

	ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE CÓPIAS DE SEGURANÇA DE DADOS	
	Proposto por: Divisão de Servidores (DISER) Divisão de Banco de Dados (DIBDA)	Aprovado por: Diretor do Departamento de Sustentação de Tecnologia da Informação e Comunicação de Dados (DETIC)

IMPORTANTE: sempre verifique no site do TJRJ se a versão impressa do documento está atualizada.

1) OBJETIVO

Estabelecer critérios e procedimentos para a segurança da informação dos registros organizacionais armazenados eletronicamente, emitindo diretrizes gerais para sua confidencialidade, integridade e disponibilidade.

2) CAMPO DE APLICAÇÃO E VIGÊNCIA

Esta Rotina Administrativa (RAD) se aplica à Divisão de Servidores da Secretaria-Geral de Tecnologia da Informação (SGTEC/DISER) e à Divisão de Banco de Dados da Secretaria-Geral de Tecnologia da Informação (SGTEC/DIBDA), passando a vigorar a partir de 25/01/2024.

3) DEFINIÇÕES

TERMO	DEFINIÇÃO
<i>Backup</i>	Cópia de segurança de caráter preventivo, preferencialmente feita <u>em</u> meio de armazenamento externo, <u>diverso do armazenamento original</u> .
Confidencialidade da informação	Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
Disponibilidade da informação	Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
Integridade da informação	Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.
Fita	Meio de armazenamento magnético.
<i>Hardware</i>	Componente físico dos equipamentos de informática.
Sala-cofre	Ambiente físico adequado, refrigerado, seguro, protegido por sistemas de controle e monitoração do ambiente, para proteger os computadores servidores e dados corporativos.

Base Normativa	Código:	Revisão:	Página:
Ato Executivo nº 2.950/2003	RAD-SGTEC-021	16	1 de 14

**ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE
CÓPIAS DE SEGURANÇA DE DADOS**

<u>APPLIANCE</u>	<u>Dispositivo de hardware dedicado para as tarefas de backup</u>
Unidade robótica de <i>backup</i>	<i>Hardware</i> responsável pela gravação e recuperação das fitas de <i>backup</i> , conforme políticas estabelecidas no <i>Netbackup</i> .
Netbackup	Software responsável pela configuração, gerenciamento e execução das políticas de backup.
HPSM	<u>Hewlett-Packard Service Manager</u> - Software de gerenciamento de serviços de TI <u>criado pela fabricante HP</u> , utilizado pela SGTEC para abertura de incidentes e requisições.
Política de <i>Backup</i>	Onde são definidas regras que o <i>software</i> de <i>backup</i> automático utilizará para realizar o <i>backup</i> .
Restore	Restauração dos dados armazenados por backup
Script	Conjunto de comandos agrupados com função específica escrito em determinada linguagem de programação.
Servidores de Domínio e Infraestrutura	Sistema responsável pela autenticação e acesso dos usuários aos recursos de rede.
Servidores de Arquivos	Servidor para salvaguarda de arquivos departamentais.
<i>Software</i>	1.Qualquer programa (sistema operacional ou aplicativos) utilizado nos equipamentos de informática do PJERJ; 2.Componente lógico dos equipamentos de informática.

4) REFERÊNCIAS

- NBR ISO/IEC 17799:2001 e NBR ISO/IEC 27002/2013 – Código de prática para a gestão da segurança da informação;
- ATO NORMATIVO TJ N.º 08/2019 - Estabelece as normas para Gestão de Segurança da Informação (GSI) do Poder Judiciário do Estado do Rio de Janeiro.
- Resolução TJ/OE n.º 05/2019 - Institui a Política de Segurança da Informação do Poder Judiciário do Estado do Rio de Janeiro.
- Ato Normativo TJ n.º 27/2020 – Estabelece as normas de gestão de acessos aos recursos computacionais do PJERJ.

