MARINGÁ PREVIDÊNCIA
Presidência da MGAPREV
Unidade de Controle Interno da MGAPREV
Avenida Carneiro Leão, 135, Galeria do Edifício Europa - Bairro zona 01, Maringá/PR
CEP 87013-965, Telefone: (44) 3220-7728 - www.maringaprevidencia.com.br

MANUAL

MANUAL 09
Segurança da Informação

MAPEAMENTO E MANUALIZAÇÃO
2025

Sumário

Histórico das alterações		
Revisão	**Data**	**Descrição**
00	23/08/2019	Elaboração inicial
01	24/01/2023	Atualização
02	10/11/2025	Atualização*

*Esta atualização consolidou e atualizou os manuais de Cópias de segurança de sistemas e banco de dados, Controle de acesso físico ao CPD e Concessão de acesso aos sistemas.

1. INTRODUÇÃO

O ambiente de TI da Maringá Previdência é mantido na infraestrutura da Prefeitura Municipal de Maringá, sob responsabilidade da Agência Maringá de Tecnologia e Inovação.

Os principais softwares utilizados são:

I. Softprevi, da empresa Actuary, fornecido na modalidade SaS (Software as a Service – Software como serviço);
II. Elotech Gestão Pública;
III. Senior.

Quanto ao controle de acesso lógico, a infraestrutura da Prefeitura é responsável por determinar quais são as permissões que cada usuário tem dentro da rede da Prefeitura. Desta forma, na camada de rede essa responsabilidade fica para o domínio e o AD, administrado pela Gerência de Infraestrutura Tecnológica.

O mapeamento e manualização visa assegurar a padronização de execução, desempenho, qualidade e reprodutividade dos processos.

O presente manual, após aprovação do Diretor-Presidente, passa a integrar o conjunto de procedimentos padrão da Maringá Previdência.

2. REGULAMENTAÇÃO UTILIZADA

I. POLÍTICA DE GOVERNANÇA EM PRIVACIDADE E PROTEÇÃO DE DADOS 2024 (7322164);
II. POLÍTICA DE CONTROLE DE ACESSO DA PREFEITURA DE MARINGÁ 2024 (7322154);
III. POLÍTICA DE BACKUP PREFEITURA MUNICIPAL DE MARINGÁ 2024 (7322160);
IV. PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA 2024 (7322153);
V. POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS - ACTUARY (7322125);
VI. TERMOS E CONDIÇÕES DE USO DA PLATAFORMA SOFTPREVI - ACTUARY (7322151).

3. OBJETIVO

Este manual tem por objetivo determinar as responsabilidades dos envolvidos e descrever como são executados o processo de cópias de segurança dos sistemas e bancos de dados, o processo de liberação de acesso físico, o processo de liberação de acesso lógico aos

sistemas utilizados pela Maringá Previdência.

4. RESPONSABILIDADES

Os responsáveis pelos processos de Segurança da Informação estão definidos conforme a matriz de responsabilidade a seguir.

Para análise da matriz, considera-se:

P – Principal responsável;
C – Co-responsável.

ATIVIDADES	AMTECH	ACTUARY	CONTROLE INTERNO	SETOR DEMANDANTE
Processo de cópias de segurança de sistemas e banco de dados dos respectivos sistemas sob responsabilidade	P	P		
Controle de acesso físico das respectivas unidades	P	P		
Concessão de acesso à rede e sistemas da Prefeitura de Maringá	P			C
Concessão de acesso ao sistema Softprevi - Actuary		P	P	C

5. MANUALIZAÇÃO DAS ATIVIDADES

5.1. PROCESSO DE CÓPIAS DE SEGURANÇA DE SISTEMAS E BANCO DE DADOS

5.1.1. Procedimentos de backup - Agência Maringá de Tecnologia e Inovação

São realizados pela Prefeitura Municipal de Maringá o backup da base de dados dos sistemas presentes na organização em um período diário, semanal e mensal de forma automática, conforme segue:

Agendamento: Automático
Mídia: FITA LTO (mídias armazenadas em cofre, localizado em sala climatizada)
Rotina: Diário, Semanal, Mensal

5.1.1.1. Rotina de Backup e Tempo de Retenção

TIPO	PERÍODO	RETENÇÃO
Backup diário	Processado de segunda a quinta-feira	Dos sete últimos backups
Backup semanal	Backup diário processado às sextas-feiras	Das quatro últimas semanas
Backup mensal	Backup diário processado na último sábado do mês	Eterna

5.1.1.2. Armazenamento e transporte

As cópias de segurança são armazenadas em fitas LTO individuais.

