



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO

ATO N.º 115/GP/TRT 19ª, DE 30 DE AGOSTO DE 2022

Aprova a norma para a realização de cópias de segurança (backup), testes e recuperação de dados no âmbito do Tribunal Regional do Trabalho da 19ª Região.

O DESEMBARGADOR VICE-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA NONA REGIÃO, NO EXERCÍCIO DA PRESIDÊNCIA, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), instituída pela Resolução CNJ n. 370, de 28 de janeiro de 2021;

CONSIDERANDO a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), instituída pela Resolução CNJ n. 396, de 7 de junho de 2021;

CONSIDERANDO a inexistência no âmbito deste Tribunal de formalização quanto à realização de cópias de segurança (*backup*) e recuperação de dados;

CONSIDERANDO que a perda de informações computacionais pode significar prejuízo à prestação jurisdicional por meio da paralisação de atividades essenciais do Tribunal;

CONSIDERANDO que a realização de cópias de segurança é fundamental para a continuidade da prestação jurisdicional em caso de perda de dados ou desastres.

RESOLVE:

Art. 1º **Aprovar** a norma para realização de cópias de segurança (*backup*) e recuperação de dados no âmbito do Tribunal Regional do Trabalho da 19ª Região, na forma do Anexo, para observância e aplicação em todo o Regional.

Art. 2º Este Ato entrará em vigor a partir da data de sua publicação.

Dê-se ciência, cumpra-se e
Publique-se.

Original assinado

JOÃO LEITE DE ARRUDA ALENCAR

Desembargador Vice-Presidente, no exercício da Presidência

Publicado no B.I. n.º 9 e no D.E.J.T. de 1º/9/2022.



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO

ATO N.º 115/GP/TRT 19ª, DE 30 DE AGOSTO DE 2022

ANEXO ÚNICO

NSI003 – CÓPIAS DE SEGURANÇA E RECUPERAÇÃO DE DADOS

1. OBJETIVO

- 1.1. Estabelecer diretrizes e padrões para realização de cópias de segurança (*backup*), testes e recuperação de dados realizados pela Secretaria de Tecnologia da Informação e Comunicação (Setic), no âmbito do Tribunal Regional do Trabalho da 19ª Região.

2. MOTIVAÇÕES

- 2.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.
- 2.2. Garantia de que a salvaguarda das informações seja realizada de forma otimizada, atendendo às necessidades do Tribunal.

3. REFERÊNCIAS NORMATIVAS

- 3.1. Decreto nº 9.637 de 26.12.2018, que institui Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.
- 3.2. Instrução Normativa nº 1/GSIPR, de 27.05.2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.
- 3.3. Resolução nº 396 de 07/06/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- 3.4. Resolução Nº 370 de 28/01/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).
- 3.5. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.
- 3.6. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação.



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO

ATO N.º 115/GP/TRT 19ª, DE 30 DE AGOSTO DE 2022

4. CONCEITOS E DEFINIÇÕES

Para os efeitos deste documento são estabelecidos os seguintes conceitos e definições:

- 4.1. **Backup:** cópia de segurança gerada para possibilitar o acesso ou recuperação futura dos dados, tem por finalidade garantir a recuperação contra desastres, falhas ou comprometimento da integridade, além de permitir o controle histórico, rastreabilidade, auditoria, retorno ao estado anterior, entre outros;
- 4.2. **Backup intradiário:** possui retenção pequena e contém versões de algumas horas do dia;
- 4.3. **Backup diário:** possui retenção pequena, mas contém versões diárias dos arquivos (possibilita o *backup* de várias versões e a navegação por estas versões).
- 4.4. **Backup semanal / mensal / anual:** possui retenção maior, mas só contém a última versão dos dados no momento do *backup*.
- 4.5. **Backup completo:** contém todos os dados existentes no momento do *backup*.
- 4.6. **Backup incremental:** contém somente os dados novos ou modificados desde o último *backup*.
- 4.7. **Dado:** informação em formato digital que pode ser transmitida ou processada. Pode corresponder a documentos, imagens, softwares, dados propriamente ditos (arquivos, bancos de dados), conteúdo multimídia ou qualquer outro registro de conteúdo passível de armazenamento em algum tipo de mídia.
- 4.8. **Disco rígido local:** dispositivo de armazenamento de dados utilizado pelos computadores pessoais e estações de trabalho.
- 4.9. **Gestor Executivo:** servidor da área comercial responsável pelo produto, sistema ou serviço;
- 4.10. **Gestor Técnico:** servidor da Setic responsável pelo produto, sistema ou serviço;
- 4.11. **Mídia de backup ou gravação:** meio físico no qual é armazenado um *backup*.
- 4.12. **Réplica:** cópia dos dados em outro ambiente físico com as mesmas configurações do original.
- 4.13. **RPO (Recovery Point Objective):** o quanto é necessário voltar no tempo para encontrar uma cópia íntegra dos dados, ou seja, o tempo máximo de perda de dados.
- 4.14. **RTO (Recovery Time Objective):** tempo estimado para restaurar os dados ou para tornar os sistemas disponíveis novamente.
- 4.15. **Versão do arquivo:** sempre que um arquivo for criado ou alterado, é criada uma nova versão deste arquivo no *backup*.

