TUTORIAL DE ELABORAÇÃO DE UM PLANO DE CONTINGÊNCIA PARA PRESERVAÇÃO DIGITAL

João Andrade

INTRODUÇÃO

Neste tutorial será apresentado um modelo para a elaboração de um plano de contingenciamento para Preservação Digital (PCPD), a partir da aplicação de duas ferramentas desenvolvidas para prevenção de ameaças e contenção de risco, a Matriz de Orientação (MOCR) e a Escala de Mensuração (EMCR) em Cenário de Risco. Pesquisas, atuais, apontam este instrumento documental como a melhor opção para orientar gestores e corpo técnico de instituições memoriais, nas situações de caos instalado.

Isto posto, é preciso estar ciente de que erradicar o risco é impossível, pois toda e qualquer atividade que envolve os organismos vivos, está sujeita a ameaças e perigos dos mais diversos graus e intensidade. A psique humana, por exemplo, que cria mecanismos para sobrevivência, como a falácia da plenitude que nos faz crer, sem questionar, na falsa sensação de segurança, até que algo aconteça, mas mesmo assim este mecanismo é tão perfeito que mesmo depois do fato ocorrido, apenas estados de alerta são ativado pelo cérebro, mas nunca a falsa sensação de segurança é posta em questão.

Segundo Gregory Schmidt (2010) é inevitável, a probabilidade, de que uma catástrofe de grandes proporções afete uma instituição[1]. Trazendo sua perspectiva para a Ciência da Informação, alinhada à pesquisas no âmbito da Preservação Digital, as quais demonstram que é, logicamente, impossível evitar danos e perdas digitais, mas que a mitigação da cadeia de risco é uma possibilidade, é consensual que o desenvolvimento de metodologias capazes de antever o efeito da incerteza são imprescindíveis às práticas da garantia de longevidade de acervos digitais.

Não existe bola de cristal, como nas estórias fantásticas, que possa prever o futuro, contudo é possível moldá-lo segundo nossa própria perspectiva[2]. Da mesma forma que não se cria uma cultura de previdência da noite para o dia, é preciso antes preparar e conscientizar grupos de decisão conduzidos pela necessidade de segurança e preservação do patrimônio"[3]. No entanto, o planejamento estratégico é, entre outros, atributo fundamental à gestão da Preservação Digital, operando como uma metodologia fiável no agora que busca vislumbrar o amanhã para manter o estado das coisas (status quo) no futuro.

Visto por este prisma, a elaboração do documento de plano de contingenciamento depende da observação atenta e dedicada de aspectos, critérios, etapas e procedimentos para que o instrumento possa ser eficiente e eficaz, do contrário será apenas mais um texto que logo cairá no esquecimento ou não terá êxito em sua aplicação.

A seguir compreenderemos o conceito de plano de contingenciamento e sua aplicabilidade, em seguida serão apresentadas as ferramentas de orientação e mensuração do risco, para então, partirmos para o propósito deste tutorial, oguia de elaboração do Plano de Contingência para Preservação Digital (PCPD).

2. O que é e para quê serve o plano de contingência?

Plano de contingência é um instrumento documental, no qual se legislam as responsabilidades estabelecidas por uma instituição de memória para atender a uma emergência. Em suas cláusulas devem estar descritas as medidas a serem tomadas em situação de caos instalado, no intuito de dispor de estratégias e técnicas para que se possam antecipar aos prejuízos que venham a ser causados pela negligência humana e/ou falhas mecânicas de equipamentos eletro-eletrônicos.

Por finalidade estes instrumentos visam treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate em casos de eventualidades sinistras.

Este tutorial tem como fundamento as definições do Ministério da Integração Nacional e Secretaria Nacional de Proteção e Defesa Civil (2017); do United Nations High Commissioner for Refugees - UNHCR (2003) e das pesquisadoras Rebecca Frank e Elizabeth Yakel (2013), especialistas na área. Segundo o Ministério e Secretaria brasileiros, o plano de contingência pode ser definido como o documento que registra o planejamento elaborado a partir da percepção do risco de determinado tipo de desastre, estabelecendo procedimentos e responsabilidades (MI; SEDEC, 2017, p. 22). O UNHCR define-o como "um processo de planejamento antecipado, em um estado de incerteza, em que os cenários e os objetivos são acordados, as ações gerenciais e técnicas definidas e sistemas de resposta potenciais implementados para prevenir ou responder melhor a uma situação de emergência ou crítica" (UNHCR, 2003, p. 10).

Enquanto as pesquisadoras da University of Michigan School of Information, entendem o plano como um “documento que descreve as políticas e procedimentos desenvolvidos para prevenir, preparar, responder e recuperar os Repositórios Digitais de um possível desastre” (FRANK; YAKEL, 2013, p. 2 - tradução própria).

