

MODELO OPERACIONAL DA INFRAESTRUTURA DE TI DO TCU

Neste documento, o Modelo Operacional de Infraestrutura de TI do TCU será denominado, de forma resumida, apenas como Modelo Operacional.

Os motivadores do modelo operacional (Figura 1) são:

- I. Segurança da Informação: Mitigar riscos de segurança cibernética.
- II. Inovação: Acelerar inovação e a transformação digital.
- III. Transparência: Democratizando as informações para agilizar as tomadas de decisões e orientado a indicadores.

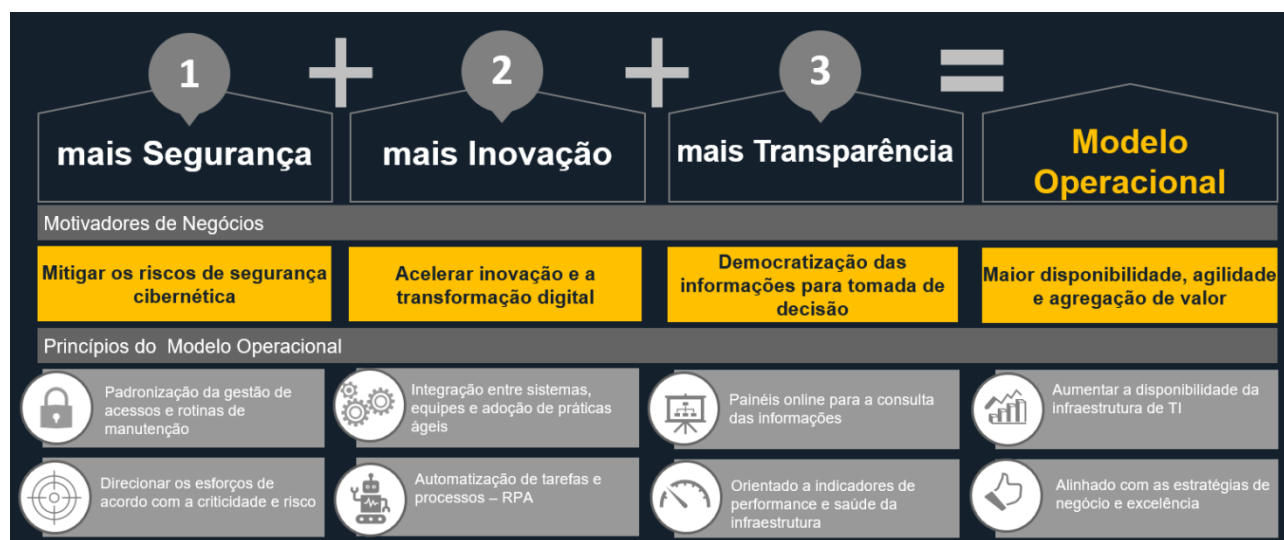


Figura 1: Motivadores do modelo operacional

1. Visão geral dos processos e boas práticas

1.1. O modelo operacional da infraestrutura de Tecnologia da Informação do TCU é composto por 14 processos e/ou boas práticas ilustrados na Figura 2, sendo eles:

- 1.1.1. Central de serviços
- 1.1.2. Gestão de Eventos
- 1.1.3. Gestão de Configuração
- 1.1.4. Gestão de Incidentes
- 1.1.5. Gestão de Problemas
- 1.1.6. Gestão de Mudanças
- 1.1.7. Gestão de Crise

- 1.1.8. Gestão de Demandas
- 1.1.9. Gestão de Liberação
- 1.1.10. Manutenção Sistemática
- 1.1.11. Gestão de Disponibilidade
- 1.1.12. Gestão de Capacidade
- 1.1.13. Gestão de Acesso
- 1.1.14. Gestão do Conhecimento

1.2. A lista descrita no item 1.1 não é exaustiva e ao longo do tempo alterações podem ocorrer, sendo possível adicionar, alterar ou remover processos após a validação e aprovação por parte dos responsáveis pela gestão da infraestrutura de TI do Tribunal.

1.3. A Figura 2 ilustra as principais entradas (usuários do TCU, ferramentas de monitoramento, agendamento das manutenções sistemáticas e funcionários das secretarias diretamente relacionadas à área de Tecnologia da Informação – TI), a interligação de alguns processos (gestão de eventos, manutenção sistemática, incidentes, problemas, mudança, crise, demandas e de liberação) para atender tanto à sustentação do ambiente produtivo como a sua evolução. Por fim, também são descritos outros processos transversais (central de serviços, gestão da disponibilidade, configuração, capacidade, acesso e conhecimento) que deverão ser seguidos pelos profissionais da contratada, segundo planejamento previamente aprovado pelo Tribunal e a contratada.

1.4. A interligação dos processos com o objetivo de **sustentação do ambiente produtivo** (esteira de sustentação) começa com a identificação de um evento (por meio de ferramentas de monitoramento), agendamento de alguma manutenção sistemática (previamente planejada, acordada e documentada) ou pelo acionamento por algum usuário relatando algum problema/bug (indisponibilidade ou perda de performance). Após uma triagem, um incidente será registrado. Este incidente pode disparar os processos de crise ou de problemas de acordo com os gatilhos descritos nos itens 3.7.4 e 3.5.4. A esteira de sustentação finaliza com os ajustes no ambiente produtivo, que deverá ser formalizado pela gestão de mudanças (caso tenha alguma alteração).

1.5. A interligação dos processos com o objetivo de **evoluir o ambiente produtivo** (esteira de evolução) começa com a necessidade de negócio (alinhado com o plano diretor de TI – PDTI), capitaneado pelas equipes internas da TI (SETID) e registrado na gestão de demandas. Após o

desenvolvimento da demanda é feita a passagem para produção (gestão de liberação) e finalizada com a implantação no ambiente produtivo, que deverá ser formalizada pela gestão de mudanças.

