ESCOLA DE GUERRA NAVAL

CC (T) Christina Elisabeth Koppke

RECUPERAÇÃO DE ATAQUES CIBERNÉTICOS: PROCEDIMENTOS E TECNOLOGIA

Rio de Janeiro

2022

CC (T) Christina Elisabeth Koppke

RECUPERAÇÃO DE ATAQUES CIBERNÉTICOS:
PROCEDIMENTOS E TECNOLOGIA

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior.

Orientador: CF (FN) Salvador Mota Júnior

Rio de Janeiro

Escola de Guerra Naval

2022

RESUMO

Os avanços tecnológicos aumentaram exponencialmente a incidência e os tipos de ciberataques, cada vez mais sofisticados e perigosos, consistindo em potencial ameaça para as Organizações Militares (OM) que hospedam seus sistemas digitais no CD-MB. Estes ataques podem causar sérios prejuízos às OM mantenedoras, como, por exemplo, o sequestro, a destruição ou a exposição dos dados, descredibilizando-as junto aos seus usuários e contribuindo para enfraquecer a imagem da MB perante a sociedade brasileira. Por este motivo, é imperioso que as OM elaborem planos de contingência ou de recuperação de desastre para recompor a integridade e a disponibilidade de seus sistemas digitais, associados a tecnologias atualizadas, confiáveis e seguras em uso no CD-MB, como medidas para neutralizar os ciberataques ou reduzir o impacto de seus efeitos. Assim, a presente pesquisa se propôs a analisar como os requisitos estratégicos para recuperação de sistemas digitais, definidos nas Doutrinas e Normas de TIC da MB, estão implementados pelas OM que hospedam seus SD no CD-MB; e o seu alinhamento com as soluções tecnológicas atualmente em uso naquele Centro de Dados para elevar a resiliência organizacional militar sob exploração ou ataque cibernético. Este trabalho foi alicerçado em pesquisa documental e bibliográfica sobre a elaboração de procedimentos ou planos para recuperação da integridade e disponibilidade de sistemas digitais e sobre uma tecnologia para uso em conjunto com tais procedimentos. Adicionalmente, foi aplicado questionário a uma parcela das OM que hospedam seus sistemas digitais no CD-MB, a fim de analisar seus procedimentos de recuperação. Com base na análise das informações obtidas, esta pesquisa concluiu que um número expressivo de OM da amostra implementou pelo menos um dos requisitos estratégicos para recuperar a integridade e a disponibilidade de seus SD associados à tecnologia implementada no CD-MB e que a maioria das boas práticas para elaboração dos procedimentos de recuperação foi implementada por apenas 50% ou menos das OM. Neste sentido, sugere-se normatizar a elaboração dos procedimentos e a realização de inspeções ou auditorias para verificar a sua conformidade e eficácia.

Palavras-chave: Ataque cibernético. Integridade de sistema digital. Disponibilidade de sistema digital. Plano de contingência. Plano de recuperação de desastre. Continuidade de negócios. Centro de Dados da Marinha.

LISTA DE ABREVIATURAS E SIGLAS

ADMIN	Administrador da Rede Local
APF	Administração Pública Federal
BIA	*Business Impact Analysis*
CD-MB	Centro de Dados da Marinha do Brasil
CTIM	Centro de Tecnologia da Informação da Marinha
CTIR Gov	Centro de Prevenção, Tratamento e Resposta a Incidentes do Governo
DCTIM	Diretoria de Comunicações e Tecnologia da Informação da Marinha
DGMM	Diretoria Geral do Material da Marinha
Eciber-MB	Espaço Cibernético de interesse da Marinha
EMA	Estado-Maior da Armada
MB	Marinha do Brasil
ODS	Órgão de Direção Setorial
OM	Organização Militar
PCN	Plano de Continuidade de Negócios
PLCONT	Plano de Contingência
PRD	Plano de Recuperação de Desastre
RECIM	Rede de Comunicações Integradas da Marinha
RTO	*Recovery Time Objective*
SD	Sistema Digital
Sefti	Secretaria de Fiscalização de Tecnologia da Informação
SGCN	Sistema de Gestão de Continuidade de Negócios
SI	Segurança da Informação
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO

A popularização da Internet alavancou a criação de soluções de Tecnologia da Informação e Comunicação (TIC), para os mais variados propósitos, tornando os indivíduos e as organizações, tanto públicas quanto privadas, cada vez mais dependentes da sua utilização. Estes avanços tecnológicos criaram facilidades para o dia a dia das pessoas e tornaram as informações disponíveis em quase todos os lugares e momentos. Entretanto, a evolução tecnológica tornou os sistemas de informações digitais — ou apenas sistemas digitais (SD) — vulneráveis a ataques cibernéticos cada vez mais sofisticados, perigosos e capazes de causar sérios danos às organizações que os mantém e aos seus usuários. Neste sentido, a adoção de medidas de proteção e recuperação são absolutamente necessárias para neutralizar os ataques cibernéticos ou reduzir o impacto de seus efeitos.

A Marinha do Brasil (MB) possui um Centro de Dados (CD-MB) inserido na estrutura organizacional do Centro de Tecnologia da Informação da Marinha (CTIM), utilizado para hospedar seus sistemas digitais (SD) operativos e os corporativos administrativos. Estes últimos são sistemas utilizados por toda a MB e apoiam os principais processos e atividades das Organizações Militares (OM) mantenedoras e que, portanto, são críticos para o funcionamento da Marinha. As OM mantenedoras são responsáveis por refletir as suas regras de negócios em seus respectivos sistemas digitais, de forma a mantê-los atualizados e aderentes à sua missão. O CD-MB hospeda, opera e mantém um conjunto diversificado de tecnologias, além de uma infraestrutura robusta, resiliente, atualizada e segura, que, somadas, proporcionam alta disponibilidade, confidencialidade, integridade e autenticidade aos sistemas digitais hospedados.

Apesar de os SD usufruírem da robustez tecnológica do CD-MB e do arcabouço empregado pela Marinha para fortalecer a segurança e a proteção do seu espaço cibernético (Eciber-MB), o risco de um ataque que intencione comprometer a integridade e/ou a disponibilidade destes sistemas não é nulo, e, portanto, não pode ser desprezado. Estas ações hostis, abrangendo os contextos de paz/tensão, relativo à Segurança da Informação, e de conflito, relativo à Guerra Cibernética, podem impedir o acesso e a operação dos SD, impossibilitando o seu uso, o que causará danos ao funcionamento da Marinha e enfraquecerá sua imagem perante seus usuários e a sociedade brasileira.

A presente pesquisa se justifica porque medidas de mitigação para reduzir ou neutralizar o impacto de exploração ou ataque cibernético devem ser adotadas pelas OM mantenedoras dos SD hospedados no CD-MB, a fim de restabelecê-los à condição normal de operação e possibilitar a continuidade da entrega de seus serviços. Procedimentos de recuperação documentados em Planos de Contingência (PLCONT) e de Recuperação de Desastre (PRD) podem contribuir de forma bastante significativa na redução do tempo de indisponibilidade dos sistemas e aumentar a resiliência das OM sob exploração ou ataque cibernético.

Perante o exposto, o objetivo desta pesquisa é analisar como os requisitos estratégicos para recuperação de sistemas digitais, definidos nas Doutrinas e Normas de TIC da MB, estão implementados pelas OM mantenedoras de sistemas digitais hospedados no CD-MB; e o seu alinhamento com as soluções tecnológicas atualmente empregadas por aquele Centro de Dados para elevar a resiliência organizacional militar sob exploração ou ataque cibernético.

Para alcançar este objetivo principal, pretende-se responder ao seguinte questionamento: como os requisitos estratégicos de Proteção Cibernética, relacionados à recuperação da disponibilidade de sistemas digitais e definidos nas Doutrinas e Normas de TIC da MB, estão implementados pelas OM mantenedoras de sistemas digitais hospedados no CD-MB; e qual o seu alinhamento com as tecnologias empregadas naquele Centro de Dados, para reduzir o impacto de ataques no curso de uma exploração ou ataque cibernético? Outras questões de estudo foram identificadas, a saber: Como devem ser elaborados os procedimentos de recuperação da disponibilidade de sistemas digitais à luz da bibliografia e das normas técnicas que versam sobre o tema? Qual tecnologia implementada no CD-MB pode ser utilizada em favor da recuperação da disponibilidade dos sistemas digitais por ele hospedados? Existem oportunidades de melhoria nos procedimentos de recuperação adotados pelas OM mantenedoras de sistemas digitais hospedados no CD-MB?

Esta pesquisa é relevante porque Planos de Contingência (PLCONT) e de Recuperação de Desastre (PRD) adequados, completos e atualizados, somados às tecnologias em uso no CD-MB, podem ser bastante eficazes na recomposição de sistemas digitais hospedados naquele Centro de Dados, caso, eventualmente, eles tenham a sua integridade e/ou disponibilidade comprometida por exploração ou ataque cibernético. Estes sistemas digitais requerem alta disponibilidade e, portanto, conhecer as estratégias de recuperação

elaboradas por suas OM mantenedoras permitirá identificar oportunidades de melhoria para elevar a sua eficácia.

A metodologia empregada na presente pesquisa consiste em pesquisa documental nas Doutrinas e Normas de TIC da MB, a fim de identificar os requisitos estratégicos relacionados à recuperação da integridade e da disponibilidade dos SD comprometidos por exploração ou ataque cibernético; pesquisa bibliográfica, para conhecer as melhores práticas na elaboração de procedimentos para recomposição de SD; pesquisa na documentação oficial do fabricante da tecnologia implementada no CD-MB, disponível em seu sítio eletrônico, a qual poderá ser empregada em favor da recuperação da integridade e da disponibilidade de SD. Consiste, ainda, na aplicação de um questionário a oito OM mantenedoras de SD hospedados no CD-MB, formulado com perguntas fechadas e abertas, a fim de coletar dados para analisar seus procedimentos de recuperação à luz dos requisitos estratégicos definidos nas Doutrinas e Normas de TIC da MB e da tecnologia utilizada no CD-MB. O questionário também permitirá analisar se os procedimentos das OM foram elaborados de acordo com as melhores práticas definidas na bibliografia e nas normas técnicas que versam sobre continuidade de negócios.

Para atender ao objetivo proposto, este trabalho foi organizado em quatro capítulos, iniciando pela presente introdução. O capítulo dois aborda a fundamentação teórica, a qual descreve a gestão da continuidade de negócios e sua importância para as organizações; identifica os requisitos estratégicos nas Doutrinas e Normas de TIC da MB para recuperar a integridade e a disponibilidade de SD; descreve as melhores práticas para a elaboração de procedimentos para a recomposição de SD; descreve a importância do *backup* para restaurar a integridade e a disponibilidade de SD; e, por fim, descreve uma tecnologia implementada no CD-MB para favorecer a recomposição dos SD hospedados. O capítulo três apresenta a análise documental e bibliográfica; a análise dos dados obtidos por meio da aplicação do questionário às OM mantenedoras de SD hospedados no CD-MB; e identifica oportunidades de melhoria acerca de seus procedimentos de recuperação. Por fim, o capítulo quatro discorre sobre a conclusão da pesquisa.

2 FUNDAMENTOS TEÓRICOS

Este capítulo descreve a gestão da continuidade de negócios e sua importância na definição de uma estrutura de resposta que permita o funcionamento das organizações quando atingidas por um evento adverso indesejável. Em seguida, são identificados os requisitos estratégicos nas Doutrinas e Normas de TIC da Marinha voltados à elaboração de uma estrutura de resposta e continuidade para recuperar a integridade e a disponibilidade de sistemas digitais que apoiam os principais processos e atividades de negócio das OM. Na sequência, são apresentadas as boas práticas para a elaboração do Plano Contingência (PLCONT) e do Plano de Recuperação de Desastre (PRD) para sistemas digitais; a importância do *backup* para as estratégias de recuperação da integridade e da disponibilidade dos sistemas digitais; e a descrição de uma tecnologia implementada no CD-MB para favorecer a recomposição dos sistemas digitais por ele hospedados.

