



MAPEAMENTO DOS PROCESSOS DO RPPS:

TECNOLOGIA DA INFORMAÇÃO

1ª Edição

2022

**FUNDO MUNICIPAL DE PREVIDÊNCIA SOCIAL DOS
SERVIDORES DE SANTA HELENA DE GOIÁS
CNPJ: 15.282.487/0001-10**

Rua Eduvaldo Velos do Carmo, nº. 510 – Centro
75920-000 – Santa Helena de Goiás - Goiás
Fone: (64) 3641-8766
www.santahelanaprev.go.gov.br
grasiene@santahalaprev.go.gov.br
juvencio@santahelenaprev.go.gov.br
cleber@santahelenaprev.go.gov.br

SUMÁRIO

SUMÁRIO	3
APRESENTAÇÃO.....	6
CONCEITUALIZAÇÃO.....	7
METODOLOGIA.....	9
FUNDAMENTO LEGAL	10
RESOLUÇÕES	10
NORMAS MUNICIPAIS.....	10
ESTRUTURA ADMINISTRATIVA DO SANTAHELENAPREV	11
ESTRUTURA INTERNA.....	11
ESTRUTURA DE PRESTAÇÃO DE SERVIÇO	11
ORGANOGRAMA	12
1. DOS PROCESSOS DE TECNOLOGIA DA INFORMAÇÃO .13	
INTRODUÇÃO	14
2. CONCEITUAÇÃO E IMPORTÂNCIA.....15	
2.1 O QUE É TECNOLOGIA DA INFORMAÇÃO?	15
2.2 POR QUE USAR A TECNOLOGIA DA INFORMAÇÃO?	15
2.3 OBJETIVO DO MAPEAMENTO DA TECNOLOGIA DA INFORMAÇÃO DENTRO DO SANTAHELENAPREV	16
2.4 FUNCIONAMENTO DA TECNOLOGIA DA INFORMAÇÃO DO SANTAHELENAPREV	16
2.5 ÁREAS OBJETO DE MAPEAMENTO	17

3.	CONTROLE DE ACESSO FÍSICO.....	18
	POLÍTICAS DE CONTROLE DE ACESSO E UTILIZAÇÃO.....	19
4.	CONTROLE DE ACESSO LÓGICO.....	21
	POLÍTICAS DE CONTROLE DE ACESSO LÓGICO E UTILIZAÇÃO.....	22
5.	BACKUPS E PROCEDIMENTO DE CONTINGÊNCIA	25
	CÓPIAS DE SEGURANÇA DOS SISTEMAS INFORMATIZADOS E DOS BANCOS DE DADOS.....	26
6.	DAS FASES PROCESSUAIS	29
6.1	<i>FASES PROCESSUAIS DO CONTROLE DE ACESSO FÍSICO..</i>	<i>30</i>
6.2	<i>FASES PROCESSUAIS DO CONTROLE DE ACESSO LÓGICO</i>	<i>31</i>
6.3	<i>CÓPIAS DE SEGURANÇA DOS BANCOS DE DADOS</i>	<i>32</i>
6.4	<i>CÓPIAS DE SEGURANÇA DOS SISTEMAS INFORMATIZADOS</i>	
	33	

Fundo Municipal de Previdência Social – FEPS de Santa Helena de Goiás

DIRETORIA DO SANTAHELENAPREV

Grasiene Teobalda de Oliveira
Gestora

Juvêncio Vieira de Sousa Neto
Diretor Financeiro

Cleber Gomes da Silva
Direto de Benefícios

CONSELHO ADMINISTRATIVO/FISCAL

Simone Maria Dantas
Presidente do CMP

Ana Carolina Dantas Medeiros Cruz
Membro

Taianne Clemente de Araújo Nogueira
Membro

Celi Mara de Souza
Membro

Luiza Carla Ferreira
Membro

APRESENTAÇÃO

Este mapeamento tem como principal objetivo orientar e informar os conceitos essenciais sobre a metodologia dos Processos de Tecnologia da Informação do Fundo Municipal de Previdência Social dos Servidores de Santa Helena de Goiás - SANTAHELANAPREV, auxiliando na implantação e melhoramento da gestão dos processos, através da disseminação do conhecimento em Mapeamento de Processos da área, inclusive com o detalhamento das etapas e representação dos fluxos operacionais.

CONCEITUALIZAÇÃO

PROCESSO

Trata-se de um conjunto de atividades correlacionadas, desenvolvidas com o objetivo de gerar resultados (claramente definidos) à organização, com início e fim determinados. Envolvem um ordenamento lógico e, normalmente, são atividades de rotina (cotidianas), utilizadas para transformar entradas (insumos, ou “inputs”) em saídas (resultados, ou “outputs”), buscando o alcance de uma meta ou objetivo. De forma simplificada, o processo é a sequência de passos utilizados para a realização das rotinas da organização: Processos-Chave/Macroprocessos, Processos Estruturantes, E Processos de Apoio.

MANUAL

É todo e qualquer conjunto de normas, procedimentos, funções, atividades, políticas, objetivos, instruções e orientações que devem ser obedecidas e cumpridas pelos servidores da instituição, bem como a forma como estas serão executadas, quer seja individualmente, ou em conjunto.

MANUALIZAÇÃO

A ação ou resultado de reunir didaticamente, em um manual, orientações sobre os procedimentos adequados ao desenvolvimento de um processo.

