CARTILHA DE BOAS PRÁTICAS DA GESTÃO DA CONTINUIDADE DE TI

AUDIN
Auditoria Interna do
Ministério Público da União

CARTILHA DE BOAS PRÁTICAS DA GESTÃO DA CONTINUIDADE DE TI

BRASÍLIA – DF
2021

MINISTÉRIO PÚBLICO DA UNIÃO
AUDITORIA INTERNA
SGAS 604, Lote 23 - Procuradoria da República no Distrito Federal, 2º pavimento
Avenida L2 Sul, Brasília/DF CEP: 70.200-640

Auditor-Chefe
Ronaldo da Silva Pereira

Auditor-Chefe Adjunto
Eduardo de Seixas Scozziero

Chefe de Gabinete
André Felipe Flores da Silva

Diretoria de Auditoria de Infraestrutura
Josi Brandão Silva

Elaboração
Diogo Alves de Sousa
Rogério da Silva Barbosa

MINISTÉRIO PÚBLICO DA UNIÃO
AUDITORIA INTERNA
SGAS 604, Lote 23 - Procuradoria da República no Distrito Federal, 2º pavimento
Avenida L2 Sul, Brasília/DF CEP: 70.200-640

Missão

Adicionar valor e melhorar as operações do Ministério Público da União para o alcance de seus objetivos em prol da sociedade, por meio de orientação e avaliação sistemática e disciplinada de seus processos de governança, de gestão de riscos e de controle.

Visão

Ser órgão de excelência nas atividades de auditoria interna e parceiro no controle da gestão do Ministério Público da União

Valores

Transparência, ética, imparcialidade, excelência, independência e inovação.

SUMÁRIO

OBJETIVO

O objetivo desta cartilha é apresentar, de forma consolidada, as principais recomendações e orientações desta Auditoria Interna do Ministério Público da União (Audin-MPU) resultantes dos trabalhos de auditoria, com foco no processo de Gestão da Continuidade de TI, realizados nos ramos do Ministério Público da União e na Escola Superior do Ministério Público da União – ESMPU.

O trabalho em tela foi elaborado considerando normativos, jurisprudência do TCU, boas práticas, pontos positivos identificados nas unidades auditadas e os assuntos mais recorrentes em relatórios de auditoria. Ademais, as recomendações, aqui apresentadas, representam oportunidades de melhorias que foram identificadas em algumas das unidades auditadas. Assim, as Unidades do MPU poderão fortalecer os controles nos pontos críticos verificados, utilizando-se desta cartilha como referência. Os temas serão apresentados em ordem decrescente de impacto para o processo auditado.

Importante ressaltar que, em um primeiro momento, serão abordados apenas os aspectos mais relevantes de cada assunto. Outros aspectos poderão ser explorados em trabalhos futuros.

1. VISÃO GERAL DO OBJETO

A continuidade de negócios é definida como uma capacidade organizacional, cujo objetivo é "[…] continuar a entrega de produtos e serviços em um nível aceitável com capacidade predefinida […]", conforme definido na ABNT NBR ISO 22301:2020. Portanto, a Gestão da Continuidade de Tecnologia da Informação, objeto do trabalho realizado, tem por escopo dar sustentação à continuidade dos serviços de Tecnologia da Informação (TI) que dão

suporte aos processos de negócio críticos da organização "[...] para evitar perdas e [...] preparar para mitigar e gerenciar disrupções[1]", tal qual prescrito na norma supracitada.

Os trabalhos de auditoria foram realizados nas seguintes Unidades:

- STIC/MPF;
- DTI/PGT/MPT;
- STI/PGJ/MPDFT;
- DTI/PGJM/MPM;
- STI/ESMPU.

Para fins de entendimento desta cartilha, **serão utilizados como sinônimos os termos gestão de continuidade de TI e gestão de continuidade de serviços de TI.**

2. CRITÉRIOS

Para subsidiar a realização dos trabalhos de auditoria no processo de Gestão da Continuidade de TI foram selecionados alguns critérios para a avaliação das ações de gestão implementadas nas unidades, considerando normativos internos e externos, jurisprudência do TCU e boas práticas.