2.1. Continuidade de Negócios

A permanente evolução e transformação da sociedade moderna requer que as organizações, sejam elas públicas ou privadas, ajustem-se às novas demandas e necessidades decorrentes deste progresso. Dada a sua constante mudança, influenciada pelo ambiente externo em que estão inseridas, as organizações devem estar atentas aos riscos, ameaças e vulnerabilidades, internos ou externos, que possam comprometer a entrega de seus produtos e serviços.

Planejar de forma antecipada as respostas que venham a mitigar estes eventos adversos, aumenta a competitividade e a credibilidade da organização e contribui para fortalecer a sua imagem perante o público que consome seus produtos e serviços. Este processo consiste na continuidade de negócios, e é definido como a “capacidade de uma organização continuar a entrega de produtos ou serviços em um nível aceitável com capacidade predefinida durante uma disrupção” (ABNT, 2020a, p. 2). Disrupção é um evento adverso, previsto ou não, “que causa um desvio não planejado e negativo da expectativa de entrega de produtos e serviços de acordo com os objetivos da organização” (ABNT, 2020a, p. 3).

A partir destes conceitos, é possível concluir que as organizações, as governamentais inclusive, independentemente do seu tamanho, devem se preocupar com a continuidade de negócios, pois a natureza dos eventos adversos podem ser evitáveis ou não.

A estrutura de resposta a uma disrupção deve ser preparada antecipadamente, mediante o conhecimento prévio dos riscos, ameaças e vulnerabilidades que possam impactar o negócio da organização (MARINHO, 2018). Esta estrutura de resposta é fruto de um Sistema de Gestão de Continuidade de Negócios (SGCN) implementado pela organização, cuja finalidade é desenvolver a continuidade de negócios adequada para os impactos que ela pode ou não admitir após uma disrupção, ou seja, prepara a organização para que sua entrega de produtos e serviços não seja interrompida na eventualidade de um evento adverso (ABNT, 2020a). Ainda que a estrutura de resposta admita algum nível de degradação do serviço fornecido, o fato de a sua entrega não ser interrompida aumentará a sua resiliência organizacional e robustecerá a sua reputação e a sua credibilidade (ABNT, 2020a).

Segundo Marinho (2018) e a ABNT (2020b), a gestão da continuidade de negócios de uma organização envolve os seguintes processos:

a) Análise dos riscos, ameaças e vulnerabilidades associados ao negócio, ou seja, à entrega dos produtos e serviços (MARINHO, 2018);

b) Análise de impacto nos negócios (*Business Impact Analysis* — BIA), cujo objetivo é definir os processos críticos da organização e os impactos negativos a eles associados quando comprometidos por um incidente (MARINHO, 2018);

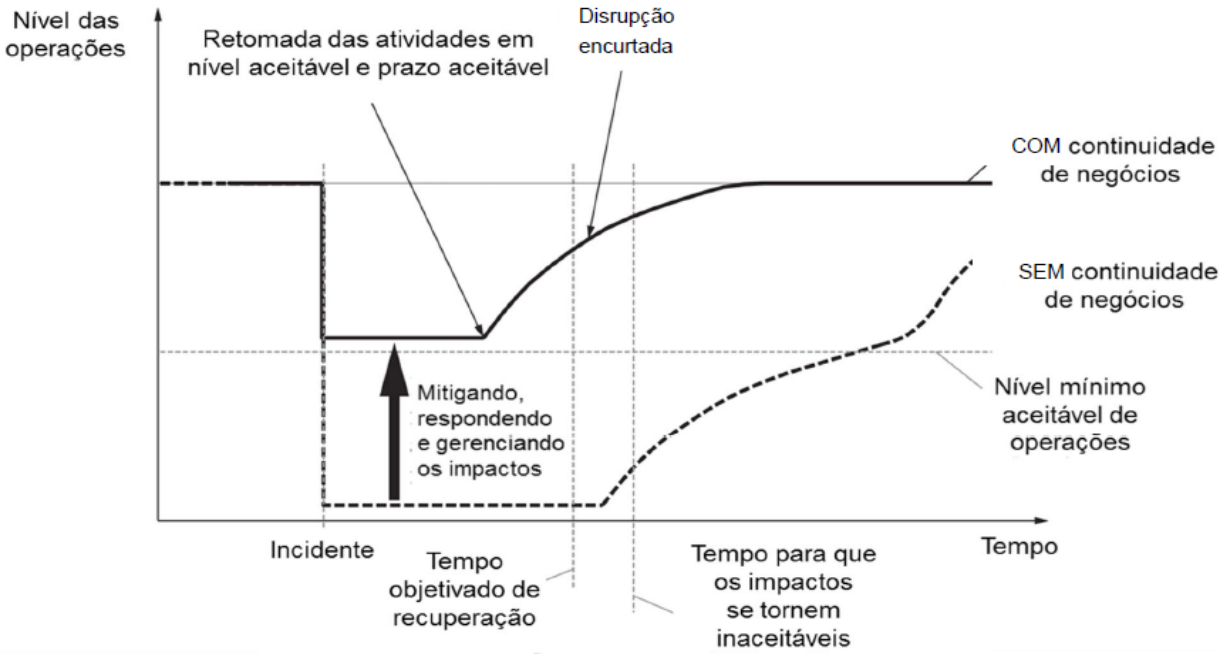
c) Definição das prioridades, capacidades, prazos e estratégias para retomar a entrega de produtos e serviços após uma disrupção (ABNT, 2020b);

d) Definição de uma estrutura de resposta — soluções e planos — para a retomada das atividades dentro do tempo aceitável após uma disrupção (ABNT, 2020b); e

e) Análise e atualização regulares da estrutura de resposta, a fim de garantir a sua eficácia (ABNT, 2020b).

A continuidade de negócios permite à organização reconhecer o que deve ser feito para proteger seus recursos, como, por exemplo, os sistemas digitais, a cadeia de suprimentos e as partes interessadas, antes que a disrupção aconteça (ABNT, 2020a). Desta forma, é possível a criação de uma estrutura de resposta eficaz que mantenha a organização funcionando, ainda que com alguma degradação, sendo um diferencial competitivo em relação aos seus concorrentes (MARINHO, 2018). A Figura 1 ilustra a eficácia da gestão da continuidade de negócios na mitigação de impactos em face de um evento adverso inopinado.

Figura 1 — Ilustração da gestão da continuidade de negócios sendo eficaz diante de uma disrupção súbita



Fonte: ABNT, 2020b, p. xiv.

A análise de riscos, ameaças e vulnerabilidades e a análise de impacto nos negócios (BIA) são processos importantes da gestão da continuidade de negócios, pois o resultado destas análises permitirá a preparação antecipada de estratégias de mitigação como resposta às disrupções. De acordo com Marinho (2018), ameaças são condições externas à organização, e que, normalmente, não podem ser controladas, como, por exemplo, uma inundação ou uma pandemia. As ameaças podem ser identificadas, mas estão fora do controle da organização. As vulnerabilidades ou fraquezas são condições internas à organização, devendo ser identificadas, tratadas e eliminadas, sempre que possível (MARINHO, 2018). Os riscos podem ser externos ou internos à organização, são percebidos pela probabilidade de sua ocorrência e podem ser mitigados em relação às vulnerabilidades ou ao impacto que provocam quando se concretizam (MARINHO, 2018). Já um BIA evidenciará os custos tangíveis e intangíveis que a interrupção de um processo crítico terá para a organização (MARINHO, 2018).

Uma vez concluída a análise de riscos, ameaças e vulnerabilidades e a análise de impacto nos negócios (BIA), a organização poderá preparar a sua estrutura de resposta à disrupção. Segundo Marinho (2018), a estrutura de resposta pode abarcar soluções alternativas e temporárias, definidas em um Plano de Contingência, as quais poderão ser

empregadas quando ocorrerem eventos que interrompam as atividades normais da organização, permitindo que a mesma continue funcionando. A estrutura de resposta deve ser suportada por planos e procedimentos de continuidade de negócios que visem ao emprego de soluções para retomar as atividades da organização dentro de um limite de tempo aceitável (ABNT, 2020b). Marinho (2018) sugere que a organização elabore um Plano de Recuperação de Desastre (PRD), cuja finalidade é documentar como deve ocorrer a recuperação de ativos, como, por exemplo, os sistemas digitais, que suportam os processos e as atividades críticos para o funcionamento da organização. A criticidade está diretamente relacionada ao tempo de tolerância da indisponibilidade do ativo sem que acarrete prejuízos significativos (MARINHO, 2018).

No contexto das organizações militares (OM) da MB, a preparação antecipada de estratégias que visem à continuidade da entrega de seus serviços durante uma disrupção é fator de sucesso, e demonstra qualidade de gestão e resiliência organizacional. A gestão de riscos prevista no Programa Netuno[1], e executada pelas OM, permite o planejamento de respostas adequadas para a redução das ameaças, o monitoramento e o controle dos riscos. A grande maioria das OM tem seus processos e atividades de negócio apoiados por sistemas digitais, tornando-as cada vez mais dependentes de TIC. Logo, é importante que as OM identifiquem os riscos associados à TIC, para o planejamento de uma estrutura de resposta consistente e eficaz voltada à recuperação da integridade e da disponibilidade desses sistemas e da infraestrutura tecnológica empregada na sua operação, caso atingidos por um incidente.

Ainda relativamente à análise de riscos, destacam-se, especialmente, as ameaças cibernéticas, as quais evoluem em uma velocidade exponencialmente mais rápida que as soluções para mitigá-las ou neutralizá-las (MARINHO,2018). Portanto, o risco de ataques cibernéticos é um perigo real, para o qual as OM devem desenvolver uma estrutura de resposta e de continuidade para minimizar os eventuais danos.

1 O Programa Netuno é um processo administrativo que objetiva o aprimoramento da qualidade da gestão das organizações militares da MB; e que abarca a gestão de riscos para identificar, analisar, planejar respostas e controlar os riscos, a fim de aumentar a probabilidade e o impacto de eventos positivos e reduzir os negativos (BRASIL, 2021c).

2.2. Requisitos estratégicos para recuperar a integridade e a disponibilidade de sistemas digitais

Esta seção identifica requisitos estratégicos nas Doutrinas e Normas de TIC da Marinha para elaboração de uma estrutura de resposta e continuidade que vise recuperar a integridade e a disponibilidade de sistemas digitais que apoiam os principais processos e atividades de negócio das OM quando afetados por um evento negativo indesejável.

A Doutrina Cibernética da Marinha — EMA-419 (BRASIL, 2021a) define o Espaço Cibernético de interesse da Marinha (Eciber-MB) da seguinte forma:

> […] o Espaço Cibernético de interesse da MB (ECiber-MB) é uma parcela delimitada do Eciber e formado por ativos de TIC, onde dados e informações digitais são criados, armazenados, modificados, processados e trafegados e conformam o meio onde se atua virtualmente, possuindo caráter administrativo ou militar (BRASIL, 2021a, p. 30).

A partir deste conceito, depreende-se que os sistemas digitais das OM, corporativos ou não, administrativos e operativos, seus dados e todos os equipamentos empregados para a sua operação e disponibilidade, estão inseridos no Eciber-MB, para o qual é implementado um conjunto de ações e medidas que visa garantir a sua integridade, resiliência e continuidade em face de Exploração Cibernética e/ou de Ataque Cibernético.

