PLANO DE RECUPERAÇÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO: SEGUNDO MELHORES PRÁTICAS.

Aliny Gleicia Tristão[1]
Orientador: M. William Divino Ferreira[2]

RESUMO

Os ataques realizados com sucesso crescem exponencialmente e estão provocando diferentes tipos de interrupções nos Serviços de Tecnologia da Informação, entre eles, aqueles que sustentam as operações críticas do negócio. Estar preparado para o processo de recuperação, através da combinação de ações de prevenção e recuperação, minimiza o impacto sobre a organização e as eventuais perdas de informações. O Plano de Recuperação dos Serviços de Tecnologia da Informação compõe-se de procedimentos como: enumerar serviços críticos, analisar vulnerabilidades, definir papéis e responsabilidades, testar e documentar procedimentos de restauração. Através desse conjunto de procedimentos é possível validar a melhor forma de realizar a recuperação dos serviços. Este Plano é uma das etapas do Plano de Continuidade do Negócio, que faz parte da Política de Segurança da informação, referenciado em normas como: ABNT NBR ISO 22301:2013, ABNT NBR ISO/IEC 27002:2013 e ISO/IEC 27035:2016. Este artigo reunirá as boas práticas apresentadas nestas normas e na biblioteca ITIL que convém serem aplicadas na elaboração do Plano de Recuperação de Serviços de Tecnologia da Informação.

Palavras-chave: Plano de Recuperação de serviços de Tecnologia da Informação. Continuidade de Negócios. Política de Segurança da Informação. Melhores Práticas. ISO IEC 27K. ITIL.

ABSTRACT

Due to successful attacks, interventions on the information technology systems are growing and they are causing services descontinuaty. Be prepared for the recovery process by combining prevention and recovery actions, minimizing the impact on an organization, and eventual loss of information. The Recovery Plan for Information Technology services consists of procedures such as enumerating critical services, analyzing vulnerabilities, defining roles and responsibilities, testing and documenting restoration procedures. Through a set of procedures and possible the best way to perform a service recovery is possible. This regulation is one of the steps of the Business Continuity Plan, which is part of the Information Security Policy, referenced in standards such as: ABNT NBR ISO 22301: 2013, ISO / IEC 27002: 2013 and ISO / IEC 27035: 2016. This article will gather as good practices presented in these norms and in the ITIL library that are convenient to apply in the elaboration of the Plan of Recovery of Information Technology Services.

Keywords: Recovery Plan for Information Technology services. Business Continuity. Information Security Policy. Best Practices. ISO IEC 27K. ITIL.

1 INTRODUÇÃO

Um dado, antes de ser processado, tem pouco valor, mas, após o processamento, ele se torna uma informação que pode gerar conhecimento,

[1]Graduação em Redes de Computadores. E-mail:alinytristao@gmail.com
[2] Mestre em Engelharia da Computação. E-mail:wferreira7@gmail.com

agregando valor aos negócios. Conclui-se que informação constitui um ativo estratégico para tomada de decisão segundo a norma NBR ISO/IEC 27002:2013.

A importância da informação cresce junto com a necessidade de protegê-la contra o grande número de ameaças ou vulnerabilidades que podem prejudicar os serviços críticos de Tecnologia da Informação (TI) e comprometer os princípios básicos da segurança da informação: a integridade, a confiabilidade e a disponibilidade.

A segurança da informação, é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

Planejar, estabelecer, implementar, operar, monitorar, rever, manter e melhorar continuamente um sistema de gestão documentado, preparando a organização para responder e recuperar-se de eventos que possam interromper o funcionamento normal, são requisitos apresentados na norma NBR ISO/IEC 22301.

A abordagem de diferentes processos que envolvem a recuperação de serviços de TI, em normas como NBR ISO/IEC 27002, NBR ISO/IEC 22301 ou padrões internacionais como ITIL, colaboram para a elaboração de um Plano de Recuperação de Serviços, completo e eficiente. A falta de recursos financeiros para aquisição das diferentes normas e biblioteca ITIL, juntamente com a restrição de tempo para o estudo delas nas rotinas de grande parte dos profissionais de Tecnologia da Informação, inviabilizam o acesso a esse conhecimento, por esse motivo apresentado neste artigo.