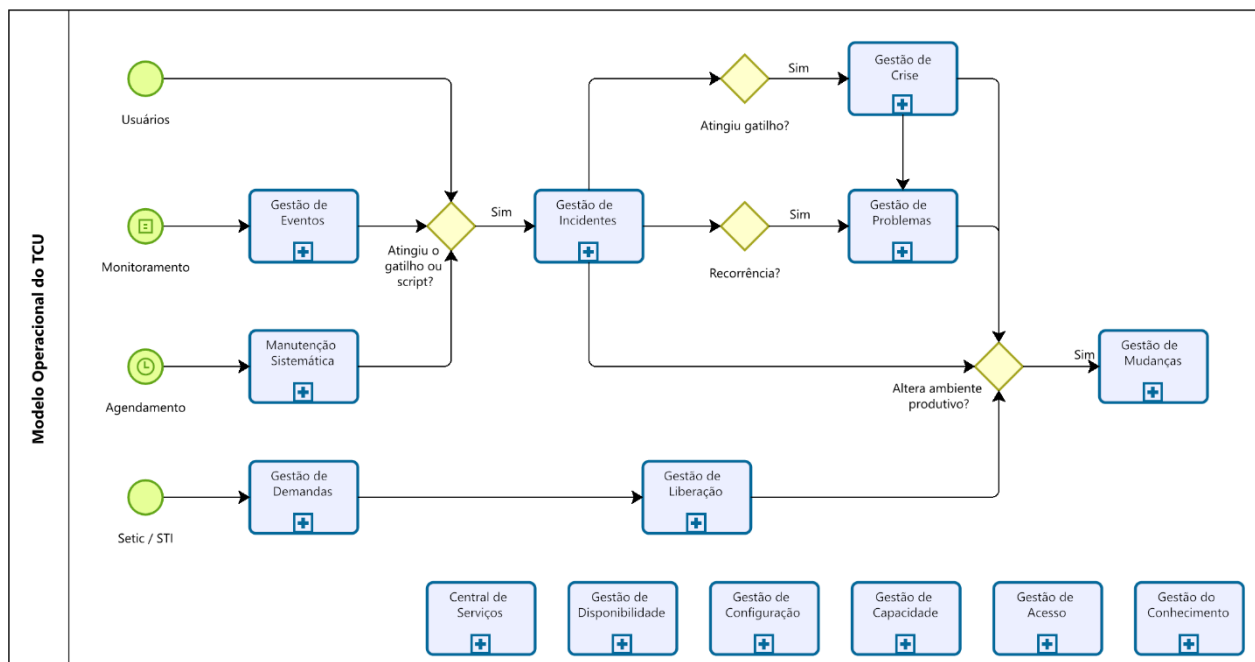


Figura 2: Modelo Operacional da infraestrutura de TI do TCU

1.6. Os processos transversais suportam a esteira de sustentação (item 1.4) com atividades e tarefas que objetivam a redução de acionamentos, parametrização de todas as ferramentas de gestão e aquisição, armazenamento e distribuição do conhecimento.

1.7. É obrigatória a utilização das ferramentas de gestão de serviços do TCU. Os profissionais da contratada alocados ao contrato deverão fazer seu o credenciamento prévio para a utilização das ferramentas de gestão.

1.8. Os números oficiais serão coletados das ferramentas de gestão do TCU e utilizados para a elaboração dos relatórios gerenciais e medição dos níveis de serviço pela Central de Serviços (descrita no item 3.1 abaixo), possibilitando o acompanhamento funcional do modelo operacional e subsidiando sua evolução.

2. Indicadores de acompanhamento do modelo operacional

2.1. Os indicadores de acompanhamento do modelo operacional têm como objetivo acompanhar a evolução de cada um dos processos, de forma a identificar pontos de melhorias, direcionar recursos (investimentos e força de trabalho) e esforços para atingir os motivadores de negócio e princípios do modelo operacional (Figura 1).

2.2. Na tabela 1 abaixo, entende-se como um "item" qualquer evento, incidente, problema, mudança ou crise que venha a acionar qualquer um dos processos do modelo operacional, sendo válidos e calculados para cada um deles individualmente:

Tabela 1: Lista dos indicadores a serem calculados para cada processo do modelo operacional

#	Indicadores	Descrição
1	Quantidade de itens abertos	Quantidade de itens abertos por dia, semana e mês
2	Quantidade de itens fechados	Quantidade de itens fechados por dia, semana e mês
3	Quantidade de itens em atraso (backlog)	Quantidade de itens em backlog por dia, semana e mês
4	Porcentagem de itens em backlog	Quantidade de itens em backlog dividido por itens abertos por mês
5	Quantidade de itens por prioridade, tempo de resposta e tempo de resolução	Quantidade de itens por prioridade, tempo de resposta e tempo de resolução por dia, semana e mês
6	Aderência ao NMS	Aderência ao NMS definido para cada item

2.3. Além dos indicadores da Tabela 1, apenas a Central de Serviços (item 1.1.1) deverá elaborar pesquisa e calcular, com exclusividade, os indicadores descritos na Tabela 2:

Tabela 2: Indicadores específicos para a Central de Serviços

#	Indicadores	Descrição
1	Porcentagem de retenção de incidentes	Quantidade de incidentes resolvidos em relação aos registrados pela Central de Serviços.
2	Satisfação dos usuários	Pesquisa trimestral/semestral para coletar a percepção dos principais usuários com relação aos atendimentos da Central de Serviços.

3. Detalhamento dos processos e boas práticas

3.1. Central de Serviços

3.1.1. A central de serviços é o ponto de contato único entre os usuários finais e as equipes responsáveis pelo suporte aos itens de configuração da infraestrutura.

- 3.1.2. Responsável por divulgar comunicados de mudança (manutenção e/ou indisponibilidade) da infraestrutura para os principais usuários utilizando os meios de comunicação da TI.
- 3.1.3. Os usuários podem acionar a Central de Serviços por telefone, e-mail ou pela própria ferramenta de gestão de serviços em um regime de 24 horas por dia, 7 dias da semana (24x7). Meios alternativos de acionamento, tais como mensagens pelo aplicativo Microsoft *Teams* ou pelo WhatsApp, podem ser utilizadas em casos de indisponibilidade ou impossibilidade de acesso aos meios já citados, sempre com a prévia anuência dos responsáveis pela fiscalização do contrato de serviço em questão.
- 3.1.4. É responsável por fazer cobranças periódicas às diversas equipes de suporte da infraestrutura (senso de dono do incidente) objetivando a coleta de status (registrando na ferramenta de gestão) e auxiliar na resolução do incidente (fazendo escalonamentos internos no TCU, direcionar e/ou adicionar outras equipes de suporte).
- 3.1.5. Responsável por orquestrar todas as salas de crise. A lista das principais atividades está descrita no item 3.7.
- 3.1.6. Responsável pela abertura dos problemas (gestão de problema) provenientes das salas de crise e recorrências de incidentes (descritos no item 3.4.14).
- 3.1.7. Responsável pelo monitoramento dos ativos tecnológicos configurados nas ferramentas de monitoramento (Zabbix, APM entre outras) por meio dos eventos que são gerados pela Gestão de Eventos (item 3.2).
- 3.1.8. Responsável por executar as manutenções sistemáticas presenciais (item 3.10) no Data Center do TCU, acompanhar e fazer a gestão de acesso físico (item 3.13) de fornecedores às estruturas do TCU e execução de trabalhos presenciais na estrutura do TCU (a lista de atividades que serão executadas será previamente alinhada, documentada e aprovada).
- 3.1.9. Responsável por fazer interface entre os usuários, as ferramentas de monitoramento e demais equipes. A Figura 3 ilustra o papel fundamental da Central de Serviços nessa interface. Após receber uma ligação/mensagem dos usuários ou ser alertado por algum evento do monitoramento, a Central de Serviços faz uma triagem (seguindo um script de atendimento) para tentar resolver o incidente. Caso não

consiga resolver, irá direcionar o incidente para as demais equipes de suporte (seguindo uma tabela de escalonamento para suporte de 2º nível, 3º nível ou suporte local). Todos os acionamentos deverão ser registrados na ferramenta de gestão.