Apesar de os sistemas digitais usufruírem do arcabouço empregado pela Marinha para salvaguardar o Eciber-MB, o risco de um ataque que intencione comprometer a disponibilidade destes sistemas não é nulo, e, portanto, não pode ser desprezado. Essas ações hostis, abrangendo os contextos de paz/tensão, relativo à Segurança da Informação, e de conflito, relativo à Guerra Cibernética, podem impedir o acesso e a operação dos sistemas digitais. Por este motivo, medidas de mitigação devem ser adotadas, para reduzir o tempo de indisponibilidade do sistema digital e restabelecê-lo à sua condição normal de operação.

De acordo com a Doutrina Cibernética da Marinha — EMA-419 (BRASIL, 2021a), todos os recursos computacionais, tais como dispositivos e serviços, conectados às redes da MB são alvos em potencial de Exploração Cibernética[2] e/ou de Ataque Cibernético[3]. Nas

2 Exploração Cibernética é uma atividade de levantamento de dados e informações para conhecimento da conformação da estrutura do Eciber objetivado, a fim de obter facilidades em um eventual Ataque Cibernético (BRASIL, 2021a).

3 Ataque Cibernético pode ser definido como um “conjunto de atividades com características ofensivas, [...]. Tais atividades compreendem interromper, negar, degradar, corromper ou destruir informações no Eciber de interesse”(BRASIL, 2021a, p.55).

situações em que um recurso computacional seja colocado fora de serviço por uma ação hostil, contramedidas planejadas deverão ser acionadas, como, por exemplo, os Planos de Contingência, para restabelecer a sua disponibilidade (BRASIL, 2021a). Medidas defensivas passivas (atividade de Proteção Cibernética) devem ser executadas de forma permanente por todas as OM, de acordo com as normas de Segurança da Informação (SI) da MB (BRASIL, 2021a). Estas medidas defensivas passivas visam ao monitoramento contínuo e à análise de atividades no Eciber-MB, para reduzir as vulnerabilidades e negar o acesso ao inimigo, contribuindo para o aumento da resiliência cibernética do Eciber-MB (BRASIL, 2021a). Entretanto, caso ocorra o comprometimento de algum recurso computacional, a Doutrina diz que:

> Para permitir a continuidade das atividades no ECiber-MB após um AtqCiber ou por desastres não intencionais, também compreendem a adoção de técnicas de mitigação de danos por meio da ativação de Planos de Contingência, Planos de Emergência e Planos de Recuperação (detalhados na DGMM-0540) para a recomposição dos sistemas atacados (BRASIL, 2021a, p. 61).

Portanto, estratégias de recuperação documentadas em planos contribuem para o restabelecimento dos sistemas e a redução do tempo em que ficam indisponíveis após um ataque cibernético ou um sinistro não intencional.

A Doutrina de Tecnologia da Informação da Marinha — EMA-416 (BRASIL, 2007) define como requisito básico para a infraestrutura de TI da MB a adoção de soluções de contingência para os sistemas digitais, visando à sua alta disponibilidade, ainda que em situações especiais ou de crise.

A Norma de Tecnologia da Informação da Marinha — DGMM-540 (BRASIL, 2019) prevê a necessidade de um gerenciamento de serviços de TI eficiente e eficaz, de acordo com as melhores práticas, a fim de aumentar a sua disponibilidade e confiabilidade, dentre outros efeitos positivos desejados. O gerenciamento dos serviços de TI deve estar em permanente alinhamento com as necessidades de TI da MB e buscar o aumento da qualidade dos serviços prestados (BRASIL, 2019). O gerenciamento de serviços de TI engloba algumas atividades relacionadas à entrega e suporte dos serviços, dentre elas, o Gerenciamento da Continuidade. Esta atividade tem o objetivo de gerenciar os riscos relacionados aos serviços críticos de TI que possam comprometer a sua disponibilidade, prevendo a recuperação de

tais serviços em uma contingência (BRASIL, 2019). Ainda de acordo com a Norma, o Gerenciamento da Continuidade:

> Procura minimizar o impacto das severas interrupções, garantindo o fornecimento de um nível mínimo de serviço, assegurando assim que os mínimos recursos técnicos (sistemas computacionais, redes, aplicações, telecomunicações, suporte técnico e central de serviços) possam ser recuperados nos tempos necessários e acordados (BRASIL, 2019, p. 27).

Logo, o impacto de um ataque cibernético que provoque a indisponibilidade de sistemas digitais hospedados no CD-MB está sob o guarda-chuva do Gerenciamento da Continuidade, e requer a adoção de uma solução que garanta a sua operação, mesmo com restrições.

Ainda de acordo com a Norma de Tecnologia da Informação da Marinha — DGMM-540 (BRASIL, 2019), os Planos de Contingência (PLCONT) são documentos que têm o objetivo de salvaguardar a plena operação da rede local e a recuperação das informações digitais que venham a ser comprometidas por acidente, desastre ou ataque. Dentre as diretrizes para elaboração do PLCONT, destaca-se a necessidade de descrever as ações e procedimentos de forma objetiva, para que todos os usuários credenciados tenham pleno conhecimento; assim como de ele ser ativado pelo Administrador da Rede Local (ADMIN) anualmente, no mínimo, para fins de treinamento (BRASIL, 2019). Embora a Norma enfatize a necessidade de PLCONT para a rede local, entende-se que este requisito é extensivo aos sistemas digitais críticos, dada a sua importância para a execução de diversas atividades da Marinha.

De acordo com a Política de *Backup* e Recuperação de Informações Digitais para a MB — DCTIMARINST 30-19 (BRASIL, 2021b), o Plano de Contingência (PLCONT) é um documento que relaciona os procedimentos que deverão ser executados pelas OM a fim de restabelecer a disponibilidade de seus serviços de TI. A recuperação de desastre é uma estratégia de recuperação de serviços de TI comprometidos por danos de grave abrangência, e a adoção de uma política de proteção de dados (*backup*) é fundamental para garantir a segurança, proteção, integridade e disponibilidade das informações digitais da MB (BRASIL, 2021b). Neste contexto, a norma diz que o *backup* é fundamental para recuperar os serviços críticos de TI que venham a sofrer disrupções causadas por eventos adversos. Logo, o

PLCONT e o Plano de *Backup*[4] devem estar em conformidade com a gestão de continuidade de negócios das OM (BRASIL, 2021b). Ao definirem o Plano de *Backup,* as OM devem considerar a criticidade das informações digitais para as suas necessidades de negócio, objetivando uma proteção que consiga abranger uma eventual recuperação de desastre (BRASIL, 2021b).

Ao analisar as informações extraídas das Doutrinas e Normas de TIC da Marinha, é possível notar o interesse em relação à adoção de contingências para os sistemas digitais críticos da MB, em razão da necessidade de se reduzir o tempo de indisponibilidade decorrente de disrupção causada por acidentes, desastres ou ataques. A solução de contingência adotada pelas OM deve ter os procedimentos para sua ativação documentada em um Plano de Contingência (PLCONT). Da mesma forma, os procedimentos para recuperação do sistema digital em seu ambiente principal devem estar documentados em um Plano de Recuperação de Desastre (PRD). Portanto, a solução de contingência, o Plano de Contingência (PLCONT) e o Plano de Recuperação são requisitos estratégicos da MB para a recuperação da disponibilidade de sistemas digitais, e devem ser implementados pelas OM como parte da sua estrutura de resposta a eventos adversos, permitindo, assim, a sua continuidade de negócios. A recomposição dos sistemas digitais dentro de uma janela de indisponibilidade aceitável aumentará a credibilidade da OM, fortalecerá a sua imagem e demonstrará a sua resiliência organizacional militar.

É importante destacar a preocupação com a adoção de medidas que visam reduzir o impacto de ataques cibernéticos no âmbito da Administração Pública Federal (APF). O Centro de Prevenção, Tratamento e Resposta a Incidentes do Governo (CTIR Gov) emitiu a recomendação 04/2022, sobre o Plano de Continuidade do Negócio (PCN), o qual ressalta que a manutenção de uma infraestrutura cibernética resiliente, com capacidade de continuar operando mesmo no curso de uma disrupção, requer um PCN (BRASIL, 2022b). O documento orienta que as organizações revisem o seu plano de recuperação de desastre e a sua política de *backup*, tendo em vista se tratarem de instrumentos para a redução do impacto de incidentes cibernéticos e para elevar a resiliência da organização (BRASIL, 2022b). O Tribunal de Contas da União (TCU), por meio da Secretaria de Fiscalização de Tecnologia da Informação (Sefti), programou uma série de auditorias relacionadas à gestão da segurança da

4 Documento que tem o objetivo de identificar as informações digitais que serão protegidas pelo *backup*, assim como os requisitos necessários para manter tais cópias de segurança disponíveis para restauração (BRASIL, 2021b).

informação e da segurança cibernética no âmbito da APF, com o objetivo de estimular os órgãos à prática da boa gestão. Para o corrente ano, estão programadas auditorias para avaliar a capacidade de resposta dos órgãos da APF a incidentes cibernéticos (TCU, 2021).

2.3. Boas práticas para a elaboração de procedimentos de recuperação da integridade e da disponibilidade de sistemas digitais

O propósito desta seção é identificar boas práticas, de acordo com Marinho (2018) e a ABNT (2020b), para elaboração do Plano de Contingência (PLCONT) e do Plano de Recuperação de Desastre (PRD) para sistemas digitais, entendidos como partes integrantes da estrutura de resposta preparada pelas organizações a fim de minimizar os impactos de uma disrupção.

a) A organização deve definir qual será o RTO (*Recovery Time Objective,* ou Objetivo do tempo de recuperação) para o sistema digital, o qual pode ser definido como o período de tempo aceitável entre o início da disrupção que causou a indisponibilidade do sistema e o retorno à sua normalidade de operação. O RTO pode ser entendido também como o tempo de tolerância da disrupção, ou seja, o tempo em que se pode admitir a inoperância do sistema digital sem que isto ocasione prejuízos significativos para a organização. O estabelecimento do RTO pela organização, com o objetivo de retomar suas atividades prioritárias em um nível aceitável, permite a identificação de estratégias de recuperação que reduzam o tempo de indisponibilidade e os impactos decorrentes da disrupção (ABNT, 2020b);

b) A adoção de uma solução de contingência, recurso alternativo e temporário, para o sistema digital, garante a continuidade dos serviços essenciais por ele apoiados durante o período da disrupção. Segundo Marinho (2018), o emprego de soluções alternativas permite que a organização continue funcionando, caso ocorram eventos que interrompam a normalidade de funcionamento do sistema. A solução alternativa visa fornecer resultados aceitáveis por um período de tempo limitado, até o retorno da normalidade operacional (ABNT, 2020b);

c) A organização deve elaborar um Plano de Contingência (PLCONT), para nortear as ações necessárias à ativação da contingência do sistema digital; assim como um Plano de Recuperação de Desastres (PRD), para orientar a recuperação da disponibilidade do sistema digital em seu ambiente principal. A estrutura de resposta da organização a uma eventual

disrupção que venha a comprometer a sua continuidade de negócios deve ser suportada por planos e procedimentos, os quais devem identificar as medidas a serem adotadas para retomar as atividades interrompidas, dentro do tempo objetivado de recuperação (ABNT, 2020b);

d) O Plano de Contingência (PLCONT) e o Plano de Recuperação de Desastres (PRD) devem definir, de forma clara, o seu propósito e escopo. Cada plano de continuidade de negócios da organização deve declarar o seu propósito e o seu escopo, de forma clara e objetiva, a fim de orientar as equipes de trabalho que irão utilizá-lo (ABNT, 2020b);