2 O QUE É ITIL

O ITIL (Information Technology Infrasctructure Library – Biblioteca de Infraestrutura de Tecnologia da Informação) surgiu de uma demanda do governo britânico por mais qualidade nos serviços de TI a ele prestados. Desta forma, foram desenvolvidas melhores práticas para gerenciar a utilização eficiente e responsável dos recursos de TI, independente do fornecedor que prestasse o serviço. É o resultado de anos de observação e estudos, sugerindo que área de TI seja vista como uma provedora de serviços e que esses serviços, uma vez estratégicos, devem ser tratados por todo seu ciclo de vida, sendo mensurados e gerenciando o valor que agregam ao negócio.

2.1 ESTRUTURA ITIL

Estrutura-se em cinco livros. O eixo do ITIL, versão três, tem como núcleo de condução das atividades o livro de Estratégia de Serviço, norteando os demais livros. Circundando todos, está o livro de Melhoria Contínua de Serviço. Processos e funções são distribuídos ao longo do ciclo de vida se dividindo em três grupos de conceitos: Um de análise de requisitos e definição inicial, onde estão dois livros, Estratégia e Desenho do Serviço; o outro grupo de conceito é o de implantação no ambiente produtivo/operacional, com o livro Transição de Serviço; e por último, operação e melhoria em produção, com os livros: Operação de Serviço e Melhoria Contínua de Serviço.

2.1.1 Desenho de Serviço

O principal objetivo de desenhar serviços, segundo FELÍCIO (2012), é para que estejam de acordo com as expectativas do negócio, promovam maior eficiência e eficácia durante o seu ciclo de vida, diminua prazos e custos, desenvolva métricas e medições.

Os processos de Desenho de Serviço segundo ITIL versão 3 (três) são: Gerenciamento do Nível de Serviço – responsável por manter, melhorar e entregar a qualidade esperada pelo negócio, através de contratos de Acordos de Nível de Serviço (ANS) conhecidos como: Service Level Agreement (SLA) e Acordos de Nível Operacional (ANO), medindo o desempenho, justificando os custos relacionados ao negócio; Gerenciamento do Catálogo de Serviço – responsável por manter um catálogo com uma lista atualizada dos serviços que estão em operação, compondo o Portfólio disponível e visível ao cliente; Gerenciamento de Disponibilidade – responsável por manter todos os aspectos da disponibilidade e indisponibilidade de serviço, avaliando impactos e riscos de cada componente para o negócio; Gerenciamento de Segurança da Informação – o objetivo é alinhar a segurança de TI com a segurança do negócio e garantir que a segurança da informação seja efetivamente gerenciada em todos os serviços e atividades; Gerenciamento de Fornecedores – é responsável por gerenciar fornecedores e os serviços entregues por eles, verificar a qualidade e analisar contratos, garantindo o devido retorno sobre o investimento; Gerenciamento de Capacidade – é responsável por fornecer a

capacidade de acordo com a demanda gerada pelo negócio, contrabalanceando as reais necessidades de serviço do negócio para atender a demanda; Gerenciamento de Continuidade dos Serviços de TI (GCSTI) – é responsável por garantir a continuidade do negócio, avaliando impactos, gerenciando riscos, com o plano atualizado de continuidade de serviços.

2.1.2 Transição de Serviço

Provê direcionamento para desenvolver e melhorar as capacidades de transferir serviços novos ou alterados para produção de maneira efetiva e com os riscos controlados. Os seguintes processos fazem parte da Transição de Serviços, segundo ITIL v3: Planejamento e suporte à transição, Gerenciamento de Mudança, Gerenciamento de ativos de serviço e configuração, Gerenciamento de liberação e distribuição, Validação e testes do serviço, Avaliação e Gerenciamento do Conhecimento.

A Transição de Serviço efetua o planejamento pragmático dos serviços, incluindo: desenho renovado dos processos de mudança, liberações e configurações, garantia da qualidade e riscos do projeto, gerenciamento da organização e mudanças culturais durante a transição, sistema de conhecimento em gerenciamento de serviços, integração dos projetos na transição, criação e seleção de modelos de transição.