Na tabela abaixo consta a relação dos principais critérios utilizados.

CRITÉRIO	DESCRIÇÃO
Resolução nº 171/2017 - CNMP	Institui a Política Nacional de Tecnologia da Informação do Ministério Público (PNTI-MP). Tem por objetivo alinhar as práticas de governança e gestão de TI em todas as unidades e os ramos do Ministério Público. Para isso, as unidades deverão instituir políticas de governança e gestão para a regulamentação, dentre outros, dos macroprocessos de TI definidos.

[1] ABNT NBR ISO 22301:2020. Disrupção: incidente, seja previsto ou não, que causa um desvio não planejado e negativo na expectativa de entrega de produtos e serviços de acordo com os objetivos da organização

CRITÉRIO	DESCRIÇÃO
ABNT NBR ISO 22301:2020	Define a estrutura e os requisitos para a implementação e manutenção de um sistema de gestão de continuidade de negócios (SGCN).
ABNT NBR ISO/IEC 27002:2013	Controles de segurança da informação dispostos em forma de referência para seleção pela organização interessada durante implementação de um sistema de gestão de segurança da informação (SGSI), baseado na ABNT NBR ISO/IEC 27001.
ABNT NBR ISO/IEC 20000-1:2020	Define requisitos para sistema de gestão de serviços de TI.
COBIT 5	Fornece orientações sobre governança e gestão corporativa da TI, considerado modelo de boas práticas mundialmente aceito.
Acórdão TCU nº 1109/2021 – Plenário	Trabalho de auditoria sobre a efetividade dos procedimentos de backup das organizações públicas federais realizado pelo Tribunal de Contas da União – TCU.

Tabela 1 - Relação de Critérios

3. REGULAMENTAÇÃO DA GESTÃO DA CONTINUIDADE DE TI

3.1. Recomendação

Regulamentar as ações de governança e de gestão relativas ao Macroprocesso de Continuidade de Serviços de TI, preferencialmente em alinhamento à estratégia de Continuidade de Negócios do órgão, se houver, e em conformidade com a Resolução CNMP nº 171/2017 e demais boas práticas aplicáveis.

3.2. Normativos

A regulamentação do Macroprocesso Gestão da Continuidade dos Serviços de TI pelas unidades e ramos do Ministério Público é requisito definido pela PNTI-MP, que especifica o seguinte:

> Art. 24. A regulamentação da gestão da continuidade dos serviços será contemplará:
>
> I – análise de impacto;
>
> II – definição de estratégias;
>
> III – desenvolvimento de plano de continuidade dos serviços de TI essenciais, incluindo testes e revisões periódicas.

Os requisitos indicados na PNTI-MP para regulamentação do referido macroprocesso são detalhados na tabela abaixo.

CRITÉRIO	REQUISITOS	REFERÊNCIA
Resolução CNMP n° 171/ 2017 – PNTI-MP	Instituição de políticas de governança e gestão para regulamentação da gestão do macroprocesso continuidade dos serviços de TI.	Art. 18.
	Instituição de comitê gestor e gestor para, respectivamente, governar e gerir o macroprocesso de continuidade de TI.	Art. 19.
	Regulamentação da gestão da continuidade dos serviços de TI contempla: análise de impacto; definição de estratégias; e desenvolvimento do Plano de Continuidade dos Serviços de TI essenciais, incluindo testes e revisões periódicas.	Art. 24.

Tabela 2 - Requisitos para regulamentação do macroprocesso de Gestão da Continuidade de TI

3.3. Conclusões

O Conselho Nacional do Ministério Público (CNMP), considerando sua atuação reguladora e integradora, instituiu a Resolução nº 171/2017, cuja finalidade é alinhar as práticas de governança e gestão de TI em todas as unidades e ramos do Ministério Público, fomentando e auxiliando o aprimoramento da governança e gestão da TI.