e) O Plano de Contingência (PLCONT) e o Plano de Recuperação de Desastres (PRD) devem definir todos os recursos necessários para, respectivamente, disponibilizar o sistema digital no ambiente alternativo de contingência e recuperar a integridade e a disponibilidade do sistema digital em seu ambiente principal. Eles devem identificar onde estão localizados tais recursos e como acessá-los (são exemplos de recursos: equipamentos, software, *backup*, documentos, recursos humanos, serviços contratados com terceiros, entre outros). Segundo Marinho (2018), é preciso determinar e preparar antecipadamente os recursos que serão empregados nas estratégias de resposta às disrupções;

f) Os planos de continuidade de negócios devem definir os papéis, as responsabilidades e a hierarquia das equipes de trabalho, de forma clara e objetiva, de acordo com as suas competências (ABNT, 2020b). O PLCONT deve definir, no mínimo, as esquipes de trabalho responsáveis pela ativação do PLCONT e pela declaração ou comunicação da situação de contingência; pela gestão do incidente — para garantir a mobilização das equipes e assegurar que os recursos necessários estejam disponíveis; pela execução dos procedimentos descritos no plano para disponibilizar o sistema digital no ambiente alternativo de contingência; e pela desmobilização da contingência, com atividades de retomada da operação do sistema digital no seu ambiente principal (ABNT, 2020b). O PRD deve definir as equipes de trabalho e as respectivas responsabilidades referentes à execução dos procedimentos para recuperar a disponibilidade do sistema digital em seu ambiente principal (ABNT, 2020b);

g) O Plano de Contingência (PLCONT) e o Plano de Recuperação de Desastres (PRD) devem ser suficientemente detalhados, em relação aos procedimentos (passo a passo) que deverão ser executados pelas equipes de trabalho para disponibilizar o sistema digital no ambiente alternativo de contingência e para desmobilizá-lo, ou seja, para que retorne à

normalidade de operação no seu ambiente principal. Marinho (2018) diz que os planos de continuidade de negócios devem abarcar procedimentos pormenorizados sobre como recuperar as atividades críticas da organização dentro do tempo aceitável. Seguir o passo a passo documentado no plano reduz o risco de falhas e aumenta a eficácia das estratégias de recuperação (MARINHO, 2018);

h) O Plano de Contingência (PLCONT) deve identificar as restrições relacionadas à operação do sistema digital no ambiente alternativo de contingência, caso existam. Segundo Marinho (2018), os procedimentos de operação em regime de contingência devem estar voltados para a melhor resposta possível, mesmo com degradação, pois o principal objetivo deve ser a minimização do tempo de indisponibilidade. O fato de a organização continuar o atendimento aos seus usuários, embora com alguma degradação, aumenta a sua confiabilidade e fortalece a sua imagem (MARINHO, 2018);

i) As equipes de trabalho definidas no PLCONT e no PRD devem receber treinamento regular sobre as ações que deverão empreender, de acordo com seus papéis e responsabilidades previamente definidos, para que os propósitos dos planos sejam eficazmente alcançados. As equipes de trabalho devem receber educação e treinamento sobre seus deveres e responsabilidades, relacionados às respostas a incidentes implementadas pela organização (ABNT, 2020b). As equipes devem ser treinadas regularmente, inclusive quando novos membros se integrarem à estrutura de resposta a incidente (ABNT, 2020b);

j) O Plano de Contingência (PLCONT) e o Plano de Recuperação de Desastres (PRD) devem ser exercitados regularmente, a fim de garantir a eficácia de seus propósitos, em conformidade com as necessidades de negócio da organização. A adoção de um programa de exercícios para os planos e procedimentos de continuidade de negócios da organização permite a validação da sua eficácia, promove a conscientização e o desenvolvimento de competências das equipes de trabalho e assegura que os planos e os procedimentos estejam completos, atualizados e adequados (ABNT, 2020b). A confiabilidade dos planos e dos procedimentos de continuidade de negócios somente pode ser atestada após eles serem exercitados (ABNT, 2020b);

k) Os exercícios do Plano de Contingência (PLCONT) e do Plano de Recuperação de Desastres (PRD) devem ser documentados, com o registro de eventuais falhas nos procedimentos. O objetivo de documentar os exercícios é corrigir os procedimentos

incorretos, desatualizados ou incompletos, para garantir a consecução do propósito dos planos. Um programa de exercícios robusto e realista consegue identificar oportunidades de melhorias, cujos resultados devem ser documentados, para assegurar a prontidão e a eficácia dos planos de continuidade de negócios da organização (ABNT, 2020b); e

l) O Plano de Contingência (PLCONT) e o Plano de Recuperação de Desastres (PRD) devem prever como os dados do sistema digital serão recuperados e atualizados. O *backup* é o instrumento para cópia e restauração de dados, o qual deve ser empregado nas estratégias de recuperação de desastres, consistindo em parte do esforço que a organização deve empreender para recuperar o seu sistema digital (MARINHO, 2018).

2.4. A importância do *backup* para a recomposição da integridade e disponibilidade de sistemas digitais

Qualquer estratégia para a recuperação de um sistema digital que teve a integridade dos seus dados comprometida por um ataque cibernético, e que se tornou indisponível em decorrência do referido ataque, deve estar baseada em uma restauração feita a partir de uma cópia de segurança, ou *backup* (MARINHO, 2018). Toda a estratégia de recuperação deve ser construída a partir do pressuposto de que existe uma cópia íntegra dos dados, apta a ser restaurada, de forma a tornar o sistema digital novamente disponível. Nesse sentido, a realização de *backups* regulares, com retenções apropriadas a cada objetivo de recuperação, é de fundamental importância para tornar um sistema digital novamente íntegro e disponível após uma disrupção causada por um ataque cibernético.

A Política de *Backup* e Recuperação de Informações Digitais para a MB — DCTIMARINST 30-19 (BRASIL, 2021b) define *backup,* ou cópia de segurança, como “o ato de copiar as informações digitais para mídias de armazenamento secundárias, com o objetivo de salvaguardá-las de perdas ou corrupção, permitindo recuperá-las e torná-las novamente íntegras e disponíveis” (BRASIL, 2021b, p.1). A abrangência e a frequência com que os *backups* são produzidos pela organização devem refletir os seus requisitos de negócios, seus requisitos de segurança da informação e a criticidade dos dados para a sua continuidade de operação (ABNT, 2013).

É importante destacar que as cópias de segurança, ou *backup,* devem ser armazenadas em dispositivos de armazenamento específicos para tal finalidade; portanto, estes não devem ser mantidos no mesmo local de origem dos dados salvaguardados (BRASIL,

2021b). O atendimento a esta premissa confere proteção ao *backup,* e é essencial para garantir a eficiência de uma eventual recuperação, pois, um ataque cibernético que vise comprometer a integridade e a disponibilidade dos dados do sistema digital, como o *ransomware*[5]*,* por exemplo, uma vez que tenha tido sucesso no seu intento, comprometerá todos os dados armazenados, inclusive o *backup*. Soluções de contingência para sistemas digitais em ambiente alternativo também podem ter os dados comprometidos no ataque, caso os dados sejam atualizados por meio de replicação — síncrona ou assíncrona.

O Centro de Prevenção, Tratamento e Resposta a Incidentes do Governo — CTIR Gov, emitiu o alerta 06/2022 sobre *Ransomware-as-a-Service AvosLocker* (BRASIL, 2022a)*,* ressaltando a importância da adoção de políticas de proteção de dados para o plano de continuidade de negócios (PCN) das organizações, incluindo um plano de recuperação. Recomenda, ainda, manter cópias dos *backups offline*, ou seja, desconectadas da rede, de forma a impedir o seu acesso por usuários maliciosos. Essas e outras recomendações elencadas no documento têm o objetivo de aumentar a resiliência das organizações em face do *ransomware*.

Dada a importância do *backup* para as estratégias de recuperação dos sistemas digitais, é fundamental assegurar a sua integridade e confiabilidade. Tais requisitos são garantidos por meio dos testes de recuperação, os quais devem ser executados e documentados regularmente (BRASIL, 2021b). Os testes de recuperação são fundamentais para checar se o tempo de recuperação do *backup* está aderente aos requisitos definidos no plano de continuidade de negócios (PCN) da organização (ABNT, 2013).

Como o sistema digital implementa e reflete os requisitos do negócio que apoia, sofrendo manutenções corretivas e evolutivas ao longo de todo o seu ciclo de vida, é imprescindível que as atualizações implementadas no sistema sejam reproduzidas em seus *backups*. Logo, os *backups* devem ser regularmente reavaliados, atualizados e testados para o sucesso das estratégias de recuperação do sistema digital, aumentando, assim, a resiliência organizacional em face de ameaças que possam comprometer a sua integridade e disponibilidade.

---

5 Malware que impede o acesso aos dados armazenados em um equipamento por meio da sua criptografia, e exige pagamento para restabelecer o acesso. O malware, uma vez que tenha obtido acesso ao equipamento, criptografa os dados e informações digitais e exige o pagamento, mediante extorsão, para torná-los novamente disponíveis (LAB, 2022, BRASIL, 2021d).

2.5. Tecnologia implementada no CD-MB para favorecer a recuperação da integridade e disponibilidade dos sistemas digitais

Esta seção se destina a descrever uma tecnologia implementada no Centro de Dados da Marinha do Brasil (CD-MB) e a analisar o seu emprego em benefício das OM clientes do serviço de hospedagem, no que se refere à elaboração de estratégias de recuperação da integridade e disponibilidade dos sistemas digitais manutenidos por estas OM. A descrição da tecnologia está fundamentada na documentação oficial do respectivo fabricante, disponível em seu sítio eletrônico.

A Marinha do Brasil (MB) possui um Centro de Dados[6] (CD-MB), integrado à estrutura organizacional do Centro de Tecnologia da Informação da Marinha (CTIM), para a hospedagem dos sistemas de TIC da MB. Este serviço abarca a hospedagem de sistemas digitais corporativos[7]; sítios intranet e Internet das organizações militares; assim como serviços de TIC que o CTIM opera, mantém e disponibiliza para toda a MB (MARINHA DO BRASIL, 2018).

O CD-MB hospeda, opera e mantém um arcabouço de tecnologias, ancoradas em uma infraestrutura robusta, resiliente, atualizada e segura (MARINHA DO BRASIL, 2008), que, somadas, asseguram alta disponibilidade, confidencialidade, integridade e autenticidade aos sistemas digitais, serviços de TIC e sítios hospedados. As OM clientes do serviço de hospedagem do CD-MB são responsáveis por realizar as manutenções em seus respectivos sistemas digitais, durante todo o seu ciclo de vida, de forma a garantir o atendimento aos requisitos de negócio da OM (BRASIL, 2019).

Para robustecer o serviço de hospedagem, o CD-MB oferece o serviço de cópias de segurança, ou *backup*, cuja finalidade é a proteção dos dados dos sistemas digitais, serviços de TIC e sítios hospedados, garantindo sua recuperação em caso de perdas ou falhas, com o objetivo de restabelecê-los à sua condição de normalidade operacional. Todos os serviços que o CTIM disponibiliza à MB estão detalhadamente discriminados em seu Catálogo de Serviços[8] (MARINHA DO BRASIL, 2008), em que é possível encontrar informações

---

6 Centro de Dados é um conjunto de componentes de alta tecnologia, que operam de forma integrada, fornecendo serviços de processamento e armazenamento em larga escala para uma organização (VERAS, 2009).

7 Sistemas Digitais (SD) Corporativos são "sistemas desenvolvidos para atender a gestão das OM da MB, […], sendo utilizados por toda a MB em função das funcionalidades e regras de negócio. Fazem uso da RECIM e deverão ser hospedados no Centro de Dados da MB" (BRASIL, 2019, p. 128).