As mídias de cópia de segurança são armazenadas em um cofre trancado, localizado em sala climatizada, distante do local principal o suficiente, para o caso de desastre ou impedimento, mas que não comprometa o acesso para a recuperação quando for necessário.

5.1.1.3. Recuperação de Desastre (Disaster)

As cópias de segurança específicas para uma recuperação de desastre devem levar em consideração os sistemas operacionais, aplicações e dados que possibilitem uma completa recuperação da aplicação.

Em caso de desastre, faz-se necessário que a infraestrutura disponibilizada em local de contingência tenha as mesmas característica e configurações que o local original.

5.1.1.4. Teste e Descarte

Regularmente as mídias devem ser testadas e analisadas, para garantir a confiabilidade, integridade e disponibilidade nos casos de uso emergencial e aderente aos requisitos necessários à recuperação. As mídias devem ser substituídas no período indicado pelo fabricante ou em casos de erro das mesmas, resguardando os princípios de segurança em relação ao sigilo das informações e descarte de mídias.

5.1.2. **Procedimentos de backup - ACTUARY (empresa fornecedora do software previdenciário)**

5.1.2.1. Rotina de Backup

Procedimentos de contingência consiste na realização do backup do banco de dados diário, o backup realizado das máquinas virtuais das empresas de Cloud contratadas pela Actuary.

O backup é realizado diariamente, geralmente entre os horários de 01:00h e 06:00h, junto ao datacenter da empresa Oracle Brasil, com sede em São Paulo, com replicação em Vinhedo-SP, com a qual possuem Contrato de Prestação de Serviços, com objeto de disponibilização do ambiente em nuvem para armazenamento de dados e disponibilização das aplicações desenvolvidas pela Actuary, ou seja, os dados ficam em dois data centers físicos em locais diferentes, além de ter uma cópia diária no data center da Actuary.

O referido backup é replicado diariamente para o datacenter da Actuary, com sede em Curitiba, Paraná.

Os backups são mantidos num período máximo de 3 (três) meses, sendo que o responsável técnico todo esse procedimento de backup é o Diretor de Tecnologia da Actuary, Sr. Rodrigo Traleski.

5.2. **PROCESSO DE CONTROLE DE ACESSO FÍSICO**

As credenciais: crachá de identificação funcional e logins de acesso dos sistemas

de informações, são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso físico e/ou lógico podem ser exercidos.

Cabe ressaltar que os controles de autorização, identificação e autenticação garantem que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação.

5.3. **PROCESSO DE CONCESSÃO DE ACESSO AOS SISTEMAS**

5.3.1. **Acesso lógico - Agência Maringá de Tecnologia e Inovação**

5.3.1.1. Solicitação de acesso

A chefia imediata do funcionário solicita ao setor de suporte da Prefeitura via SEI, a liberação de acesso ou a atualização de acesso já existente, indicando as permissões necessárias para o funcionário/login.

O acesso lógico aos recursos da rede local deverá ser realizado por meio de sistema de controle de acesso, administrado e mantido pelo setor de Tecnologia da Informação – TI, conforme responsabilidades e atribuições específicas de cada usuário.

Terão direito ao acesso lógico apenas os usuários cujas atividades demandem o uso de recursos de tecnologia da informação. Para fins desta norma, consideram-se usuários: servidores ocupantes de cargo efetivo ou em comissão, empregados públicos em exercício, funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade na Prefeitura Municipal de Maringá.

O acesso às estações de trabalho da Prefeitura será efetuado mediante identificação única (login) e senha de acesso, fornecidos pelo setor de TI, após solicitação formal do titular da unidade requisitante, com aprovação do gestor imediato. Os privilégios de acesso deverão ser definidos pela área requisitante à qual o usuário está vinculado, limitando-se às atividades estritamente necessárias à execução de suas funções, conforme perfis de acesso estruturados por setor e/ou atividade.