5. REALIZAÇÃO DE CÓPIAS DE SEGURANÇA

- 5.1. A realização de cópias de segurança (*backup*) será de forma automatizada e protegerá os arquivos gravados nas pastas privativas de cada unidade do



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO

ATO N.º 115/GP/TRT 19ª, DE 30 DE AGOSTO DE 2022

Tribunal, além dos dados dos sistemas e serviços computacionais disponibilizados pelo TRT.

- 5.2. Os dados armazenados em discos rígidos locais de estações de trabalho e notebooks não serão protegidos, não sendo garantida sua recuperação em caso de erro físico nas mídias de gravação ou instabilidade no sistema operacional instalado na máquina.
- 5.3. A unidade responsável pela execução das atividades de cópia, testes e recuperação de *backups* é a Divisão de Infraestrutura Tecnológica - DIT.
- 5.4. Cabe ao gestor executivo do produto, sistema ou serviço, definir, com apoio do gestor técnico, os requisitos para realização do *backup*, tais como: os dados que devem estar contemplados no *backup*, tempo de retenção, quantidade de versões armazenadas, *RTO*, *RPO*, dentre outros que se fizerem necessários por definições administrativas, técnicas ou legais.
- 5.5. O gestor técnico deve solicitar, formalmente, à área responsável pelas atividades de *backup*, a inserção dos dados do produto, sistema ou serviço nas rotinas de *backup*, informando os requisitos de manutenção destes dados ao longo do tempo, sempre que o gestor executivo autorizar sua entrada em produção.
- 5.6. A Setic poderá recusar pedidos de criação de rotinas de backup de ativos, isolada ou cumulativamente, quando a criação impactar negativamente outras rotinas já implementadas ou quando o custo de criação for maior que o valor do ativo para o Tribunal.
- 5.7. Em caso de alteração dos requisitos para realização do *backup*, o gestor técnico deverá atualizar a área responsável pelas atividades de *backup* com as novas demandas, visando a correta salvaguarda das informações.
- 5.8. Poderão ser utilizadas técnicas de replicação *online* de dados, a exemplo de replicação entre bancos de dados ou *storages*, como forma de proteção para os dados mais críticos, visando maior disponibilidade, diminuição de *RPO* e *RTO* ou distribuição de carga.
- 5.9. Os dados objeto de réplica *online* deverão ser distribuídos, preferencialmente, em *datacenters* distintos, de acordo com as melhores práticas e com a estratégia definida pela equipe responsável.
- 5.10. As cópias de segurança deverão ser armazenadas, preferencialmente, em meio físico que proporcione maior celeridade aos processos de gravação e recuperação, como dispositivos de gravação não sequencial, a exemplo de unidades de armazenamento em massa (*storages*).
- 5.11. As mídias de gravação sequencial (fitas) deverão ser utilizadas, preferencialmente, como meios secundários de armazenamento, por demandarem, em geral, maior tempo para acesso ao seu conteúdo.
- 5.12. Os *backups* armazenados em fitas poderão ter cópias, em conjunto diverso de fitas, armazenado em local físico diferente.
- 5.13. O Tribunal deverá manter local para armazenamento de fitas offline com acesso físico restrito e controlado, ademais sem acesso remoto.