8 O Catálogo de Serviços tem como função orientar as OM e os usuários da Rede de Comunicações Integradas da Marinha (RECIM) nos processos de solicitação e uso dos serviços de TIC oferecidos e mantidos pelo CTIM, de acordo com as Normas EMA-416 e DGMM-540 (MARINHA DO BRASIL, 2008).

sobre as características de cada serviço de TIC, seus respectivos públicos-alvo e procedimentos de solicitação.

Ao analisar as informações sobre o serviço de hospedagem de sistemas digitais, constantes no Catálogo de Serviços (MARINHA DO BRASIL, 2008), é possível concluir que este é fundamentado na tecnologia de virtualização[9], com o emprego do software *VMware vSphere*. Os sistemas digitais são executados em máquinas virtuais[9], disponibilizadas pelo CD-MB de acordo com os recursos de computação solicitados pela OM cliente. Já o serviço de cópias de segurança utiliza a tecnologia *Commvault Backup & Recovery*, uma ferramenta de proteção de dados que implementa as cópias de segurança de acordo com a Política de *Backup* e Recuperação de Informações Digitais para a MB — DCTIMARINST 30-19. As OM clientes que desejam ter os dados dos seus sistemas digitais salvaguardados pelo serviço de cópias de segurança devem preencher o Plano de *Backup*, cujo modelo se encontra disponível no Catálogo de Serviços (MARINHA DO BRASIL, 2008). O CD-MB executa os *backups*, de acordo com as informações fornecidas pelas OM clientes no Plano de *Backup*. Este documento é um acordo firmado entre as partes na prestação do serviço; logo, o CD-MB não executa *backup* sem a solicitação expressa e formal da OM cliente mantenedora do sistema digital hospedado.

A tecnologia *Commvault Backup & Recovery*, de acordo com a documentação técnica disponível no sítio Internet do fabricante, *Commvault* (COMMVAULT SYSTEMS, 2021), consiste em uma solução de *backup* e recuperação que visa à proteção dos dados da organização, que podem estar distribuídos em diversas localidades, tendo como principais características: (a) uma única interface *web* personalizável capaz de gerenciar, operar e monitorar as tarefas de *backup* e recuperação; (b) ampla cobertura de objetos a serem protegidos, como arquivos, aplicativos, banco de dados, máquinas virtuais, entre muitos outros; (c) integração com diversos tipos de repositórios de dados, possibilitando que as organizações implementem diferentes estratégias de proteção para seus dados e políticas de retenção apropriadas. A tecnologia possibilita, inclusive, a replicação dos *backups* para um local remoto, contribuindo para as estratégias de recuperação de desastres e continuidade de negócios das organizações; (d) pode ser empregada para proteger as máquinas virtuais

9 A virtualização de servidores consiste no compartilhamento do hardware de um computador físico (processamento, memória e armazenamento) com vários computadores virtuais (ou máquinas virtuais — VM), a fim de permitir o uso mais eficiente e otimizado destes recursos (VMWARE, 2022). O uso da virtualização em um Centro de Dados amplia sua capacidade de oferta de serviços de hospedagem.

VMware vSphere, sendo possível salvaguardar a máquina virtual completa, ou seja, todo o seu conteúdo (sistema operacional, arquivos, aplicação e banco de dados), assim como os componentes individualizados da máquina virtual, consistindo em uma maior granularidade de restauração; e (e) permite o envio de alertas sobre falhas na execução de tarefas para os e-mails dos usuários previamente informados.

A análise das informações sobre a tecnologia *Commvault Backup & Recovery,* a partir dos documentos técnicos do fabricante, permite concluir que ela consiste de uma solução de proteção de dados para uso corporativo, robusta e versátil e que consegue endereçar as diretrizes para operacionalização dos *backup* descritas na Política de *Backup* e Recuperação de Informações Digitais para a MB — DCTIMARINST 30-19 (BRASIL, 2021b). A versatilidade da tecnologia permite a implementação de variadas estratégias de proteção para diferentes propósitos de recuperação. Logo, a tecnologia *Commvault Backup & Recovery*, empregada no serviço de cópias de segurança do CD-MB, pode ser utilizada em favor das OM clientes em suas estratégias de recuperação, de forma a reduzir o tempo de indisponibilidade do sistema digital, tornado-o novamente íntegro e operacional, aumentando a resiliência das OM sob exploração ou ataque cibernético. Contudo, é importante destacar novamente que a definição dos dados a serem protegidos pelo *backup* é de responsabilidade da OM cliente, a qual deve avaliar a criticidade destes dados para as suas necessidades de negócio. O sucesso da estratégia de recuperação elaborada pela OM com o emprego da tecnologia *Commvault Backup & Recovery* é estritamente dependente do conteúdo do *backup*.

3 ANÁLISE DOS DADOS E RESULTADOS DA PESQUISA

O objetivo deste capítulo é analisar as informações obtidas a partir das pesquisas documental e bibliográfica descritas no capítulo anterior, assim como avaliar os dados obtidos por meio da aplicação do questionário do Apêndice A, referente aos procedimentos de recuperação da disponibilidade dos sistemas digitais (SD) hospedados no CD-MB.

3.1. Análise documental e bibliográfica

Conforme os estudos do capítulo anterior, foi possível constatar que, de acordo com as Doutrinas e Normas de TIC da Marinha, a solução de contingência, o Plano de

Contingência (PLCONT) e o Plano de Recuperação de Desastre (PRD) são requisitos estratégicos para se recuperar a integridade e a disponibilidade de sistemas digitais; e devem, portanto, ser implementados pelas OM que hospedam seus SD no CD-MB. A solução de contingência deve ser adotada como medida alternativa e temporária, para que o sistema digital continue operando durante o período da disrupção, e, assim, possa garantir a continuidade dos serviços essenciais por ele apoiados. O PLCONT deve documentar os procedimentos para a ativação da solução de contingência adotada pelas OM; e o PRD deve documentar os procedimentos para a recuperação do SD em seu ambiente principal, neste caso, no CD-MB. Essas medidas mitigadoras têm o propósito de assegurar a continuidade de negócios da OM, ou seja, garantir a prestação dos seus serviços mesmo no curso de uma disrupção causada por eventos adversos, tais como exploração ou ataque cibernético. A capacidade da OM em continuar funcionando, ainda que com algum nível de degradação, demonstra preparo, prontidão e resiliência organizacional militar, contribuindo para o fortalecimento da imagem da Marinha perante a sociedade brasileira.

É desejável que tanto o PLCONT quanto o PRD sejam elaborados de acordo com as melhores práticas identificadas na seção 2.3, no que couber, pois, dessa forma, a eficácia dos planos será robustecida e o tempo de indisponibilidade dos SD será reduzido.

De acordo com a seção 2.4, a execução regular de *backup,* ou cópia de segurança, é essencial para a recomposição de SD que tiveram a integridade dos seus dados comprometida por um ataque cibernético e que, por conseguinte, tornaram-se indisponíveis. Logo, o PLCONT e o PRD devem prever que a restauração dos dados do SD ocorrerá a partir de um *backup* íntegro e confiável, previamente testado, regularmente reavaliado e atualizado e que esteja em conformidade com os propósitos dos planos. Nesse sentido, as OM clientes do CD-MB têm a seu favor a tecnologia *Commvault Backup & Recovery,* solução corporativa de *backup* e recuperação de dados que permite implementar variadas estratégias de proteção para os SD hospedados. O PLCONT e o PRD das OM podem ser elaborados a partir dos tipos de *backup* executados pela tecnologia e disponibilizados pelo CD-MB, com o propósito de reduzir o tempo de indisponibilidade de seus SD.

3.2. Análise dos dados obtidos a partir da aplicação do questionário

O questionário do Apêndice A foi elaborado para as OM mantenedoras de SD hospedados no CD-MB, e tem o propósito de identificar se os procedimentos de

recuperação da integridade e disponibilidade desses SD, eventualmente comprometidos por um ataque cibernético, foram elaborados à luz dos requisitos estratégicos definidos nas Doutrinas e Normas de TIC da MB, quais sejam: a solução de contingência, o Plano de Contingência (PLCONT) e o Plano de Recuperação de Desastres (PRD). O questionário também visa identificar se os procedimentos preveem a utilização da tecnologia *Commvault Backup & Recovery*, empregada no serviço de cópias de segurança do CD-MB; assim como identificar se foram elaborados de acordo com as melhores práticas definidas na bibliografia e normas técnicas sobre a continuidade de negócios. O questionário foi elaborado com perguntas fechadas e abertas, totalizando 22 perguntas, as quais foram respondidas pelas equipes de TI das OM.

Foram selecionadas oito OM mantenedoras de SD hospedados no CD-MB para responder ao questionário. O critério de escolha das OM buscou selecionar aquelas inseridas na estrutura de diferentes Órgãos de Direção Setorial (ODS), pois houve o entendimento de que a diversidade de atividades fins dessas OM, apoiadas por seus respectivos SD, contribuiria para o cumprimento do propósito geral da presente pesquisa.

A análise foi realizada a partir dos dados consolidados de acordo com as respostas das oito OM ao questionário aplicado. Estes dados estão dispostos nos Quadros e Tabelas constantes do Apêndice B, sendo que as Tabelas 1, 3 e 4 relacionam cada pergunta do questionário à quantidade de OM para cada resposta possível. A Tabela 1 do Apêndice B apresenta a quantidade de OM que elaboraram os procedimentos de recuperação de seus SD à luz dos requisitos estratégicos definidos nas Doutrinas e Normas de TIC da MB. A Tabela 3 do Apêndice B apresenta a quantidade de OM que empregam as melhores práticas nos procedimentos de recuperação da integridade e disponibilidade de seus sistemas digitais (SD). A Tabela 4 do Apêndice B apresenta a quantidade de OM que previram a utilização da tecnologia *Commvault Backup & Recovery* em seus procedimentos de recuperação.

Com base nos dados constantes na Tabela 2 do Apêndice B, verifica-se que somente uma das OM participantes da pesquisa não possui solução de contingência, PLCONT e PRD — requisitos estratégicos para a recuperação da integridade e disponibilidade de SD. Também é possível constatar que somente uma OM tem ambos os planos implementados; que 37,5% das OM possuem somente PLCONT; e que 37,5% das OM possuem somente PRD. É importante salientar que o PLCONT e o PRD são planos de continuidade de negócios voltados a propósitos distintos. Na hipótese de um ataque

cibernético que cause a indisponibilidade do SD, a ativação da contingência como solução alternativa e temporária, apoiada pelo PLCONT, irá salvaguardar a continuidade operacional enquanto durar a disrupção. Porém, independentemente de a OM possuir ou não solução de contingência, é essencial a implementação do PRD, uma vez que tal plano de continuidade de negócios objetiva orientar as ações que deverão ser empreendidas para a recomposição do SD em seu ambiente operacional principal. Logo, é desejável que todas as OM que têm seus SD hospedados no CD-MB tenham seus PRD adequadamente documentados; assim como, na medida do possível, também adotem uma solução de contingência. Dessa forma, as OM estarão em conformidade com os requisitos estratégicos definidos nas Doutrinas e Normas de TIC da MB; os riscos de um elevado tempo de indisponibilidade serão minimizados; e a sua resiliência organizacional militar em face de eventos negativos indesejáveis, como as disrupções causadas por ataques cibernéticos, será robustecida.

Ao analisar os dados consolidados na Tabela 3 do Apêndice B, onde cada pergunta está relacionada a uma boa prática na elaboração de planos de continuidade de negócios, observa-se que a maioria dessas recomendações é implementada por apenas 50% ou menos das OM participantes da pesquisa em seus PLCONT e/ou PRD. Alguns desses dados chamam mais atenção em função da criticidade que representam, e serão analisados a seguir.

