Histórico de Emissão/Revisão e Aprovação				
Revisão	**Data**	**Descrição**	**Emissão/Revisão**	**Aprovação**
00	27/09/2023	Emissão Inicial	Adriano José Toledo Bueno	Claudia Leoncio da Silva

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 a 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 deter 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 a seus dispositivos e periféricos;
- software a 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 PIRAPREV

Dentro do PIRAPREV o objetivo de realizar o mapeamento da área de Tecnologia de Informação está amplamente ligado à 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 PIRAPREV

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 VÉRTICE-IT, 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 armazenamento de dados.

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

3. 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 a 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 ciência da Política de Segurança da Informação;

3. Solicita acesso ao Gestor do RPPS;

4. Gestor analisa a solicitação;

5. Caso autorizado, o gestor oficializa empresa contratada responsável pela guarda do banco de dados (lógico) autorizando e discriminando os níveis de acesso, conforme Política da Segurança da Informação;

6. O acesso é concedido;

3.1 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 da 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 RPPS.

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 da 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 removidas. 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.

4. BACKUPS E PROCEDIMENTO DE CONTINGÊNCIA

Na Administração Pública é recente a preocupação com a gestão dos documentos arquivísticos. Mas, com o 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 cedido 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 1 ano;

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 Piraprev.

4.1 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 - 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 1 ano;

2. Backup Automatizado Full diário às 22:00

- Contingência em Nuvem Privada e ambiente distinto;

- Retenção dos Arquivos está para 1 ano;

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 1 ano;

- Recebimento de conclusão com sucesso e com falha enviada 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.

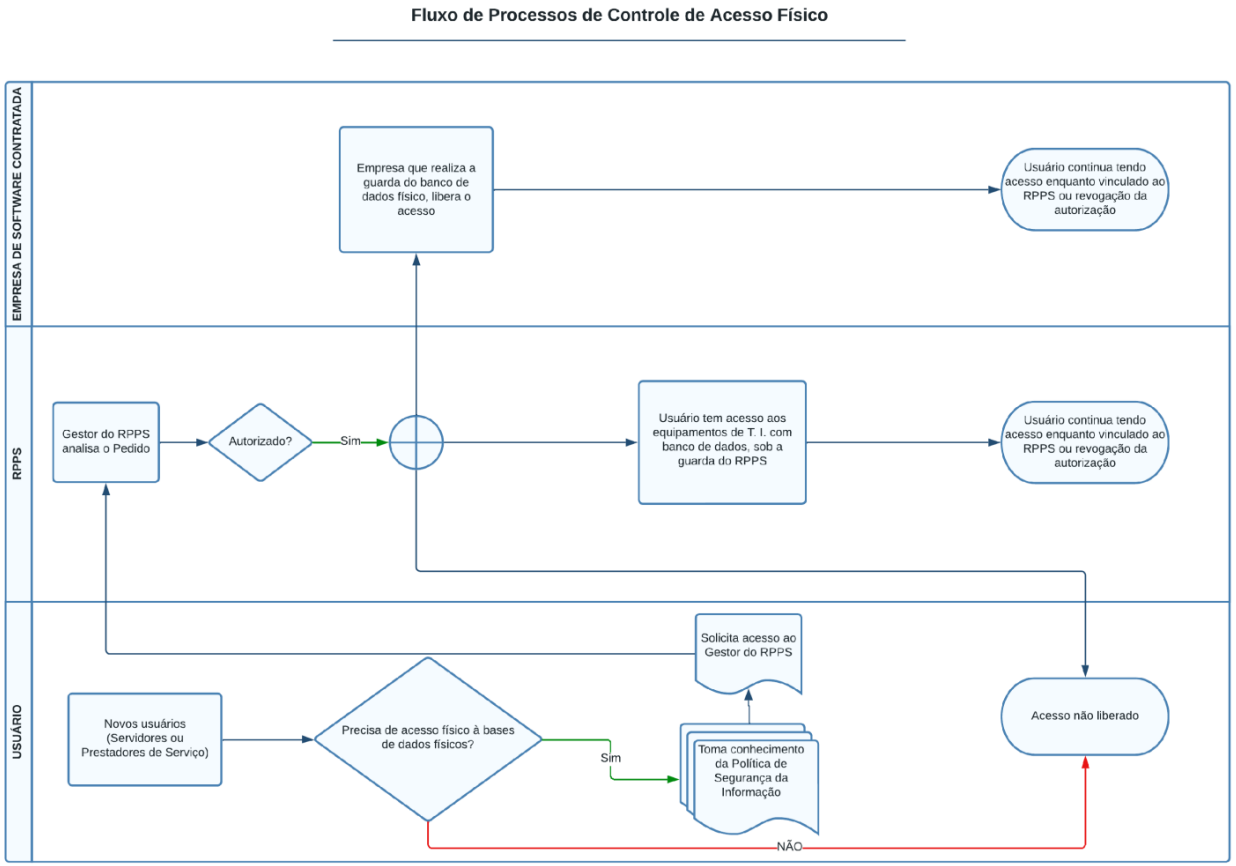
Uma vez normalizado o procedimento de backup afetado, estes são testados para se certificar de que não mais estão vulneráveis a fim de garantir que funcionarão corretamente quando recolocados em produção.