Base Normativa	Código:	Revisão:	Página:
Ato Executivo nº 2.950/2003	RAD-SGTEC-021	16	2 de 14

**ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE
CÓPIAS DE SEGURANÇA DE DADOS**

- Portaria CNJ nº 162/2021, de 10 de junho de 2021 – Aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).
- Documentação dos fabricantes de Hardware e *Software* utilizados na abrangência deste procedimento;

5) RESPONSABILIDADES GERAIS

FUNÇÃO	RESPONSABILIDADE
<u>Diretor do Departamento de Sustentação de Tecnologia da Informação e Comunicação de Dados da Secretaria-Geral de Tecnologia da Informação (SGTEC/DETIC)</u>	• Manter o ambiente computacional em situação satisfatória de desempenho e integridade; • manter os contratos de manutenção e suporte dos servidores.
<u>Diretor da Divisão de Servidores da Secretaria-Geral de Tecnologia da Informação (SGTEC/DISER)</u>	• <u>Fornecer ao Serviço de Processamento de Dados e Monitoramento de Infraestrutura de Tecnologia da Informação e Comunicação de Dados da Secretaria-Geral de Tecnologia da Informação (SGTEC/SEPRO) infraestrutura para o correto armazenamento das fitas de <i>backup</i>.</u>
<u>Diretor da Divisão de Banco de Dados ou chefe de serviço diretamente subordinado a essa Direção, da Secretaria-Geral de Tecnologia da Informação (SGTEC/DIBDA)</u>	• Analisar e levantar as características do banco de dados a ser preservado; • estudar e sugerir a melhor e mais recomendada forma de <i>backup</i> para aquele banco de dados; • analisar e solucionar a razão para falha de determinada rotina elaborada pelo DIBDA, de <i>backup</i>; • fornecer solução para o erro, relativo as rotinas elaboradas pelo DIBDA, comunicado pelo SEPRO durante a execução de determinada rotina de <i>backup</i>; • solicitar suporte de terceiros em caso de tecnologia ou erro não documentado nas rotinas elaboradas pelo DIBDA.

**ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE
CÓPIAS DE SEGURANÇA DE DADOS**

FUNÇÃO	• RESPONSABILIDADE
<u>Chefe do Serviço de Processamento de Dados e Monitoramento de Infraestrutura de Tecnologia da Informação e Comunicação de Dados da Secretaria-Geral de Tecnologia da Informação (SGTEC/SEPRO)</u>	• Implementar política de <i>backup</i> automática; • executar e monitorar a(s) rotina(s) de <i>backup</i> no(s) período(s) pré-determinado(s); • comunicar prontamente falhas que interrompam a execução das rotinas de <i>backup</i> aos administradores responsáveis; • comunicar eventuais erros apresentados durante a execução da rotina de <i>backup</i> aos administradores responsáveis; • manter as fitas de <i>backup</i> corretamente armazenadas e catalogadas; • executar o procedimento manual de destruição das fitas LTO; • solicitar suporte de terceiros em caso de falha na unidade robótica.

6) DIRETRIZES

6.1 As políticas de backup podem ser divididas segundo plataformas e sistemas usados e foram definidas de acordo com a seguinte estruturação:

ALVO DO BACKUP	PERIODICIDADE	RETENÇÃO	DESCARTE DA FITA
<u>Banco de Dados Oracle dos Sistemas Judiciais</u>	<u>Diário / Semanal</u>	<u>1 semana / 1ano</u>	<u>Destruição manual da fita conforme item 6.6</u>
<u>Banco de Dados Oracle dos Sistemas Administrativos</u>	<u>Diário / Semanal</u>	<u>1 semana / 1ano</u>	<u>Destruição manual da fita conforme item 6.6</u>
<u>Banco de dados Oracle da Consulta Processual</u>	<u>Diário / Semanal</u>	<u>1 semana / 1ano</u>	<u>Destruição manual da fita conforme item 6.6</u>
<u>Banco de dados Postgres do Portal Corporativo Liferay</u>	<u>Diário</u>	<u>1 semana</u>	<u>Destruição manual da fita conforme item 6.6</u>
<u>Banco de dados Caché de Sistemas da Corregedoria</u>	<u>Diário</u>	<u>1 semana</u>	<u>Destruição manual da fita conforme item 6.6</u>