MAPEAMENTO

Muitos dos processos organizacionais, principalmente na área pública, não estão definidos e padronizados, pois as normativas que os regulam apresentam as regras gerais e necessárias, mas não o passo a passo e suas variações. Assim, os processos tendem a ser executados de forma diferente a depender da gestão atuante, ou até mesmo, dentro da mesma gestão. O mapeamento de processo surge como ferramenta capaz de solucionar essa questão, pois apresenta de forma gráfica e sequencial as atividades do processo, inclusive observações e arquivos relacionados. Com o intuito de atingir o objetivo supracitado.

METODOLOGIA

O MAPEAMENTO dos processos do SANTAHELENAPREV tem como objetivo elaborar um fluxograma eficiente, iremos adotar no que couber o BPMN (Business Process Modeling Notation) que é uma notação que permite representar todas as atividades internas de um processo. A notação é formada por um conjunto de imagens que são dispostas na forma de diagrama para representar os processos, e dessa forma, demonstrar o seu real funcionamento. Os elementos da notação estão divididos em três: eventos, atividades e decisões. Apesar da notação BPMN possuir seus conceitos e definições, o SANTAHELENAPREV também adotará notações específicas.

FUNDAMENTO LEGAL

Lei nº 13.709 de 14 de Agosto de 2018.

RESOLUÇÕES

Resolução nº 17/2019 – Conselho de Previdência.

NORMAS MUNICIPAIS

Lei Municipal 2.605 de 21 de dezembro de 2011 e posteriores alterações.

Lei Municipal 2.744 de 16 de outubro de 2014

Lei Municipal nº 3.063, de 12 de maio de 2020.

ESTRUTURA ADMINISTRATIVA DO SANTAHELENAPREV

ESTRUTURA INTERNA

A organização do SANTAHELENAPREV, de acordo com a Lei Complementar Municipal Nº 2605/2011 e suas alterações, é a seguinte:

I – 01 (um) cargo de provimento em comissão de Gestor de Previdência;

II – 01 (um) cargo de provimento em comissão de Diretor Financeiro;

III – 01 (um) cargo de provimento em comissão de Diretor de Benefícios.

ESTRUTURA DE PRESTAÇÃO DE SERVIÇO

Assessoria Contábil;

Assessoria Jurídica;

Assessoria de Compensação Previdenciária;

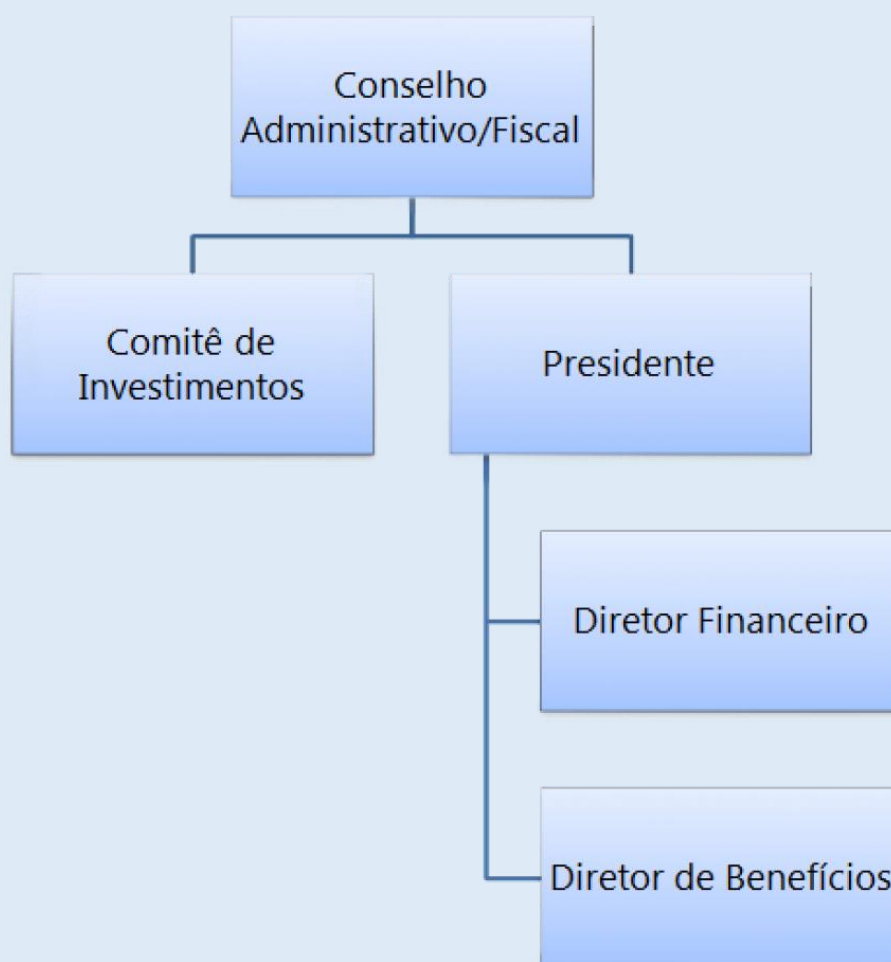
Assessoria de Investimentos;

Consultoria Previdenciária;

Junta Médica;

Assessoria/Consultoria Atuarial.

ORGANOGRAMA



1. DOS PROCESSOS DE TECNOLOGIA DA INFORMAÇÃO

INTRODUÇÃO

O termo Informática passou nos últimos anos a ser substituído pela expressão Tecnologia da Informação (TI), que designa o conjunto de recursos tecnológicos e computacionais para a geração e uso da informação, abrangendo as redes de computadores, centrais telefônicas inteligentes, fibra ótica e comunicação por satélite.

Vários especialistas das mais diversas áreas têm afirmado que as organizações bem-sucedidas no século XXI serão aquelas centradas no conhecimento, intenso fluxo de informações e pessoas treinadas participando de decisões.