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.

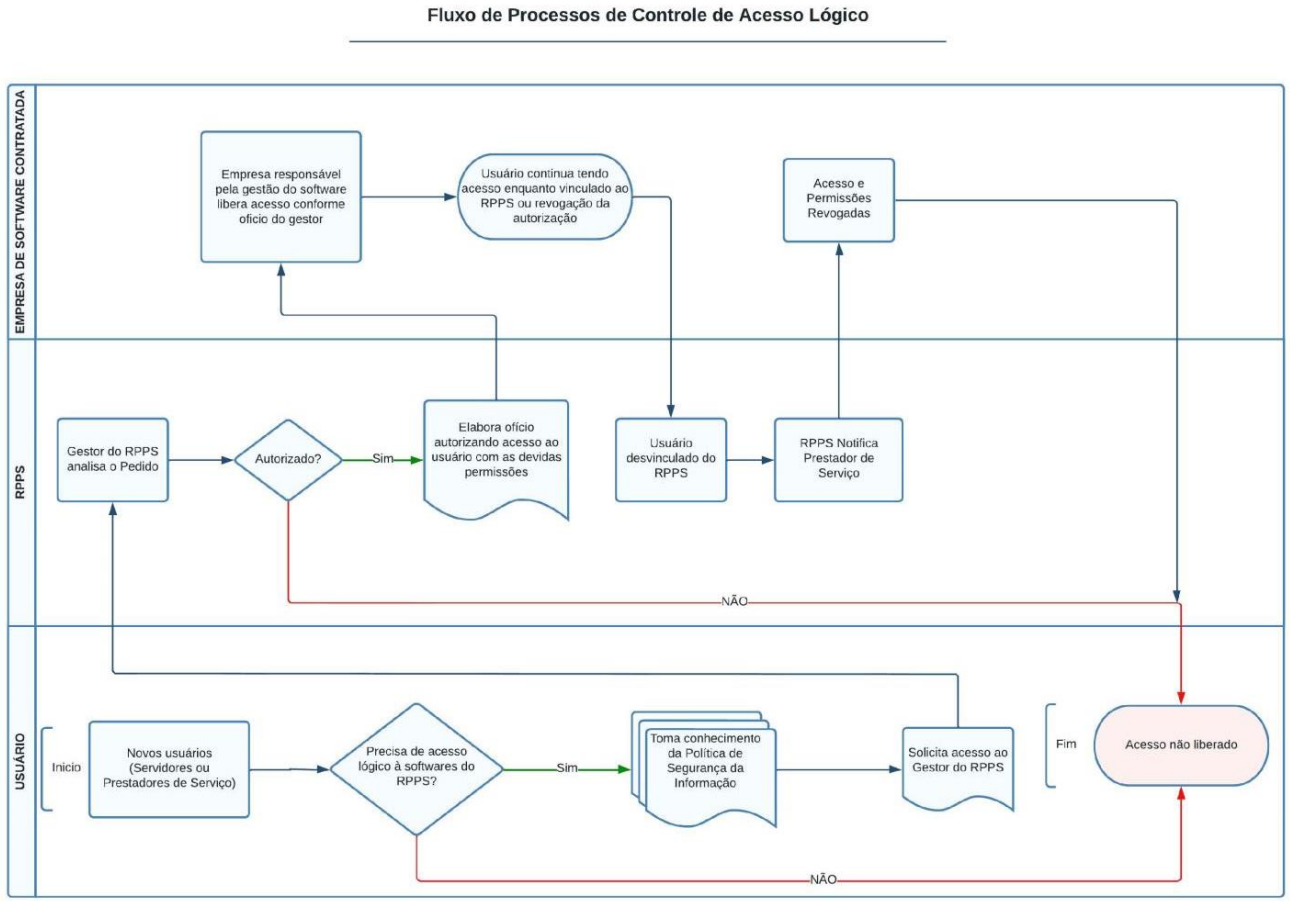
5. DAS FASES PROCESSUAIS