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO

ATO N.º 115/GP/TRT 19ª, DE 30 DE AGOSTO DE 2022

- 5.14. As mídias de *backup*, quando transportadas, deverão ser protegidas de extravio e de eventos que possam causar dano físico.
- 5.15. A movimentação de mídias de *backup* deverá ser realizada por servidor designado, com registro, no mínimo, da identificação da mídia, data e hora da movimentação.
- 5.16. As mídias a serem descartadas deverão ser destruídas de forma a impedir sua reutilização ou acesso aos dados por pessoas não autorizadas.
- 5.17. A periodicidade de realização das cópias, o tempo de retenção, o RPO e o RTO dos *backups* observarão, em geral, as seguintes regras (excetuados os dados que possuem regramento próprio):

Grupo de Backup		Arquivos em pastas privativas das unidades	Bancos de dados	Máquinas Virtuais
Backup Intradiário	Tipo	-	Incremental	-
	Dias e horários	-	Todos os dias, a cada 3 (três) horas.	-
	Retenção	-	7 dias	-
Backup Diário	Tipo	Incremental	-	Incremental
	Dias e horários	Entre 0 e 6 h	-	Entre 0 e 6 h
	Retenção	90 dias	-	14 dias
Backup Semanal	Tipo	-	Completo	-
	Dias e horários	-	Entre 0 e 6 h. (em dias da semana diferentes para cada banco de dados)	-
	Retenção	-	90 dias	-
Backup Mensal	Tipo	Completo	Completo	-
	Dias e horários	Primeiro sábado de cada mês.	Entre 0 e 6 h. (primeira semana do mês)	-
	Retenção	Serão armazenados por 12 meses	12 meses	-
Backup Anual	Tipo	Completo	Completo	-
	Dias e horários	Primeira semana de janeiro	Primeira semana de janeiro	-
	Retenção	05 anos	05 anos	-
RPO (tempo máximo de perda dos dados)		24 horas	3 horas	24 horas
RTO (tempo estimado para a restauração)		Em média, 1 hora para cada 180 GB de dados.	30 horas	1 hora

- 5.18. No caso de serviços armazenados em nuvem, a responsabilidade pela segurança dos dados será da prestadora de serviços, com prazo de retenção previsto em contrato, de acordo com a norma de *backup*.

6. RECUPERAÇÃO DE DADOS



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO

ATO N.º 115/GP/TRT 19ª, DE 30 DE AGOSTO DE 2022

- 6.1. A recuperação de arquivos, sempre que não puder ser realizada pelo próprio usuário, será solicitada à Setic, através de abertura de chamado de suporte técnico específico para este fim.
- 6.2. A recuperação de bases de dados de sistemas deverá ser autorizada pelo respectivo gestor executivo, em comunicação formal direcionada à Setic, descrevendo detalhadamente a motivação e a data de referência a ser considerada na recuperação.
- 6.3. Em caso de desastre, todas as áreas necessárias, sejam elas internas ou externas à Setic, deverão ser designadas pela administração a atuar com prioridade, com todos os meios disponíveis, para atender às necessidades de recuperação dos dados e equipamentos necessários ao restabelecimento dos serviços.

7. TESTES DE RECUPERAÇÃO DE DADOS

- 7.1. Periodicamente serão realizados testes de recuperação de dados.
- 7.2. Os testes serão baseados em dados pré-selecionados que garantam a efetividade, eficiência e confiabilidade do procedimento, na periodicidade e forma estabelecidas no quadro que segue:

Grupo de <i>backup</i>	Periodicidade	Recuperação	Validação
Arquivos em pastas privativas das unidades	Trimestral	Restauração, por amostragem, de qualquer versão anterior à última de, ao menos, 1 (um) arquivo de, no mínimo, 5 (cinco) unidades distintas.	Verificação da integridade dos arquivos recuperados.
Bancos de Dados	Trimestral	Restauração de qualquer versão de <i>backup</i> do período em análise, utilizando ambiente isolado da produção. Os testes devem envolver todos os principais bancos de dados dos sistemas administrativos e judiciários. Os testes podem acontecer em momentos diferentes, desde que, num mesmo trimestre, todos os principais bancos de dados tenham sido alvo de, pelo menos, um teste.	Testar, por amostragem, o acesso às estruturas do banco de dados restaurado.
Máquinas Virtuais	Trimestral	Restauração de máquinas virtuais, em número não inferior a 5% do total de máquinas virtuais, por tecnologia de virtualização. Os testes devem ser realizados em ambiente isolado da produção.	Testar o funcionamento dos principais serviços básicos da máquina em relação ao seu sistema operacional. Testar o serviço provido pela máquina ou a existência e a integridade de seus principais arquivos de configuração.