Base Normativa Ato Executivo nº 2.950/2003	Código: RAD-SGTEC-021	Revisão: 16	Página: 4 de 14
--	---------------------------------	-----------------------	---------------------------

ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE CÓPIAS DE SEGURANÇA DE DADOS

6.2 As cópias de segurança (backup) podem ser armazenadas em fitas magnéticas, disco e/ou nuvem;

6.3. A identificação da fita é realizada por etiqueta colada em seu dorso, com uma numeração impressa com o código de barras para que o *software* de *backup* automaticamente a identifique.

6.4. O controle de acesso ao ambiente interno da sala cofre é feito por identificação biométrica.

6.5. Os procedimentos de *backup* são realizados apenas por operadores previamente autorizados e com acesso à sala cofre.

6.5. Dos registros das atividades de *backup*:

6.5.1. *Backup* eletrônico: os registros das atividades de *backup* automático contêm informações tais como horário de início e fim dos procedimentos, volume de dados gravados, servidor e tipo de *backup*, sendo estes registros controlados e armazenados eletronicamente pelo *software* de *backup* automático.

6.6. Do descarte das fitas magnéticas LTO:

6.6.1. As fitas LTO que apresentam falhas são separadas e relacionadas no formulário Controle de Descartes das Fitas (RAD-SGTEC-021-04) e destruídas manualmente.

7) ELABORAR E MANTER PROCEDIMENTOS DE *BACKUP*

7.1. Identifica a plataforma de *hardware*, o sistema operacional do servidor, o meio de armazenamento externo disponível para aquele servidor e o *software* do banco de dados ali instalado.

7.2. Estima a quantidade de objetos de banco e sua adequação ao limite de espaço do meio de armazenamento.

7.3. Estuda a melhor política ou a mais recomendada pelo fabricante do banco de dados.

7.4. Analisa a sua adequação à situação presente.

7.5. Escreve *script* de teste para mensurar tempo de execução.

7.6. Procura melhor horário e períodos de execução do procedimento, seja ele manual ou automático.

Base Normativa	Código:	Revisão:	Página:
Ato Executivo nº 2.950/2003	RAD-SGTEC-021	16	5 de 14

ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE CÓPIAS DE SEGURANÇA DE DADOS

7.7. Para a manutenção dos procedimentos de *backup* dos bancos de dados são executadas as seguintes atividades:

- (DIBDA): Auxiliar e orientar permanentemente os operadores do SEPRO quando do surgimento de dúvidas ou novos procedimentos de *backup*, bem como na catalogação das fitas para facilitar a sua recuperação quando for necessário o *restore*.
- (SEPRO): Periodicamente acompanhar as execuções, medindo tempos de execução e quantidade de dados que está sendo copiada.

7.8. No caso de ocorrer falha na execução do procedimento, averigua a origem de falhas nas execuções de *backup* e procura a solução para ocorrência do erro na execução do *backup*.

7.9. Acompanha o surgimento de novas tecnologias que forneçam velocidades de gravação superior ou novas formas de realização de *backup*.

8) EXECUTAR BACKUP

8.1. Executar Backup Automático:

8.1.1. Executa o programa *NETBACKUP*.

8.1.1.1. Cria o catálogo para todos os tipos de meios de armazenamento, definindo o tempo de retenção e expiração.

8.1.1.2. Verifica, utilizando o programa *NETBACKUP*, as fitas que estão armazenadas no cofre cujo prazo de retenção expirou liberando-as para reutilização.

8.1.1.3. Verifica, utilizando o programa *NETBACKUP*, quais fitas estão totalmente ocupadas, solicitando sua liberação para o devido armazenamento até que expire o tempo de retenção.

8.1.2. Coloca na unidade robótica de *backup*, as fitas liberadas para reutilização (8.1.1.2) realizando em seguida, utilizando programa *NETBACKUP*, a devida reintegração delas.