5.1 FASES PROCESSUAIS DO CONTROLE DE ACESSO FÍSICO



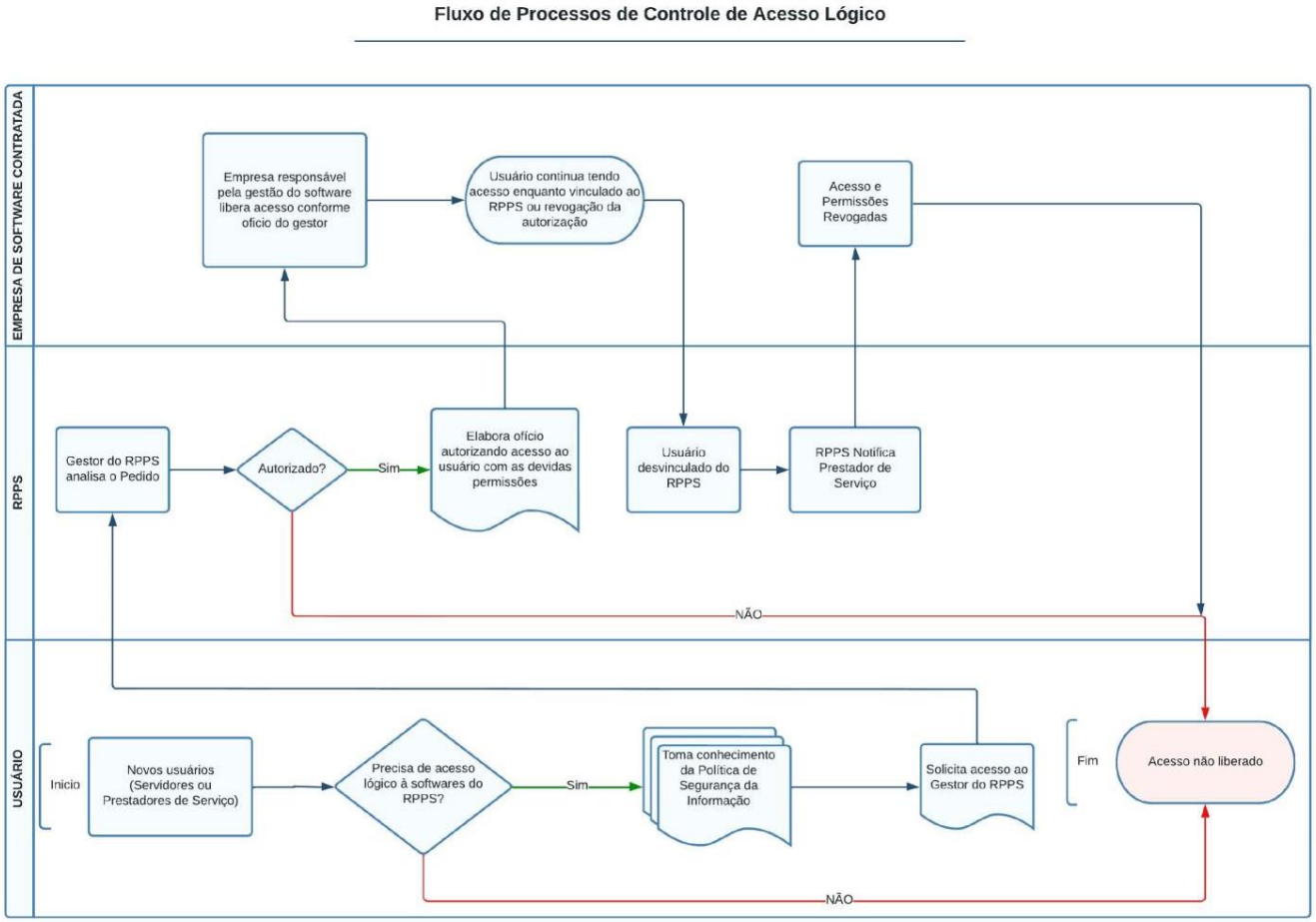
Fluxograma 1 - Fluxo de Processos de Controle de Acesso Físico