É importante destacar que os planos de contingenciamento ou desastre podem ser interpretados como políticas para Preservação Digital, as quais podem ser elaboradas com base em resoluções, normas, atos administrativos, leis, modelos e padrões. Podendo ser analisadas sob os aspectos: organizacional, legal e técnico” (SILVA JUNIOR; MOTA, 2012, p.51). Em outras palavras, é um instrumento oficial que deve ser certificado e autenticado pelo Estado brasileiro por uma agência reguladora, no âmbito da Preservação Digital, que detenha as responsabilidades de garantia de acesso contínuo e de longo prazo a estoques digitais.

3. Ferramentas de orientação e mensuração do risco

3.1 Matriz de Orientação para o cenário de risco (Matriz OCR)

A Matriz OCR é uma ferramenta que auxilia na construção do PCPD, deve ser aplicada durante a etapa de elaboração do plano, antes mesmo de qualquer outra ação. Este documento deve ser assinado e datado pelo Técnico responsável de Análise de Risco em Preservação Digital, sendo anexado no dossiê final da documentação do Plano de Contingenciamento.

O modelo consiste em uma planilha onde na parte superior, na primeira linha deve constar o termo “cenário”, neste campo deve ser descrito o cenário onde as eventualidades podem acontecer e o código da Matriz OCR. O termo repositório digital só será aplicado para os acervos que estão ligados a uma Caixa LOCKSS ou do NTI de uma Universidade qualquer outra forma de armazenamento de estoques digitais será tratada como storage ou armazenamento digital[1]. Assim o cenário pode ser um repositório digital, um storage, uma sala onde se encontra instalada a infraestrutura de armazenamento dos estoques digitais ou a sala de operação da equipe.

A primeira coluna da planilha deve ser preenchido com o termo “ameaça”, nele deve ser descrita a informação do agente causador do dano[2]. A próxima coluna “vulnerabilidade” descreve as fragilidades encontradas no cenário. terceira coluna “sinistro”, trata da previsão, nela são descritos os prejuízos causados pelas ameaças por conta das vulnerabilidades. Na quarta coluna é descrita a “salvaguarda” ou medidas de previdência, como se defender das ameaças, sanar ou mitigar as vulnerabilidades evitando o sinistro. Cada cenário deve ter sua própria Matriz OCR, pois cada caso é um caso e deve ser analisado individualmente, mesmo que ao final da sindicância o somatório dos resultados proporcionem um panorama genérico.

A aplicação da Matriz OCR está condicionada ao desenho de possibilidades, isto é, eventos de risco, como segue na lista abaixo.

- Determinar a causa fundamental do problema;
- Identificar o estopim do fato;
- Listar os sinais de aviso prévio;
- Descrever pontos de relevância;
- Indicar e descrever o que pode ser feito no momento da ocorrência de forma emergencial;

Modelo de Matriz de orientação para o cenário de risco (Matriz OCR)

Cenário da Matriz OCR: Sala do Servidor **Código da Matriz OCR:** 0001/23

Ameaça	**Vulnerabilidades**	**Sinistro**	**Salvaguarda**
1. Pane da rede elétrica do edifício onde se encontra instalado o servidor (storage)	1. Deficiência na Infraestrutura do sistema elétrico. 2. Falha na manutenção do quadro elétrico falha. 3.Falha na manutenção do sistema de nobreak falha. 4.Pane na rede elétrica externa.	Provocar Curto no sistema elétrico do edifício. Danificar equipamentos mais sensíveis como HD. Perda de dados em processo.	Ter backup dos dados em dois discos de marcas diferentes e mais um terceiro backup off-site. Backup em fita. Cópia da coleção digital em outras instituições membros da rede colaborativa.

Fonte: Elaboração própria.

3.2 Escala de Mensuração no cenário de risco (Escala MCR)

A Escala MCR é a ferramenta que depende da Matriz OCR para compor o corpo de base da estrutura de construção do PCPD, deve ser aplicada durante a etapa de elaboração do plano, após o preenchimento da Matriz OCR de mesmo código. Este documento deve ser assinado e datado pelo Técnico responsável de Análise de Risco em Preservação Digital, sendo anexado no dossiê final da documentação do Plano de Contingenciamento.

O modelo consiste em uma planilha onde na parte superior, na primeira linha deve constar o termo “cenário”, neste campo devem ser descritas as mesmas informações da Matriz OCR referente. Na primeira coluna devem ser descritos os atributos do cenário, variáveis que devem ser consideradas como agentes passíveis de potencializar o risco. Podem ser desde a infraestrutura do servidor, como o software do sistema, a conexão da rede (ethernet ou internet) ou as condições prediais até as condições de trabalho dos colaboradores[1].

