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

SANTA HELENA PREV

SUMÁRIO

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

DIRETORIA DO SANTAHELENAPREV

Grasiene Teobalda de Olvieira
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 especificas.

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 SANTAHELANAPREV, 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;

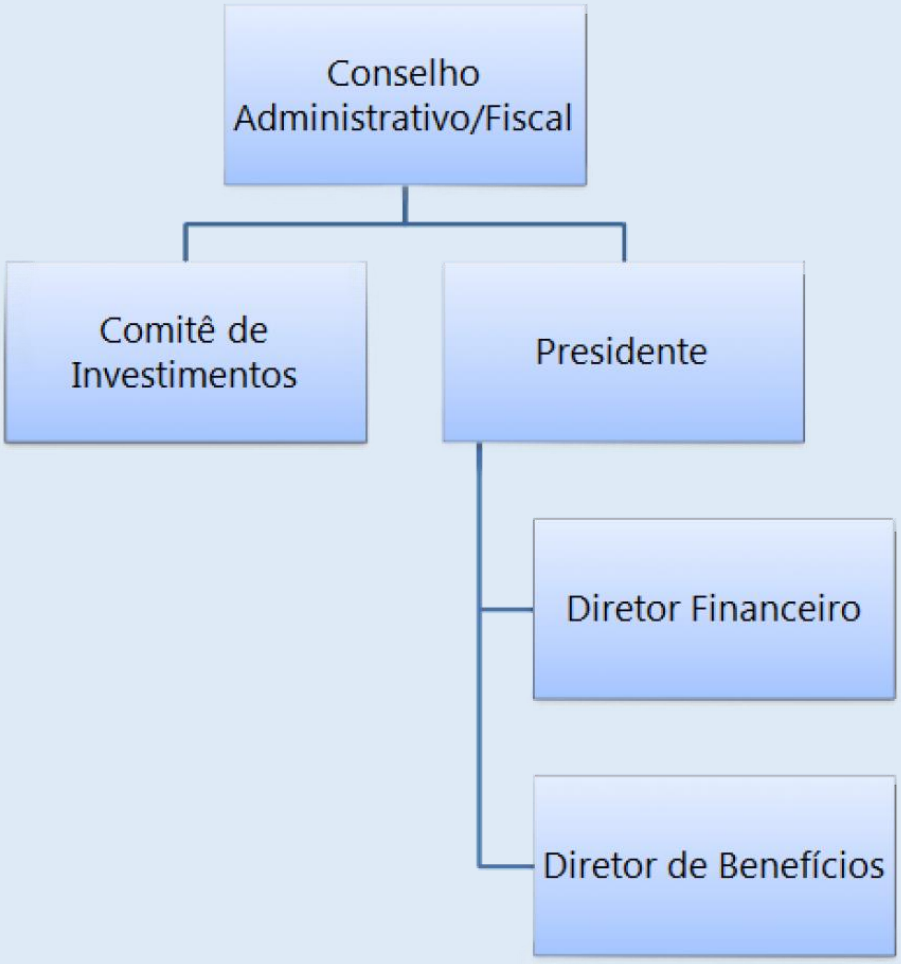
Assessoria de Investimentos;

Consultoria Previdenciária;

Junta Médica;

Assessoria/Consultoria Atuarial.