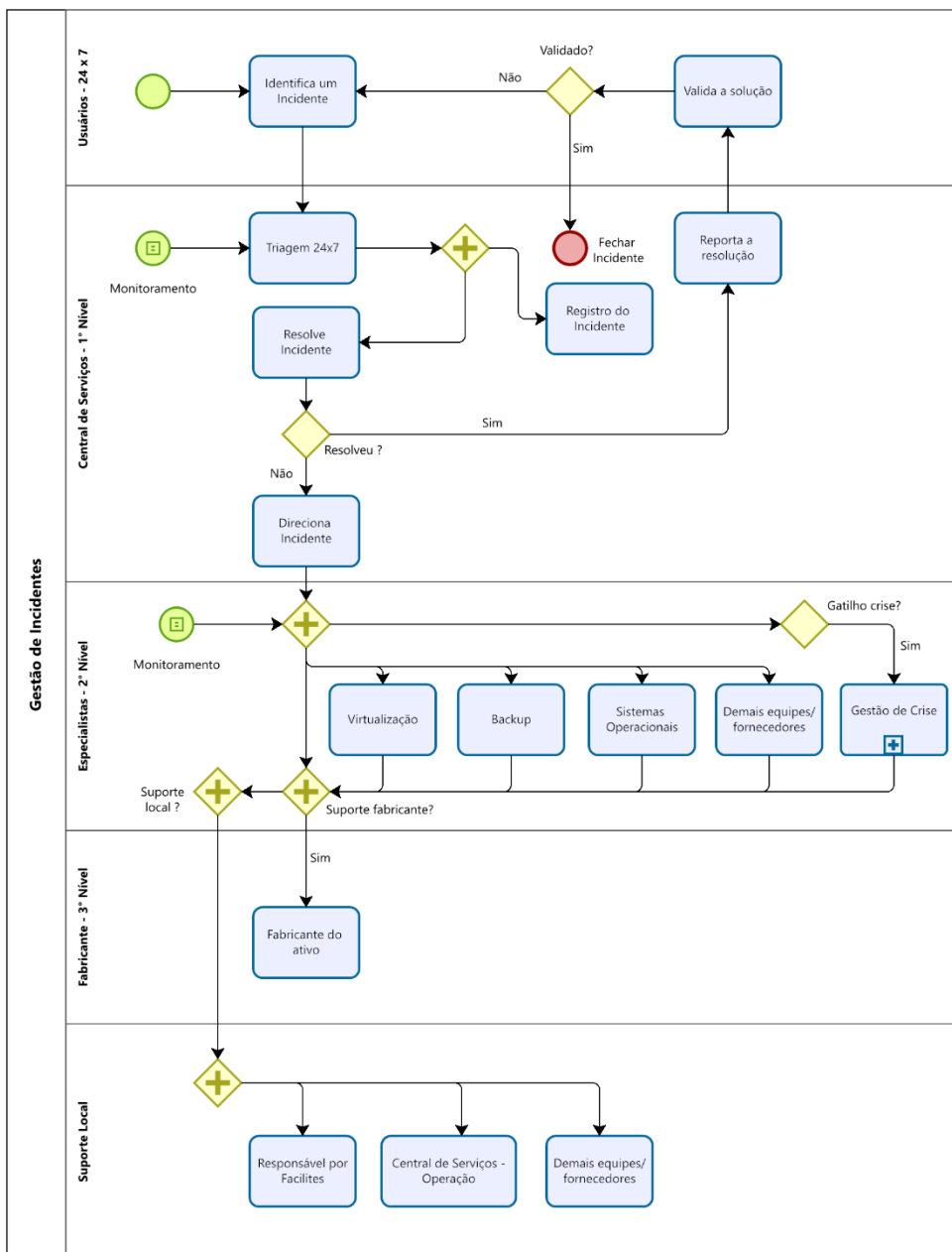


Figura 3: Fluxograma de atuação da Central de Serviços na gestão de incidentes

3.1.10. A Central de Serviços deverá calcular os indicadores descritos nas Tabela 1 e Tabela 2.

3.2. Gestão de Eventos

3.2.1. Um evento é definido como uma ocorrência ou mudança de estado de algum item de configuração relevante da infraestrutura de TI.

- 3.2.2. O objetivo da Gestão de Eventos é gerar alertas ou notificações dos eventos configurados para os principais itens de configuração. Os eventos são previamente configurados pela Gestão de Configuração (item 3.3) nas ferramentas de monitoramento (Zabbix, APM entre outras) ou nas ferramentas próprias das soluções tecnológicas.
- 3.2.3. Os eventos podem ser categorizados em:
- I. Informação: não necessidade da abertura de um incidente.
 - II. Atenção: abertura de um incidente com prioridade 3.
 - III. Alta: abertura de um incidente com prioridade 2.
 - IV. Desastre: abertura de um incidente com prioridade 1.
- 3.2.4. A abertura dos incidentes (considerando as categorias do item 3.2.3) poderão ser feitas de forma automática (integração entre as ferramentas de monitoramento e a ferramenta de gestão de serviços de TI) ou manualmente. A abertura do incidente manualmente será feita pela equipe da Central de Serviços considerando como gatilho um evento gerado pelas ferramentas de monitoramento.
- 3.2.5. Deverá ser feito saneamento e revisões dos eventos de forma a aprimorar e aperfeiçoar a Gestão dos Eventos. Caso a ocorrência de um evento, independentemente de sua categoria, se torne muito frequente deverá ser aberto um problema (Gestão de Problema) para analisar a causa raiz. Este problema deverá ser direcionado para equipe responsável pelo suporte ao item de configuração de forma a identificar a causa raiz das recorrências. Após análise feita pela equipe responsável pelo item de configuração, tarefas poderão ser direcionadas para a equipe de Gestão de Configuração para possíveis ajustes nas ferramentas de monitoramento.
- 3.2.6. Periodicamente, deverão ser feitas análises na base de dados das ferramentas de monitoramento para identificar padrões, comportamentos e correlações entre os eventos.
- 3.2.7. Deverá calcular os indicadores descritos na Tabela 1.