Esta escala mede a evolução do grau do risco (dano), a partir dos atributos do cenário, os quais estão diretamente ligados à Matriz OCR. A mensuração ocorre a partir do fluxo espectral desde um nível mais baixo até o seu estado crítico ou à perda total do acervo digital. A evolução do fluxo espectral é medida pela graduação da variação das cores do espectro. Verde significa um nível baixo, amarelo requer atenção e o vermelho, hora de tomar uma atitude. O espectro gradual da cor roxa aponta para um estágio crítico, crise para o lilás, colapso para o violeta e roxo para a perda total[1].

Medida gradualmente da esquerda para a direita, a mensuração em progressão crescente considera o primeiro nível para o risco como ótimo, que recebe pontuação 0 (zero) ou fora de risco, sem cor representativa (transparente). O próximo estágio é representado por uma contagem do número 1 até o 9, subdividida em três níveis: o primeiro é aquele onde há ameaças que podem alcançar do nível 1 ao 3, é considerado leve (sob ameaça), evoluindo a partir do espectro gradual; o seguinte do 4 ao 6 é um nível intermediário, as ameaças são tantas que colocam os ativos digitais em uma situação muito vulnerável (em perigo), também evolui sobre o espectro gradual; o terceiro estágio vai do 7 ao 9, ultrapassando as barreiras dos anteriores, colocando o estoque digital em uma situação que pode levar a uma “crise do sistema”, o estágio de crise do sistema é grave, mas ainda há possibilidade de desacelerar a evolução do risco, todavia não tomando as devidas providências o estágio seguinte é o colapso do sistema, um nível gravíssimo, nessa altura pouco ou quase nada pode ser feito para evitar o sinistro. O último nível é o sinistro propriamente dito ou o risco instalado, perda total.

Modelo de Escala de Mensuração no Cenário de Risco (Escala MCR)

Cenário da Matriz OCR: Sala do Servidor	**Código da Matriz OCR:** 0001/23

Atributos do Cenário	Graduação do risco (dano)											
	FORA DE RISCO (0)	SOB AMEAÇA			EM PERIGO			EM RISCO			SISTEMA EM CRISE (10)	COLAPSO DO SISTEMA (25)	PERDA TOTAL (50)
		1	2	3	4	5	6	7	8	9			
Infraestrutura predial interna da sala de operação (profissionais) - Elétrica													
Infraestrutura predial interna da sala de operação (profissionais) - instalação dos pontos de energia elétrica (tomadas, interruptores, lâmpadas)													
Infraestrutura predial interna da sala de operação (profissionais) - Iluminação													
Infraestrutura predial interna da sala de operação (profissionais) - Climatização													
Infraestrutura predial interna da sala de operação (profissionais) - Ergonomia dos assentos													
Infraestrutura predial interna da sala de operação (profissionais) - Ergonomia das ferramentas (teclado, mouse, fones, monitor)													
Infraestrutura predial externa													
Infraestrutura predial interna													
Infraestrutura predial interna da sala do servidor (storage)													
Infraestrutura predial externa (elétrica)													
Infraestrutura predial interna (elétrica)													

Infraestrutura predial interna da sala do servidor (elétrica)												
Infraestrutura predial interna da sala do servidor (instalação dos pontos de energia elétrica - tomadas, interruptores, lâmpadas)												
Infraestrutura predial interna da sala do servidor (climatização)												
Infraestrutura predial interna da sala do servidor (climatização - mensuração da temperatura)												
Infraestrutura predial interna da sala do servidor (storage) - Sistema de Internet (equipamento)												
Infraestrutura predial interna da sala do servidor (storage) - Conexão de Internet												
Acesso à sala do servidor (storage)												
Operação do servidor (storage)												
Manutenção do servidor do servidor (storage) - Hardware												
Manutenção do servidor do servidor												
(storage) - Hardware, troca de peças e acessórios												
Manutenção do servidor do servidor (storage) - Equipamento periférico (nobreak)												
Manutenção do servidor do servidor (storage) - Software												
Manutenção Sistema de Backups (HDs do Servidor)												
Manutenção Sistema de Backups (HDs Externo)												
Manutenção Sistema de Backups (Fitas LTO)												
Manutenção Sistema de Backups (Outros dispositivos de armazenamento)												

Infraestrutura Computacional (Software)												
Infraestrutura Computacional (Versão do Software)												
Infraestrutura Computacional (Experiência com Frontend da página)												
Infraestrutura Computacional (Profissional) - Terminal de Trabalho												
Infraestrutura Computacional (Profissional) - Estação de Trabalho												
Infraestrutura Computacional (Profissional) - Impressora												
Infraestrutura Computacional (Profissional) - Conexão de Internet												
Profissional - Capacitação em Preservação Digital												
Profissional - Capacitação para operar o sistema do Repositório Digital												
Profissional - Satisfação com o suporte de TI												
Profissional - Satisfação em operar com Preservação Digital												
Profissional - Satisfação financeira em operar com Preservação Digital												

Fonte: Elaboração Própria.

