



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 30/10/2025.

3) DEFINIÇÕES

TERMO	DEFINIÇÃO
<i>Backup</i>	Cópia de segurança de caráter preventivo, preferencialmente feita em meio de armazenamento externo, diverso do armazenamento original.
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.
APPLIANCE	Dispositivo de hardware dedicado para as tarefas de backup

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

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	<i>Hewlett-Packard Service Manager</i> - Software de gerenciamento de serviços de TI criado pela fabricante HP, 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 27002:2022 - Segurança da Informação, segurança cibernética e proteção à privacidade
- NBR ISO/IEC 27001/2022 - Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos
- Lei nº 13.709/18 - Lei Geral de Proteção de Dados Pessoais (LGPD)
- ATO NORMATIVO TJ nº 08/2019 - Estabelece as normas para Gestão de Segurança da Informação (GSI) do Poder Judiciário do Estado do Rio de Janeiro.
- Resolução TJ/OE nº 05/2019 - Institui a Política de Segurança da Informação do Poder Judiciário do Estado do Rio de Janeiro.

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

- Ato Normativo TJ nº 27/2020 – Estabelece as normas de gestão de acessos aos recursos computacionais do PJERJ.
- 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
Diretor do Departamento de Sustentação de Tecnologia da Informação e Comunicação de Dados da Secretaria-Geral de Tecnologia da Informação (SGTEC/DETIIC)	• Manter o ambiente computacional em situação satisfatória de desempenho e integridade; • manter os contratos de manutenção e suporte dos servidores.
Diretor da Divisão de Servidores da Secretaria-Geral de Tecnologia da Informação (SGTEC/DISER)	• Fornecer ao Serviço de <u>Datacenter e Backup</u> da Secretaria-Geral de Tecnologia da Informação (SGTEC/<u>SEDAT</u>) infraestrutura para o correto armazenamento das fitas de <i>backup</i>.
Diretor da Divisão de Banco de Dados ou chefia de serviço diretamente subordinado a essa Direção, da Secretaria-Geral de Tecnologia da Informação (SGTEC /DIBDA)	• 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 <u>SEDAT</u> 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
Chefe do Serviço de Datacenter e Backup da Secretaria-Geral de Tecnologia da Informação (SGTEC/ SEDAT)	• 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
Banco de Dados Oracle dos Sistemas Judiciais	Diário / Semanal	1 semana / 1ano	Destruição manual da fita conforme item 6.6
Banco de Dados Oracle dos Sistemas Administrativos	Diário / Semanal	1 semana / 1ano	Destruição manual da fita conforme item 6.6
Banco de dados Oracle da Consulta Processual	Diário / Semanal	1 semana / 1ano	Destruição manual da fita conforme item 6.6
Banco de dados Postgres do Portal Corporativo Liferay	Diário	1 semana	Destruição manual da fita conforme item 6.6
Banco de dados Caché de Sistemas da Corregedoria	Diário	1 semana	Destruição manual da fita conforme item 6.6

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

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

- 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.
- 6.6** **Dos registros das atividades de *backup*:**
- 6.6.1** **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.
- 6.7** **Do descarte das fitas magnéticas LTO:**
- 6.7.1** 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.
- 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 SEDAT quando do surgimento de dúvidas ou novos procedimentos de *backup*, bem como na

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

catalogação das fitas para facilitar a sua recuperação quando for necessário o *restore*.

- (SEDAT): 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.

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/:x:/r/sites/DGTEC-SEPRO/_layouts/15/Doc.aspx?sourcedoc=%7BAA5DDC40-29E0-4A09-9AAE-B4D46F09980B%7D&file=INCIDENTES%20DE%20BACKUP.xlsx&action=default&mobileredirect=true as informações de incidentes de backup, o status do incidente e procedimento de mitigação realizado.

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.

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/:x:/r/sites/DGTEC-SEPRO/_layouts/15/Doc.aspx?sourcedoc=%7B90738293-2D9C-47D3-8444-3FDFE83567ED%7D&file=Restaura%C3%A7%C3%A3o%20de%20backup%20-%202025.xlsx&action=default&mobileredirect=true as informações referentes à execução dos procedimentos e conclusão dos *restores*, informando aos administradores responsáveis eventuais erros apresentados durante a execução.