3.3. Gestão de Configuração

- 3.3.1. A gestão de configuração envolve a coleta e a gestão das informações de todos os itens de configuração (IC) disponíveis na infraestrutura do TCU. Um item de configuração é qualquer ativo/componente que necessite ser gerenciado para que possa entregar um serviço de Tecnologia.
- 3.3.2. Deverá gerenciar todo o ciclo de vida do item de configuração nas diversas ferramentas de gestão, desde a concepção dos padrões / parâmetros / taxonomia até o descomissionamento e/ou desativação do item de configuração nas ferramentas de gestão.
- 3.3.3. Os itens de configuração podem ser categorizados em:
 - I. IC crítico: Em caso de falha, do mesmo e/ou de um de seus componentes, resulte em qualquer um dos cenários:
 - Atraso e/ou não realização das sessões do plenário e/ou na instrução de processos urgentes;
 - Impacto na imagem / reputação do TCU com a indisponibilidade de algum serviço para a sociedade; e
 - Impacto financeiro da não execução das atividades de controle externo;
 - II. IC não crítico: Não classificado como crítico e que em caso de falha, do mesmo e/ou de um de seus componentes, resulte em atraso das atividades de uma equipe e/ou secretaria interna ao TCU.
- 3.3.4. A Classificação dos IC's como críticos serão feitas em conjunto com a equipe fiscalizadora do contrato.
- 3.3.5. Deverão ser feitos saneamentos e revisões dos itens de configuração de forma a aprimorar e aperfeiçoar a Gestão de Configuração.
- 3.3.6. Deverá ser elaborado e mantido uma matriz de interconexão entre os IC's.
- 3.3.7. Deverá calcular os indicadores descritos na Tabela 1.
- 3.4. Gestão de Incidentes
 - 3.4.1. Um incidente corresponde a uma interrupção não planejada de um serviço de TI, redução da qualidade de um serviço de TI ou falha de um item de configuração.

- 3.4.2. A gestão de incidentes tem por objetivo restaurar o funcionamento normal de um item de configuração ou serviço o mais rápido possível, além de minimizar os impactos adversos causados pelos incidentes nas operações do TCU.
- 3.4.3. As seguintes atividades fazem parte da gestão de incidentes:
- I. Registrar, categorizar e priorizar incidentes;
 - II. Investigar, diagnosticar e encaminhar incidentes;
 - III. Resolver incidentes; e
 - IV. Fechar incidentes e notificar o usuário final.
- 3.4.4. As origens de um incidente são:
- I. Proativa: identificado na gestão de eventos de acordo com a categorização do evento. É recomendada a automatização da abertura de incidentes provenientes das ferramentas de monitoramento, de forma que a data/hora de abertura do incidente coincida com a data/hora que o evento foi gerado.
 - II. Reativa: identificado quando algum usuário entra em contato com a Central de Serviços (Figura 3) ou quando as diversas equipes de suporte identificam o mau funcionamento do ambiente produtivo. Quando as diversas equipes de suporte identificam um incidente, elas mesmas deverão registrar o incidente na ferramenta de gestão.
- 3.4.5. Deverá ser gerado apenas um incidente para tratar o mau funcionamento de um item de configuração independente de qual equipe irá atuar. A configuração na ferramenta de gestão poderá ser feita por filas de atendimento.
- 3.4.6. Deverão ser definidos padrões/*templates* de registro dos incidentes na ferramenta de gestão. Esses padrões deveram ser definidos tanto para abertura como para o fechamento dos incidentes.
- 3.4.7. Os incidentes serão categorizados por meio de uma matriz de prioridades. A matriz de prioridades considera o impacto e a urgência, sendo:
- I. Impacto: medida de criticidade para o negócio.
 - II. Urgência: velocidade necessária para resolver o incidente.
- 3.4.8. A combinação de impacto e urgência (Tabela 3) geram quatro prioridades:
- I. P1: Crítico

- II. P2: Alto
- III. P3: Médio
- IV. P4: Baixo

Tabela 3: Matriz de prioridade

Matriz de prioridade		Impacto		
		Baixo	Médio	Alto
Urgência	Baixa	P4	P4	P3
	Média	P4	P2	P1
	Alta	P3	P2	P1

- 3.4.9. Para cada prioridade será definido Nível Mínimo de Serviço (NMS), contemplando: Disponibilidade de atendimento, tempo de resolução (em horas), tempo entre o início do incidente e início do atendimento, tempo médio para reparar e/ou restaurar o serviço.
- 3.4.10. A contratada deverá abrir incidentes e fazer os devidos acionamentos para os diversos fornecedores/fabricantes que atuam, em conjunto, para a sustentabilidade da infraestrutura do Tribunal. Além da abertura dos incidentes, também deverão fazer toda a gestão do ciclo de vida desse incidente junto ao fornecedor/fabricante, repassando informações, conhecimento e qualquer item necessário para a resolução.
- 3.4.11. O NMS só poderá ser suspenso quando estiver aguardando decisões do TCU ou a atuação de uma outra equipe que não tenha contrato por medição de níveis de serviços – NMS. É proibido qualquer suspensão do incidente que prejudique o tempo total de atendimento e que não se enquadre nas hipóteses mencionadas. A justificativa para suspensão do NMS deve ser registrada.
- 3.4.12. Caso a solução de um incidente necessite de qualquer alteração no ambiente produtivo, deverá ser aberta e aprovada uma mudança, conforme as descrições da Gestão de Mudança (item 3.6).
- 3.4.13. O fechamento de qualquer incidente está condicionado à documentação da solução implementada/adotada na base de conhecimento bem como a associação ao procedimento operacional utilizado para fazer as resolvê-lo (item 3.14.3).
- 3.4.14. Deverá calcular os indicadores descritos na Tabela 1.

3.5. Gestão de Problemas

- 3.5.1. Um problema é uma causa desconhecida de um ou mais incidentes e é caracterizado, dentro outros gatilhos, pela ocorrência de múltiplos incidentes semelhantes.
- 3.5.2. Os objetivos da gestão de problemas são: reduzir a quantidade de incidentes, analisar a causa raiz dos incidentes recorrentes, aumentar a disponibilidade dos serviços e criar uma base de conhecimento.
- 3.5.3. As seguintes atividades fazem parte da gestão de problemas:
 - I. Detectar o problema;
 - II. Registrar e priorizar o problema;
 - III. Investigar, diagnosticar e resolver o problema; e
 - IV. Fechar o problema e comunicar aos interessados.
- 3.5.4. O registro de um problema deverá ser uma demanda na categoria de solicitação com prioridade 5 (item 3.8.5).
- 3.5.5. As origens ou gatilhos de um problema poderão ser:
 - a. Proativa: as equipes de suporte e/ou os fiscais do TCU identificam recorrência de incidentes (como padrão, serão considerados a recorrência a partir de 5 incidentes).
 - b. Reativa: é aberto um problema ao término de uma sala de crise (item 3.7).
 - c. Ao longo da execução contratual, outras origens (gatilhos) podem ser identificadas.
- 3.5.6. Deverá ser gerado apenas um problema para identificar a causa raiz (de acordo com as origens descritas no item 3.5.4) independente de qual equipe que irá atuar. A configuração na ferramenta de gestão poderá ser feita com a criação de várias atividades e cada atividade associada a uma equipe.
- 3.5.7. Deverá ser definido apenas uma equipe como coordenadora do problema, independentemente do envolvimento de outras equipes. A definição do coordenador do problema estará relacionada com qual equipe contribuirá mais para

resolver a causa raiz. Após esta definição, ela será responsável por toda gestão, execução e NMS. Salvo exceções devidamente alinhadas com os fiscais dos contratos de atendimento envolvidos.