Base Normativa	Código:	Revisão:	Página:
Ato Executivo nº 2.950/2003	RAD-SGTEC-021	16	6 de 14

ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE CÓPIAS DE SEGURANÇA DE DADOS

8.1.3. Os procedimentos de *backup* iniciam automaticamente, conforme políticas previamente estabelecidas.

9) MONITORAR *BACKUP*

9.1. Acompanha a execução de todos os procedimentos de *backup* executados automaticamente.

9.2. Comunica prontamente falhas que interrompam a execução das rotinas de *backup* aos administradores responsáveis.

9.3. Em caso de falha na execução do *backup*, abre um registro de incidente no *software* HPSM (HP Service Manager).

9.4. Registra no portal:

<https://tjrj.sharepoint.com/sites/DGTEC->

[SEPRO/Biblioteca%20de%20Documentos/Forms/AllItems.aspx](https://tjrj.sharepoint.com/sites/DGTEC-SEPRO/Biblioteca%20de%20Documentos/Forms/AllItems.aspx) as informações referentes à execução dos procedimentos e conclusão dos *backups*, informando aos administradores responsáveis eventuais erros apresentados durante a execução.

10) EXECUTAR *RESTORE*

10.1. Executar *Restore* Automático:

10.1.1. Executa o programa *NETBACKUP*.

10.1.2. Informa o período desejado para recuperação dos dados e a respectiva política.

10.1.3. Após a localização das respectivas fitas pelo catálogo, inicia o procedimento de recuperação dos dados.

11) MONITORAR *RESTORE*

11.1. Acompanha a execução do procedimento de *restore* executado.

Base Normativa	Código:	Revisão:	Página:
Ato Executivo nº 2.950/2003	RAD-SGTEC-021	16	7 de 14

**ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE
CÓPIAS DE SEGURANÇA DE DADOS**

11.2. Comunica prontamente falhas que interrompam a execução do procedimento de *restore* aos administradores responsáveis.

11.3. Em caso de falha na execução do *backup* abre um registro de incidente no *software* HPSM (HP Service Manager).

11.4. Registra no portal:

[https://tjrj.sharepoint.com/sites/DGTEC-](https://tjrj.sharepoint.com/sites/DGTEC-SEPRO/SitePages/P%C3%A1gina%20Inicial.aspx)

[SEPRO/SitePages/P%C3%A1gina%20Inicial.aspx](https://tjrj.sharepoint.com/sites/DGTEC-SEPRO/SitePages/P%C3%A1gina%20Inicial.aspx) as informações referentes à execução dos procedimentos e conclusão dos *restores*, informando aos administradores responsáveis eventuais erros apresentados durante a execução.

12) INDICADORES

NOME	FÓRMULA	PERIODICIDADE
<u>Falhas em políticas de backup de bancos de dados</u>	<u>Número de falhas em políticas de backup em 30 dias</u>	<u>Mensal</u>
<u>Falhas em procedimentos de <i>restore</i> de banco de dados</u>	<u>Número de falhas em procedimentos de backup em 30 dias</u>	<u>Mensal</u>
<u>Backups não realizados</u>	<u>Número de backups não realizados no mês por causa de falha em política relacionada a ele</u>	<u>Mensal</u>

ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE CÓPIAS DE SEGURANÇA DE DADOS

13) GESTÃO DA INFORMAÇÃO DOCUMENTADA

13.1. As informações deste processo de trabalho são geridas pela UO e mantidas em seu arquivo corrente, de acordo com a tabela de gestão da informação documentada apresentada a seguir:

IDENTIFICAÇÃO	CÓDIGO CCD*	RESPONSÁVEL	ACESSO	ARMAZENAMENTO	RECUPERAÇÃO	PROTEÇÃO	RETENÇÃO (ARQUIVO CORRENTE - PRAZO DE GUARDA NA UO**)	DISPOSIÇÃO
Livro de Registro Diário Digitalizado	0-0-3 a	<u>SGTEC-DETEC</u>	Restrito	https://tjrj.sharepoint.com/sites/DGTEC-SEPRO/SitePages/Página%20Inicial.aspx	Data e Assunto	Condições apropriadas	2 anos	Eliminação na UO
Controle de descartes das fitas LTOs (FRM- <u>SGTEC-021-04</u>)	0-6-2-2 g	<u>SGTEC-DETEC</u>	Restrito	Pasta	Número do Volume	Condições apropriadas	1ano	Eliminação na UO

Legenda:

* CCD = Código de Classificação de Documentos.