De acordo com a Tabela 2 do Apêndice B, somente 50% das OM conhecem o RTO (*Recovery Time Objective* ou Objetivo do tempo de recuperação) do seu SD, fato que pode prejudicar a recuperação das atividades impactadas pela sua indisponibilidade, uma vez que:

> Para conseguir a retomada da entrega de produtos e serviços da organização, convém que os procedimentos documentados para retomar cada atividade:
> - atendam ao tempo objetivado de recuperação da atividade que suporta o produto ou serviço; e
> - sejam suficientemente confiáveis (ABNT, 2020b, p. 45).

Logo, o PLCONT e o PRD das OM até podem atingir seus propósitos, atendendo ao requisito da confiabilidade; porém, se o tempo de restabelecimento do SD estiver além do aceitável, a OM poderá ter sérios prejuízos em relação ao seu negócio e à sua imagem. A recomposição do SD deve ocorrer dentro do RTO estabelecido pela organização, para evitar consequências indesejáveis decorrentes da disrupção (IIA, 2008).

Das OM que participaram da pesquisa, 37,5% afirmaram que seus PLCONT e/ou PRD definem de forma clara e objetiva seu propósito e escopo; assim como identificam os recursos necessários para disponibilizar o SD no ambiente alternativo de contingência e para recuperar a disponibilidade do SD no CD-MB (TABELA 3, APÊNDICE B). A maioria das OM portanto, não emprega tais boas práticas, necessárias para orientar as equipes de trabalho que utilizarão os planos e para reduzir a incidência de erros ou falhas na sua execução, de acordo com a ABNT (2020b).

Conforme a Tabela 3 do Apêndice B, apenas 25% das OM indicaram que seus PLCONT e/ou PRD detalham os procedimentos que deverão ser executados pelas suas equipes de trabalho. A implementação dessa boa prática é desejável, pois, segundo Marinho (2018), seguir o passo a passo documentado nos planos, reduz o risco de falhas e o tempo de execução, contribuindo diretamente para que o propósito geral seja atingido de forma eficaz.

Somente 25% das OM responderam que as equipes de trabalho recebem treinamento regular sobre as ações que deverão empreender para disponibilizar o SD no ambiente alternativo de contingência e para recuperar a disponibilidade do SD no CD-MB (TABELA 3, APÊNDICE B). A falta de treinamento das equipes aumenta o risco de falhas na execução dos planos, principalmente quando há trocas entre seus membros. Portanto, é necessário treinar as equipes para que atuem de acordo com as suas responsabilidades previamente definidas e documentadas (ABNT, 2020b).

Em relação à prática de testes/exercícios regulares dos planos de continuidade de negócios, de acordo com o Quadro 1 do Apêndice B, somente 50% das OM indicaram que testam seus planos, sendo que 37,5% das OM realizam testes semestrais, anuais e bienais de seus PLCONT. Já em relação ao PRD, uma OM realiza testes bienais; e outra afirmou que realiza os testes, mas não citou a frequência deles (QUADRO 1, APÊNDICE B). Exercitar os planos de continuidade de negócios é imprescindível para que as organizações validem a sua eficácia, desenvolvam as competências das equipes de trabalho e assegurem que os planos sejam confiáveis, completos, atualizados e adequados (ABNT, 2020b). A frequência dos testes/exercícios e a atualização dos planos devem estar alinhadas com as atualizações e manutenções corretivas e evolutivas do SD. Ainda em relação aos testes/exercícios regulares, todas as OM que possuem PLCONT e/ou PRD afirmaram que não têm a prática de documentá-los para registro de eventuais falhas (QUADRO 1, APÊNDICE B). O objetivo de

documentar os testes/exercícios é corrigir os procedimentos incorretos, desatualizados ou incompletos, e, assim, garantir que o propósito dos planos será alcançado (ABNT, 2020b).

Apenas 50% das OM responderam que seus PLCONT definem como ocorre a desmobilização da contingência (TABELA 3, APÊNDICE B). É importante documentar como deverá ocorrer o retorno à normalidade de operação do SD em seu ambiente principal, principalmente porque nesta mudança será necessária a atualização dos dados do SD. Nesse contexto, o PRD pode contribuir de forma muito positiva e atuar de forma complementar ao PLCONT.

Uma das OM respondentes afirmou já ter tido a experiência de não conseguir a ativação da contingência por falhas em seu PLCONT (TABELA 3, APÊNDICE B). Variados motivos, com ocorrência simultânea inclusive, podem ocasionar a falibilidade do PLCONT. É por esta razão que os testes/exercícios regulares e a respectiva documentação dos resultados são tão importantes. A frequência dos testes contribui para reduzir a possibilidade de falhas (ABNT, 2020b), e ela deve ser estabelecida com critério e de acordo com as mudanças que ocorrem no SD e no seu ambiente operacional.

Todas as OM que afirmaram possuir PLCONT responderam demandar a recuperação de *backup* pelo CD-MB, por meio da tecnologia *Commvault Backup & Recovery,* para ativação da respectiva contingência (TABELA 4, APÊNDICE B). Dentre tais OM, somente uma delas afirmou que o tempo de recuperação do *backup,* acordado com o CD-MB no Plano de *Backup,* não está em conformidade com o RTO definido para o SD (QUADRO 2, APÊNDICE B). Nesse caso, é necessário que a OM compatibilize o RTO do seu SD com o tempo mínimo possível para restauração do *backup*. Tal adequação é possível com a execução de testes periódicos de recuperação do *backup,* em conformidade com as diretrizes da Política de *Backup* e Recuperação de Informações Digitais para a MB — DCTIMARINST 30-19 (BRASIL, 2021b) — e alinhados aos testes/exercícios regulares do PLCONT.

Todas as OM que afirmaram possuir PRD responderam demandar a recuperação de *backup* por meio da tecnologia *Commvault Backup & Recovery,* para recompor a disponibilidade do SD em seu ambiente principal — CD-MB. Dentre estas OM, 2 afirmaram conhecer o RTO de seus SD, e que o tempo de recuperação do *backup* está em consonância com ele (QUADRO 2, APÊNDICE B). Como visto na seção 2.5, a tecnologia *Commvault Backup & Recovery* possibilita a proteção de uma ampla variedade de objetos, permitindo às OM a definição de diferentes

estratégias de recuperação, de acordo com os riscos associados à operação do SD. O sucesso do PLCONT e/ou do PRD das OM é estritamente dependente do conteúdo do *backup;* logo*,* testar os planos com regularidade garante que o conteúdo do *backup* é aderente aos seus propósitos, e assegura que tais planos são eficazes e confiáveis.

Diante dos resultados apresentados, é possível concluir que 87,5% das OM participantes da pesquisa implementaram pelo menos um dos requisitos estratégicos para recuperar a disponibilidade de seus SD, caso sejam comprometidos por um ataque cibernético. O mesmo número de OM utiliza a tecnologia *Commvault Backup & Recovery* para os procedimentos de recuperação de *backup*, documentados em seus PLCONT e/ou PRD. Apesar do resultado satisfatório, existem oportunidades de melhoria acerca dos planos das OM, principalmente em relação à adoção das boas práticas identificadas para a sua elaboração.

4 CONCLUSÃO

Os sistemas digitais operativos e os corporativos administrativos da MB, dada a sua criticidade, são hospedados no CD-MB, ambiente que hospeda, opera e mantém um conjunto de componentes de alta tecnologia que asseguram alta disponibilidade, confidencialidade, integridade e autenticidade a esses SD. Apesar da robustez tecnológica do CD-MB e do arcabouço empregado pela MB para fortalecer a segurança e a proteção do Eciber-MB, os sistemas digitais podem sofrer exploração ou ataques cibernéticos, cada vez mais sofisticados e perigosos, abrangendo tanto o contexto da Segurança da Informação quanto o da Guerra Cibernética. Essas hostilidades podem comprometer a integridade e a disponibilidade dos SD, impossibilitando o seu uso e causando danos à continuidade de negócios das OM que têm seus principais processos e atividades por eles apoiados.

Uma vez que os ciberataques são reconhecidamente uma ameaça factual para os sistemas digitais, é necessário que as OM mantenedoras preparem estratégias de recuperação e continuidade de forma antecipada, a fim de garantir que, uma vez atacados, o tempo da disrupção e a interrupção da operação dos SD sejam os menores possíveis. Ainda que os processos e atividades apoiados pelo SD sofram algum nível de degradação decorrente da disrupção, o fato de o sistema retornar à operação dentro de um limite de tempo aceitável e conhecido aumentará a resiliência organizacional da OM e fortalecerá a sua reputação e a sua credibilidade, uma vez que elas serão minimamente impactadas.

A MB prevê, em suas Doutrinas e Normas de TIC, a necessidade de as OM mantenedoras de SD adotarem uma solução de contingência, em razão da necessidade de redução do tempo de indisponibilidade decorrente de disrupção causada por acidentes, desastres ou ataques. Tal solução deve ser apoiada por um PLCONT, o qual documentará os procedimentos para a ativação da contingência, dentre outras informações relevantes. Adicionalmente, as OM devem desenvolver estratégias que visem recuperar o SD em seu ambiente operacional principal, documentadas em um Plano de Recuperação de Desastre (PRD). Logo, a solução de contingência, o PLCONT e o PRD consistem em requisitos estratégicos estabelecidos pela MB para a recuperação da integridade e da disponibilidade dos SD, e devem ser elementos da gestão de continuidade de negócios das OM mantenedoras para a mitigação de eventos adversos.

A presente pesquisa concluiu que 87,5% das OM da amostra implementaram pelo menos um dos requisitos estratégicos para recuperar a integridade e a disponibilidade de seus SD, caso eles sejam comprometidos por um ataque cibernético. É um número bastante satisfatório, dada a relevância e o número de usuários dos SD manutenidos pelas OM. No entanto, 37,5% das OM possuem somente o PLCONT; e 37,5% das OM possuem somente o PRD. Como esses planos de continuidade de negócios são voltados a finalidades diversas, é fundamental que todas as OM implementem o PRD, para nortear as ações a serem empreendidas para a recomposição do SD em seu ambiente operacional principal. A solução de contingência apoiada pelo PLCONT é importante, mas é alternativa e temporária, enquanto durar a disrupção.

O CD-MB disponibiliza o serviço de cópias de segurança, ou *backup,* para as OM mantenedoras de SD hospedados*,* cuja finalidade é a proteção dos dados, para garantir a sua recuperação em caso de perdas ou falhas. As estratégias de recuperação das OM devem ser construídas a partir do pressuposto de que existe uma cópia íntegra e atualizada dos dados, apta a ser restaurada, de forma a tornar o SD novamente íntegro e disponível. O CD-MB realiza os *backups* com o uso da tecnologia *Commvault Backup & Recovery,* uma ferramenta corporativa, robusta e versátil que permite às OM implementar estratégias de proteção para diferentes objetivos. Por exemplo, é possível proteger a máquina virtual completa em um *backup,* e somente os dados do SD em outro. Dessa forma, na hipótese de um ataque cibernético que comprometesse a máquina virtual, seria possível adotar uma estratégia de recuperação que restaurasse a máquina virtual e os dados do SD a partir do *backup* mais

recente. As OM têm a responsabilidade de definir os dados a serem protegidos no Plano de *Backup* acordado com o CD-MB, de acordo com as suas necessidades de negócio.