A questão da Tecnologia da Informação no Setor Público ainda é um desafio, pois extremamente complicado mudar a estrutura, a cultura, os processos e os hábitos dos servidores públicos, muito habituados a procedimentos retrógrados.

Mas, entender o uso e os impactos que a tecnologia da informação passou a ser essencial, para o desenvolvimento de qualquer setor.

E no setor público não é diferente, pois necessita criar meios para atender de forma efetiva o usuário, criar forma de continuidade da gestão, eis que há uma sazonalidade na prestação de serviço, ante a mudança contínua de gestão, além de ter várias informações privadas e confidenciais que precisam estar cobertas pela segurança da informação.

Com a mencionada sazonalidade, a criação de processos de contingência e administração de dados passou a ser extremamente necessária.

2. CONCEITUAÇÃO E IMPORTÂNCIA

2.1 O QUE É TECNOLOGIA DA INFORMAÇÃO?

O termo "Tecnologia da Informação" serve para designar o conjunto de recursos tecnológicos e computacionais para a geração da informação. A TI está fundamentada nos seguintes componentes:

- hardware e seus dispositivos e periféricos;
- software e seus recursos;
- sistemas de telecomunicações;
- gestão de dados e informações.

2.2 POR QUE USAR A TECNOLOGIA DA INFORMAÇÃO?

Algumas das razões que levaram disseminação do uso da TI:

- única maneira de fazer determinado trabalho;
- melhorar processos internos;
- aplicar controles melhores;
- reduzir custos;
- melhorar a qualidade e disponibilidade das informações importantes interna e externamente organização;
- agregar valor aos serviços e produtos ofertados por uma organização.

Mas, o principal benefício que a tecnologia da informação traz para as organizações é a sua capacidade de melhorar a qualidade e a disponibilidade de informações aos usuários.

2.3 OBJETIVO DO MAPEAMENTO DA TECNOLOGIA DA INFORMAÇÃO DENTRO DO SANTAHELENAPREV

Dentro do SANTAHELENAPREV o objetivo de realizar o mapeamento da área de Tecnologia de Informação está amplamente ligada a continuidade das informações dentro do departamento. Pois, com o mapeamento há uma sedimentação de todas as questões de Informática ligadas as atividades do Instituto, assim como de procedimentos que devem ser adotados, para guarda e proteção de dados.

2.4 FUNCIONAMENTO DA TECNOLOGIA DA INFORMAÇÃO DO SANTAHELENAPREV

Dentro de uma organização, a unidade, departamento ou setor de Tecnologia da Informação responsável por todas as suas funções de informática.

O Instituto de Previdência não tem um departamento de TI em seu quadro de pessoal, devida ao seu porte ainda pequeno. Por essa razão, faz-se a terceirização de suporte, sistemas e guarda de arquivos digitais.

Com relação ao suporte, parte é solicitada ao TI da Prefeitura Municipal, porque é essa que detém o controle das redes de internet. Já o suporte técnico de manutenção de hardware, é feito por meio de contratações específicas e pontuais de empresas locais. E os softwares são locados, por meio de licitação.

Hoje o RPPS tem contratação de software de folha de pagamento, gestão previdenciária, site e guarda de dados.

As empresas contratadas se submetem, via Termo, às questões estabelecidas em Política de Segurança da Informação do Instituto.

2.5 ÁREAS OBJETO DE MAPEAMENTO

Como já mencionado o SANTAHELENAPREV é uma autarquia municipal ainda pequena, com pouca diversidade de colaboradores.

Pautados nisso, pressupõe-se que ainda não há necessidade de mapeamento de todas as áreas de tecnologia de informação. Então será realizado mapeamento das seguintes áreas:

3. CONTROLE DE ACESSO FÍSICO

Por óbvio que em qualquer empresa pública ou privada há o acesso físico aos sistemas que contém os dados cotidianos.

Em 2018 foi publicada a Lei de Segurança da Informação, para regulamentar a proteção de dados pessoais, inclusive digitais, abarcando pessoa natural e jurídica, pública ou privada, para garantir direitos fundamentais de liberdade e privacidade.

Para atender os critérios legais da Lei mencionada, o Instituto criou Política de Segurança da Informação aplicada a todos os servidores públicos, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento do Instituto.

Então, a partir da criação da Política de Segurança da Informação, qualquer usuário dos equipamentos informatizados do Instituto de Previdência, devem, preteritamente, tomar conhecimento e ciência do conteúdo regulamentado.

Na referida política foi realizada a conceituação de todas as formas de acesso à informação: pública, interna, confidencial e restrita.

Além de estabelecer critérios para treinamento do servidor admitido, acesso a logins e senhas, propriedade intelectual e uso de ambiente de Web.

As etapas do processo de controle de acesso lógico seguirão conforme demonstrado no fluxograma do módulo 5 – Etapas Processuais, conforme descrito:

1. Usuário necessita de acesso aos dados ou softwares do RPPS;

2. Toma conhecimento da Política de Segurança da Informação;
3. Solicita acesso ao Gestor do RPPS;
4. Gestor analisa a solicitação;
5. Caso autorizado, gestor oficializa empresa contratada responsável pela guarda do banco de dados (físico) autorizando e discriminando os níveis de acesso, conforme Política da Segurança da Informação;
6. Acesso é concedido;

POLÍTICAS DE CONTROLE DE ACESSO E UTILIZAÇÃO

O Controle de Acesso Físico aos bancos de dados do RPPS se dará da seguinte forma:

- a) O Acesso aos ambientes considerados neste item será controlado via leitores de crachás (limitado ao sistema de crachás ou similar) ou livro de registros, crachás autorizados, trancas e chaves.
- b) Todos os sistemas que possuem acesso através de "console local" serão "trancados" para prevenir o uso não autorizado;
- c) Câmeras de vídeo acompanharão pontos de entrada e saída dos centros de dados, estas câmeras devem estar localizadas no interior do centro de dados, ou protegidas contra ataque ou desativação;
- d) As câmeras devem ser monitoradas. Seus dados serão armazenados por pelo menos seis meses;
- e) Pontos de rede devem ter acesso restrito e DHCP desabilitado. Visitantes que adentrarem locais onde existam pontos de rede deverão ser constantemente acompanhados;
- f) O acesso a dispositivos portáteis será restrito aos administradores responsáveis.
- g) Devem existir procedimentos que auxiliem os funcionários a distinguir entre funcionários e visitantes (exemplo: crachás).

h) Os IDs utilizados devem distinguir nitidamente funcionários de visitantes.

i) Visitantes precisam de autorização e acompanhamento para adentrar áreas críticas. Devem utilizar crachás que possuam ID. Tais crachás não irão permitir o acesso desacompanhado às áreas físicas que armazenam dados críticos.

j) Crachás de visitantes devem possuir data / horário de vencimento, e devem ser solicitados na data de vencimento ou no horário de saída.

k) Crachás vencidos de visitantes e crachás de funcionários demitidos serão prontamente cancelados.

l) Serão utilizados registros para visitantes que adentrem as instalações referenciadas neste item, para fins de auditoria. Os mesmos irão conter horários e datas de entrada e saída, nome da empresa representada, nome do funcionário interno responsável por autorizar o acesso físico.

m) Os registros serão mantidos por um prazo mínimo de cinco anos, a não ser que seja proibido por lei.

4. CONTROLE DE ACESSO LÓGICO

O controle de acesso lógico a dados ou qualquer tipo de informação do Instituto está previsto na Política de Segurança da Informação, que estabelece critérios para acesso aos sistemas para servidores internos e prestadores de serviços, acesso ao ambiente web e propriedade intelectual.

Para garantir a segurança da informação, as empresas de softwares, contratadas pelo Instituto, apenas devem fornecer acesso às bases de dados lógicas do RPPS à servidores com autorização expressa do Gestor(a). Sendo necessário que seja oficiado às empresas, pelo(a) mesmo(a), qual o usuário terá acesso ao respectivo software, e quais as permissões atribuídas a este. Bem como o período de acesso.

As etapas do processo de controle de acesso lógico seguirão conforme demonstrado no fluxograma do módulo 5 – Etapas Processuais, conforme descrito:

1. Usuário necessita de acesso aos dados ou softwares do RPPS;
2. Toma conhecimento da Política de Segurança da Informação;
3. Solicita acesso ao Gestor do RPPS;
4. Gestor analisa a solicitação;
5. Caso autorizado, gestor oficia empresa contratada responsável pela guarda do banco de dados (lógico) autorizando e discriminando os níveis de acesso, conforme Política da Segurança da Informação;
6. Acesso é concedido;

POLÍTICAS DE CONTROLE DE ACESSO LÓGICO E UTILIZAÇÃO

O Controle de Acesso lógico ao banco de dados do RPPS se dará da seguinte forma:

a) O acesso aos recursos computacionais e a informações críticas será controlado automaticamente por software administrado e gerenciado pela equipe de segurança da Empresa de Tecnologia da Informação responsável pela guarda de dados contratada. Serão realizados procedimentos operacionais diários para a manutenção das contas de usuário.

b) Todo o controle de adição, exclusão e modificação de usuários, será efetuado com registro sistêmico e autorizado pela equipe de segurança da informação empresa contratada.

c) Cada funcionário irá possuir um ID / "nome de usuário" (único) e uma senha. A partir destes, terá acesso a componentes do sistema e informação limitada, de acordo com a necessidade da função exercida no ambiente empresa contratada.

d) Deverá ser utilizado um formulário de autorização assinado pelos administradores, especificando e detalhando privilégios quaisquer solicitados.

e) O controle de acesso para recursos locais utiliza uma política padrão para "negar tudo", logo, qualquer acesso a qualquer recurso computacional deverá ser estabelecido de acordo com a necessidade de cada usuário para o funcionamento do negócio e desempenho da função dentro do mesmo.

f) Todos os usuários serão autenticados através de uma senha (além de um ID de usuário) para acesso aos recursos computacionais e sistemas.

g) Todo e qualquer acesso remoto aos sistemas e servidores empresa contratada, se dará através do uso de um "nome de usuário" e senha únicos. Além disso, todos os acessos devem se dar somente via canais criptografados (VPN 128bits) ou através do uso de tokens / VPN.

- h) Cada ID de usuário e seus privilégios específicos deverão constar em um “formulário de autorização” juntamente à respectiva assinatura e documentação.
- i) Quaisquer alterações de senha serão precedidas pela identificação do usuário.
- j) Todas as senhas serão criadas com um valor único por usuário para todos os usuários. As mesmas deverão ser alteradas imediatamente após o primeiro uso.
- k) Funcionários demitidos serão imediatamente removidos do sistema.
- l) Usuários inativos por mais de sessenta dias terão suas contas removidas do sistema, exceto quando com justificativa homologada pelo Departamento de RH do ORT.
- m) Contas para prestadores de serviço, utilizadas para suporte e manutenção remota, serão habilitadas apenas durante o tempo necessário. Estes procedimentos serão acompanhados por funcionários da equipe de segurança da informação empresa contratada.
- n) Usuários que possuam acesso a informações críticas deverão estar cientes dos procedimentos relativos às senhas e seus respectivos regulamentos.
- o) Quaisquer contas e IDs genéricos serão removidos. Não serão permitidos IDs compartilhados para processos que envolvam administração do sistema, processos críticos, ou ainda acesso à informação crítica.
- p) Uma conta de usuário será automaticamente bloqueada após três tentativas falhas de “logon” no sistema. Este bloqueio deverá durar trinta minutos, ou até que o usuário seja habilitado pelo administrador responsável.
- q) O sistema possuirá um “time-out” (tempo limite) de quinze minutos, ou seja, usuários inativos por mais de quinze minutos deverão realizar um novo “logon” no sistema.
- r) Serão autenticados todos os acessos a servidores críticos (ex.: banco de dados), para administradores e aplicativos. Será permitido um