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO

ATO N.º 115/GP/TRT 19ª, DE 30 DE AGOSTO DE 2022

- 7.3. A unidade responsável pela execução dos testes de recuperação periódicos é a Divisão de Infraestrutura Tecnológica - DIT, podendo contar com o apoio de outras áreas dentro da Setic para validação.
- 7.4. Se recuperações de dados forem realizadas em períodos iguais ou menores que os definidos para os testes, a equipe responsável pela execução dos testes poderá, a partir dos resultados obtidos, considerar que tais ações têm validade como teste naquele período.
- 7.5. Os procedimentos relativos aos testes de recuperação devem ser registrados, em ferramenta de controle definida pela própria Setic, com informações sobre os dados, períodos, pessoas e áreas envolvidas.
- 7.6. Qualquer teste que resulte em falha, onde o arquivo de *backup* utilizado não tenha sido capaz de prover as informações necessárias ao restabelecimento completo das funcionalidades do banco de dados analisado, deve ser informado à direção da Setic, que analisará as providências a serem tomadas. Esta falha deve constar dos registros dos testes de recuperação realizados.

8. ATUALIZAÇÃO DA NORMA

- 8.1. As diretrizes previstas na presente norma serão atualizadas sempre que necessário, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.



Tribunal Regional do Trabalho
19ª Região | Alagoas

Manual de Processo

Processo de realização de cópias de segurança
(backup) e recuperação de dados

Versão do documento: 1.0
agosto 2022



Sumário

Objetivo	3
Propósito	3
Escopo	3
Definições e abreviações	3
Benefícios esperados	4
Regras Gerais	4
Interfaces com demais processos	4
Papéis e Responsabilidades	4
Indicadores de Desempenho	5
Controles de execução	5
Fluxograma	7
Descrição das Tarefas	8
Fluxograma	12
Descrição das Tarefas	13



Objetivo

Definir o processo de realização de cópias de segurança (backup), testes e recuperação de dados a ser implantado pela Secretaria de Tecnologia da Informação e Comunicação do Tribunal Regional do Trabalho da 19ª Região.

Propósito

Este processo tem como propósito garantir a continuidade do negócio e disponibilidade dos dados, mesmo após corrupção de dados e desastres, considerando o Tempo de Recuperação (RTO – *Recovery Time Objective*) e Ponto de Recuperação (RPO – *Recovery Point Objective*) adequados para cada serviço..

Escopo

Este processo é aplicável a todo dado presente na infraestrutura computacional do TRT19 que sofre backup, garantindo que os parâmetros e procedimentos sejam corretamente aplicados e nos que não sofrem backup, monitorando se alterações externas (normativas, legais, entre outras) ou alterações no ativo que contém o dado, o torne passível a sofrer backup.

Definições e abreviações

- **Dado:** informação em formato digital que pode ser transmitida ou processada. Pode corresponder a documentos, imagens, softwares, dados propriamente ditos (arquivos, bancos de dados), conteúdo multimídia ou qualquer outro registro de conteúdo passível de armazenamento em algum tipo de mídia.
- **Incidente:** qualquer evento que não faz parte da operação de um serviço e que causa uma interrupção deste ou uma redução da sua qualidade.
- **Backup:** cópia de segurança gerada para possibilitar o acesso ou recuperação futura dos dados, tem por finalidade garantir a recuperação contra desastres, falhas ou comprometimento da integridade, além de permitir o controle histórico, rastreabilidade, auditoria, retorno ao estado anterior, entre outros;
- **Ferramenta de Backup e Recuperação:** Conjunto de programas especializados no planejamento, identificação, processamento e controle de Backup e Recuperação de dados;
- **Gestor Executivo:** servidor da área comercial responsável pelo produto, sistema ou serviço;
- **Gestor Técnico:** servidor da Setic responsável pelo produto, sistema ou serviço;
- **Acordo de Nível de Serviço (ANS):** acordo firmado entre a área de Tecnologia da Informação e Comunicação (TIC) e as áreas de negócio do Tribunal. Descreve o serviço de Tecnologia da Informação e Comunicação, suas metas de nível de serviço, além dos papéis e responsabilidades das partes envolvidas no acordo;
- **Requisito:** Consiste numa exigência que deve ser atendida para que algo ou alguém esteja em conformidade com algum critério técnico, processual ou legal.
- **Recuperação:** Retorno dos dados a uma condição anterior, usável e funcional.