5.2 FASES PROCESSUAIS DO CONTROLE DE ACESSO LÓGICO



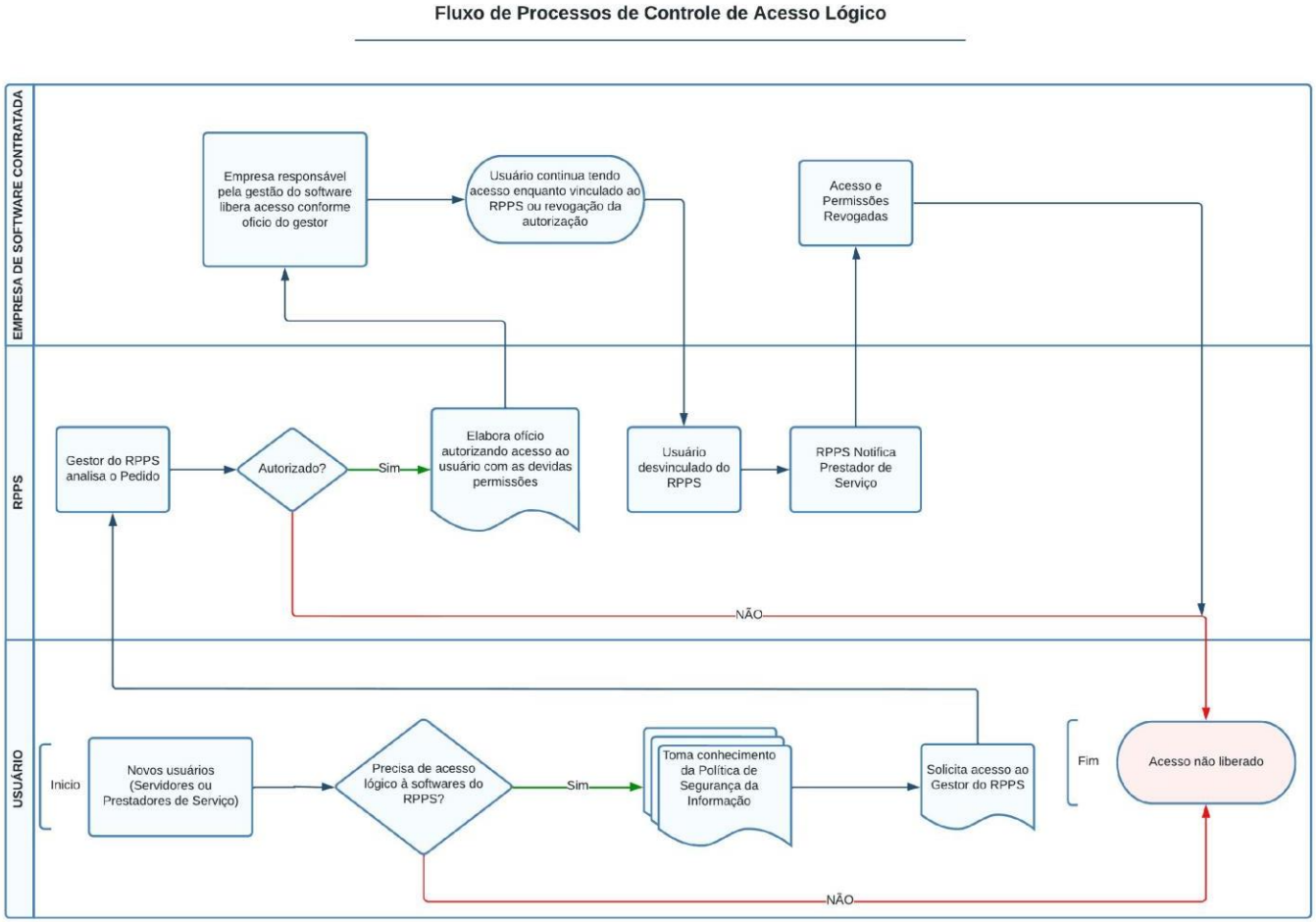
Fluxograma 2 - Fluxo de Processos de Controle de Acesso Lógico

5.3 CÓPIAS DE SEGURANÇA DOS BANCOS DE DADOS



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

5.4 CÓPIAS DE SEGURANÇA DOS SISTEMAS INFORMATIZADOS



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