ORGANOGRAMA



MAPEAMENTO DOS PROCESSOS DE TECNOLOGIA DA INFORMAÇÃO DO RPPS

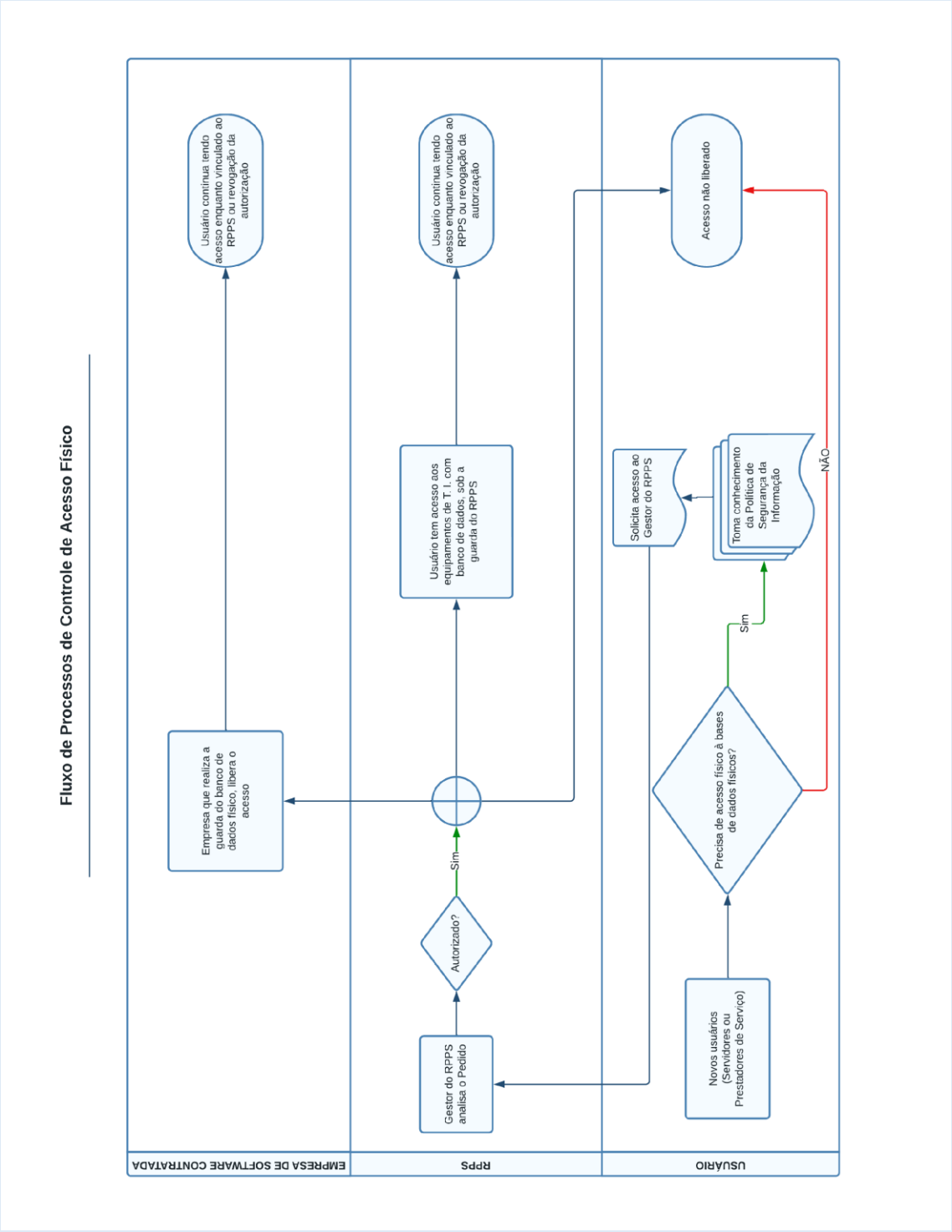
1. CONTROLE DE ACESSO FÍSICO

ETAPAS PROCESSUAIS

As etapas do processo de controle de acesso lógico seguirão conforme demonstrado no fluxograma ao término desse tópico, conforme:

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 (físico) autorizando e discriminando os níveis de acesso, conforme Política da Segurança da Informação;
6. Acesso é concedido;

FLUXOGRAMA - CONTROLE DE ACESSO FÍSICO



POLÍTICAS DE CONTROLE DE ACESSO E UTILIZAÇÃO

O Controle de Acesso Físico ao 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.