O escopo da Transição de Serviço envolve: gerenciamento e coordenação dos processos, funções e sistemas utilizados para empacotar, construir, testar e entregar uma liberação em produção; processos que suportam todas as fases do ciclo de vida do serviço: Gerenciamento de mudanças; Gerenciamento de ativos de serviços e configurações; Gerenciamento do Conhecimento.

Agrega valor para o negócio com melhorias no tratamento de mudanças nos serviços: adaptação rápida a novos requerimentos; aumento do sucesso na implantação de mudanças; melhor predição de níveis de serviço e produtividade.

2.1.3 Operação de Serviço

Os principais objetivos da Operação de Serviço, segundo FELICIO (2012), são: manter, conduzir, operar, controlar e gerenciar as operações no dia-a-dia,

sendo responsável pela tecnologia utilizada para entregar os serviços, garantindo a estabilidade a um custo justificável.

Os processos são: Gerenciamento de Eventos – controla e gerencia os eventos ocorridos na infraestrutura de TI. Gerenciamento de Incidentes – é responsável por restabelecer a operação dos serviços de TI no menor tempo possível, com o menor impacto para o negócio, garantindo o Acordo de Nível de Serviço. Cumprimento de Requisição – canal direto que deve ser utilizado pelos usuários para requisições diversas. Gerenciamento de Problemas – minimizar o impacto nos negócios, encontrando a causa raiz dos incidentes, prevenindo a recorrência de incidentes e o impacto ao negócio. Gerenciamento de Acessos – garantir aos usuários os devidos acessos autorizados, impedindo os acessos não autorizados.

2.2 DEFINIÇÕES

Ameaça: Pessoa, situação ou evento natural do ambiente (externo ou interno), que é visto como causa potencial de um incidente ou desastre provocando danos segundo ISO/IEC 27000:2016.

Vulnerabilidade: uma fraqueza que ocorre acidental ou intencionalmente e pode ser causada pela falta de controle, permitindo que a ameaça ocorra e afete os interesses do negócio, segundo ISO/IEC 27000:2016.

Risco: A probabilidade de uma ameaça para a existência de uma ou mais vulnerabilidades com impactos adversos resultantes para a instituição, segundo ITIL v3.

Impacto: É o efeito que provoca a ocorrência de um incidente ou acidente, segundo ITIL v3. O risco é medido através de aspectos econômicos, imagem, de reputação, diminuição da capacidade de resposta e competitividade, a interrupção das operações, consequências jurídicas e físicas para as pessoas afetadas. Mede o nível de degradação de um dos seguintes elementos da Continuidade: confiabilidade, disponibilidade e capacidade de recuperação, segundo NBR ISO/IEC 27002:2013.

Controle: O processo, política, dispositivo, prática ou qualquer medida que modifica o risco, segundo ISO/IEC 27000:2016.

Evento – É qualquer ocorrência que tenha um significado para a gerência da infraestrutura de TI ou para a entrega do serviço, segundo ISO/IEC 27000:2016. Um evento pode, ou não, gerar um registro informativo ou alerta que deverão ser tratados pelo processo de Gerenciamento de Incidentes, ou pela área técnica de forma proativa, a fim de evitar que se torne um incidente.

Incidentes - Uma interrupção não planejada ou redução na qualidade de um serviço de TI. Falha em um item de configuração (IC) que ainda não tenha impactado o serviço é também um incidente segundo FELÍCIO (2012).

Incidentes Graves – São aqueles que têm um alto impacto nas áreas de negócio. Procedimentos separados são necessários para tratá-los, com limites de tempo menores e com maior prioridade.

Desastre - É um acontecimento que afeta de tal forma um serviço ou sistema que a restauração do seu nível de desempenho original exige considerável esforço, segundo ITIL v3. Um incidente chega a ser insignificante comparado a um desastre, pois o negócio pode parar parcial ou totalmente.

Problema - é a causa subjacente de um ou mais incidentes, segundo FELÍCIO (2012). Um Incidente tem uma relação com o efeito que uma interrupção causa no serviço, e um Problema tem uma relação com a causa raiz que fez com que houvesse a interrupção de um determinado serviço de TI.

Solução de Contorno - reduz ou elimina o impacto de um incidente ou problema, o qual ainda não existe uma solução definitiva documentada. Uma vez que, em determinadas ocasiões, o processo de Gerenciamento de Incidentes pode não ter achado uma solução de contorno, o processo de Gerenciamento de Problemas o identifica e informa para que o serviço seja restaurado de forma mais rápida, até que à solução definitiva possa ser aplicada, conforme FELÍCIO (2012).