12) INDICADORES

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

NOME	FÓRMULA	PERIODICIDADE	META
<u>Percentual de backups concluídos com sucesso</u>	<u>(Qtde total de jobs de backup com sucesso / qtde total de jobs de backup)*100</u>	<u>Mensal</u>	<u>>= 95%</u>
<u>Percentual de backups não concluídos ou com falha.</u>	<u>(Qtde de backups não concluídos ou com falha / qtde total de jobs de backup)</u>	<u>Mensal</u>	<u>=< 5%</u>
<u>Percentual de backups de banco de dados concluídos com sucesso</u>	<u>(Qtde total de Jobs de backup de banco de dados com sucesso / qtde total de jobs de backup de banco de dados)*100</u>	<u>Mensal</u>	<u>>= 95%</u>
<u>Percentual de backups de banco de dados não concluídos ou com falha.</u>	<u>(Qtde de backups de banco de dados não concluídos ou com falha / qtde total de jobs de backup)</u>	<u>Mensal</u>	<u>=< 5%</u>

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*	RESPON-SÁVEL	ACESSO	ARMAZE-NAMENTO	RECUPE-RAÇÃO	PROTEÇÃO	RETENÇÃO (ARQUIVO CORRENTE - PRAZO DE GUARDA NA UO**)	DISPO-SIÇÃO
Livro de Registro Diário Digitalizado	0-0-3a	SGTEC/ DETIC	Restrito	https://tjri.sharepoint.com/sites/DGTEC-SEPRO/Registro%20do%20diretorio/Forms/AllItems.aspx	Data e Assunto	<u>Controle de Acesso por política de segurança no Active Directory</u>	1 ano	Eliminação na UO
Controle de descartes das fitas LTOs (FRM-SGTEC-021-04)	0-6-2-2g	SGTEC/ DETIC	Restrito	Pasta	Número do Volume	<u>Armazenamento em local com acesso controlado</u>	1ano	Eliminação na UO

Legenda:

*CCD = Código de Classificação de Documentos.

**UO = Unidade Organizacional.

***SGCON/DEGEA = Departamento de Gestão de Acervos Arquivísticos, da Secretaria-Geral de Gestão do Conhecimento.

Notas:

- Eliminação na UO - procedimento - Organizar os Arquivos Correntes das Unidades Organizacionais.
- SGCON/DEGEA – procedimentos – Arquivar, Desarquivar e Digitalizar Documentos no DEGEA; Avaliar, Selecionar e Destinar os Documentos do Arquivo Intermediário e Gerir Arquivo Permanente.
- 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 Cópias de Segurança de Dados.

Base Normativa Ato Executivo nº 2.950/2003	Código: RAD-SGTEC-021	Revisão: 17	Página: 8 de 14
--	---------------------------------	-----------------------	---------------------------