Dessa forma, a conformidade a essa norma torna-se requisito essencial à gestão eficaz, eficiente e efetiva.

Frisa-se que o prazo para implantação dos planos de ação que atenderiam aos requisitos contidos nessa resolução foi encerrado em julho de 2021. Contudo, na 1ª Sessão Extraordinária do Plenário Virtual[2] do CNMP, realizada dia 14 de julho de 2021, o prazo final para conclusão dos planos de trabalhos das unidades foi prorrogado, mediante Proposição n.º

[2] Disponível em https://www.cnmp.mp.br/portal/todas-as-noticias/14446-modificado-prazo-para-entrega-de-plano-de-trabalho-da-politica-nacional-de-tecnologia-da-informacao-do-mp?highlight=WyJwbnRpIl0= . Acessado em 02/08/2021.

1.00845/2021-46 [3]. O Comitê de Políticas Estratégicas – CPE/CNMP estabelecerá novos prazos para cumprimento.

Para a regulamentação do macroprocesso de Gestão da Continuidade de Serviços de TI à luz da PNTI-MP, sugerem-se os documentos abaixo listados como **referência**:

- **Portaria Normativa nº 584**, de 29 de outubro de 2018 – PGJ/MPDFT;
- **Resolução CETI nº 6**, de 7 de março de 2016 – MPT.

4. PLANO DE CONTINUIDADE DE SERVIÇOS DE TI

4.1. Recomendação

Elaborar Planos de Continuidade de Serviços de TI, fazendo constar procedimentos adequados para a garantia da continuidade dos processos críticos da Unidade, relativos aos sistemas críticos e os serviços de TI que os suportam, em conformidade com as normas e boas práticas aplicáveis.

4.2. Normativos e Boas Práticas

A PNTI-MP definiu que a regulamentação da Gestão da Continuidade dos Serviços de TI deverá contemplar o "desenvolvimento de plano de continuidade dos serviços de TI essenciais, incluindo testes e revisões periódicas".

Baseado na compilação dos requisitos para o plano de continuidade de TI dispostos nas normas ABNT e COBIT 5, elaborou-se a tabela abaixo como orientação para elaboração dos referidos planos.

CRITÉRIO	REQUISITOS
ABNT NBR ISO 22301/2020	Liderança e comprometimento da alta administração com respeito ao SGCN, assegurando que a política e os objetivos da continuidade do negócio são estabelecidos e compatíveis com o direcionamento estratégico da organização.

[3] Disponível em: https://www.cnmp.mp.br/portal/images/Propostas/PROP_RES_ALTERA_RES_171.pdf . Acessado em 02/08/2021.

CRITÉRIO	REQUISITOS
	Alta administração estabelece uma política de continuidade de negócios.
	A organização estabelece procedimentos documentados para responder à incidentes de interrupção, e como continuar ou recuperar suas atividades dentro de um prazo predefinido.
	A organização possui e testa os procedimentos de continuidade de negócios, para garantir que estes são compatíveis com os seus objetivos de continuidade.
	A organização determina o que precisa ser monitorado e medido.
	A organização determina os métodos para monitoramento, medição, análise e avaliação, conforme o caso, para assegurar resultados válidos.
	A organização determina quando o monitoramento e a medição devem ser realizados.
	A organização determina quando os resultados do monitoramento e da medição devem ser analisados e avaliados.
	A organização avalia o desempenho e a eficácia do SGCN.
	A organização realiza uma análise crítica pós-incidente e registra os resultados quando um incidente que cause interrupção e resulte na ativação dos seus procedimentos de continuidade dos negócios ocorre.
	A Organização realiza avaliação dos procedimentos de continuidade dos negócios.
ABNT NBR ISO 27002/2013	A continuidade da segurança da informação é contemplada nos sistemas de gestão da continuidade do negócio da organização.
ABNT NBR ISO 20000/2020	São avaliados e documentados os riscos à continuidade de serviços de TI.
	São criados, implementados e mantidos um ou mais Planos de Continuidade de Serviço.
COBIT 5 - DSS04 - Gerenciar a Continuidade	Identificação dos processos de negócios internos e terceirizados e os serviços críticos para o negócio ou necessários para atender obrigações legais e contratuais.
	Identificação dos processos essenciais de suporte ao negócio e serviços de TI relacionados.
	Identificação dos potenciais cenários que podem dar origem a disrupção dos serviços.
	Realização de análises de impacto no negócio.
	Avaliação dos riscos que podem causar perda da continuidade de negócio e definição de medidas de tratamento.
	Definição de requisitos de continuidade.
	Identificação das pessoas chave.
	Identificação das necessidades de recursos e custos para estratégias de continuidade.
	Estratégias de continuidade aprovadas pela Alta Administração.