Processo - É um conjunto de atividades inter-relacionadas com um objetivo especifico. Possui entradas de dados, informações e produtos para, através da identificação dos recursos necessários ao processo, transformar estas entradas nos objetivos previstos, segundo ITIL v3.

Erro conhecido - É um incidente ou problema para o qual a causa raiz é conhecida e para o qual foi identificada uma solução de contorno temporária ou alternativa permanente, segundo FELÍCIO (2012).

Base de Dados de Erros Conhecidos (BDEC) – Onde são armazenados os erros conhecidos, com os procedimentos de contorno e soluções definidas, segundo FELÍCIO (2012).

Serviço de TI - É um conjunto de funções relacionadas, que suportam uma ou mais áreas do negócio conforme ITIL v3. Composto de pessoas, processos e tecnologias (hardwares, softwares e comunicações de dados).

Item de Configuração (IC): é qualquer componente ou outro ativo de serviço que precise ser gerenciado de forma a entregar um serviço de TI, conforme em FELÍCIO (2012). Incluem serviços de TI, hardware, software, instalações, pessoas e documentação formal, tais como documentação de processos e acordos de nível de serviço. ICs estão sob controle do processo gerenciamento de mudança.

Linha de Base de Configuração: Configuração de um serviço, produto ou infraestrutura acordado com o cliente que é usado como um ponto de referência, ou base. Podendo ser alterado somente de acordo com os processos de gerenciamento de mudanças, conforme FELÍCIO (2012).

2.3 PRINCIPAIS PROCESSOS RELACIONADOS COM O PLANO DE RECUPERAÇÃO DE SERVIÇOS DE TI EM ITIL V3

2.3.1 Processo de Gerenciamento da Continuidade do Serviço de TI - GCSTI

Segundo FELÍCIO (2012), o GCSTI visa suportar o processo de Gerenciamento da Continuidade do Negócio (GCN) com a garantia de que a infraestrutura técnica e de serviços sejam recuperadas dentro do prazo especificado e acordado com o cliente. Isso pode ser alcançado criando e/ou mantendo planos de continuidade atualizados através de constante análise de risco, em conjunto com o gerenciamento da disponibilidade e segurança.

Responsabilidades atribuídas a este processo segundo ITIL v3: avaliar o risco e impacto da perda dos serviços de TI; definir o tempo de restauração dos diferentes serviços; identificar serviços primordiais para o negócio e as medidas de prevenção adicionais; elaborar a abordagem que será utilizada para a restauração dos serviços; criar medidas para prevenir e reduzir os efeitos do impacto de um desastre; estruturar, manter e testar um plano de recuperação que seja bem detalhado para restaurar os serviços no período definido. Estão dentro deste

processo: A análise de impacto no negócio, conhecido como Business Impact Analysis (BIA) que consiste em uma técnica usada na identificação dos requisitos mínimos necessários de sistemas para manter os processos de negócio críticos. A determinação desses requisitos vem tanto do impacto da perda de um processo de negócio, quanto das perdas financeiras, ou danos à imagem corporativa, além da quebra de regulamentos e leis; a análise de risco consiste no levantamento feito sobre as ameaças e níveis de vulnerabilidade. Cada ameaça é associada a uma possível interrupção nos serviços críticos, tanto de TI, quanto do negócio. Dessa tarefa geralmente são originados um relatório e um plano para aplacar os riscos.

O processo de Gerenciamento de Continuidade de Serviço de TI conforme o ITIL v3: investiga, desenvolve, implementa opções para recuperação de serviços e interage, particularmente, com os seguintes processos: Gerenciamento do nível de serviço, fornecendo informações sobre as obrigações dos serviços de TI, por exemplo o SLA acordado; Gerenciamento da disponibilidade, desenvolvendo e implementando medidas de prevenção; Gerenciamento da configuração, fornecendo informações sobre o que é preciso restaurar depois de um desastre; Gerenciamento de capacidade, garantindo que as exigências do negócio tenham suporte dos recursos de TI; Gerenciamento de mudança, garantindo que todos os planos do gerenciamento da continuidade dos serviços de TI estejam atualizados e corretos.