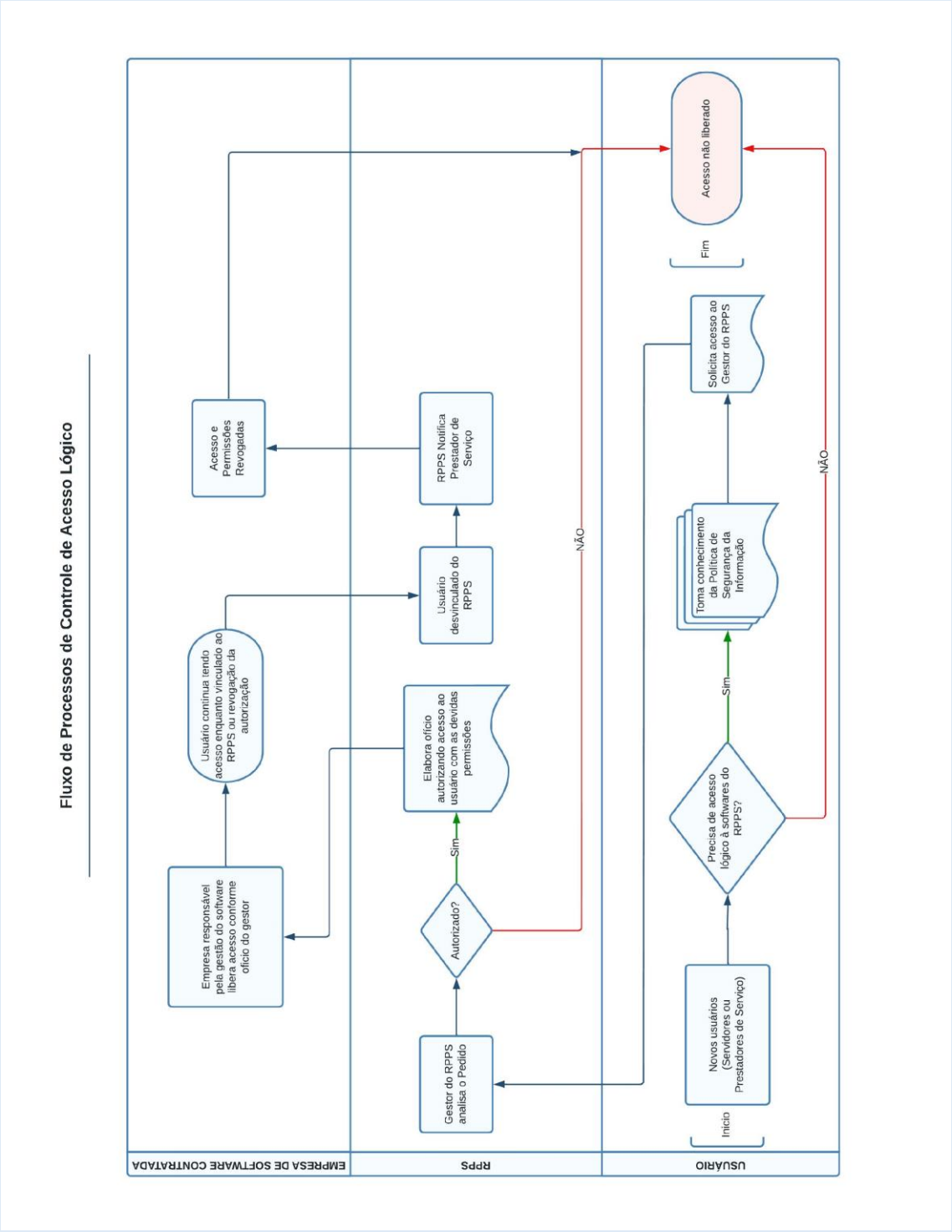
2. CONTROLE DE ACESSO LÓGICO

ETAPAS PROCESSUAIS

As etapas do processo de controle de acesso lógico seguirão conforme demonstrado no fluxograma, 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;

FLUXOGRAMA - CONTROLE DE ACESSO LÓGICO



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.