número limitado de contas individuais de “login” a estes servidores, limitadas aos administradores responsáveis.

s) Não serão permitidas consultas diretas “SQL” a quaisquer bancos de dados.

5. BACKUPS E PROCEDIMENTO DE CONTINGÊNCIA

Na Administração Pública é recente a preocupação com a gestão dos documentos arquivísticos. Mas, com avanço do uso dos meios digitais nas repartições públicas, o papel está perdendo espaço. Sobretudo pela praticidade e economicidade de espaço físico, já que um arquivo físico demanda um investimento com armazenamento, acondicionamento e condições ambientais adequadas.

Mas, é cediço que a guarda de documentos deve ser prioridade em qualquer organização tanto pública como privada, pois é a forma que elas possuem para comprovar o cumprimento de uma obrigação e prestação de contas.

Assim, independentemente de o arquivo ser em papel ou digital, os documentos precisam ser guardados e, principalmente, conservados. No RPPS não é diferente.

Devido ao crescimento da produção dos documentos digitais há de se ressaltar a preocupação com o acesso dos documentos digitais ao longo do tempo, a fim de garantir sua autenticidade e legalidade.

Com o surgimento da Lei nº 12.527, de 2011, a Lei de Acesso à Informação, houve a regulamentação do direito constitucional de acesso às informações públicas e o dever de ofício da Administração Pública de promover a transparência de seus atos para a sociedade.

Assim, a importância de organizar, divulgar e de preservar as informações arquivísticas ganhou uma grande relevância e a implementação de um sistema informatizado – SIGAD – passou a ser fundamental para gerir corretamente a informação arquivística.

Dentro do Instituto ainda há alguns documentos que são arquivados fisicamente, principalmente porque ainda não há a possibilidade de guarda exclusivamente digital, que deveria ser autorizada por Lei, para alguns tipos de documentos. Mas, como diversos dados estão sedimentados em sistemas operacionais, há previsão de guarda e sigilo de dados nos contratos.

Além de ter sido efetivado contrato com empresa de Tecnologia da Informação para realização de backups diários, com os seguintes objetos:

1. Serviço de instalação e configuração de espaço de 2TB(Terabytes) de armazenamento em nuvem própria;
2. Sincronismo automatizado com a Nuvem Privada;
3. Manutenção corretiva de sistemas;
4. Atendimento e Suporte aos Usuários de Sistemas e Web;
5. Serviços de Suporte Especializado em banco de dados Postgresql 9.6 ou superior;
6. Backup diário, com retenção de arquivos em até 5 anos;
7. Backup Diário completo do banco de dados, podendo ser restaurado todo o servidor virtual ou arquivos, desde que o ponto de recuperação não tenha sido sobrescrito.
8. Suporte Local nas unidades organizacionais;
9. Todos os requisitos precisam garantir confidencialidade, integridade, disponibilidade e autenticidade, suporte e atualizações dos Sistemas da Santa Helena Prev.

CÓPIAS DE SEGURANÇA DOS SISTEMAS INFORMATIZADOS E DOS BANCOS DE DADOS

Com o conhecimento da importância da guarda e preservação dos dados do RPPS, serão realizadas cópias de segurança dos sistemas informatizados e dos bancos de dados do RPPS, das seguintes formas:

Backup completo: é uma operação básica e completa de backup que faz uma cópia de todos os seus dados para outra mídia, como um disco, uma

fita ou um CD. Assim, uma cópia completa de todos os seus dados é disponibilizada em um único conjunto de mídia. Esse tipo de backup leva mais tempo e requer muito espaço de armazenamento; por isso, normalmente é usado em combinação com um backup diferencial ou incremental.

Backup incremental: essa operação copia somente os dados que foram modificados desde a última operação de backup. Os aplicativos de backup registram e rastreiam a data e a hora em que todas as operações de backup ocorrem. Esta operação é mais rápida e requer menos mídia de armazenamento do que uma solução completa de backup.

Backup diferencial: Similar ao tipo incremental, os backups diferenciais copiarão todos os dados alterados de um episódio anterior, mas toda vez que forem executados, continuarão a copiar todos os dados alterados desde o backup completo declarado anteriormente.

Fase Inicial - Automação de Backups

Horário Backup Sistema/Arquivos

1. Backup Automatizado Diferencial a cada 5 minutos;

- Contingência em Nuvem Privada e ambiente distinto;
- Retenção dos Arquivos está para 5 anos;

2. Backup Automatizado Full diário às 22:00

- Contingência em Nuvem Privada e ambiente distinto;
- Retenção dos Arquivos está para 5 anos;

Horário Backup Banco de Dados

1. Backup Incremental as 12:00 / 19:00;
 2. Backup Full Diário às 23:00;
- Retenção dos Arquivos está para 5 anos;

Recebimento de conclusão com sucesso e com falha enviado para e-mail de pessoas autorizadas;

Fase 2 - Notificar e registrar

Em caso de falha abertura automática do chamado para resolução da equipe de Suporte Técnico;

Fase 3 - Correção Falha

A fase de recuperação se inicia quando a fase de resposta foi concluída. Nesta fase, a Equipe de Respostas a Incidentes recupera a operação normal dos sistemas de backups. Esta providência pode requerer a recuperação de dados advindos de backups previamente realizados.