Nesta etapa, o sistema deve gerar os metadados técnicos extraídos por meio de software de código aberto (MediaInfo) e exportados em XML no padrão PBCore. Importante identificar as informações que permitem o registro de criação do representante digital; serão trabalhados metadados em PREMIS com complementação em reVTMD para o registro do histórico de processos.

As informações correspondentes ao processo de digitalização para a criação do representante digital são, por exemplo: resolução, proporção de tela, tamanho, formato, fita digitalizada, placa utilizada, sistema operacional etc.;

2.1 Como elaborar o plano de contingência?

A elaboração e a execução do plano de contingência contribui diretamente para que Instituições de Memória alcancem sua missão de serem bons ancestrais. O planejamento estratégico deve ser aplicado a partir de uma perspectiva sistêmica, isto é de uma iniciativa coletiva e participativa, isto é interoperável, pois a articulação entre todos os envolvidos na equipe traz benefícios que vão desde uma melhor utilização de recursos materiais, humanos e financeiros, à mitigação de impactos de acidentes digitais até uma maior eficiência na gestão.

A Ciência da Informação - C.I., ainda, não dispõe de uma normatização técnica específica para Gestão da Preservação Digital, contudo a Rede Cariniana do Instituto Brasileiro de Ciência e Tecnologia - Ibict e o Laboratório Liber da Universidade Federal de Pernambuco - UFPE estão na vanguarda dos esforços, dedicando pesquisas, nas últimas duas décadas, para a consolidação de tal regulamentação. No entanto, em face da interdisciplinaridade da C.I. para elaborar nossa versão de PCPD esta iniciativa se apoia nas normas ABNT NBR ISO/IEC 27005:2019 - Tecnologia da Informação, técnicas de segurança e gestão de riscos de segurança da informação e ABNT ISO 3100:2009 - Gestão de Risco (princípios e diretrizes) para definir e desambiguar conceitos de risco e perigo.

A partir desta perspectiva o princípio norteador da Gestão do Risco em Preservação Digital (GRPD) para elaboração do PCPD é a ciência dos conceitos de ameaça, perigo, previdência, sinistro, risco e vulnerabilidade.

- Ameaça - É o prenúncio de um acontecimento prejudicial; um sinal[1].

- Perigo - São condições que podem causar ou contribuir para a ocorrência do risco[2].

- Risco - É o efeito da incerteza sobre os objetivos[3].

Nesta perspectiva estes aspectos do sinistro são entendidos como índices de graduação para danos aos estoques digitais. O Sinistro deve ser compreendido, assim, como um sinônimo de dano ou um prejuízo que pode ser total ou parcial, dependendo da intensidade do impacto do agente maléfico (malefício) sobre os ativos[1] ou acervos digitais. A ação do malefício sobre a memória digital depende da condição de vulnerabilidade, ao qual esta se encontra exposta.

Façamos um exercício de representação imagética, seja no campo das ideias, numa planilha digital ou por meio do tradicional lápis e papel, exercite sua imaginação descrevendo quais as principais fragilidades que podem colocar um acervo em situação de alerta. Agora observe o resultado de sua observação preditiva. Você criou um mapa da situação, descrevendo as fragilidades do acervo. Consciente da situação, a partir do panorama idealizado, você fez uma viagem no tempo, indo para o futuro do seu acervo.

De volta ao presente, conhecendo as vulnerabilidades, agora faça uma nova lista descrevendo os prejuízos que podem atingir o acervo com base em cada item da coluna vulnerabilidades.

Agora que você já conhece suas vulnerabilidades, é preciso fazer um exercício de previdência, pois as ameaças, os perigos e o risco devem ser considerados como agentes operacionais, quero dizer, são a ação que atua sobre o acervo digital, mesmo que ainda não tenham sido descritos, você já previu as fragilidades e os possíveis danos ou as consequências, através da previdência agora é chegada a hora de exercitar a garantia, isto é, no próximo exercício será preciso pensar medidas de proteção, assegurado que o acervo pode ou não sair da zona de perigo.

Realizados o exercício de observação preditiva, você agora tem em mãos um mapa para orientar a tomada de decisão sobre as ações para garantir e manutenção da longevidade de um acervo digital. Na etapa de planejamento este exercício permite a confecção da Matriz de Orientação do Cenário de Risco (Matriz OCR). O próximo passo para construção do PCPD é a aplicação da Escala de Mensuração no Cenário de Risco (Escala MCR), esta ação é exercício prático, não há como prever os acontecimentos, pois será necessário observar os fatos.