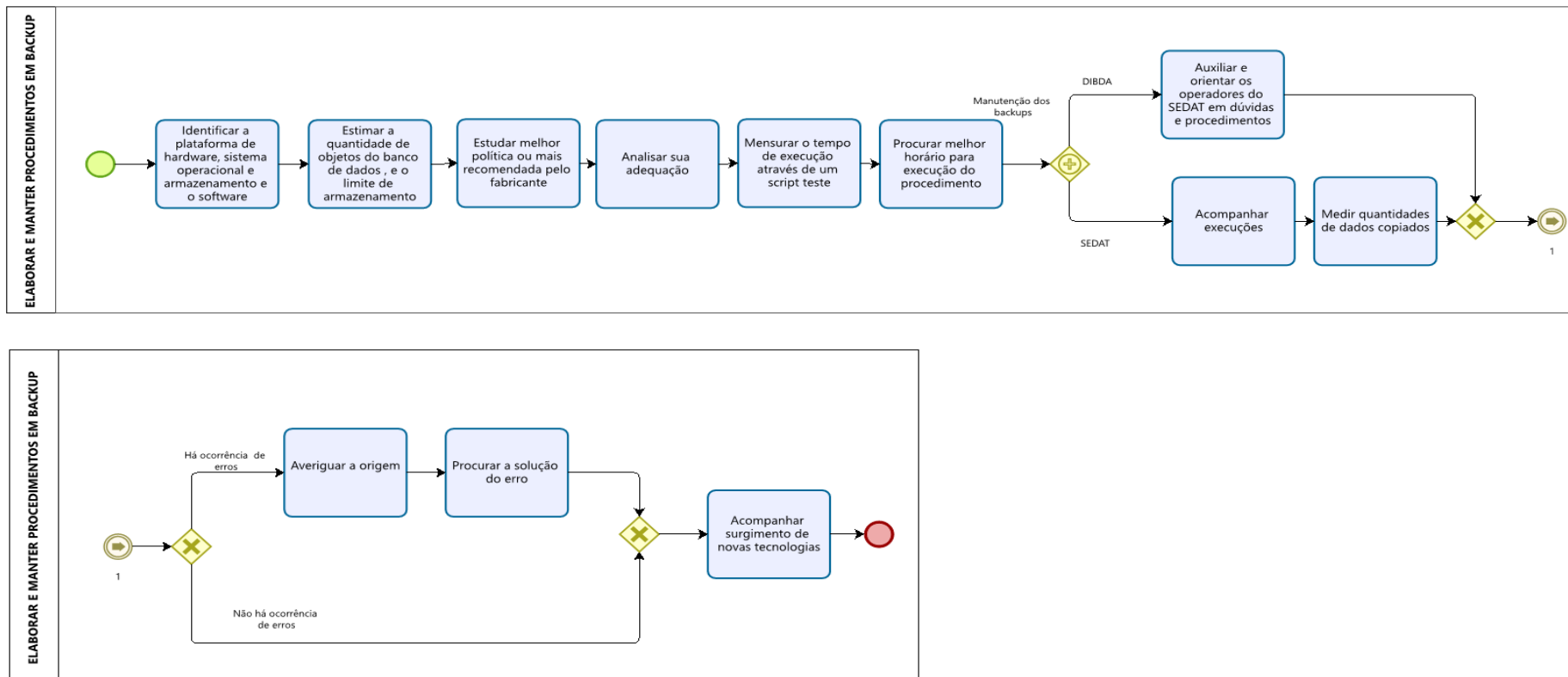
14) ANEXOS

- 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

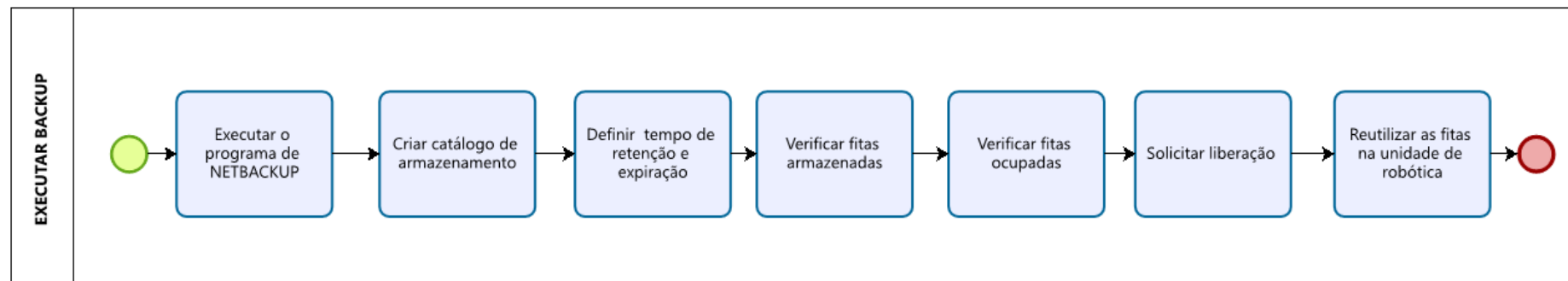
=====

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

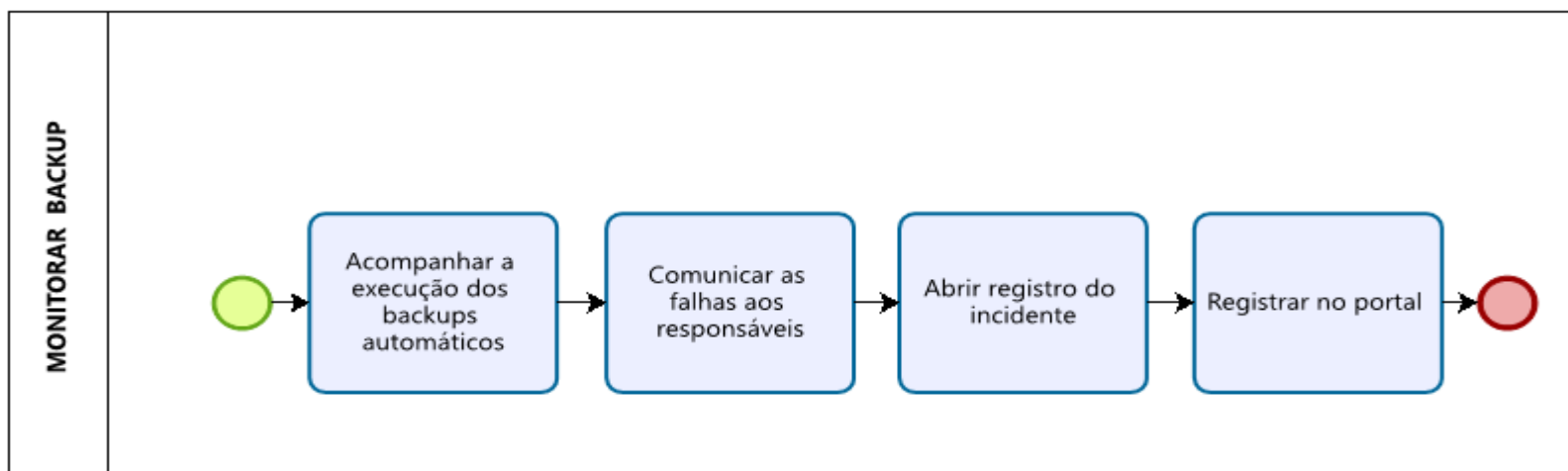
ANEXO 1 – FLUXOGRAMA DO PROCESSO DE TRABALHO - ELABORAR E MANTER PROCEDIMENTOS DE *BACKUP*