- 3.5.8. Deverão ser definidos padrões/*templates* de registro dos problemas na ferramenta de gestão. Esses padrões deveram ser definidos para abertura bem como para o fechamento dos problemas.
- 3.5.9. Para cada prioridade será definido NMS (níveis mínimos de serviço) contemplando: disponibilidade de atendimento, tempo de resolução (em horas), tempo entre o início do problema e início do atendimento, entre outros.
- 3.5.10. O NMS de um problema só poderá ser suspenso quando estiver aguardando definições do TCU ou atuação de outra equipe que não tem contrato por medição de níveis de serviços – NMS. É proibido qualquer suspensão do NMS do problema que prejudique o tempo total, salvo exceções quando alinhado com os fiscais.
- 3.5.11. Caso a solução do problema necessite de qualquer alteração no ambiente produtivo, deverá ser aberta uma mudança e ter as aprovações necessárias conforme as descrições da Gestão de Mudança.
- 3.5.12. Após a entrada em produção das correções de um problema, será definido período de operação assistida, como padrão serão 30 (trinta) dias corridos, e caso ocorram incidentes neste período, estes deverão ser vinculados ao problema, que deverá voltar para a etapa de investigação.
- 3.5.13. O fechamento de qualquer problema está condicionado à documentação da solução implementada/adotada na base de conhecimento do TCU.
- 3.5.14. Deverá calcular os indicadores descritos na Tabela 1.

3.6. Gestão de Mudanças

- 3.6.1. Uma mudança é qualquer adição, modificação ou remoção no ambiente produtivo podendo ou não gerar indisponibilidade de um item de configuração.
- 3.6.2. Os principais objetivos da gestão de mudança são assegurar que as mudanças sejam implantadas, minimizar o risco de impactos negativos para o negócio e dar mais transparência às atividades que serão executadas.

- 3.6.3. As mudanças deverão ser apresentadas nas reuniões semanais do CAB (*Change Advisory Board*) pelas próprias equipes responsáveis pelas mudanças.
- 3.6.4. É obrigatória a participação dos Gerentes técnicos ou, na ausência dessa função, dos prepostos dos contratos nas reuniões semanais do CAB.
- 3.6.5. As seguintes atividades fazem parte da gestão de mudanças:
- I. Registrar e priorizar a requisição de mudança;
 - II. Elaborar o planejamento (incluindo as datas das possíveis indisponibilidades);
 - III. Fazer mapeamento de risco relacionado à mudança;
 - IV. Definir planos de testes, comunicação, implantação e recuperação/*roll back* relativos à mudança;
 - V. Solicitar as aprovações junto ao CAB (caso seja necessário devido a categorização, item 3.6.8); e
 - VI. Fechar a mudança e comunicar os interessados.
- 3.6.6. Deverá ser registrada uma mudança para incidente ou problema que necessite da intervenção no ambiente de produção. Poderão ser agrupados incidentes ou problemas em uma única mudança de forma a reduzir as indisponibilidades do ambiente produtivo.
- 3.6.7. Deverão ser definidos padrões/*templates* de registro das mudanças na ferramenta de gestão. Esses padrões deverão ser definidos tanto para abertura como para o fechamento das mudanças.
- 3.6.8. As mudanças serão categorizadas de acordo com a urgência (grau de indisponibilidade do item de configuração) e impacto (criticidade dos processos de negócio afetados pela mudança), sendo:
- I. Emergencial: alterar o ambiente produtivo em até 24 horas do registro da mudança. Neste caso, reunião extraordinária (emergencial) do CAB deve ser convocada para tratar a mudança.
 - II. Normal: a mudança precisa ser aprovada nas reuniões semanais do CAB.

III. Padrão: mudanças previamente aprovadas e que não precisam da análise do CAB, a não ser que ocorram alterações na mudança que deve ser novamente submetida à apreciação.

3.6.9. Independente da categorização, as mudanças precisam executar todas as atividades do item 3.6.5 e ser apresentadas/listadas nas reuniões semanais do CAB.

3.6.10. Para as mudanças categorizadas como padrão, deverá ser elaborado um mapa de entregas/*release* ao longo do ano. Por exemplo: mensalmente é aplicado *patches* de vulnerabilidade do sistema operacional. No mapa de entregas são descritos quais as datas e itens de configuração serão impactados por mês.

3.6.11. Deverá calcular os indicadores descritos na Tabela 1.

3.7. Gestão de Crise

3.7.1. O principal objetivo da gestão de crise é engajar todas as equipes com capacidade e conhecimento para restaurar um item de configuração classificado como crítico (item 3.3.3) o mais rápido possível, reduzindo os impactos de sua indisponibilidade para a área de negócio.

3.7.2. A organização e gestão de sala de crise será gerenciada e coordenada pela Central de Serviços (item 3.1.5). As seguintes atividades deverão ser executadas pela Central de Serviços:

- I. Acionar e/ou escalonar a equipe que tratará o incidente, incluindo os fiscais dos contratos envolvidos ou pessoas por estes designadas.
- II. Analisar o impacto do incidente, obtendo informações com usuários e/ou fiscais do TCU quando necessário.
- III. Abrir uma sala de crise na ferramenta colaborativa do TCU (atualmente é utilizado o Microsoft *Teams*) e adicionar todas as equipes necessárias para recuperar o serviço.
- IV. Enviar comunicados periodicamente, a cada 30 (trinta) minutos ou 1 (uma) hora a critério do fiscal, para os gestores e fiscais do TCU com o status da sala de crise.

- V. Gerar uma ata da sala de crise com a linha do tempo das principais intervenções/ações e enviar para os gestores e fiscais do TCU imediatamente após o término da sala de crise.
 - VI. Ao término da sala de crise, deverá abrir um problema para a equipe que resolveu o incidente e registrar as intervenções no ambiente produtivo por meio da Gestão de Mudanças (mudança emergencial do item 3.6.8).
- 3.7.3. Durante uma sala de crise, após concordância da equipe de fiscalização do TCU, são autorizadas intervenções no ambiente produtivo sem a existência de uma mudança previamente aprovada, o que deverá ser registrado posteriormente. No caso de tentativas frustradas, devidamente documentadas, de comunicação com a equipe TCU, a equipe da contratada poderá realizar as ações que julgar necessárias para o restabelecimento do serviço.
- 3.7.4. Os gatilhos para a abertura de uma sala de crise serão:
- I. Incidentes críticos (P1) sem solução após 1 (uma) hora para os itens de configuração críticos.
 - II. Risco de parada de produção por evento crítico em componentes do monitoramento.
 - III. Escalonamento de incidente por parte dos gestores e fiscais do TCU.
 - IV. Falhas catastróficas do ambiente (item 3.7.5).
- 3.7.5. Uma falha catastrófica no ambiente de infraestrutura de TI é um evento que prejudica substancialmente, danifica, desliga ou incapacita todo ou parte de um ou mais itens de configuração categorizados como críticos.
- 3.7.6. Sendo um incidente de segurança cibernética, deverá ser envolvida, imediatamente, a equipe de segurança da informação do TCU, a qual será responsável pela condução da sala de crise (processo de trabalho específico). Após o alinhamento com a equipe de segurança da informação do TCU e em comum acordo, a sala de crise da contratada deverá ser fechada e todas as atividades serão conduzidas pela equipe de segurança do Tribunal.
- 3.7.7. A Figura 4 ilustra as fases de uma sala de crise, sendo:
- I. Gestão de Incidente: toda gestão de incidente descrita no item 3.4 e para fins de crise, serão considerados os incidentes de prioridade 1 e os outros gatilhos descritos no item 3.7.4.