CRITÉRIO	REQUISITOS
	Elaboração do plano de continuidade de negócios.
	Realização de exercício, teste e revisão do plano de continuidade de negócios.
	PCN revisado, mantido e melhorado.

Tabela 3 - Compilação dos requisitos para Plano de Continuidade de Serviços de TI

4.3. Conclusões

O plano de continuidade de TI trata-se de "procedimentos documentados que orientam as organizações a **responder, recuperar, retornar e restaurar** serviços de TI..." (grifo nosso), conforme definido na ABNT NBR ISO 20000-1:2020.

Portanto, dada a imprescindibilidade dos planos de continuidade para a gestão da continuidade da TI, recomenda-se o estabelecimento e adequada manutenção desses planos, considerando os processos de negócio críticos e os respectivos serviços de TI que os suportam.

A Tabela 3 pode ser utilizada como referência para elaboração dos referidos planos de continuidade, bem como o seguinte modelo:

- **Resolução CETI nº 16, de 13 de setembro de 2017** – Modelo para planejamento e desenvolvimento dos Planos de Continuidade de Serviços de TIC – MPT.

5. PROCESSO DE GESTÃO DE CONTINUIDADE DE TI

5.1. Recomendação

Estabelecer, implantar, operar, manter e monitorar processo para gestão da Continuidade de Serviços de TI, em conformidade com as normas vigentes e as boas práticas aplicáveis, considerando as prioridades e capacidade da unidade.

5.2. Normativos e Boas Práticas

A norma ABNT NBR ISO 22301:2020, em relação ao Sistema de Gestão de Continuidade de Negócios, definiu (grifo nosso):

O SGCN, assim como outros sistemas de gestão, possui os seguintes componentes:

- Uma política;
- Pessoal competente com responsabilidades definidas;
- **Processos de gestão** relativos a:
    1) Política;
    2) Planejamento;
    3) Implementação e operação;
    4) Avaliação de desempenho;
    5) Análise crítica pela direção;
    6) Melhoria contínua;
- Documentações que apoiem o controle operacional e possibilitem a avaliação de desempenho.

O COBIT 5 indicou os habilitadores como "[...] fatores que, individualmente e em conjunto, influenciam se algo irá funcionar – neste caso, a governança e a gestão corporativas da TI.". As sete categorias de habilitadores prescritas são (grifo nosso):

- Princípios, políticas e modelos são veículos para a tradução do comportamento desejado em orientações práticas para a gestão diária;
- **Processos** descrevem um conjunto organizado de práticas e atividades para o atingimento de determinados objetivos e produzem um conjunto de resultados em apoio ao atingimento geral dos objetivos de TI;
- Estruturas organizacionais são as principais entidades de tomada de decisão de uma organização;
- Cultura, ética e comportamento das pessoas e da organização são muitas vezes subestimados como um fator de sucesso nas atividades de governança e gestão;
- Informação permeia qualquer organização e inclui todas as informações produzidas e usadas pela organização. A Informação é necessária para manter a organização em funcionamento e bem governada, mas no nível operacional, a informação por si só é muitas vezes o principal produto da organização;

- Serviços, infraestrutura e aplicativos incluem a infraestrutura, a tecnologia e os aplicativos que fornecem à organização o processamento e os serviços de tecnologia da informação;
- Pessoas, habilidades e competências estão associadas às pessoas e são necessárias para a conclusão bem-sucedida de todas as atividades bem como para a tomada de decisões corretas e tomada de medidas corretivas.