** UO = Unidade Organizacional.

*** SGADM /DEGEA = Departamento de Gestão de Acervos Arquivísticos, da Secretaria-Geral de Administração.

Notas:

- a) Eliminação na UO - procedimento - Organizar os Arquivos Correntes das Unidades Organizacionais.
- b) SGADM /DEGEA – procedimentos – Arquivar e Desarquivar Documentos no DEGEA; Avaliar, Selecionar e Destinar os Documentos do Arquivo Intermediário e Gerir Arquivo Permanente.
- c) Os dados lançados no Sistema Corporativo são realizados por pessoas autorizadas e recuperados na UO. O armazenamento, a proteção e o descarte desses dados cabem à SGTEC, conforme RAD-SGTEC-021 – Elaborar e Manter Rotinas de Armazenamento de Segurança dos Bancos de Dados e Servidores de Aplicação.

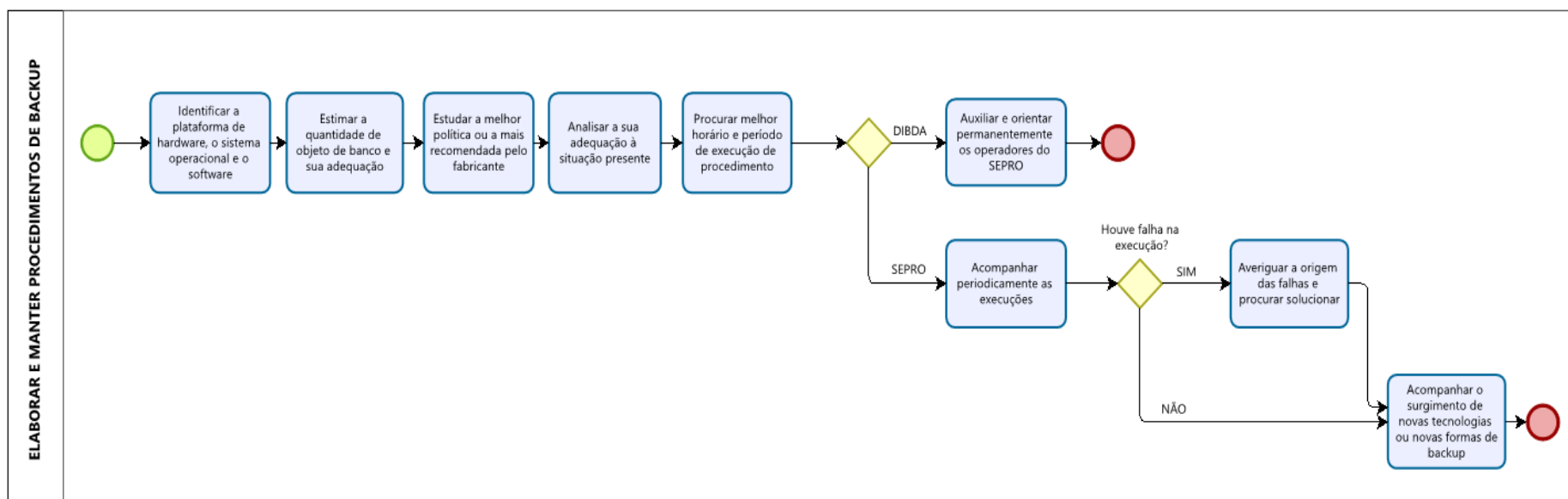
14) ANEXOS

- Anexo 1 – Fluxograma do processo de trabalho Elaborar e Manter Procedimentos de Backup;
- Anexo 2 – Fluxograma do processo de trabalho Executar Backup;
- Anexo 3 – Fluxograma do processo de trabalho Monitorar Backup;
- Anexo 4 - Fluxograma do processo de trabalho Executar *Restore*;
- Anexo 5 – Fluxograma do processo de trabalho Monitorar Restore.