A partir da Matriz OCR utilize o modelo de Escala MCR para mensurar o grau de atividade do agente maléfico sobre o acervo. A atribuição da pontuação do espectro de graduação depende exclusivamente de um olhar técnico, sensível, porém especialista. Um médico não precisa olhar uma tabela para medicar diagnosticar um paciente, mas precisa saber a dosagem de uma medicação para tratar certas doenças. Quando a situação estiver além dos graus do risco, considere que a situação é grave, a estrutura está em colapso, mas ainda pode retroceder, todavia quando há uma crise instalada é certo que o esforço para baixar para o nível anterior vai exigir muitos esforços, mas mesmo assim ainda que a probabilidade seja quase zero, ainda assim é possível rever a situação.

Com o auxílio da Matriz OCR a Escala MCR foi preenchida, a partir da análise dos resultados dessas ferramentas o procedimento de auditoria pode ser realizado e a resposta da auditoria irá apontar se a Instituição receberá ou não a certificação.

Com esta documentação o Plano de Contingenciamento (PCPD) é estruturado e pronto para ser anexado a documentação de Preservação Digital do acervo, biblioteca ou setor da Instituição.

A confecção de um plano de contingenciamento é dispendiosa e requer o investimento de tempo e recursos para sua conclusão e manutenção. Assim é preciso atender pré-requisitos como:

- Definir do modelo de plano de contingência (caso a instituição não possua um modelo próprio);
- Elaborar um cronograma de trabalho com prazos e recursos, prevendo para cada um deles o tempo de execução, a equipe envolvida e os recursos necessários;
- Formar força tarefa ou grupo de trabalho;
- Aprovar planos de ação, de trabalho e cronograma de execução do plano de contingência.

2.1.1 Critérios fundamentais

Antes de partir para as etapas de elaboração do plano alguns critérios prévios precisam ser conhecidos para que se possam alcançar resultados eficientes e eficazes (ANDRADE, 2018, p.111):

1. Administrar, Organizar e acompanhar a todas as etapas e procedimentos do processo de contingenciamento do risco, desde o planejamento à aplicação do instrumento;
2. Mobilizar gestores e corpo técnico da necessidade de seguir os padrões estabelecidos no documento;
3. Realizar manutenção técnica, regularmente, em equipamentos mecânicos, eletrônicos e digitais, bem como a observação das condições de infraestrutura do ambiente, bem como onde está instalada a infraestrutura do Armazenamento Digital (Storage) e/ou Repositórios Digital;
4. Manter a estabilidade do quadro operativo, pois muitas variações na equipe de operação podem comprometer o fluxo de produção aumentando a possibilidade de instalação do risco;
5. Promover ações de habilitação e capacitação periódica, a fim de que a equipe esteja constantemente atualizada e certificada das boas práticas que descrevem as normas padrão de execução da função.

2.1.2. Pilares da estrutura do plano de contingência

Os Planos de contingenciamento podem ser estruturados a partir de três questões basilares:

a) Hipótese do sinistro - Exercício de reflexão que busca prospectar motivos diversos e adversos de possibilidades de instalação do risco.
b) Preparação - Após descrever uma lista de possibilidades para a instalação do risco é hora de pensar como evitar que a potencialidade seja efetivada.
c) Elaboração de respostas estratégicas ao momento da ocorrência - refere-se àquilo que se pode fazer a respeito de uma ocorrência incluindo as ações de socorro, assistência ao que se perdeu e que está se perdendo, buscando restabelecimento da ordem.

Para além desses pilares, se recomenda, ainda, uma série de procedimentos que devem ser considerados, tais como:

a) Estudo de cenários de risco;
b) Desenvolvimento de sistemas de monitoramento;
c) Ações de assistência e recuperação da informação prejudicada.

Vale salientar que os planos de contingência devem ser elaborados para cenários de riscos específicos, ainda que não seja possível determinar com exatidão seus impactos. Para tanto, se deve trabalhar com cenários de riscos de forma a pensar em impactos potenciais e planejar aspectos para resposta: recursos necessários, tarefas e responsáveis (ANDRADE, 2018, p. 112).

3. Quais as etapas para elaboração do Plano Contingência?

Para se elaborar um documento que descreva a contingência do risco em Preservação Digital para Repositórios Institucionais algumas etapas precisam ser seguidas. Considerando o fato de que as necessidades de cada ocasião são sempre particulares o documento pode e deve ser adaptado à realidade de cada circunstância de acordo com o cenário de risco.

As etapas de elaboração do plano de contingência são um complexo sistêmico, onde cada etapa se desdobra em procedimentos que devem ser seguidos atentamente. Visto a práxis de contingenciamento estar ambientada em um ecossistema dinâmico, no qual o cenário está em constante transformação. Por este motivo o documento precisa manter um ciclo permanente de atualização.

No quadro a seguir estão dispostas as etapas e seus respectivos procedimentos para a confecção do Plano Contingência para Preservação Digital (PLCPD).

Quadro 1. Descrição das etapas de elaboração do Plano de Contingência.