2.3.2 Gerenciamento de Configuração e Ativos de Serviço de TI.

Sistema de Gerenciamento de Configuração (SGC) é um conjunto de ferramentas, dados e informações, usados para dar suporte ao gerenciamento de configuração e ativo de serviço de TI, segundo ITIL v3. Coleta, armazena, atualiza, analisa e apresenta dados sobre todos os itens de configuração, incidentes, problemas, erros conhecidos, mudanças, liberações e seus relacionamentos.

O SGC se estrutura em três camadas, FELÍCIO (2012): Camada de Dados, de Integração e de Processamento do Conhecimento. O processo de Gerenciamento de Configuração deve garantir que todos os itens de configuração (IC) estejam devidamente registrados e que as informações relevantes e características estejam claras e precisas. Além disso, é fundamental que a base de dados de configuração contenha informações de referência para que a performance atual dos itens de configuração possa ser comparada com os parâmetros

estabelecidos no processo do desenho do serviço, a fim de garantir que as ações corretivas sejam prontamente adotadas sempre que um desvio é identificado.

Cada IC deve ser devidamente classificado para permitir sua rápida identificação e rastreamento. Exemplos de categorias são: hardware, software, serviços, documentação, processos, pessoas. As principais atividades dentro do processo de gerenciamento de configurações são conforme apresentado pelo ITIL:

- Planejamento: Define o escopo que será controlado (serviços, aplicativos, infraestrutura, locais), as políticas, os papéis e responsabilidades, as interfaces com outros processos, as ferramentas a serem usadas;
- Identificação: Define o critério para seleção de IC e seus componentes, associa um ID para cada e específica atributos relevantes.
- Controle da configuração: Mantêm o controle efetivo dos IC´s. Garante que não sejam removidos, alterados ou inseridos sem um procedimento definido;
- Controle e reporte do ciclo de vida: É fundamental que os itens sejam controlados durante todo o ciclo de vida.
- Verificação e auditoria: Garante que as informações dos IC´s que estão registradas no banco de dados de configurações estejam atualizadas e fieis a configuração real do IC.

Este processo também pode entregar um modelo de serviços ativos e de infraestrutura por meio de registro dos relacionamentos entre os ICs, que é usado para facilitar a resolução de problemas e a implementação de mudanças, pois permite verificar o impacto das mudanças no planejamento financeiro, uma vez que verifica a capacidade de utilização dos mesmos, para novas liberações. Todos os processos dentro do ITIL estão vinculados ao gerenciamento de configuração, ou pelo menos consultarão o banco de dados dele.

2.3.3 Gerenciamento de Incidentes

O Gerenciamento de Incidentes tem como objetivo principal restaurar a operação do serviço normal, o mais rápido possível e minimizar o impacto causado sobre as operações do negócio, visando sempre a melhor qualidade de serviço e disponibilidade, segundo FELÍCIO (2012); busca também, a eficiência e eficácia do processo; produz informações gerenciais, como relatórios de atendimento e de tipos de incidentes; gerencia o trabalho das equipes de suporte nível I e II; gerencia os

incidentes graves; desenvolve e mantém processos e procedimentos levando em consideração: Limites de Tempo – Acordados para todas as fases do processo, baseado nas metas de tempo de resposta e resolução dentro do SLA e usados como metas nos Acordos de Nível Operacional e contratos com os fornecedores; Modelos de Incidentes – Que determinam os passos necessários para executar o processo de recuperação de incidentes corretamente; processam com maior eficiência os incidentes comuns, pois o processo de resolução já existe.

Atividades do Gerenciamento de Incidentes conforme o ITIL v3: Identificação - o processo é iniciado com a identificação do incidente; Registro - todos os incidentes precisam ser registrados em um sistema; Classificação: Classificar todas as requisições registradas; Priorização - priorizar de acordo com o impacto e urgência; Diagnóstico - averiguar o que não está funcionando adequadamente, qual a causa, possíveis soluções já existentes, e se necessário uma solução de contorno; Escalação - se o incidente não puder ser resolvido pela central de serviços, ele será escalado dentro do tempo hábil para outro nível de suporte com maior capacidade técnica; Investigação e diagnóstico – Caso seja escalonado para outro nível, repete esta etapa; Resolução e recuperação: identifica uma solução a ser testada e aplicada; Fechamento: a central de serviços categorizará o motivo do incidente, documentará, e disponibilizará para que o usuário responda a pesquisa de satisfação.