3. BACKUPS E PROCEDIMENTO DE CONTINGÊNCIA

ETAPAS DOS PROCESSOS DE CÓPIAS DE SEGURANÇA DOS SISTEMAS INFORMATIZADOS E DOS BANCOS DE DADOS

- **Fase Inicial - Automatização 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**

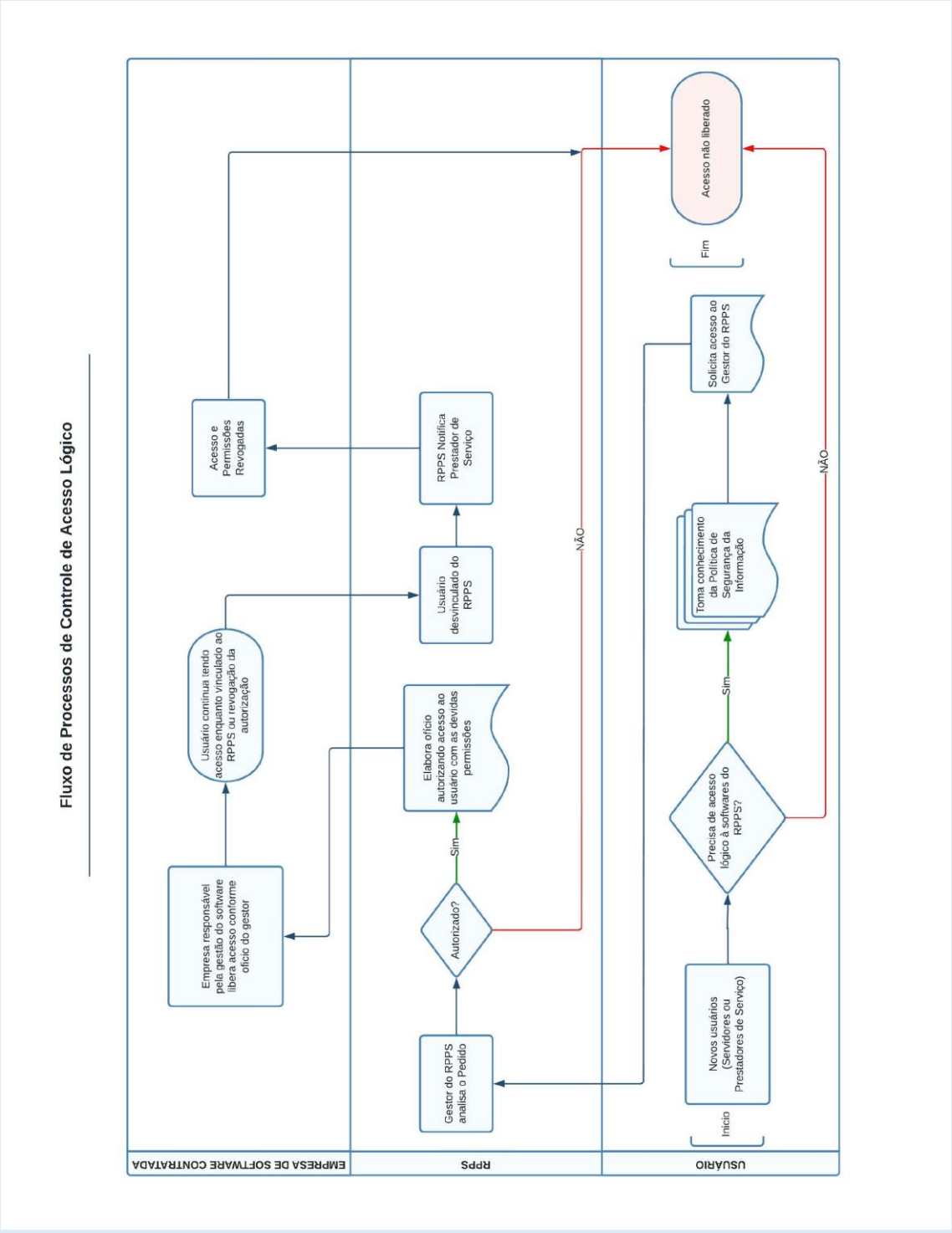
A fase de recuperação se inicia quando a fase de resposta foi concluída. Nesta fase, a Equipe de Respostas a Incidentes recupera a operação normal dos sistemas de backups. Esta providência pode requerer a recuperação de dados advindos de backups previamente realizados.

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.

FLUXOGRAMA - CÓPIAS DE SEGURANÇA DOS SISTEMAS INFORMATIZADOS



FLUXOGRAMA - CÓPIAS DE SEGURANÇA DOS BANCOS DE DADOS