- **RPO (Recovery Point Objective):** o quanto é necessário voltar no tempo para encontrar uma cópia íntegra dos dados, ou seja, o tempo máximo de perda de dados.
- **RTO (Recovery Time Objective):** tempo estimado para restaurar os dados ou para tornar os sistemas disponíveis novamente.

Benefícios esperados

Com a implementação deste processo no TRT da 19ª Região espera-se:

- minimizar a perda acidental dados;
- garantir a integridade dos dados do negócio;
- garantir a continuidade do negócio, mesmo diante de um incidente ou desastre.

Regras Gerais

- A inserção de produto, sistema ou serviço nas rotinas de backup, testes e recuperação, deverá ser solicitada formalmente pelo gestor técnico, sempre que sua entrada em produção seja autorizada pelo gestor executivo. Todo e qualquer incidente ou requisição de serviço deve passar pela Central de Serviços;
- Registrar todos os detalhes relevantes dos testes de recuperação;
- Resolver as solicitações de recuperação de dados o mais breve possível;
- Manter os usuários informados do progresso de sua solicitação.

Interfaces com demais processos

A seguir estão descritas as principais interfaces deste processo com outros processos de gestão de Tecnologia da Informação e Comunicação do TRT19:

- **Gestão de incidentes e cumprimento de requisição:** O pedido de restauração de dados deve ser realizado via abertura de requisição;
- **Gerenciamento de mudanças:** alteração na norma de backup, resultado de sua revisão periódica, deve, quando necessário produzir RDM's tratadas por esse processo.

Papéis e Responsabilidades

Papel	Executores	Responsabilidades
Dono do Processo	Diretor da Divisão de Infraestrutura Tecnológica	• Revisar a Norma de cópia de segurança (backup) e recuperação de dados; • Prezar pelo cumprimento da Norma de cópia de segurança (backup) e recuperação de dados;



Gestor Técnico	Servidor da Setic responsável pela informação que está sendo armazenada em backup	• Coletar requisitos junto aos gestores executivos dos sistemas /serviços; • Emitir sugestões de melhorias no processo;
Divisão de Infraestrutura Tecnológica	Servidor da área de infraestrutura de TIC	• Classificar ativos quanto à classe de backup • Executar a Norma de cópia de segurança (backup) e recuperação de dados; • Elaborar e revisar procedimentos de backup, testes e recuperação de dados; • Manter todas as partes envolvidas informadas; • Monitorar a execução das rotinas de backup.
Setor de Atendimento de Serviços de TIC	Servidor da área de atendimento de serviços de TIC	• Receber as solicitações de backup e restore; • Notificar qualquer evento relevante acerca de Backup e Restore; • Prover a recuperação de backup de sistemas de arquivos dos usuários.

Indicadores de Desempenho

Os indicadores descritos a seguir irão avaliar o desempenho do processo.

Descrição do Indicador	Método de apuração / fórmula de cálculo	Frequência
Percentual de falhas nos testes de recuperação	$(\text{n}^\circ \text{ falhas nos testes de recuperação} / \text{n}^\circ \text{ total de testes de recuperação}) \times 100$	anual