Etapas	Procedimentos
Preparação	1. Constituição de uma Força Tarefa (*Task Force*); 2. Delimitação do Cenário de Risco (MOCR e EMCR);
Análise	3. Análise do cenário de risco.
Desenvolvimento	4. Definição de ações de previdência (Salvaguarda).
Implementação	5. Aplicação e operacionalização do modelo.
Auditoria	6. O plano não é um documento invariável devendo ser periodicamente revisto.
Certificação	7. Confere selo de autenticidade de que o Repositório está de acordo com as normas.

Fonte: ANDRADE, 2018, p. 131.

O desdobramento das etapas de desenho do plano está distribuído em procedimentos distintos, mas que se relacionam entre si. O primeiro (procedimento n.1) é a habilitação ecapacitação profissional para atuar com Preservação Digital. Através de oficinas ou uma habilitação por meio de um curso de Tecnólogo, de dois anos ou uma Graduação, de quatro anos em Preservação Digital, uma ideias para o futuro, pois é a educação e a atualização profissional seguindo os fluxo da necessidade de cada época que leva a ciência ao progresso. Alvin Toffler (1980) nos lembra que o analfabeto do século XXI não será aquele que não sabe ler nem escrever, mas aquele que não será capaz de aprender, desaprender e reaprender, em outras palavras se adaptar[1].

A próxima ação é a constituição do grupo de trabalho (procedimento n.2) que irá atuar na elaboração e execução do plano. Ainda na etapa de preparação é de fundamental importância delimitar o cenário de risco (procedimento n.3), isto é, mapear o ambiente onde a intervenção irá atuar, este procedimento é realizado com o apoio de dos instrumentos documentais Matriz OCR e Escala MCR.

Após o mapeamento das ameaças, das vulnerabilidades e descrita a previsão do sinistro é preciso analisar o cenário de risco (procedimento n.4). A análise minuciosa dos documentos Matriz OCR e Escala MCR irá gerar um panorama amplo da situação que auxiliará gestores a tomarem as melhores decisões para garantia de longevidade dos ativos digitais, bem como facilitará a atuação destes em situação de caos instalado. Contudo é preciso ir adiante e definir as ações a serem desenvolvidas (procedimento n.5). Esta salvaguarda é a resposta à graduação do dano ao qual os estoques digitais estão ou podem estar expostos.

O procedimento anterior habilita a enxergar o panorama do desenvolvimento das ações para contingenciamento do risco. A partir desta etapa se pode seguir para a etapa de implementação do modelo (procedimento n.6), onde o modelo será aplicado com a colaboração de toda a equipe, neste momento o plano de contingência será posto em prática.

Os dados coletados por meio dos documentos Matriz OCR e Escala MCR serão armazenados e o resultado do ranking da graduação do dano resultante do somatório dos estágios das Escala MCR, irão ter um período de maturação, o qual será avaliado por uma nova força tarefa, esta, composta por especialistas externos (banca examinadora), os quais no ano seguinte irão aplicar o saber aprendido com sua experiência anterior em seu próprio locus, realizando visita técnica de auditoria (procedimento n.7).

O produto da etapa de auditoria irá convergir para etapa de certificação do RI (procedimento n.8), com esta certificação o repositório estará apto a participar de programas de incentivo para sua melhoria ou no caso do resultado ser negativo, uma comissão especial será formada para auxiliar e garantir que o repositório irá superar sua dificuldade, retornando para o nível de excelência exigido para um Repositório Institucional Certificado - RIc.

3.1 Procedimentos para elaboração do Plano Contingência

Procedimento n.1: Capacitação e habilitação de profissionais

O Plano de Contingência só terá eficácia quando cada ator na Preservação Digitais estiver habilitado e capacitado para desempenhar seu papel no processo de longevidade digital. Desta forma, antes de tomar qualquer decisão quanto ao planejamento da contingência do risco é necessário a criação de novas competências para que os profissionais estejam prontos para lidar com as ferramentas de contingenciamento. Habilitados, estes profissionais deverão propagar seu conhecimento por meio da capacitação de outros profissionais.

. Abaixo segue sugestão para corpo organizacional baseado na visão de novas funções para profissionais da informação.[1]

- Gestor de Preservação Digital (GPD) - Bacharel em gestão da informação responsável pelo gerenciamento e administração geral do sistema, tendo sob seu controle, na hierarquia, o TPD e a EOF.

- Técnico em Preservação Digital (TPD) É o profissional, com formação acadêmica nas áreas de Ciência da Informação e/ou Computação, preocupado com a correta aplicação das boas práticas de preservação de longo prazo da memória em suporte digital. As faculdades atribuídas a este perfil são a observação e manutenção das boas práticas das atividades de preservação digital, bem como de Tecnologia da Informação. Responsável direto pela equipe de operação EOF. Responde apenas ao superior hierárquico, o GPD.