- II. Pré crise: a Central de Serviços irá analisar o impacto junto aos usuários ou fiscais do TCU e irá providenciar a abertura de uma sala de crise.
- III. Durante a crise: um grupo no *Teams* é aberto exclusivamente para tratar este incidente e todas as equipes serão adicionadas. Com a sala de crise estabelecida, as equipes Técnicas irão conversar/analisar e definir quais ações serão executadas para resolver o incidente. A Central de Serviços irá orquestrar a sala de crise adicionando ou removendo pessoas a pedido das equipes Técnicas e irá enviar comunicados (e-mail, SMS, chat do *Teams* e outros meios a serem definidos) para os gestores e fiscais do TCU.
- IV. Pós crise: após resolver o incidente e restabelecer o serviço, as equipes que estão participando da sala de crise irão definir quem ficará responsável por analisar a causa raiz do incidente. A Central de Serviços abrirá um problema e estabelecerá como coordenador do problema a equipe previamente definida.

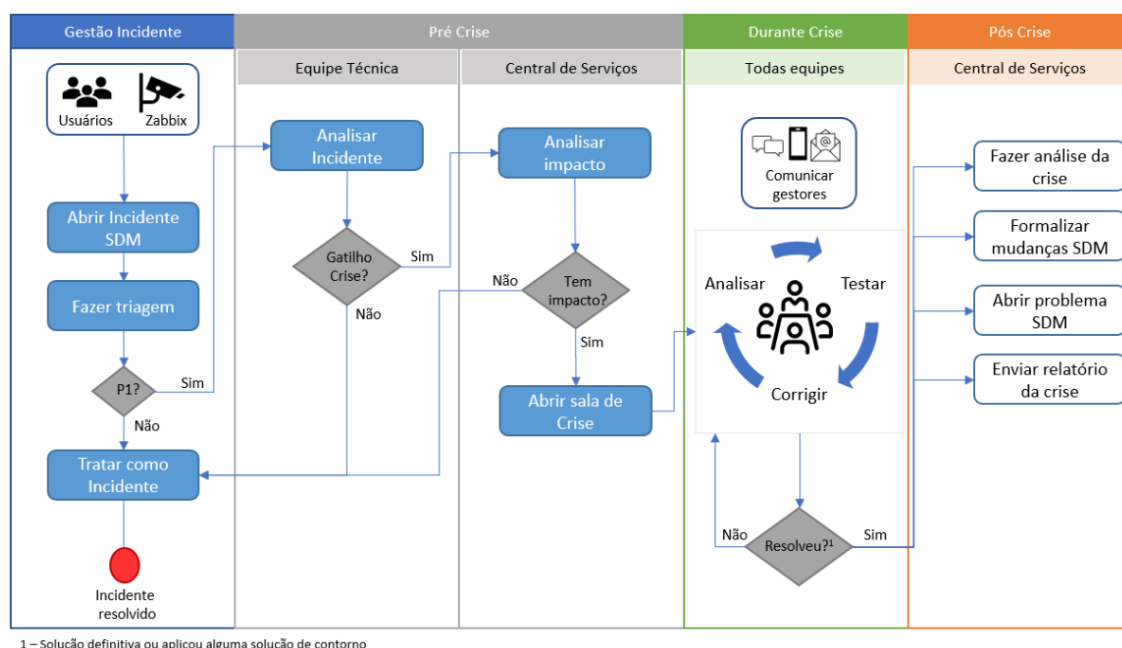


Figura 4: Fases do processo de crise

- 3.7.8. As equipes técnicas serão envolvidas e deverão participar 100% do tempo na sala de crise propondo soluções/alternativas para resolver o incidente.
- 3.7.9. Deverá calcular os indicadores descritos na Tabela 1.

3.8. Gestão de Demandas

- 3.8.1. O principal objetivo de uma demanda é a evolução do ambiente produtivo adicionando, removendo ou alterando alguma funcionalidade.
- 3.8.2. A Gestão de Demandas também se destina a melhorar a eficácia e a eficiência dos processos e serviços de infraestrutura do TCU.
- 3.8.3. As seguintes atividades fazem parte da gestão de demandas:
 - I. Registrar as demandas nas ferramentas devidas;
 - II. Quando previsto no contrato, elaborar ordem de serviços com o planejamento, custos e principais entregas para cada demanda cuja execução será fora do horário de trabalho;
 - III. Solicitar aprovação do fiscal;
 - IV. Atualizar as ferramentas de gestão com a evolução das execuções físicas (escopo e cronograma) e/ou financeiras (pagamentos já executados e/ou planejados), dando visibilidade do andamento das demandas;
 - V. Elaborar documentação e todas as atividades previstas para transição da melhoria para equipe de suporte (item 3.9).
- 3.8.4. Todas as demandas que necessitam de ordem de serviço, caso esse instrumento esteja previsto no contrato, deverão, obrigatoriamente, ser aprovadas pelo fiscal antes do início da execução.
- 3.8.5. As demandas serão categorizadas como solicitações com as seguintes prioridades:
 - I. Solicitações: São categorizadas em 5 (cinco) níveis de prioridades (combinação de impacto e urgência). As prioridades são:
 - a. P1: Crítico
 - b. P2: Alto
 - c. P3: Médio
 - d. P4: Baixo
 - e. P5: Melhoria
- 3.8.6. As atividades listadas no item 3.8.3 deverão sempre ser executadas, independente da categorização da demanda.
- 3.8.7. Deverá calcular os indicadores descritos na Tabela 1.

3.9. Gestão de Liberação / Transição

- 3.9.1. O objetivo da gestão de liberação e transição é dar suporte à equipe responsável pelo item de configuração assegurando que todos os artefatos estejam prontos antes da entrega em produção de uma demanda.
- 3.9.2. O responsável pela demanda é o responsável por elaborar todos os artefatos e fazer os acordos necessários para sua entrada em produção.
- 3.9.3. Será elaborado checklist com os artefatos que a equipe de demandas deverá acompanhar e executar durante todo o ciclo de vida da demanda. A equipe responsável pelo item de configuração também será a equipe responsável por elaborar o checklist de validação para entrada em produção.
- 3.9.4. Segue listagem não exaustiva dos itens que deverão estar descritos na checklist de entrada em produção:
 - I. Criação / alteração / remoção das configurações em todas as ferramentas de gestão e de monitoramento.
 - II. Criação / alteração / remoção das configurações em todas as ferramentas de segurança da informação.
 - III. Garantir que toda a equipe de suporte tenha os acessos devidos.
 - IV. Elaborar um acordo de nível operacional (ANO) com a descrição de todos os componentes existentes na solução bem como papéis e responsabilidades pelo suporte de todos os componentes.
 - V. Elaboração de uma matriz RACI descrevendo todos os componentes e atores que estão envolvidos na solução.
 - VI. Caso tenha integração com algum outro item de configuração, descrever como é esta integração e as possíveis contingências.
 - VII. Definir, junto com a área solicitante, quais serão os regimes de suporte (por exemplo: 24x7, 8x5) e quais os contratos de licença e serviços serão utilizados para o primeiro ano de produção da solução.
 - VIII. Definir e executar as atividades da manutenção sistemática (item 3.10.2).