Responsabilidades deste processo: Equipes de Suporte são classificadas em níveis. O primeiro é feito pela Central de Serviços e inclui registro, classificação, escalonamento, resolução e fechamento dos incidentes. Os segundo e terceiro níveis investigam, diagnosticam, e recuperam os incidentes. Possuem maior conhecimento técnico sobre o assunto. O terceiro nível poderá ser formado por fornecedores de software ou hardware. Os níveis podem variar dependendo do tamanho da área de TI.

O Gerenciamento de Incidentes tem relação com: o Gerenciamento de Problemas – Incidentes são causados por problemas que devem ser resolvidos. Serão reportados como erros conhecidos e utilizados para agilizar a resolução de incidentes; Gerenciamento de Configuração – utilizado para identificar os componentes associados ao serviço e avaliar o impacto de um incidente; Gerenciamento de Mudança – para implantar uma solução de contorno, pode ser necessário abrir uma requisição de mudança; Gerenciamento de Capacidade –

Fornece o desempenho dos itens de configuração. Gerenciamento de Disponibilidade – usa dados dos incidentes para mensurar a disponibilidade dos serviços; Gerenciamento de Nível de Serviços – recebe relatórios para definir as metas.

2.3.4 Gerenciamento de Problema

O objetivo principal do Gerenciamento de Problema segundo ITIL v3 é acompanhar todo o Ciclo de vida dos problemas identificando as causas principais e minimizar ao máximo seus impactos no negócio, prevenindo que problemas voltem a ocorrer.

Elementos proativos de resolução de problemas: identificar e facilitar a remoção de erros antes que eles se manifestem como reclamações ou perguntas de usuários finais. Com isso, o Gerenciamento do Conhecimento tem uma relação estreita com o de Problema, já que utilizam uma base de dados de erros conhecidos que serão usados por ambos.

Principais diferenças entre o Gerenciamento de Problema e o de Incidente: O de Incidente não faz a investigação para encontrar a causa do problema, tem foco na recuperação do serviço de forma rápida, utilizando soluções de contorno disponíveis na base de erros conhecidos, produzida pelo Gerenciamento de Problema; é totalmente reativo, ou seja, só é iniciado quando for reportado algum incidente. Já o Gerenciamento de Problema, segundo FELÍCIO (2012) pode ser reativo ou proativo. Suas atividades consistem em: Identificação; Registro; Classificação; Priorização; Investigação e diagnóstico; Identificação e erros conhecidos; Resolução de problemas; Encerramento; Revisão.

Gerenciamentos de Problema tem relação com: Mudança – Levanta requisições para corrigir erros; Gerenciamento de Configuração – é usado para identificar se existem erros em relação aos Itens de Configuração usados no serviço; Gerenciamento da Liberação e Implantação – Lança correções de problemas no ambiente de produção; Gerenciamento de Disponibilidade – trabalha em conjunto com o de Problema de forma proativa para identificar formas de reduzir o downtime (tempo de parada); Gerenciamento de Capacidade – investiga alguns problemas, auxiliando em medidas proativas de capacidade; Gerenciamento de Continuidade – se um problema não for resolvido a tempo, pode ser necessário invocar o Plano de

Continuidade; Gerenciamento de Nível de Serviço – O de Problema contribui para alcançar as metas de qualidade, ajudando a prevenir incidentes e problemas; Gerenciamento Financeiro – fornece informações de custos na prevenção e resolução de problemas.

O Gerente de Problema deve assegurar que sejam solucionados todos os problemas dentro das metas, proteger e ter propriedade do banco de dados de erros conhecidos, acompanhar o encerramento formal dos registros de problemas e organizar, conduzir, documentar e acompanhar todas as atividades de revisão.

3 PLANO DE RECUPERAÇÃO

Conforme as melhores práticas do ITIL v3, para a elaboração do Plano de Recuperação é necessário um conjunto de processos e procedimentos com papéis, responsabilidades e prazos revisados e atualizados constantemente, compondo-se por atividades minuciosamente planejadas para execução antes, durante e depois da ocorrência de um incidente ou desastre, considerando cada aspecto do serviço de TI que pode ter suas funcionalidades comprometidas.