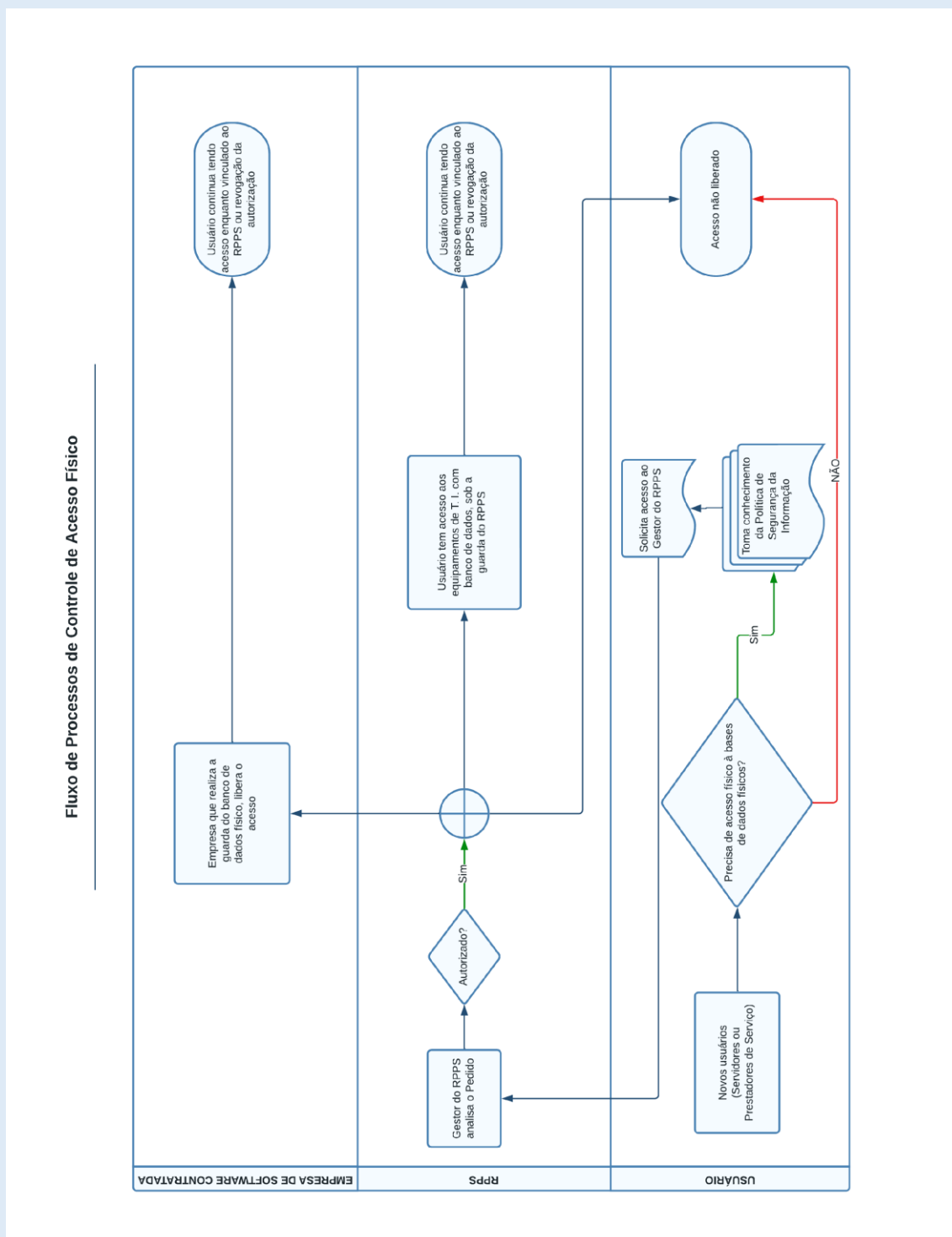
Uma vez normalizado o procedimento de backup afetado, estes são testados para se certificar de que não mais estão vulneráveis afim de garantir que funcionarão corretamente quando recolocados em produção.

Fase 4 - Registro da resolução

Após a resolução é registrado no chamado o motivo e o método usado para normalizar os backups e suas configurações.