- IX. Definir a periodicidade do backup e dos testes de *restore*. Nos testes de *restore*, definir qual procedimento deverá ser utilizado para verificar e validar os testes.
 - X. Definir quais atividades a Central de Serviços irá executar no primeiro atendimento e elaborar os procedimentos operacionais.
 - XI. Elaborar documentação da solução e/ou *as built*.
 - XII. Elaborar manual de treinamento.
 - XIII. Abrir e executar a mudança seguindo o item 3.6.
 - XIV. Listar todos os incidentes que foram registrados durante a operação assistida.
- 3.9.5. A depender da demanda, alguns itens da lista 3.9.4 não serão aplicados. Esta validação será feita em conjunto com o fiscal do TCU.
- 3.9.6. O checklist será validado pelo fiscal do TCU e, excepcionalmente, alguns itens poderão ser entregues depois do término da demanda desde que seja apresentado o planejamento de entrega.
- 3.9.7. O termo final de aceite em produção deverá ter aprovações do fiscal do TCU (responsável pelo suporte) e do solicitante da demanda. Somente após esta aprovação que a demanda poderá ser promovida a produção.
- 3.9.8. Deverá calcular os indicadores descritos na Tabela 1.
- 3.10. Manutenção sistemática
- 3.10.1. O objetivo da manutenção sistemática é estruturar rotinas básicas de verificação e validação do ambiente produtivo de forma periódica, padronizada e com escopo e tempo de execução definidos para mitigar possíveis incidentes na infraestrutura do TCU.
 - 3.10.2. A Figura 5 ilustra as etapas da manutenção sistemática sendo descritas as seguintes atividades:
 - I. Fazer um planejamento de médio prazo utilizando um mapa de 52 semanas e coletar aprovações com os fiscais do TCU.

- II. Fazer o provisionamento de materiais, ferramentas e EPIs (equipamentos de proteção individual), quando aplicáveis, que serão utilizadas durante uma manutenção sistemática bem como especificar quais alocações de outras equipes serão necessárias.
- III. Definir a lista de atividades que serão executadas. Esta lista de atividades deverá ser elaborada em conjunto com os fabricantes dos itens de configuração, refletindo as melhoras práticas, recomendações e parâmetros de referência do próprio fabricante.
- IV. Apresentar no CAB (item 3.6.3) o mapa de 52 semanas.
- V. Programar as manutenções no sistema de gestão de serviços, de forma que as manutenções sistemáticas reflitam os planejamentos definidos no mapa de 52 semanas.
- VI. Executar manutenção sistemática utilizando os materiais, ferramentas, EPIs provisionados de acordo com o planejamento feito. Deverá executar a lista de atividades previamente definidas.
- VII. Elaborar um relatório final, após o término de cada manutenção, com a lista de atividades, condições/gatilhos que geraram não conformidades, anexar as evidências coletadas no trabalho de campo, elaborar um plano de ação para as atividades não conformes, fazer uma análise crítica na situação encontrada e aprimorar as atividades para as próximas manutenções.

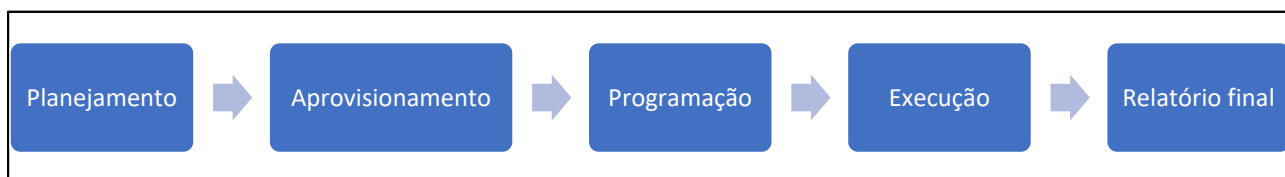


Figura 5: Etapas da manutenção sistemática

- 3.10.3. A execução de uma manutenção sistemática poderá ser presencial, remota ou híbrida a depender do item de configuração e da lista de atividades. Esta definição deverá ser em conjunto com os fiscais do TCU.
- 3.10.4. O registro de uma manutenção sistemática deverá ser uma demanda na categoria de solicitação com prioridade 1 ou 2 (item 3.8.5)

- 3.10.5. Deverão ser definidos padrões / *templates* de registro das manutenções sistemáticas na ferramenta de gestão. Esse padrão deverá ser definido tanto para abertura como para o fechamento das manutenções sistemáticas.
 - 3.10.6. Durante a manutenção sistemática, para qualquer tipo de intervenção no ambiente produtivo deverá ser registrado um incidente e descrito no relatório final.
 - 3.10.7. Identificando qualquer não conformidade durante a manutenção sistemática, as intervenções no ambiente produtivo deverão ser executadas e uma sala de crise deverá ser aberta, caso os gatilhos descritos no item 3.7.4 sejam disparados.
 - 3.10.8. As atividades descritas no plano de ação do relatório final, deverão estar associados a incidentes e/ou demandas previamente registrados na ferramenta de gestão.
 - 3.10.9. A execução das manutenções sistemáticas presenciais deverá ser, prioritariamente, executada pela equipe da Central de Serviços.
 - 3.10.10. Deverá calcular os indicadores descritos na Tabela 1.
- 3.11. Gestão de Disponibilidade
- 3.11.1. O objetivo da prática de gestão de disponibilidade é garantir que os serviços de infraestrutura de TI estejam disponíveis para as partes interessadas e desempenhem sua função quando necessário.
 - 3.11.2. A gestão de disponibilidade é categorizada em:
 - I. Alta disponibilidade: associada aos itens de configuração críticos (item 3.3.3)
 - II. Disponibilidade contínua: associada aos itens de configuração não críticos (item 3.3.3)
 - 3.11.3. Poderão ser definidos Níveis Mínimos de Serviço (NMS) específicos para cada categoria descrita no item 3.11.2. Salvo exceção e previamente aprovado pelo fiscal, um item de configuração poderá ser categorizado de forma diferente ao descrito no item 3.11.2.
 - 3.11.4. Deverão utilizar as ferramentas de monitoramento para fazer os cálculos dos indicadores de disponibilidade.