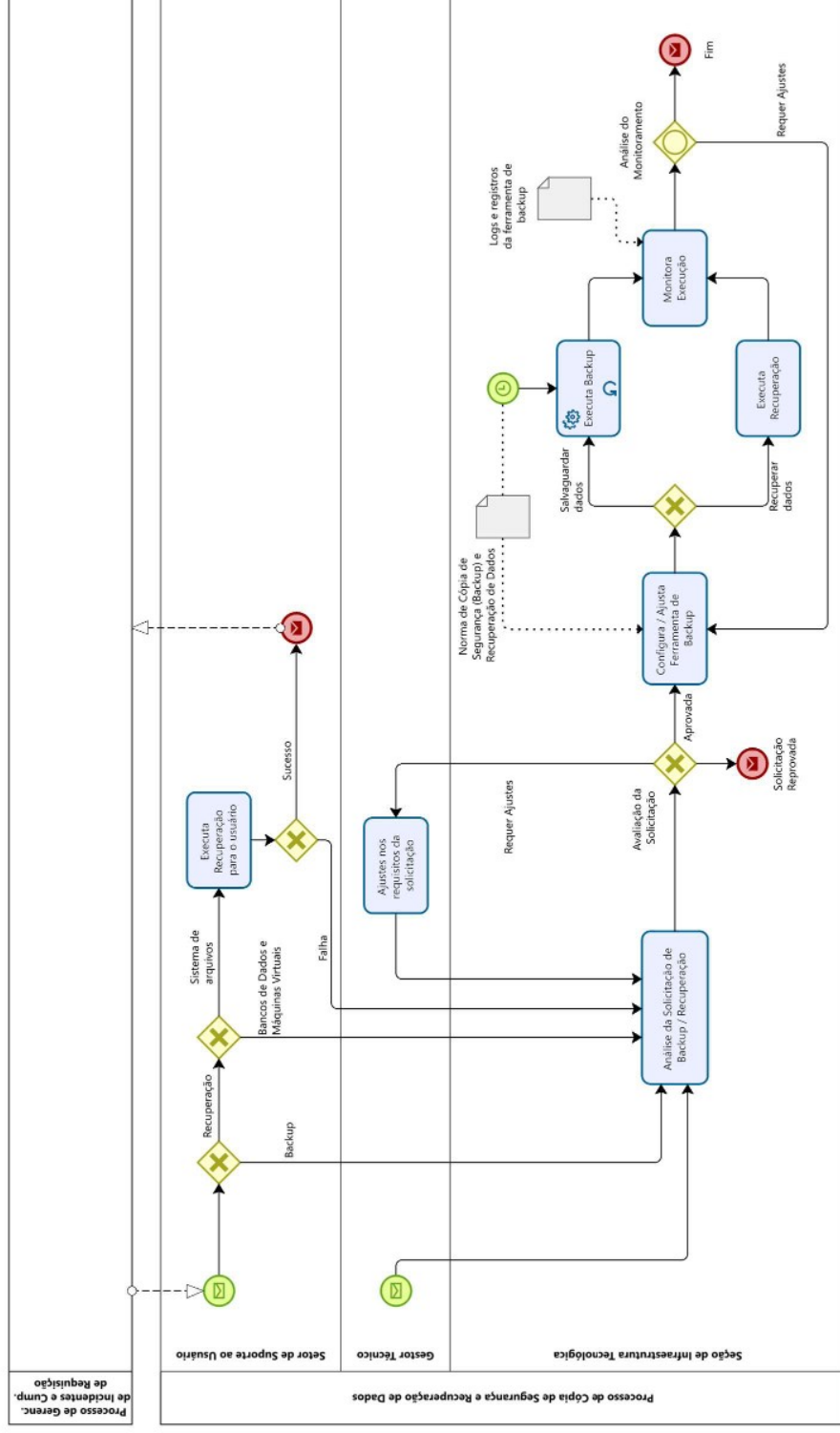
Controles de execução

Controle	Método de execução	Frequência
Auditoria	Realizar uma reunião com as equipes executoras do processo, para avaliar a aderência, os benefícios gerados e oportunidades	Anual



	de melhoria do processo. Essa reunião deve identificar se o processo necessita de revisão.	
--	--	--

Fluxograma





Descrição das Tarefas

Análise da Solicitação de Backup / Recuperação		
Descrição	Receber a solicitação de backup pelo Gestor Técnico ou a solicitação de restauração pelo Gestor executivo / Usuário, via Sistema de atendimento ao usuário de TIC.	
Papéis	Gestor Técnico / Gestor Executivo / Usuário	
Considerações importantes	O Gestor Técnico, após acordo com o Gestor Executivo, deve solicitar, à área responsável pelo sistema de backup, via Ferramenta de Gerenciamento de Demandas usada pela Setic, a implementação de rotina de backup para um determinado recurso, especificando os dados a serem protegidos, assim como, frequência e tempo de retenção das cópias, adequados às necessidades institucionais. Recomenda-se que a issue na Ferramenta de Gerenciamento de Demandas seja juntada a outra guarda-chuva, que reúna todas as demais solicitações de implementação de backup.	
Entradas	Recurso que demanda proteção de backup / restauração. Alteração nos requisitos de backup / restauração.	
Saídas	Solicitação de implementação de backup ou de recuperação de dados, com seus respectivos requisitos.	
Atividades	Analisar solicitação de backup	Verificar a completude dos requisitos.
	Analisar solicitação de recuperação	Verificar a completude dos requisitos.
Ferramentas	Ferramenta de Gerenciamento de Demandas / Sistema de atendimento ao usuário de TIC	