Esta pesquisa concluiu que 87,5% das OM da amostra utilizam os *backups* produzidos pela tecnologia *Commvault Backup & Recovery* nas suas estratégias de recuperação documentadas em seus PLCONT e/ou PRD. O uso da tecnologia, alinhado *c*om a correta definição do conteúdo dos *backup* e com estratégias de recuperação bem definidas, documentadas e testadas, contribuirá sobremaneira para reduzir os impactos causados por eventuais ataques cibernéticos ou quaisquer outras ameaças à integridade e à disponibilidade dos SD.

A bibliografia e as normas técnicas que abordam a continuidade de negócios destacam boas práticas a serem implementadas na estrutura de resposta das organizações, com o objetivo de elevar a sua eficiência e eficácia na redução dos impactos de uma disrupção. O Plano de Contingência (PLCONT) e o Plano de Recuperação de Desastre (PRD) para sistemas digitais são planos de continuidade de negócios, devem integrar a estrutura de resposta a eventos adversos das OM, e, portanto, devem ser construídos em observância às boas práticas, sempre que possível. A presente pesquisa concluiu que grande parcela das recomendações identificadas nos documentos estudados foi implementada por apenas 50% ou menos das OM da amostra em seus PLCONT e/ou PRD, consistindo, portanto, em oportunidades de melhoria a serem observadas para robustecer a eficácia dos planos.

Dentre as oportunidades de melhoria identificadas na pesquisa, destacam-se aquelas consideradas mais críticas, por consistirem em fraquezas que podem comprometer a consecução dos propósitos do PLCONT e do PRD, a saber:

a) Definição do RTO do SD, para que os planos sejam ajustados em função desse tempo objetivado de recuperação. Esta ação vai assegurar que a OM restabelecerá a integridade e a disponibilidade do SD em um tempo mínimo aceitável, sem prejuízos ao seu funcionamento, aos seus usuários e à sua imagem;

b) Descrição pormenorizada das ações a serem executadas pelas equipes de trabalho, para reduzir o risco de falhas do PLCONT e do PRD;

c) Treinamento das equipes de trabalho, para que executem as ações documentas no PLCONT e no PRD de acordo com as suas responsabilidades;

d) Definição de um programa de exercícios regular, para capacitar as equipes de trabalho e garantir a eficácia, confiabilidade e adequabilidade do PLCONT e do PRD; e

e) Documentação dos exercícios do PLCONT e do PRD, para um contínuo aperfeiçoamento dos planos e garantia da sua eficácia e confiabilidade.

Pelo exposto, é possível concluir que a presente pesquisa alcançou seu objetivo principal, qual seja: analisou como os requisitos estratégicos para a recuperação de SD, definidos nas Doutrinas e Normas de TIC da MB, estão implementados pelas OM mantenedoras de SD hospedados no CD-MB; e o seu alinhamento com as soluções tecnológicas atualmente empregadas por aquele Centro de Dados para elevar a resiliência organizacional militar sob exploração ou ataque cibernético. As questões de estudo complementares também foram respondidas, pois foi possível analisar o PLCONT e o PRD das OM participantes da pesquisa à luz da bibliografia e das normas técnicas que abordam a continuidade de negócios, e identificar as respectivas oportunidades de melhoria para elevar a eficácia dos planos. Também foi possível constatar que a tecnologia *Commvault Backup & Recovery,* em uso no CD-MB, pode ser empregada pelas OM em benefício da recuperação da integridade e da disponibilidade de seus SD.

No tocante à concepção do PLCONT e do PRD, sugere-se a normatização dos procedimentos, com o objetivo de orientar as OM, principalmente aquelas que têm seus SD hospedados no CD-MB. As instruções poderiam constar em uma nova revisão de alguma das Normas de TIC já existentes, ou ser objeto de uma nova Norma que trate especificamente sobre o tema, assim como a Política de *Backup* e Recuperação de Informações Digitais para a MB — DCTIMARINST 30-19. A normatização contribuirá para estabelecer os requisitos mínimos que deverão ser atendidos pelos PLCONT e PRD, tais como: o RTO para cada SD; os recursos necessários para a execução dos planos; os papéis e as responsabilidades das equipes de trabalho; os procedimentos a serem executados para os propósitos de cada plano; e a frequência e o registro da execução dos testes/exercícios. A normatização da elaboração do PLCONT e do PRD também favorecerá a padronização dos planos, cujos benefícios, entre outros, são a manutenção da conformidade, a redução de falhas e a facilidade no treinamento das equipes. Sugere-se que, em adição à normatização, o PLCONT e o PRD sejam objetos de inspeção ou auditoria, a fim de verificar a sua conformidade e eficácia baseada nos resultados dos testes/exercícios regulares.

Por fim, esta pesquisa concluiu que os planos de continuidade de negócios voltados para a recomposição de sistemas digitais, conjuntamente com o uso de tecnologias atualizadas, confiáveis e seguras, contribuem de forma bastante significativa para aumentar

a resiliência organizacional das OM em face de ataques cibernéticos, reduzindo ao mínimo seus efeitos e contribuindo para fortalecer a credibilidade da Marinha.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **NBR ISO 22301:** Segurança e resiliência — Sistema de gestão de continuidade de negócios — Requisitos. 2. ed. Rio de Janeiro: ABNT, 2020a.

ABNT. Associação Brasileira de Normas Técnicas. **NBR ISO 22313:** Segurança e resiliência — Sistemas de gestão de continuidade de negócios — Orientações para o uso da ABNT NBR ISO 22301. 2. ed. Rio de Janeiro: ABNT, 2020b.

ABNT. Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27002:** Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. 2. ed. Rio de Janeiro: ABNT, 2013.

BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Ransomware**. 2021. Disponível em: https://cartilha.cert.br/ransomware. Acesso em: 11 jun. 2022.

BRASIL. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Alerta 06/22:** Ransomware-as-a-Service AvosLocker. 2022a. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/alertas/2022/alerta-06-2022. Acesso em: 11 jun. 2022.

BRASIL. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Recomendação 04/22:** Plano de Continuidade do Negócio. 2022b. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/recomendacoes/2022/recomendacao-04-2022. Acesso em: 11 jun. 2022.

BRASIL. Diretoria de Comunicações e Tecnologia da Informação da Marinha. **DCTIMARINST 30-19:** Política de Backup e Recuperação de Informações Digitais para a MB. Rio de Janeiro, RJ, 2021b.

BRASIL. Diretoria-Geral do Material da Marinha, **DGMM-540:** Normas de Tecnologia da Informação da Marinha. 3. rev. Rio de Janeiro, RJ, 2019.

BRASIL. Estado-Maior da Armada. **EMA-416:** Doutrina de Tecnologia da Informação da Marinha. Brasília, DF, 2007.

BRASIL. Estado-Maior da Armada. **EMA-419:** Doutrina Cibernética da Marinha. Brasília, DF, 2021a.

BRASIL. Secretaria-Geral da Marinha. **SGM-107:** Normas Gerais de Administração. 8. rev. Brasília, DF, 2021c.

COMMVAULT SYSTEMS. **Commvault Backup & Recovery**. 2021. Disponível em: https://documentation.commvault.com/11.24/essential/index.html. Acesso em: 01 jun. 2022.

IIA. Institute of Internal Auditors. The International Professional Practices Framework. **Guia prático:** Gestão de Continuidade de Negócios. Tradução: Instituto de Auditores Internos do Brasil. 2008. Disponível em: http://iiabrasil.org.br//ippf/orientacoes-suplementares. Acesso em: 30 jul. 2022.

LAB, Kaspersky. **Ransomware:** definição, prevenção e remoção. 2022. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware. Acesso em: 11 jun. 2022.

MARINHA DO BRASIL. Centro de Tecnologia da Informação da Marinha. **Catálogo de Serviços.** Rio de Janeiro, RJ, 2008. Disponível em: https://www.ctim.mb/catalogo/catalogo-de-servicos. Acesso em: 29 mai. 2022.

MARINHA DO BRASIL. Centro de Tecnologia da Informação da Marinha. **Portaria nº 1/CTIM,** de 13 de junho de 2018. Aprova o Regimento Interno do Centro de Tecnologia da Informação da Marinha. Rio de Janeiro, RJ, 2018. Disponível em: https://www.ctim.mb/sites/default/files/interno/Port1-2018-CTIM%20Aprova%20o%20Regimento%20Interno%20do%20CTIM-010.2_0.pdf. Acesso em: 29 mai. 2022.

MARINHO, Fernando. **Guia de Plano de Continuidade de Negócios (PCN).** Rio de Janeiro: Editora GEN Atlas, 2018. 144 p.

TCU. Tribunal de Contas da União. **Estratégia de Fiscalização do TCU em Segurança da Informação e Segurança Cibernética 2020-2023.** Brasília, DF, 2021.

VERAS, Manoel. **Datacenter:** Componente Central da Infraestrutura de TI. Rio de Janeiro: Brasport, 2009. 376p.

VMWARE. **Virtualização de servidores**. 2022. Disponível em: https://www.vmware.com/br/topics/glossary/content/server-virtualization.html. Acesso em: 01 jun. 2022.

APÊNDICES

APÊNDICE A — Questionário sobre procedimentos de recuperação da disponibilidade de sistemas digitais corporativos hospedados no Centro de Dados da Marinha (CD-MB)

O presente questionário é voltado para as OM que hospedam seus sistemas digitais corporativos no CD-MB e tem o propósito de identificar como foram elaboradas as suas estratégias de recuperação, as quais serão empregadas em uma eventual disrupção causada por um ataque cibernético que cause a indisponibilidade do sistema digital corporativo, impedindo sua operação.

Para o propósito desta pesquisa, o Plano de Contingência (PLCONT) é definido como um procedimento documentado para nortear a ativação da solução de contingência implementada pela OM para o seu sistema digital corporativo. A contingência do sistema digital corporativo é uma solução alternativa para salvaguardar a sua continuidade operacional na eventualidade de um incidente que comprometa a sua disponibilidade no ambiente principal. Admite a operação com restrições até que o sistema digital esteja recuperado em seu ambiente principal. Já o Plano de Recuperação de Desastre (PRD) é definido como um procedimento documentado sobre como recuperar a disponibilidade do sistema digital em seu ambiente principal (CD-MB), tornando-o novamente íntegro e operacional. Procedimentos de recuperação documentados em Planos de Contingência (PLCONT) e Planos de Recuperação de Desastres (PRD) podem contribuir de forma bastante significativa para reduzir o tempo de indisponibilidade dos sistemas digitais corporativos e aumentar a resiliência das OM sob exploração ou ataque cibernético.

Os dados coletados na presente pesquisa serão utilizados para analisar o nível de resiliência das OM clientes do CD-MB em face de ataques cibernéticos que venham a comprometer a disponibilidade de seus sistemas digitais corporativos. Para este objetivo não são necessárias as identificações do respondente, do sistema digital e respectiva OM responsável por sua manutenção. A presente pesquisa garante a preservação do anonimato.

As perguntas que não se aplicam à realidade da OM não devem ser respondidas.

Agradeço imensamente pela valiosa colaboração!

1. A OM conhece o intervalo de tempo aceitável entre a indisponibilidade do sistema digital e o retorno à normalidade da sua operação (RTO - *Recovery Time Objective* ou Objetivo do tempo de recuperação)?

[ ] Sim. Favor informar quanto tempo: _____.

[ ] Não.

2. A OM possui uma contingência para o sistema digital hospedado no CD-MB?

[ ] Sim.

[ ] Não.

3. A OM possui um Plano de Contingência (PLCONT) para orientar a ativação da contingência do seu sistema digital em ambiente alternativo?

[ ] Sim.

[ ] Não.

4. A OM possui um Plano de Recuperação de Desastre (PRD) para orientar a recuperação da disponibilidade do seu sistema digital em seu ambiente principal (CD-MB)?

[ ] Sim.

[ ] Não.