São recursos essenciais para o plano, e devem ser elaborados ou executados antes da etapa de recuperação, do incidente ou desastre:

1. Catalogo de Serviços de TI relacionado com o Catalogo do Negócio. Conforme orientado pelo processo de Gerenciamento de Catalogo de Serviços, em Desenho de Serviço pelo ITIL v3.
2. Acordo de Nível de Serviço (SLA, ANO) para os serviços críticos, ITIL v3.
3. Banco de Dados de Configuração com a documentação dos recursos de hardware, software, infraestrutura, comunicação de dados, ambientes e seus relacionamentos com todos os sistemas críticos, seus gestores e utilizadores, segundo FELÍCIO (2012).
    - Documentação mínima para software: Configuração de hardware exigida; versão utilizada; data e hora da última execução de sucesso; forma de recuperação das transações perdidas; adaptações ao ambiente de utilização e/ou aos utilizadores; fornecedores e detalhes de licenças de uso e contratos de manutenção.
    - Documentação mínima para hardware: Especificação completa da configuração física; configuração implementadas; necessidade de espaço

em disco para o ambiente operacional e sistemas críticos; fornecedores e detalhes de licenças de uso, seguros e contratos de manutenção.

- Documentação mínima para comunicação de dados: Arquitetura da rede; pontos de conexão; tecnologia de comunicação; especificação de dispositivos: para roteamento, chaveamento, concentradores; serviço de comunicação (tipo de provedores do serviço).
- Documentação mínima para ambiente: Climatização; capacidade; temperatura, umidade e tensão para operação; energia elétrica; carga a ser suportada; estabilizador e nobreak (características e capacidade); pontos para conexão; comunicação de voz; características do prédio.

4. Análise de risco para as principais atividades da organização. Conforme apresentado no Desenho de Serviço e no processo de GCSTI.
5. Avaliação de Impacto nos Negócios – BIA, também apresentado no Desenho do Serviço no processo GCSTI.
6. Logs para auditoria de servidores, equipamentos de rede, sistemas e qualquer ativo crítico devem estar habilitados e acessíveis sempre que necessário, para as pessoas autorizadas.
7. Contato de Fornecedores, documentação disponível e de fácil acesso. Conforme processo de Gerenciamento de fornecedor, ITIL v3.
8. Política e procedimentos para cópias de segurança e retenção de arquivos, testes de restauração e documentação: Política de geração, descrição e características de cópias de segurança (ambientes externos); Recuperação das bases de dados (equipamentos e capacidade); Documentação completa dos sistemas e programas utilizados; Dependências de outros sistemas ou serviços; Instalação alternativa para execução das funcionalidades críticas; Notificação e acesso (contratos e normas estabelecidos), conforme SOMASUNDARAM (2011).
9. Níveis ou categorias definidas de incidentes ou desastre para recuperação, segundo FELÍCIO (2012).
10. Tabela de escalonamento com os contatos dos diferentes níveis.
11. Papéis x Responsabilidades, documentação de fácil acesso e disponível a toda a equipe envolvida, conforme ITIL v3.
12. Procedimentos de restauração críticos e específicos já testados.

Etapas durante e após a ocorrência do incidente ou desastre:

1º. Identificação. Convém implementar o monitoramento dos serviços críticos para que seja gerado um alerta após a ocorrência de eventos críticos conforme indicados em Gerenciamento de Segurança da Informação, segundo FELÍCIO (2012).

2º. Registro. Qualquer incidente ou desastre deve ser registrado contendo: data, hora e informações relevantes conforme o Gerenciamento de Configuração.

3º. Categorização e Classificação. Todos os incidentes ou desastres devem ser classificados e categorizados para que sejam tratados, de acordo com sua gravidade e posteriormente analisados como indicadores, segundo o processo de melhoria continua apresentado no ITIL v3, FELÍCIO (2012).

4º. Priorização. O Catalogo de Serviços deve ser consultado para identificação de quais serviços do negócio foram afetados, com seus SLAs e ANOs. Verificar também o impacto e a Urgência conforme a tabela BIA no GCSTI.