Executa recuperação para o usuário	
Descrição	Executa a recuperação de dados solicitados pelo usuário de TIC e que estavam nas pastas de rede.
Papéis	Setor de Atendimento de Serviços de TIC
Considerações importantes	Os dados disponíveis nas pastas de rede podem ser recuperados pelo Setor de Atendimento de Serviços de TIC



	através de abertura de chamado na central de serviços.	
Entradas	Solicitação de restauração através de chamado.	
Saídas	Dados recuperados na pasta da rede.	
Atividades	Restaurar dados	Restaurar dados do backup de arquivos de rede.
Ferramentas	Interface web da Ferramenta de backup e recuperação de dados	

Ajustes nos requisitos da solicitação

Descrição	Entrar em contato com gestor executivo para solicitar os requisitos faltantes para implementação do backup ou para recuperação de dados	
Papéis	Gestor Técnico	
Considerações importantes		
Entradas	Solicitação de backup / restauração	
Saídas	Solicitação de backup / restauração ajustada	
Atividades	Ajustar solicitação	Atualizar solicitação com os requisitos necessários.
Ferramentas	Ferramenta de gestão de demandas	

Configura / ajusta ferramenta de backup

Descrição	Implementar na ferramenta de backup utilizada pelo Regional, as rotinas necessárias para realização de cópia de segurança e restauração de dados do ativo em questão, de acordo com a norma e com os requisitos levantados.	
Papéis	Divisão de Infraestrutura Tecnológica	
Considerações importantes		
Entradas	Solicitação de backup / restauração; Norma de cópia de segurança (backup) e restauração de dados; Análise do monitoramento da execução	



Saídas	Configuração / Ajuste da ferramenta de backup e recuperação de dados realizado.	
Atividades		
Ferramentas	Ferramenta de backup e recuperação de dados	

Executa Backup

Descrição	Realizar uma ou mais cópias dos dados em mídia apropriada.	
Papéis	Divisão de Infraestrutura Tecnológica	
Considerações importantes		
Entradas	Solicitação de backup / restauração e Norma de cópia de segurança (backup) e restauração de dados.	
Saídas	Cópias de Segurança	
Atividades		
Ferramentas	Ferramenta de backup e recuperação de dados	