Base Normativa Ato Executivo nº 2.950/2003	Código: RAD-SGTEC-021	Revisão: 16	Página: 9 de 14
--	---------------------------------	-----------------------	---------------------------

ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE CÓPIAS DE SEGURANÇA DE DADOS

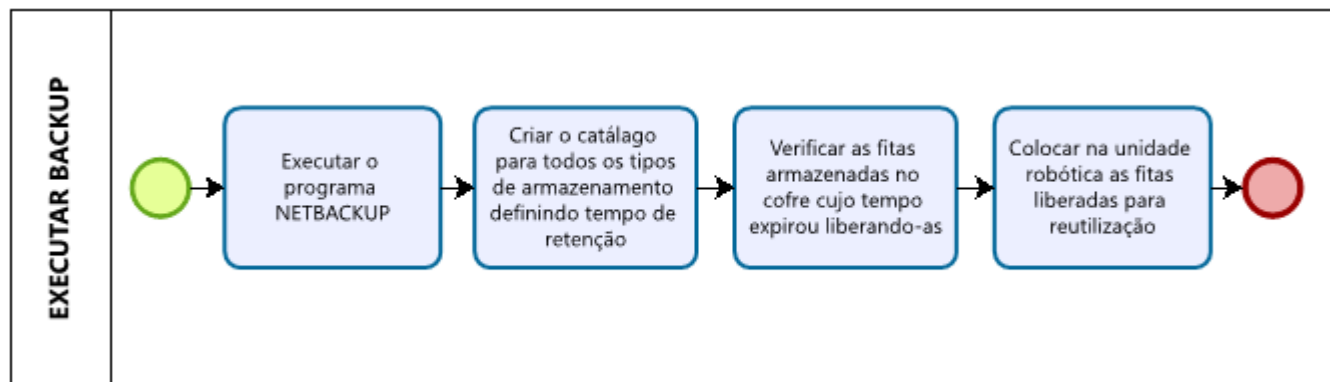
ANEXO 1 – FLUXOGRAMA DO PROCESSO DE TRABALHO ELABORAR E MANTER PROCEDIMENTOS DE *BACKUP*



Base Normativa	Código:	Revisão:	Página:
Ato Executivo nº 2.950/2003	RAD-SGTEC-021	16	10 de 14

ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE CÓPIAS DE SEGURANÇA DE DADOS

