlanCon/TI será desmobilizado sempre que forem constatadas as condições e pressupostos que descaracterizam um dos cenários de risco previstos, seja pela evolução das informações monitoradas, pela não confirmação da ocorrência do evento ou pela dimensão do impacto, em especial:

- Quando os sistemas de monitoramento reportarem restabelecimento do fornecimento de energia elétrica pela concessionária local (CELESC);
- Quando os sistemas de monitoramento reportarem restabelecimento da comunicação com o link de dados principal (rede CIASC);
- Quando os sistemas de monitoramento reportarem temperatura do(s) data center(s) dentro do limite aceitável;
- Quando os sistemas de monitoramento reportarem normalidade na comunicação com os equipamentos ou serviços essenciais.

Na ocasião da desmobilização, deverá ser confeccionado relatório de atividades a ser encaminhado às chefias de Centro para ações de prevenção e melhoria contínua.

5.5 ATRIBUIÇÃO DE RESPONSABILIDADES

Autoridade para ativação: Tem autoridade para ativar o PlanCon/TI:

a. O Chefe da DiTI ou quem ele determinar que o faça;
b. Quaisquer dos Chefes de Centro da DiTI ou quem eles determinarem que o faça;
c. O Plantão da DiTI.

Autoridade para desmobilização: Tem autoridade para desmobilizar o PlanCon/TI:

a. O Chefe da DiTI ou quem ele determinar que o faça.

5.6 ADMINISTRAÇÃO E LOGÍSTICA

Os recursos disponíveis para intervenção imediata em casos de incidentes são:

- Nobreak e banco de baterias redundantes, operando em paralelo diretamente nas conexões de energia dos equipamentos que possuem fontes redundantes;
- Grupo moto-gerador operando com testes semanais automatizados, com contrato vigente para reabastecimento de diesel e manutenção de suas peças mecânicas;
- Link redundante de fibra ótica para os data centers via quartel do 1º BBM e CEBM através do Morro da Cruz;
- Três condicionadores de ar no data center principal e dois no data center de contingência, todos ligados no sistema de nobreak e gerador;
- Alta Disponibilidade (HA) e/ou replicação de dados intra e entre os data centers, além de sistema de backup e restore orquestrado por aplicação com Tolerância a Faltas (FT) e versionamento de código em plataforma específica;
- Um extintor de incêndio em cada data center.

Quando a automatização destes recursos não permitir o funcionamento imediato, a intervenção deverá ser feita através dos protocolos de acionamento de cada Centro.

5.7 RELACIONAMENTO COM OUTROS PLANOS

As peculiaridades de cada situação adversa ou risco iminente devem ser tratadas de acordo com os planos de ação das respectivas áreas afetas.

No Manual de Gestão de Desastres da Defesa Civil (DEFESA CIVIL, 2013), é visto que o plano é apenas o documento que registra o planejamento (situação futura desejada). No plano devem ser previstas as responsabilidades de cada pessoa, grupo ou organização, as prioridades e as medidas iniciais a serem tomadas e a forma como os recursos serão empregados.

5.8 INSTRUÇÕES PARA USO DO PLANO.

O presente Plano foi estruturado de acordo com os tópicos de

Introdução; Finalidade; Situação e Pressupostos; Operações; Atribuição de Responsabilidades; Administração e Logística e Relacionamento com outros Planos, além de eventuais Anexos.

Assim, foi elaborado para ser aplicado na seguinte área de risco: Indisponibilidade ou inacessibilidade dos sistemas informatizados do CBMSC.

Para sua efetiva aplicação, deverão ser utilizadas as instalações e recursos explicitamente considerados no planejamento e em seus anexos.

6 CONCLUSÃO

Diante do exposto, percebe-se que a necessidade de se estar preparado perante os riscos e vulnerabilidades identificadas, enquanto atividade preventiva, é essencial para uma resposta adequada às adversidades, manutenção, continuidade do negócio e prestação dos serviços.

As situações de desastre e todo o conhecimento decorrente das tragédias servem como base de conhecimento para o aprendizado e embasamento para ações mais acertadas em cada novo enfrentamento.

A enorme seara de analogias que se pode fazer entre mitigação de um impacto físico, ambiental ou tecnológico permite que sejam feitas adaptações entre os métodos adotados em cada uma dessas modalidades para que se encaixe nas demais, proporcionando a interoperatividade e melhoria contínua nos processos.

Embora o trabalho ora exposto tenha alcançado os objetivos específicos caracterizando um plano de contingência, organizando de forma clara e objetiva a estrutura de TIC do CBMSC e propondo a criação de um plano de contingência de TI voltado aos serviços essenciais do CBMSC, não se pode limitar os esforços a apenas um plano adequado a esta realidade.

É de suma importância detalhar os planos de ação dentro dos Centros, nominando cada um dos responsáveis e definindo as respectivas atividades; prever outros cenários de risco, como fenômenos meteorológicos, invasões físicas e cibernéticas, dentre outras; conscientizar as lideranças, pois assim se obtém respaldo e incentivo; mobilizar o efetivo para reforçar o comprometimento de cada elemento, independente do nível técnico ou hierárquico em que se encontre; e acima de tudo treinar a execução.