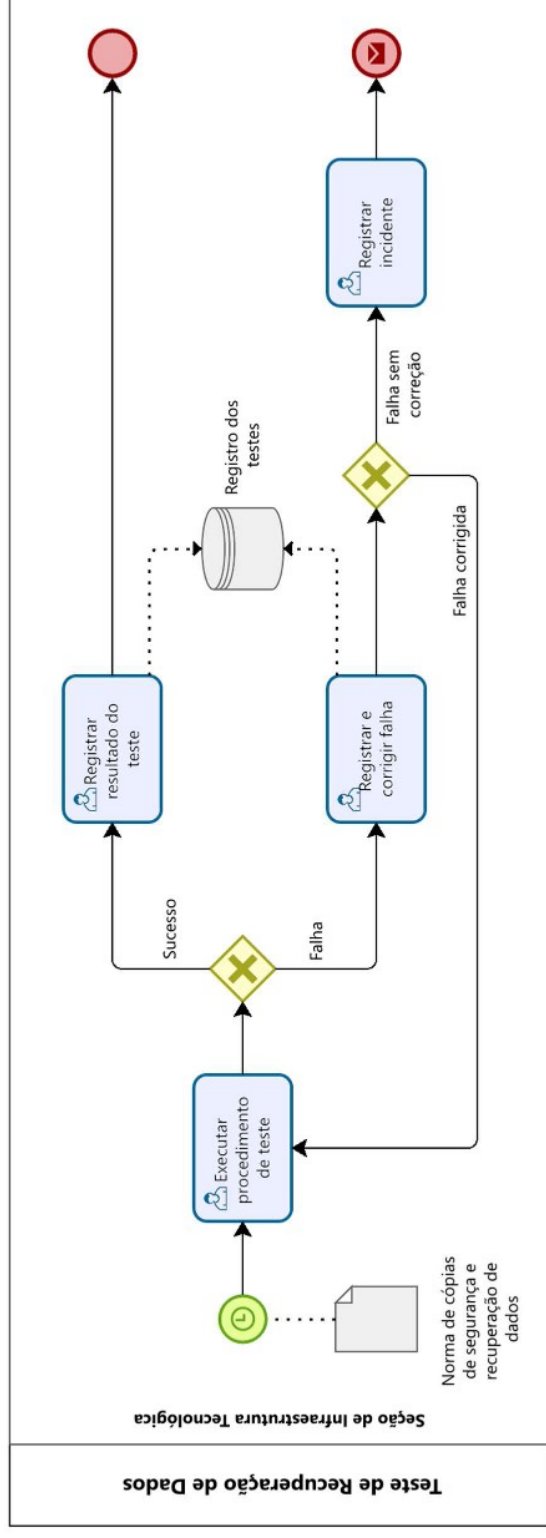
Executa Restauração

Descrição	Recuperar dados, utilizando a ferramenta de backup em uso no Regional de acordo com a solicitação do usuário final, do gestor executivo ou caso seja identificado algum incidente com perda de dados.	
Papéis	Divisão de Infraestrutura Tecnológica	
Considerações importantes	O procedimento técnico deve ser realizado de acordo com o manual de procedimento técnico da solução de backup.	
Entradas	Informação dos dados a serem recuperados.	
Saídas	Dados recuperados	
Atividades		
Ferramentas	Ferramenta de backup e recuperação de dados	



Monitora Execução		
Descrição	Verificar diariamente os logs e os registros de atividades relacionadas ao sistema de backup à procura de erros, anomalias, configurações incorretas e escassez de recursos de armazenamento.	
Papéis	Divisão de Infraestrutura Tecnológica	
Considerações importantes	Quando o monitoramento registrar falha em alguma rotina de backup ou recuperação, um novo incidente deve ser registrado e será tratado no processo de gestão de incidentes de segurança.	
Entradas	Logs e outros registros relacionados à ferramenta de backup.	
Saídas	Registro de incidente em caso de falha no backup ou recuperação.	
Atividades		
Ferramentas	Ferramenta de backup e recuperação de dados	

Fluxograma





Descrição das Tarefas

Executar procedimento de teste		
Descrição	Executar o teste coletando informações sobre o comportamento do sistema após procedimento de recuperação.	
Papéis	Divisão de Infraestrutura Tecnológica	
Considerações importantes		
Entradas	Norma de backup	
Saídas	Resultado da recuperação	
Atividades	Abrir	Abrir demanda para registrar o teste de recuperação.
	Executar	executar os procedimentos de recuperação de dados.
Ferramentas	Ferramenta de Gerenciamento de Demandas e Ferramenta de backup e recuperação de dados	

Registrar resultado de teste		
Descrição	Criar documento que contenha os dados relevantes sobre o teste como forma de registro da atividade para que sirva para melhoria.	
Papéis	Divisão de Infraestrutura Tecnológica	
Considerações importantes		
Entradas	Resultado do teste	
Saídas	Relatório de testes	
Atividades	Registrar	registrar resultado dos testes na ferramenta de gestão de demandas.
Ferramentas	Ferramenta de Gerenciamento de Demandas	



Registrar e corrigir falha		
Descrição	Registrar resultado do teste e corrigir as falhas encontradas.	
Papéis	Divisão de Infraestrutura Tecnológica	
Considerações importantes		
Entradas	Resultado dos testes	
Saídas	Falhas corrigidas	
Atividades	Registrar	registra as falhas encontradas.
	Corrige	corrige as falhas encontradas.
	Executa	executa os testes novamente.
Ferramentas	Ferramenta de Gerenciamento de Demandas e Ferramenta de backup e recuperação de dados	

Registrar incidente		
Descrição	Caso haja falha no teste de recuperação, um novo incidente deve ser registrado e será tratado no processo de gestão de incidentes de segurança.	
Papéis	Divisão de Infraestrutura Tecnológica	
Considerações importantes		
Entradas	Falhas encontradas.	
Saídas	Registro do incidente.	
Atividades	Comunicar	Comunicar para o setor de segurança.
Ferramentas	Ferramenta de Gerenciamento de Demandas.	