Além disso, o COBIT 5 estabelece o processo Gerenciar a Continuidade (DSS04) como habilitador para a gestão de TI da organização, situado no domínio Entregar, Serviço e Suporte (DSS), cuja finalidade é:

> Estabelecer e manter um plano para permitir que o negócio e a TI possam responder a incidentes e interrupções, a fim de continuar a operação de processos de negócios críticos e os serviços de TI necessários, e manter a disponibilidade de informações em um nível aceitável para a empresa.

Além da necessidade da regulamentação do Macroprocesso de Gestão da Continuidade dos Serviços de TI, a PNTI-MP também indica as diretrizes que devem orientar a realização das ações estabelecidas e, dentre elas, destacam-se: I – conformidade com as boas práticas internacionais; III – institucionalização de planos, políticas e modelos; IV – fomento da cultura de gestão por processos; e V – adequação das instâncias de governança e gestão de TI.

5.3. Conclusões

De acordo com as normas e boas práticas acima referenciadas, constata-se que o processo é um dos recursos essenciais à atividade de gestão da continuidade dos serviços de TI.

Portanto, recomenda-se a implantação de processo para gestão da continuidade de serviços de TI que estabeleça controles suficientes para garantir a continuidade dos processos críticos de negócio e consequentemente apoio para a resiliência da organização.

O modelo de implementação do processo de gestão da continuidade de TIC indicado abaixo pode ser utilizado como referência:

- **Processo de Gestão de Continuidade de TIC**[4] – SETIC/TRT 4ª Região.

6. POLÍTICA/PLANO DE BACKUP

6.1. Recomendação

Elaborar e implementar ou revisar política/plano de backup, formalmente instituído, fazendo constar critérios para as cópias de segurança contemplando os sistemas e serviços críticos de TI, em conformidade com as boas práticas aplicáveis.

6.2. Normativos, Jurisprudência do TCU e Boas Práticas

No Acórdão TCU n° 1109/2021 - Plenário foi exarada a seguinte recomendação:

> 9.1 recomendar ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), ao Conselho Nacional de Justiça (CNJ) e ao Conselho Nacional do Ministério Público (CNMP), com fundamento no art. 11 da Resolução - TCU 315/2020, que editem normativos para, cada um no seu âmbito de governança, orientar os gestores e regulamentar a **obrigatoriedade** de que as entidades e órgãos públicos **aprovem formalmente e mantenham atualizadas** políticas gerais e planos específicos de backup (para suas bases de dados e sistemas críticos, por exemplo), contemplando requisitos mínimos para endereçar os cinco subcontroles do controle 10 (Data Recovery Capabilities) do framework preconizado pelo Center for Internet Security (CIS), em especial quanto à definição do escopo dos dados a serem copiados, suas respectivas periodicidades, tipos, quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos de segurança; (grifo nosso)

Tratando da política de backup no Relatório da Unidade técnica do Tribunal de Contas da União, que deu origem ao supracitado acórdão, argumentou-se o seguinte:

> 43. A partir da formalização da política de backup e da implementação das suas prescrições, a organização estará menos sujeita aos efeitos danosos de

[4] Disponível em: https://www.trt4.jus.br/portais/governanca/processo-continuidade-tic . Acesso em 12/08/2021.

> incidentes e/ou falhas que resultem em perda de dados, evitando, assim prejuízos e paradas desnecessárias. Consequentemente, aumenta-se sua resiliência quanto a incidentes de SegInfo e ataques cibernéticos.