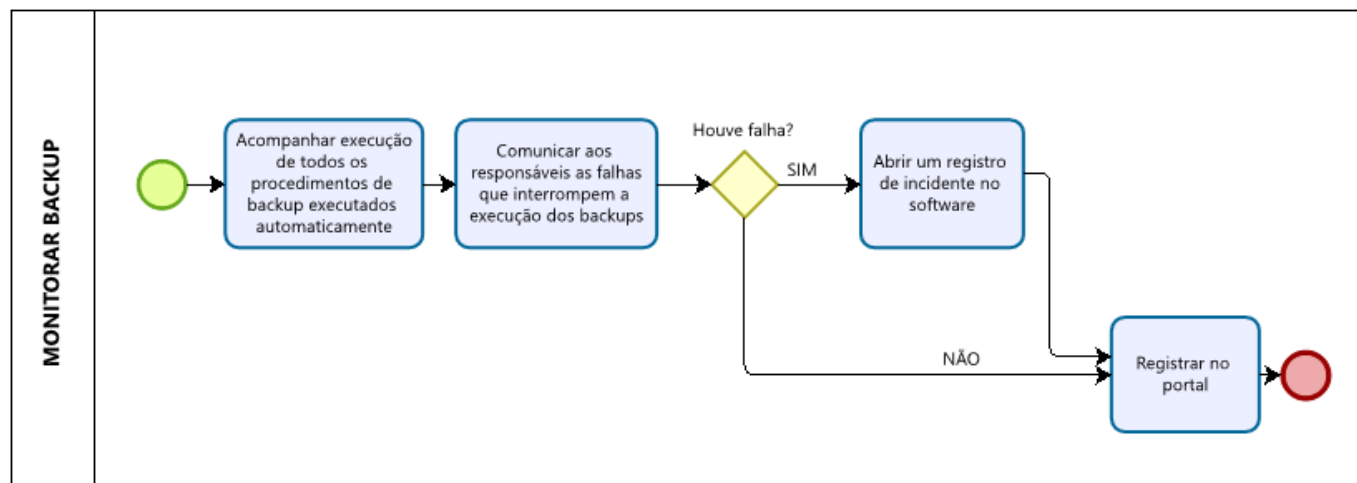
ANEXO 2 – FLUXOGRAMA DO PROCESSO DE TRABALHO EXECUTAR *BACKUP*



Base Normativa	Código:	Revisão:	Página:
Ato Executivo nº 2.950/2003	RAD-SGTEC-021	16	11 de 14

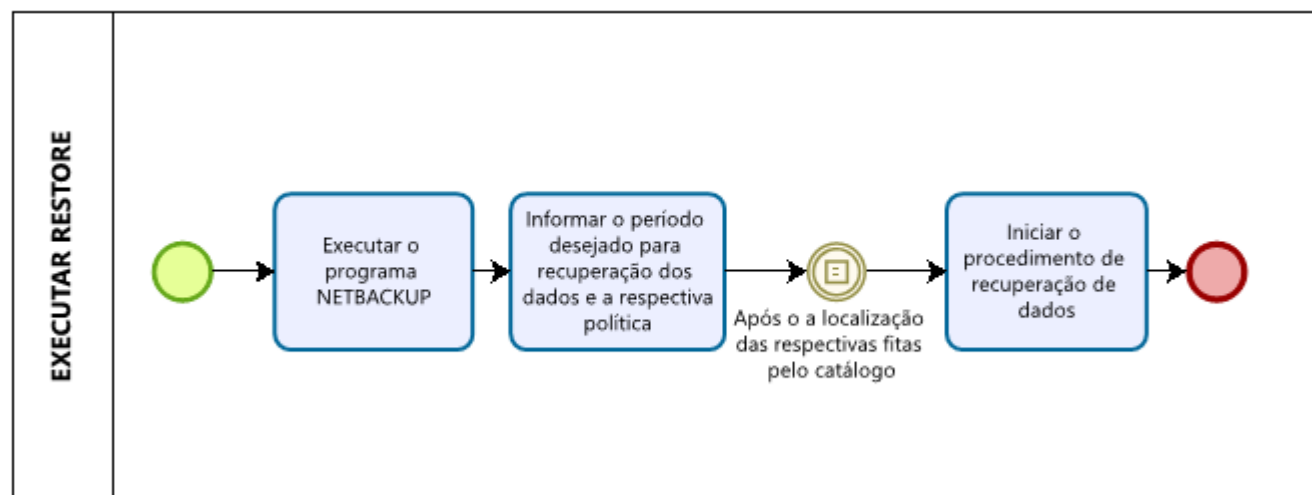
ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE CÓPIAS DE SEGURANÇA DE DADOS

ANEXO 3 – FLUXOGRAMA DO PROCESSO DE TRABALHO MONITORAR *BACKUP*



ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE CÓPIAS DE SEGURANÇA DE DADOS

ANEXO 4 – FLUXOGRAMA DO PROCESSO DE TRABALHO EXECUTAR A RESTORE



ELABORAR E MANTER ROTINAS DE ARMAZENAMENTO DE CÓPIAS DE SEGURANÇA DE DADOS

ANEXO 5 – FLUXOGRAMA DO PROCESSO DE TRABALHO MONITORAR A RESTORE