- Equipe Operativa Funcional - EOF, Este perfil (com formação acadêmica em qualquer área) remete a um profissional capacitado, habilitado e certificado para atuar no desenvolvimento de atividades de montagem das estações de trabalho para preservação digital, digitalização de acervos (documentos correntes, documentos históricos ou obras raras), processos de armazenamento e manutenção da informação em meio digital.

Procedimento n.2: Constituição de uma Força-tarefa

Acreditando que todos os participantes concluíram o primeiro procedimento, a segunda ação durante para a elaboração do plano de contingência é a constituição da equipe (Task Force) que irá se responsabilizar pelo desenvolvimento e execução do projeto, conclusão e manutenção dos resultados. O ideal é que seja um grupo membro da própria Instituição que tenha sido capacitado e certificado para atuar como Agentes de Preservação Digital, todavia não há barreiras para que a iniciativa privada também possa atuar a partir destes perfis, contanto que os colaboradores sejam capacitados e estejam habilitados para desenvolver tais competências, conforme o procedimento n.1.

Uma vez definida a Força Tarefa, deverão ser esquematizados e agendados os encontros e reuniões para entrega de resultados parciais até a efetivação do plano de contingência e mais tarde a auditoria e certificação. Assim, a primeira tarefa do grupo será a de delimitar o cenário de risco.

Procedimento n.3: Delimitação do cenário de risco

A delimitação do risco, no plano de contingência, trabalha no âmbito da suposição, dessa forma é preciso abstrair ou como se diz em Programação Orientada a Objetos (POO), lançar mão do recurso "mini-mundo" ou “Universo de Discurso”, isto é um recorte do mundo real a ser representado em linguagem de programação. Os especialistas da Task Force precisarão fazer um esforço diante de um cenário aparentemente inofensivo para supor quais as ameaças que podem estar à espreita no ambiente. Sempre levando em consideração que se uma ameaça é detectada, as vulnerabilidades são plurais. Sendo estes agentes causadores, quais podem ser, então, as consequências da instalação do risco (Previsão) e como proteger os ativos digitais de um sinistro (Salvaguarda). Estas são as perguntas que devem ser respondidas e constar na Matriz de Orientação (MOCR).

Procedimento n.4: Análise do cenário de risco

Este procedimento visa análise crítica do cenário risco, a partir dos documentos gerados pela aplicação das ferramentas Matriz OCR e Escala MCR, as quais devem fornecer aos especialistas o mapeamento dos principais fatores de risco, que em última análise são os atores que vão se apresentar no cenário do contingenciamento, em outras palavras, o risco ao qual o acervo está suscetível.

Procedimento n.5: Definição de ações de previdência

Nesta etapa é hora de determinar o que será feito para responder ao potencial desastre. São as respostas da coluna Salvaguarda da Matriz de Orientação. Para cada cenário de risco devem ser consideradas as ações e procedimentos a realizar desde o acionamento do plano de contingenciamento até o encerramento da emergência, considerando os recursos disponíveis. O que não deve ser feito em circunstância alguma é prever uma ação ou procedimento que demande um recurso que não conste na Matriz OCR.

Durante a preparação, a organização das ações e procedimentos varia, podendo ser definidos em função das características dos sinistros previstos, das condições do cenário (ambiente), das estimativas e controle dos danos, além da reabilitação dos cenários. Seguem algumas ações como sugestão:

- Monitoramento: Hierarquia do monitoramento a partir dos papéis. Do Gestor - GPD. Em um processo de preservação digital é ocupação do gestor do projeto averiguar se o ambiente (interno e externo) onde foi ou será instalado o núcleo está de acordo para receber a instalação. É também sua responsabilidade verificar se os procedimentos dos seus colaboradores estão em concordância com o padrão estabelecido no plano de contingenciamento, por meio de relatórios periódicos. Do Técnico - TPD. Cabe ao Técnico em preservação digital informar ao GPD do andamento das atividades da equipe e dos procedimentos e armazenamento, bem como produzir relatórios sobre a condição de funcionamento dos equipamentos e nível de qualidade dos objetos digitais produzidos. Da Equipe - EOF. A digitalização, limpeza do equipamento e organização do local de trabalho é sua responsabilidade, que deve ser regulada pelo TPD. Devem prestar conta dos resultados da produção ao seu superior por meio de relatório periódicos, estabelecidos conforme a necessidade do CDI.

- Alerta: Havendo discordância de algum procedimento, desde as instalações, falha no equipamento ou deficiência dos recursos humanos, o GPD deve imediatamente tomar as devidas providências. Caso o tamanho do problema fuja ao controle do gestor, este deve recorrer ao Conselho Memorial - uma assembleia formada pelos gestores, corpo técnico e representantes da equipe operativa para colaborativamente encontrarem a solução mais adequada ao problema. Da mesma forma por recorrer a Rede de apoio em Preservação Digital, à qual a Instituição está afiliada.