3.11.5. A indisponibilidade gerada devido a uma manutenção sistemática (item 3.10) ou devido a gestão de mudanças (item 3.6.8) em algum item de configuração deverão ser registradas como “*blackout*”.

3.11.6. Definições:

- I. Horas calendários: Considera 24 horas e 7 dias na semana.
- II. Horas *blackout*: Somatório das horas de manutenção planejada (devido a uma manutenção sistemática ou a uma mudança) no período analisado.
- III. Horas disponíveis: É a diferença entre as horas calendário e as horas *blackout* no período analisado.
- IV. Horas indisponíveis: Somatório das horas de indisponibilidade de um item de configuração no período analisado

3.11.7. As seguintes atividades fazem parte da gestão de disponibilidade:

- I. Definir junto aos fiscais quais itens de monitoramento serão considerados para acompanhar a disponibilidade de cada item de configuração.
- II. Configurar nas ferramentas de monitoramento os indicadores de disponibilidade.
- III. Acompanhar diariamente os indicadores de disponibilidade, fazendo uma análise crítica e um plano de ação caso os indicadores estejam abaixo do NMS.
- IV. Divulgar (diária, semanal e/ou mensalmente) para os fiscais o consolidado dos indicadores de disponibilidade.
- V. Elaborar um relatório mensal com a descrição de todos os itens de configuração bem como os indicadores de disponibilidade e NMS.

3.11.8. Deverá calcular os indicadores descritos na Tabela 1.

3.12. Gestão de Capacidade

3.12.1. O objetivo da gestão de capacidade é assegurar que a capacidade do ambiente produtivo esteja dimensionada corretamente e alinhada com as necessidades do TCU.

- 3.12.2. A análise de capacidade deverá considerar o dimensionamento dos itens de configuração (hardware e/ou software), das licenças, das equipes responsáveis pelo ambiente produtivo bem como das garantias e suporte dos fabricantes.
 - 3.12.3. A análise de capacidade deverá considerar os seguintes períodos:
 - I. Curto prazo: 6 (seis) meses.
 - II. Médio prazo: 12 (doze) meses.
 - III. Longo prazo: 36 (trinta e seis) meses.
 - 3.12.4. As seguintes atividades fazem parte da gestão de capacidade:
 - I. Definir gatilhos e implementá-los nas ferramentas de monitoramento de forma a gerar eventos que antecedam o alcance da capacidade máxima.
 - II. Avaliar o dimensionamento do ambiente produtivo com viés de crescimento vegetativo, de expansão (aumento da capacidade) ou desligamento (caso o item de configuração não esteja em utilização e/ou não atenda as demandas de negócio).
 - III. Elaborar plano de capacidade com a lista de todos os itens de configuração considerando as licenças, garantias e suporte do fabricante tanto para o hardware como para o software.
 - IV. No plano de capacidade, descrever o dimensionamento da equipe de suporte.
 - V. Fazer análise crítica do plano de capacidade sinalizando as principais divergências / ações que deverão ser implementadas para cada período analisado (item 3.12.3).
 - 3.12.5. Deverá calcular os indicadores descritos na Tabela 1.
- 3.13. Gestão de Acesso
- 3.13.1. O objetivo da gestão de acesso é controlar todo tipo de acesso (físico ou lógico) à infraestrutura do TCU, seguindo as diretrizes da segurança patrimonial e da segurança da informação.
 - 3.13.2. Todo acesso (físico ou lógico) deverá ser aprovado previamente pelo fiscal responsável pelo ativo.

- 3.13.3. Deverá ser implementado um fluxo de trabalho (manual ou automático) para armazenar:
 - I. Os termos de sigilo, confidencialidade e uso bem como o termo de proteção de dados pessoais.
 - II. As aprovações dos fiscais do TCU.
 - III. O tipo de acesso, podendo ser: adição, edição ou remoção do acesso.
 - IV. Evidências do acréscimo ou remoção do acesso.
- 3.13.4. A gestão do acesso físico à infraestrutura da TI será executada pela Central de Serviços.
- 3.13.5. A gestão de acesso lógica à infraestrutura deverá ser executada pela equipe especializada e responsável pelo item de configuração.
- 3.13.6. Periodicamente, a equipe responsável pelo item de configuração deverá fazer um saneamento dos acessos (caso não seja automático), sendo:
 - I. Mensalmente: Para itens de configuração críticos
 - II. Semestralmente: Para itens de configuração não críticos
- 3.13.7. A periodicidade do saneamento poderá ser alterada durante a execução contratual de modo a se adequar às necessidades relacionadas à segurança da informação.
- 3.13.8. As equipes responsáveis pelos itens de configuração deverão elaborar relatório mensal com o consolidado das atividades executadas, bem como a lista dos acessos existentes para cada item de configuração sob sua responsabilidade.
- 3.13.9. Deverá elaborar os calcular descritos na Tabela 1.
- 3.14. Gestão de Conhecimento
 - 3.14.1. O objetivo da gestão de conhecimento é documentar e disseminar o conhecimento acerca de processos e procedimentos entre as equipes que trabalham na infraestrutura de TI do TCU.
 - 3.14.2. Deverá tratar todo ciclo de gestão do conhecimento, sendo:
 - I. Aquisição do conhecimento: treinamentos, manuais, compartilhamento de experiências, entre outras formas.

- II. Armazenamento do conhecimento: ferramenta colaborativa (wiki, *Teams/Sharepoint*), ferramentas de gestão dos serviços, entre outras.
 - III. Distribuição do conhecimento: notificações via e-mail, *Teams* ou acessando as ferramentas de gestão dos serviços.
 - IV. Utilização do conhecimento: atendimentos executados pela Central de Serviço, fiscais do TCU e demais equipes responsáveis pelo ambiente produtivo.
- 3.14.3. Com relação ao armazenamento do conhecimento, pode-se diferenciar em:
- I. Ferramenta colaborativa wiki: utilizada para armazenar os procedimentos operacionais e de atendimento utilizados tanto pela Central de Serviços como por outras equipes.
 - II. Ferramenta colaborativa *Teams/Sharepoint*: toda documentação das demandas (item 3.8.5).
 - III. Ferramenta de gestão dos serviços: base de conhecimento utilizado e/ou gerado para atender os incidentes (item 3.4), problemas (item 3.5) ou solicitações (item 3.8).
- 3.14.4. Deverá ser validado, previamente, com o gestor do contrato os formatos dos arquivos de forma a manter a compatibilidade com os softwares e versões homologados pelo TCU.
- 3.14.5. Todo conhecimento armazenado nas ferramentas colaborativas (wiki, *Teams/Sharepoint*) deverão conter o controle de versão e a periodicidade de atualização. Caso não esteja descrito a periodicidade de atualização, deverá ser adotado como padrão de 6 (seis) meses.
- 3.14.6. Os fiscais do TCU serão responsáveis pelas conferências e aprovações das documentações elaboradas.
- 3.14.7. Deverá calcular os indicadores descritos na Tabela 1.