5º. Escalação. De acordo com o grau do problema e dentro do tempo hábil deve ser escalonado para outro nível de suporte com maior capacidade conforme Gerenciamento do Conhecimento ou Fornecedores.

6º. Investigação e diagnostico. Convém consultar a Base de Erros Conhecidos para identificar soluções já documentadas e configurações dos ICs envolvidos e seus relacionamentos, conforme o Gerenciamento de Configuração.

7º. Decisão sobre uma solução de contorno para minimizar impacto no negócio, e retomar o funcionamento de atividades críticas, segundo o Gerenciamento de Incidente e Problema.

8º. Resolução e recuperação. Consultar planos ou processos já definidos para serem seguidos conforme GCSTI. Avaliar capacidade, e os impactos das mudanças, antes de aplicar a recuperação. A principal garantia da restauração de serviços críticos é um backup funcional.

9º. Revisão. Atualizar documentações conforme gerenciamento de Mudanças.

10º. Correção de Erros Conhecidos. Documentar alterações identificadas.

11º. Fechamento. Avaliar melhorias nos processos, a satisfação do cliente e a eficiência e eficácia das métricas segundo processo de melhoria continua apresentado pelo ITIL v3.

A ISO/IEC 27035:2016 orienta no Gerenciamento de Incidentes de segurança da informação, processos para planejar, preparar; detectar e reportar; avaliar e decidir; responder e recuperar; etapas após incidente: o que aprender

com os incidentes, como se prevenir, e a documentação de evidências. O que diferencia nas etapas e processos apresentados acima é a necessidade de procedimentos específicos na identificação e coleta de evidências.

4 CONCLUSÃO

O plano de recuperação de Serviços de TI referência ações indispensáveis à restauração das funcionalidades críticas da organização, em caso de incidentes ou desastres, de acordo com prioridades e prazos estabelecidos pelos utilizadores da informação. Promovendo uma recuperação de maneira controlada, pois toda a equipe estará ciente do seu papel com relação aos procedimentos, melhorando a compreensão da inter-relação entre problemas de desempenho e problemas de capacidade, e o relacionamento com o negócio. Aumentando o tempo de disponibilidade do serviço, minimizando a interrupção de atividades, gerenciando os riscos, a fim de garantir que a organização possa dar continuidade à sua operação, ao menos em um nível mínimo predeterminado a um custo justificável.

Para a elaboração do plano, convêm seguir as abordagens de Gerenciamento de serviços de TI pela Biblioteca ITIL e relacionar com as demais normas de Tecnologia da Informação referente à continuidade do negócio ou segurança da informação. O Plano de Recuperação de Serviços de TI não substitui o Plano de Continuidade de Negócio ou a Política de Segurança da Informação e sim, se integra como parte dos processos destes.

5 REFERENCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 22301: Segurança da sociedade: Sistema de gestão de continuidade de negócios — Requisitos**. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO/IEC 27000: Information technology - Security techniques - Information security management systems - Overview and vocabulary**. Suiça, 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27002: Tecnologia da informação: Técnicas de segurança — Código de prática para controles de segurança da informação - apresentação**. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27035: Tecnologia da informação Parte 1, 2 e 3: Técnicas de segurança – Gestão de incidentes de segurança da informação.** Rio de Janeiro, 2016.

CESTARI FILHO, FELÍCIO. **ITIL v3 Fundamentos.** Rio de Janeiro: RNP/ESR, 2012

CALDER, ALAN. **ISSO 27001 / ISSO 27002 A Pocket Guide.** 2.ed United Kingdom: ITgp, 2013.

SOMASUNDARAM, G.; SHRIVASTAVA, Alok; EMC, Education Services. **Armazenamento e Gerenciamento de Informações.** 1.ed. Porto Alegre: Bookman, 2011.

SOUZA, Silvio Danilo Felipe de; SILVA, Edilberto Magalhães. **Proposta de Elaboração de um Plano de Continuidade de Negócio (PCN) de acordo com a realidade e necessidades de uma Instituição de Ensino Superior**. 2013. 20 f. Trabalho de Conclusão de Curso (Especialização em Segurança da Informação) – Faculdade SENAC, Distrito Federal, 2012.