A Seção 12.3 da ABNT NBR ISO/IEC 27002:2013 trata especificamente dos controles relativos à cópia de segurança cujo objetivo estabelecido é “proteger contra a perda [...]”. Baseado nos controles propostos, não só a realização de cópias de segurança torna-se indispensável como também, para que seja eficaz, “convém que a política de backup seja estabelecida [...]” e “[...] defina os requisitos para proteção e retenção.”.

Além disso, tratando da infraestrutura de backup, afirma que “convém que os recursos adequados para a geração de cópias de segurança sejam disponibilizados [...]”.

No COBIT 5, no escopo do Processo DSS04 – Gerenciar a Continuidade é estabelecida a prática de gestão DSS04.07 – Gerenciar Mecanismos de Backup, cujo objetivo é “manter a disponibilidade de informações críticas de negócio.”. Essa prática define as seguintes atividades:

> 01. Fazer backup de sistemas, aplicações, dados e documentação de acordo com um cronograma definido, considerando:
>
> - Frequência (mensal, semanal, diária, etc.);
> - Modo de backup (por exemplo, o espelhamento de disco para backups em tempo real vs. DVD-ROM para retenção a longo prazo);
> - Tipo de backup (por exemplo, complete vs. incremental);
> - Tipo de mídia;
> - Backups automatizados on-line;
> - Tipos de dados (por exemplo, voz, óptico);
> - Criação de registros (logs);
> - Dados de computação críticos para o usuário final (por exemplo, planilhas);
> - Localização física e lógica das fontes de dados;
> - Direitos de acesso e segurança;
> - Criptografia.
>
> 02. Certificar que os sistemas, aplicativos, dados e documentação mantida ou processados por terceiros são adequadamente apoiados por backups ou

garantidos de outra forma. Considerar exigir retorno de backups de terceiros. Considere arranjos de custódia ou depósito.

03. Definir os requisitos para armazenamento no local e fora dos dados de backup conforme os requisitos de negócios. Considere a acessibilidade necessária para fazer backup de dados.

04. Implementação da sensibilização a respeito e formação para o Plano de Continuidade de Negócio (BCP).

05. Testar periodicamente e atualizar os dados arquivados e de backup.

6.3. Conclusões

De acordo com as normas, jurisprudência e boas práticas acima descritas, é evidente a necessidade do estabelecimento e implantação de uma política de backup observando, dentre outros requisitos, a contemplação dos processos críticos de negócio, o tempo de retenção dos dados exigido e a necessidade de testes de restauração dos dados de backup.

Atenção especial também deve ser dada à gestão da infraestrutura de backup, composto de hardware e software, garantindo a adequação às necessidades da unidade, considerando todo os aspectos, incluindo a capacidade de armazenamento, vigência do suporte e da garantia e controles suficientes quando for objeto de terceirização.

As práticas aqui relacionadas podem ser utilizadas como fonte de orientação para a implantação do controle, bem como os documentos abaixo indicados:

- **Política de Backup e Restauração de Arquivos** – Ministério Público Militar.
- **Checklists para verificação de política e plano de backup**[5] - TCU

[5] Disponível em : https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp%3FfileId%3D8A81881E75036EE00175584CA573505E&sa=U&ved=2ahUKEwjPnpCb-q7yAhWiJ7kGHb00DN4QFjAAegQIBBAB&usg=AOvVaw3TNnpMH49pTHwy1D5Fhzbn . Acesso em 13/08/2021.

MINISTÉRIO PÚBLICO FEDERAL

Assinatura/Certificação do documento **AUDIN-MPU-00002009/2021 DOCUMENTO DIVERSO**

Signatário(a): **RONALDO DA SILVA PEREIRA**
Data e Hora: **26/10/2021 17:19:02**
Assinado com login e senha

Signatário(a): **EDUARDO DE SEIXAS SCOZZIERO**
Data e Hora: **26/10/2021 18:03:34**
Assinado com login e senha