5. Assinale as opções que correspondem ao PLCONT e PRD do sistema digital da OM:

[ ] a) Definem de forma clara e objetiva seu Propósito e Escopo.

[ ] b) Identificam os recursos necessários para disponibilizar o sistema digital corporativo no ambiente alternativo de contingência (PLCONT) e para recuperar a disponibilidade do sistema digital corporativo no CD-MB (PRD), onde estão

localizados estes recursos e como acessá-los. São exemplos de recursos: equipamentos, software, *backup*, documentos, recursos humanos, serviços contratados com terceiros, entre outros.

[ ] c) O PLCONT define, no mínimo, as seguintes equipes de trabalho e respectivas responsabilidades: responsável pela ativação do PLCONT/declaração da situação de contingência; responsável pela execução dos procedimentos descritos no Plano para disponibilizar o sistema digital corporativo no ambiente alternativo de contingência; e responsável pela desmobilização da contingência e respectivo retorno à normalidade de operação do sistema digital corporativo no seu ambiente principal.

[ ] d) O PRD define as equipes de trabalho e respectivas responsabilidades referentes à execução dos procedimentos para recuperar a disponibilidade do sistema digital corporativo no CD-MB.

[ ] e) Detalham o passo a passo que deverão ser executados pelas equipes de trabalho para disponibilizar o sistema digital no ambiente alternativo de contingência (PLCONT) e para recuperar a disponibilidade do sistema digital no CD-MB (PRD).

[ ] f) O PLCONT identifica de forma clara as limitações relacionadas à operação do sistema digital corporativo no ambiente alternativo de contingência, caso existam.

[ ] g) As equipes de trabalho recebem treinamento regular sobre as ações que deverão empreender para disponibilizar o sistema digital no ambiente alternativo de contingência (PLCONT) e para recuperar a disponibilidade do sistema digital no CD-MB (PRD).

[ ] h) O PLCONT é testado regularmente a fim de assegurar a sua efetividade na disponibilização do sistema digital no ambiente alternativo de contingência, em relação às necessidades de negócio da OM. Assinale a frequência da realização dos testes:

[ ] Mensalmente.

[ ] Semestralmente.

[ ] Anualmente.

[ ] Outros. Favor informar: _____.

i) O PRD é testado regularmente a fim de assegurar a sua efetividade na recuperação da disponibilidade do sistema digital no CD-MB:

[ ] Mensalmente.

[ ] [ ] Semestralmente.

[ ] Anualmente.

[ ] Outros. Favor informar: _____.

[ ] j) Os testes do PLCONT e do PRD são documentados com o registro de eventuais falhas nos procedimentos. O objetivo de documentar os testes é corrigir os procedimentos incorretos, desatualizados ou incompletos para garantir a sua eficácia.

[ ] k) O PLCONT define como ocorre a desmobilização da contingência, ou seja, como retornar à normalidade de operação do sistema digital corporativo no seu ambiente principal.

6. O PLCONT prevê que a ativação da contingência demandará a recuperação de cópia de segurança ou *backup* executada pelo CD-MB por meio da tecnologia *Commvault Backup & Recovery*?

[ ] Sim. O tempo de recuperação do *backup*, acordado no Plano de *Backup* entre a OM e o CD-MB, está em conformidade com o RTO do sistema digital? [ ] Sim. [ ] Não.

[ ] Não. Favor informar como os dados do sistema digital são atualizados na contingência: _____.

7. O PRD prevê que a recuperação da disponibilidade do sistema digital demandará a recuperação de cópia de segurança ou *backup* executada pelo CD-MB por meio da tecnologia *Commvault Backup & Recovery*?

[ ] Sim. O tempo de recuperação do *backup*, acordado no Plano de *Backup* entre a OM e o CD-MB, está em conformidade com o RTO do sistema digital? [ ] Sim. [ ] Não.

[ ] Não. Favor informar como os dados do sistema digital são recuperados e atualizados: _____.

8. A ativação da contingência ocorre dentro do intervalo de tempo aceitável de indisponibilidade do sistema digital da OM e o retorno da sua operação (RTO - *Recovery Time Objective* ou Objetivo do tempo de recuperação)?

[ ] Sim.

[ ] Não. Favor informar o principal motivo: _____.

9. A recuperação da disponibilidade do sistema digital no CD-MB ocorre dentro do intervalo de tempo aceitável de indisponibilidade e o retorno da sua operação (RTO - *Recovery Time Objective* ou Objetivo do tempo de recuperação)?

[ ] Sim.

[ ] Não. Favor informar o principal motivo: _____.

10. A OM já teve a experiência de não conseguir a ativação da contingência por falhas em seu PLCONT?

[ ] Sim.

[ ] Não.

APÊNDICE B — Consolidação dos dados da pesquisa

Tabela 1 — Número de OM que elaboraram os procedimentos de recuperação de seus SD à luz dos requisitos estratégicos definidos nas Doutrinas e Normas de TIC da MB.

PERGUNTAS	SIM		NÃO	
	OM	%	OM	%
1) A OM possui uma contingência para o SD hospedado no CD-MB?	4	50	4	50
2) A OM possui um Plano de Contingência (PLCONT) para orientar a ativação da contingência do seu SD em ambiente alternativo?	4	100	—	—
3) A OM possui um Plano de Recuperação de Desastre (PRD) para orientar a recuperação da disponibilidade do seu SD em seu ambiente principal (CD-MB)?	4	50	4	50

Fonte: Elaborado pela autora, 2022.

Tabela 2 — Número de OM que implementaram Plano de Contingência (PLCONT) e Plano de Recuperação de Desastre (PRD) e conhecem o RTO de seus SD

SITUAÇÃO	OM	%	OM conhece o RTO do SD	%	RTO em horas
OM que não possui PLCONT e PRD	1	12,5	—	—	—
OM que possui PLCONT e PRD	1	12,5	1	12,5	6
OM que possui somente PLCONT	3	37,5	2	25	2 3
OM que possui somente PRD	3	37,5	1	12,5	48
TOTAL	**8**	**100**	**4**	**50**	**..**

Fonte: Elaborado pela autora, 2022.

Tabela 3 — Número de OM que empregam as melhores práticas nos procedimentos de recuperação da integridade e disponibilidade de seus sistemas digitais (SD).

PERGUNTAS	SIM		NÃO	
	OM	%	OM	%
1) A OM conhece o intervalo de tempo aceitável entre a indisponibilidade do SD e o retorno à normalidade da sua operação (RTO - *Recovery Time Objective* ou Objetivo do tempo de recuperação)?	4	50	4	50
2) O PLCONT e o PRD definem de forma clara e objetiva seu Propósito e Escopo?	3	37,5	5	62,5
3) O PLCONT e o PRD identificam os recursos necessários para disponibilizar o SD no ambiente alternativo de contingência e para recuperar a disponibilidade do SD no CD-MB, onde estão localizados estes recursos e como acessá-los?	3	37,5	5	62,5
4) O PLCONT define, no mínimo, as seguintes equipes de trabalho e respectivas responsabilidades: responsável pela ativação do PLCONT/declaração da situação de contingência; responsável pela execução dos procedimentos descritos no Plano para disponibilizar o SD no ambiente alternativo de contingência; e responsável pela desmobilização da contingência e respectivo retorno à normalidade de operação do SD no seu ambiente principal?	3	75	1	25
5) O PRD define as equipes de trabalho e suas respectivas responsabilidades referentes à execução dos procedimentos para recuperar a disponibilidade do SD no CD-MB?	2	50	2	50
6) O PLCONT e o PRD detalham os procedimentos que deverão ser executados pelas equipes de trabalho para disponibilizar o SD no ambiente alternativo de contingência e para recuperar a disponibilidade do SD no CD-MB, respectivamente?	2	25	6	75
7) O PLCONT identifica de forma clara as limitações relacionadas à operação do SD no ambiente alternativo de contingência, caso existam?	3	75	1	25
8) As equipes de trabalho recebem treinamento regular sobre as ações que deverão empreender para disponibilizar o SD no ambiente alternativo de contingência e para recuperar a disponibilidade do SD no CD-MB?	2	25	6	75

9) O PLCONT é testado regularmente a fim de assegurar a sua efetividade na disponibilização do SD no ambiente alternativo de contingência, em relação às necessidades de negócio da OM?	3	75	1	25
10) O PRD é testado regularmente a fim de assegurar a sua efetividade na recuperação da disponibilidade do SD no CD-MB?	1	25	3	75
11) Os testes do PLCONT e do PRD são documentados com o registro de eventuais falhas nos procedimentos?	—	—	8	100
12) O PLCONT define como ocorre a desmobilização da contingência, ou seja, como retornar à normalidade de operação do SD no seu ambiente principal?	2	50	2	50
13) A ativação da contingência ocorre dentro do intervalo de tempo aceitável de indisponibilidade do SD e o retorno da sua operação (RTO — *Recovery Time Objective* ou Objetivo do tempo de recuperação)?	3	75	1	25
14) A recuperação da disponibilidade do SD no CD-MB ocorre dentro do intervalo de tempo aceitável de indisponibilidade e o retorno da sua operação (RTO — *Recovery Time Objective* ou Objetivo do tempo de recuperação)?	2	50	2	50
15) A OM já teve a experiência de não conseguir a ativação da contingência por falhas em seu PLCONT?	1	25	3	75

Fonte: Elaborado pela autora, 2022.

Tabela 4 — Número de OM que utilizam a tecnologia *Commvault Backup & Recovery nas* estratégias de recuperação da integridade e disponibilidade de seus sistemas digitais (SD).

PERGUNTAS	SIM		NÃO	
	OM	%	OM	%
1) O PLCONT prevê que a ativação da contingência demandará a recuperação de cópia de segurança ou *backup* executada pelo CD-MB por meio da tecnologia *Commvault Backup & Recovery*?	4	100	—	—
2) Em relação ao PLCONT, o tempo de recuperação do *backup*, acordado no Plano de *Backup* entre a OM e o CD-MB, está em conformidade com o RTO do SD?	3	75	1	25

3) O PRD prevê que a recuperação da disponibilidade do SD demandará a recuperação de cópia de segurança ou *backup* executada pelo CD-MB por meio da tecnologia *Commvault Backup & Recovery*?	4	100	—	—
4) Em relação ao PRD, o tempo de recuperação do *backup*, acordado no Plano de *Backup* entre a OM e o CD-MB, está em conformidade com o RTO do sistema digital?	4	100%	—	—

Fonte: Elaborado pela autora, 2022.

Quadro 1 — Número de OM que realizam testes/exercícios periódicos do PLCONT e do PRD

SITUAÇÃO	OM que testam/exercitam os planos	%	Frequência dos testes	OM que documentam os testes	%
OM que possui PLCONT e PRD	1	12,5	Bienal	—	—
OM que possui somente PLCONT	2	25	Semestral Anual	—	—
OM que possui somente PRD	1	12,5	Não informado	—	—
TOTAL	**4**	**50**	**..**	—	—

Fonte: Elaborado pela autora, 2022.

Quadro 2 — Número de OM que demandam a recuperação de *backup* pelo CD-MB, por meio da tecnologia *Commvault Backup & Recovery* e a relação com o RTO do SD

SITUAÇÃO	OM que demandam recuperação de *backup* pelo *Commvault Backup & Recovery*	OM conhece o RTO do SD	Tempo de recuperação do *backup* não está de acordo com o RTO do SD	
			OM	Motivo
OM que possui PLCONT e PRD	1	1	—	—
OM que possui somente PLCONT	3	2	1	Tempo de recuperação acordado no Plano de *Backup* acima do RTO
OM que possui somente PRD	3	1	—	—

Fonte: Elaborado pela autora, 2022.