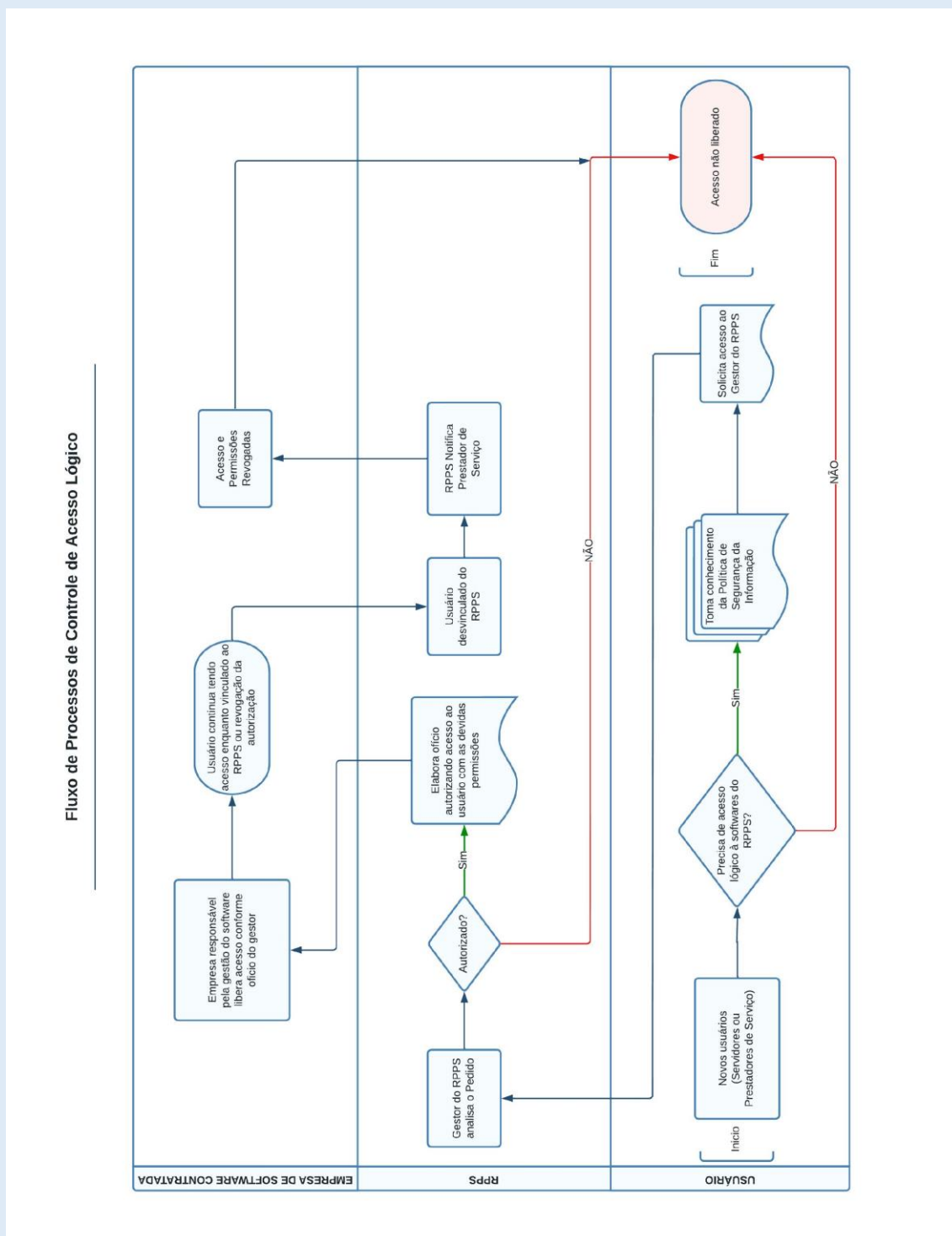
6. DAS FASES PROCESSUAIS

6.1 FASES PROCESSUAIS DO CONTROLE DE ACESSO FÍSICO



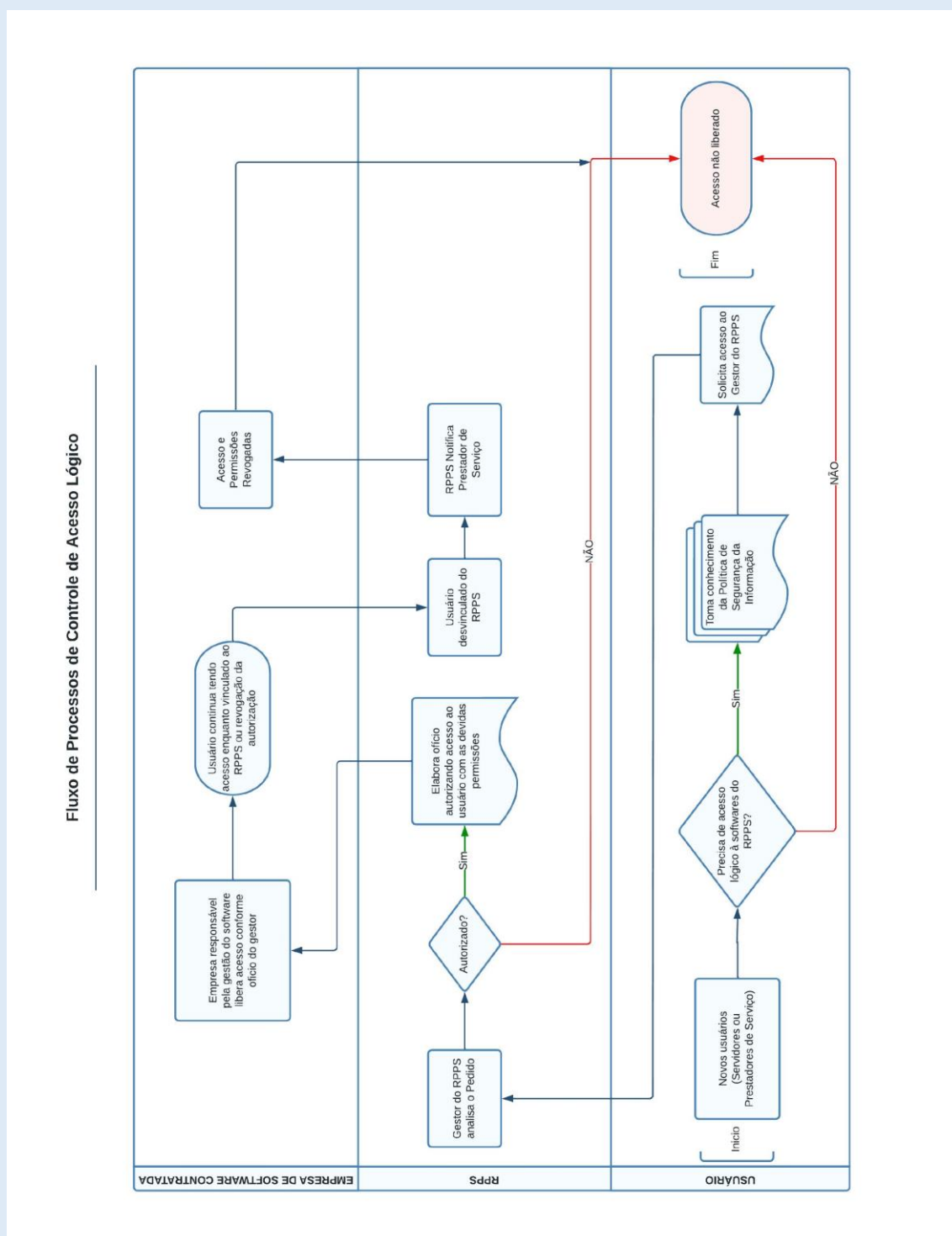
Fluxograma 1 - Fluxo de Processos de Controle de Acesso Físico