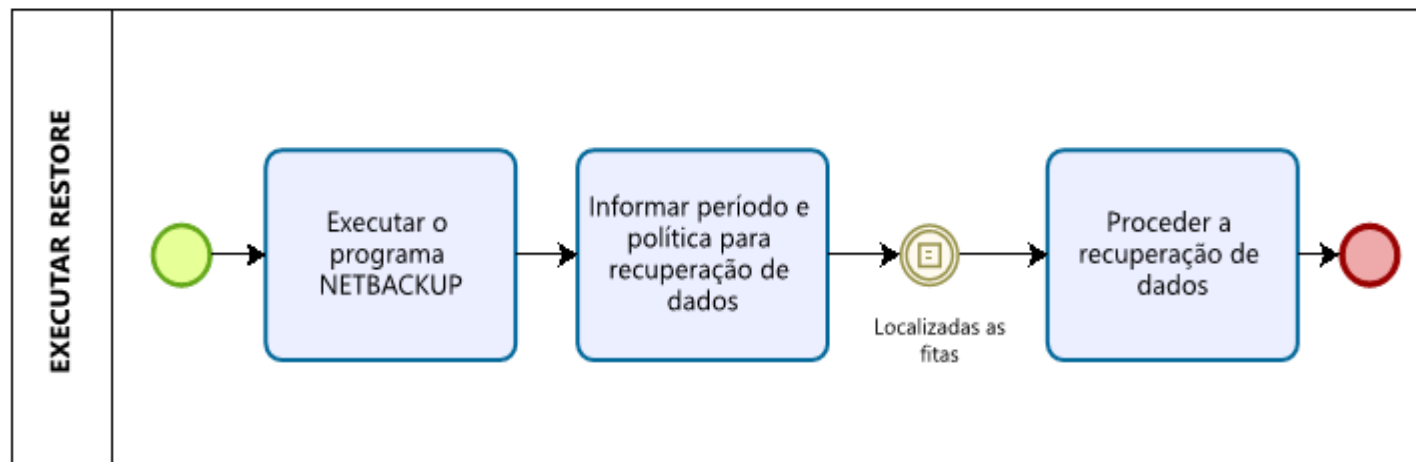
ANEXO 2 – FLUXOGRAMA DO PROCESSO DE TRABALHO - EXECUTAR *BACKUP*



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



ANEXO 4 – FLUXOGRAMA DO PROCESSO DE TRABALHO - EXECUTAR A RESTORE



ANEXO 5 – FLUXOGRAMA DO PROCESSO DE TRABALHO - MONITORAR O RESTORE