Somente com treino árduo é que as missões são cumpridas com facilidade.

REFERÊNCIAS

BRASIL. **Lei nº 7783**, de 28 de junho de 1989. Dispõe sobre o exercício do direito de greve, define as atividades essenciais, regula o atendimento das necessidades inadiáveis da comunidade, e dá outras providências. Disponível em http://www.planalto.gov.br/ccivil_03/leis/l7783.HTM. Acesso em: 22 jan. 2021.

BRASIL. Ministério da Integração Nacional. Secretaria Nacional de Proteção e Defesa Civil. **Manual de Planos de Contingência para Desastres de Movimento de Massa**. Vol. 3. Brasília/DF, 2018. Disponível em: https://www.jica.go.jp/brazil/portuguese/office/publications/c8h0vm000001w9k8-att/volume3.pdf. Acesso em: 22 jan. 2021.

CASTRO, Cleber Marques de; PEIXOTO, Maria Naíse de Oliveira; RIO, Gisela Aquino Pires do. Riscos Ambientais e Geografia: conceituações, abordagens e escalas. **Anuário do Instituto de Geociências.** Rio de Janeiro, p. 11-30. 06 dez. 2005.

CBMSC. 7º Batalhão de Bombeiro Militar. **Ciclo Operacional Completo**. 7 BBM. Notícias, 24 jul. 2017. Disponível em: https://7bbm.cbm.sc.gov.br/index.php/noticias/174-ciclo-operacional-completo. Acesso em: 22 jan. 2021.

DEFESA CIVIL DE SANTA CATARINA. **Plano de Contingência**, 2013. Disponível em: https://www.defesacivil.sc.gov.br/plano-de-contingencia-2013. Acesso em: 22 jan. 2021.

EGLER, Cláudio Antonio. Risco Ambiental como Critério de Gestão do Território: uma aplicação à zona costeira brasileira. **Território**, Rio de Janeiro, v. 1, n. 1, p. 31-41, dez. 1996. Disponível em: http://www.laget.eco.br/pdf/01_4_egler.pdf. Acesso em: 22 jan. 2021.

KOBIYAMA, Masato *et al*. **Prevenção de Desastres Naturais**: conceitos básicos. Curitiba: Organic Trading, 2006. 124 p.

MARCONDES, José Sérgio. **Tecnologia da Informação (TI)**: o que é? o que faz? importância. O que é? O que faz? Importância. 2020. Disponível em: https://gestaodesegurancaprivada.com.br/tecnologia-da-informacao-ti-o-que-e-o-que-faz/. Acesso em: 22 jan. 2021.

OLIVEIRA, Cláudio de. TIC'S Na Educação: a utilização das tecnologias da informação e comunicação na aprendizagem do aluno. **Revista Eletrônica**

Pedagogia em Ação, Belo Horizonte, v. 7, n. 1, p. 75-95, dez. 2015. Disponível em: http://periodicos.pucminas.br/index.php/pedagogiacao/article/view/11019. Acesso em: 22 jan. 2021.

SANTA CATARINA. Defesa Civil de Santa Catarina; FAPESC; UFSC. **SC Resiliente: Guia Conceitual**. [Florianópolis]: UFSC; FAPESC; Defesa Civil/SC, 2019. Disponível em https://www.scresiliente.sc.gov.br/download/guia-conceitual/?wpdmdl=570&refresh=60058f03935891610977027. Acesso em 18 jan 2021.

SECRETARIA DE ESTADO DA DEFESA CIVIL DE SANTA CATARINA. **Gestão de Desastres.** Coletânea. SDC, 2014. Disponível em: https://www.defesacivil.sc.gov.br/images/doctos/seminarios/Gestao_de_desastres_baixa.pdf
Acesso em: 22 jan. 2021.

SECRETARIA NACIONAL DE DEFESA CIVIL. **Manual de orientações para produção do plano municipal de contingência - PLAMCON**. Brasília, 2012.

SILVA, E. L da; MENEZES, E. M. **Metodologia da Pesquisa e Elaboração de Dissertação** – 4. ed. rev. atual – Florianópolis: Laboratório de Ensino a Distância da UFSC, 2005.

SOUZA, Paulo Cesar. **Protocolo de Ações no Atendimento de Acidentes com Produtos Perigosos no Estado de Santa Catarina**. 2019. 129 f. Dissertação (Mestrado) - Curso de Geografia, Universidade Federal de Santa Catarina, Florianópolis, 2019.

VIDAL, Vanderlei Vanderlino. **Cromatografia na perícia de incêndios**: técnicas para detecção de agentes acelerantes. 2007. 66 f. Monografia (Especialização) - Curso de Segurança Pública, Universidade do Sul de Santa Catarina, Florianópolis, 2007. Disponível em: https://biblioteca.cbm.sc.gov.br/biblioteca/index.php/component/docman/doc_download/34. Acesso em: 22 jan. 2021.