6.2 FASES PROCESSUAIS DO CONTROLE DE ACESSO LÓGICO



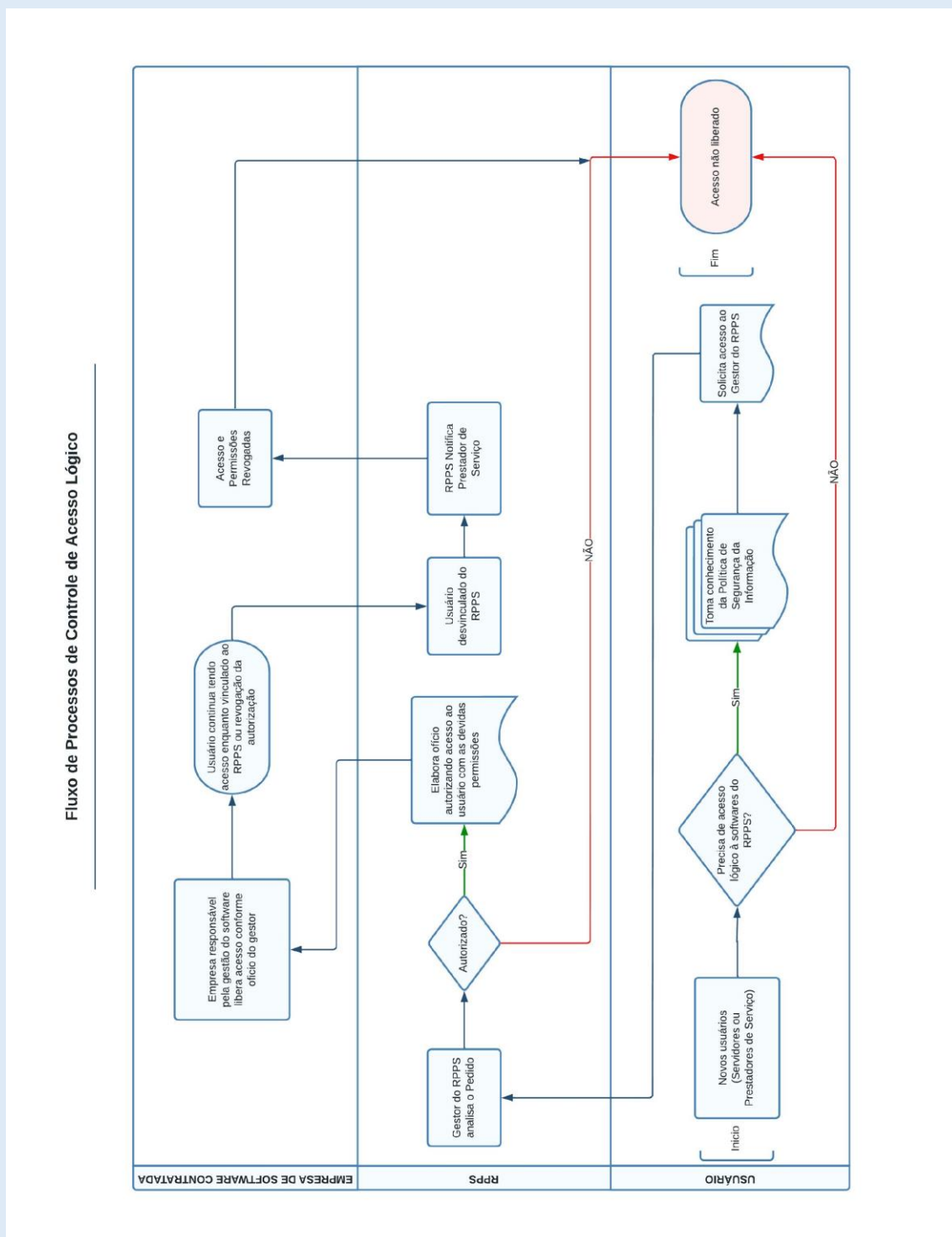
Fluxograma 2 - Fluxo de Processos de Controle de Acesso Lógico

6.3 CÓPIAS DE SEGURANÇA DOS BANCOS DE DADOS



Fluxograma 3 - Fluxo de Processos de Cópias de Seguranças dos Bancos de Dados

6.4 CÓPIAS DE SEGURANÇA DOS SISTEMAS INFORMATIZADOS



Fluxograma 4 - Fluxo de Processos de Cópias de Segurança dos Sistemas Informatizados