- Ações de socorro e assistência: Com o risco instalado no local, o objetivo é a proteção dos estoques. Deve ser solicitada a condição de estocagem, verificando em que situação se encontra cada um dos backup realizados. Em caso de perda ou dano do primeiro backup, deve ser solicitado o acionamento do segundo backup, constatando avaria no primeiro e segundo backup o armazenamento fora do ambiente (off-site) deve ser solicitado. Dependendo das características da avaria, manifestado o risco no ambiente físico ou digital é importante tomar as medidas apropriadas para cada situação.

- Restabelecimento de serviços essenciais: Definir como restabelecer as condições de segurança. Procurando identificar o que se perdeu e contabilizar o que pode ser recuperado.

Procedimento n.6: Implementação do modelo

Ao concluir o desenvolvimento do plano, há um passo essencial antes de sua implantação efetiva, que é a aplicação do modelo. É necessário fazer um ou mais testes de aplicabilidade do modelo para se ter noção de como o instrumento está reagindo na prática.

Para validar o documento deve ser realizada uma reunião em que haja a leitura do texto final. Após a leitura, a equipe da Força-tarefa, três colaboradores externos de outras Instituições da Rede de Apoio, um colaborador da Rede afiliada e mais um representante da sociedade civil devem assinar o Termo de Validação do Plano de Contingência (MI; SEDEC, 2017, p. 40 - adaptação nossa).

Após a aprovação, o documento final do plano de contingenciamento deve ser de conhecimento de todos os membros da rede colaborativa. Devendo ser disponibilizado no portal do sistema memorial ou página de Instituição, constando de contatos das instituições cadastradas e seus respectivos responsáveis pela execução.

Procedimento n.7: Auditoria

O plano de contingência deve ser desenvolvido, testado e aprovado. Após sua aprovação, o documento confere à Instituição Memorial a certificação para atuar por 12 meses. Após expirada a licença uma nova Força-tarefa deve ser constituída para fazer a auditoria tomando como base sempre o documento certificado anteriormente. A auditoria deve apontar os níveis de satisfação e deficiência do RI, a soma vertical e depois total de todos os indicadores resulta no valor do Ranking do Nível de Risco do Acervo. O protocolo que deve ser aplicado segue a ritualística do da primeira certificação.

Procedimento n.8: Certificação

Tendo em vista a imprevisibilidade de um desastre, é fundamental manter o plano de contingência atualizado, tarefa desafiadora, mas que pode ser cumprida com revisões regulares. O plano deve especificar a frequência das revisões e seus responsáveis. A certificação só será expedida após a liberação do Protocolo de Auditoria que inclui todos os procedimentos deste modelo, exceção do procedimento n.6, visto que o modelo foi implantado anteriormente.

REFERÊNCIAS

ANDRADE, João Paulo Moraes de. Contingência de risco: uma questão de segurança em Preservação Digital. 2018. 169f. Dissertação (Mestrado em Ciência da Informação) – Universidade Federal de Pernambuco, Recife, 2018.

GALINDO, Marcos. Memória em Sistemas Complexos. In: OLIVEIRA, Eliane Braga de; RODRIGUES, Georgete Medleg (Org). Memória interfaces no campo da informação. No prelo.

FRANK, Rebecca D.; YAKEL, Elizabeth. Disaster planning for digital repositories. Proceedings of the American Society for Information Science and Technology, 50(1), p. 1-10, 2013. Disponível em: <https://goo.gl/bHVKHL> Acesso em: 17 abr. 2016.

MINISTÉRIO DA INTEGRAÇÃO NACIONAL; SECRETARIA NACIONAL DE PROTEÇÃO E DEFESA CIVIL. Módulo de formação: elaboração de plano de contingência, livro base. Brasília: Ministério da Integração Nacional, 2017. Disponível em: <https://goo.gl/ohH9cr> Acesso em: 20 out. 2017.

SILVA JUNIOR, Laerte; MOTA, Valéria Gameleira da. Políticas de preservação digital no Brasil: características e implementações. Ci. Inf., Brasília, DF, v. 41 n. 1, p.51-64, jan./abr., 2012. Disponível em: <https://goo.gl/WEhvbC> Acesso em: 17 abr. 2016.

TAVARES, Aureliana. Análise de Risco e Preservação Digital: uma abordagem sistêmica na Rede Memorial de Pernambuco. 2014. 214f Dissertação (Mestrado em Ciência da Informação) – Universidade Federal de Pernambuco, Recife, 2014. – Recife. Disponível em: <https://goo.gl/NYXek4> Acesso em: 17 abr. 2016.

UNITED NATIONS HIGH COMMISSIONER FOR REFUGEES - UNHCR. Contingency planning for emergencies: a manual for local government units. 2ª edição. 2003. Disponível em: <https://goo.gl/n3thSR> Acesso em: 20 ago . 2017.