Quando houver necessidade de acesso fora do perfil padrão disponibilizado, o usuário deverá encaminhar solicitação ao seu gestor imediato, que realizará a análise e, se aprovada, enviará ao setor de TI. Este poderá conceder ou negar o pedido, devidamente justificado. Login e senha são pessoais e intransferíveis, sendo proibida sua divulgação. O setor de TI poderá bloquear o acesso sempre que identificar irregularidades.

O padrão de senha definido pelo setor de TI considera tamanho mínimo, composição (letras, números e símbolos) e regras de não repetição de senhas anteriores.

5.3.1.2. Requisitos para formação da senha

I. Mínimo de oito caracteres, com uso obrigatório de letras e números.
II. Recomenda-se o uso de letras maiúsculas e minúsculas e caracteres especiais ($, %, &, #).
III. Não deve conter sequências numéricas (123...), alfabéticas (abc...), nomes próprios, palavras de fácil dedução, datas, placas, telefones, apelidos ou abreviações.
IV. Não utilizar termos óbvios (Brasil, senha, usuário, password, system).
V. Não reutilizar as últimas cinco senhas.

O setor de TI fornecerá senha temporária no momento da criação da conta, devendo o usuário alterá-la no primeiro acesso. As senhas deverão ser renovadas a cada 90 dias, com aviso automático ao usuário.

5.3.1.3. Bloqueio, desbloqueio e cancelamento da conta de acesso

A conta de acesso será bloqueada nos seguintes casos:

I. Após 5 (cinco) tentativas consecutivas de acesso errado.
II. Solicitação formalizada do gestor imediato do usuário com a devida justificativa.
III. Quando da suspeita de mau uso dos serviços disponibilizados pelo setor de Tecnologia da Informação - TI ou descumprimento da Política de Segurança da Informação e normas correlatas em vigência.
IV. Diante das orientações formalizadas e encaminhadas para o setor de Tecnologia da Informação - TI pelo setor de Recursos Humanos, após exoneração do servidor público ou do término de contrato com cargo comissionados, ocupantes de emprego público em exercício e estagiários.
V. Quando no término contratual de empresas prestadores de serviços com acessos liberados para terceiro, sendo solicitado formalmente ao setor de Tecnologia da Informação - TI pela área responsável da gestão do contrato.
VI. Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido formal do gestor imediato ao setor de Tecnologia da Informação - TI ou este será realizado pelo próprio setor de Tecnologia da Informação - TI baseado em informações formalizadas pelo setor de Recursos Humanos.

O desbloqueio da conta de acesso à rede local será realizado apenas após solicitação formal do gestor imediato do usuário, ou do setor de Recursos Humanos ou pelo responsável da gestão contratual ao setor de Tecnologia da Informação - TI.

A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

É de responsabilidade do gestor imediato do usuário ou do setor de Recursos Humanos comunicar formalmente o setor de Tecnologia da Informação- TI o desligamento ou saída definitiva do usuário do departamento para que as permissões de acesso à rede local sejam canceladas.

5.3.1.4. Obrigações dos usuários quanto ao uso dos recursos tecnológicos

I. O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação para coibir acessos indevidos.
II. A utilização simultânea da conta de acesso à rede local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.
III. O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à rede local.
IV. O usuário deve informar ao setor de Tecnologia da Informação- TI qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.
V. É dever do usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

a. Não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros e outras formas.
b. Evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros para não gerar indisponibilidade de informações internas e externas.
c. Interromper a conexão e adotar medidas que bloqueiem o acesso de terceiros nos equipamentos de informática e aos sistemas sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo.
d. Não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso.
e. Não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas.
f. Utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas.
g. Não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis.
h. Assinar o Termo de Responsabilidade, Anexo I, da Política de Segurança da Informação da Prefeitura Municipal de Maringá quanto a utilização da respectiva conta de acesso.

5.3.2. **Acesso lógico - Softprevi ACTUARY**

5.3.2.1. Solicitação de acesso

O usuário responsável pelas liberações de acesso e cadastro de novos servidores como usuários do sistema Softprevi - Actuary é o responsável pelo Controle Interno.

O setor responsável pelo novo funcionário solicita ao setor de Controle Interno a liberação de acesso ou a atualização de acesso já existente, indicando as permissões necessárias para o funcionário/login.

Conforme solicitação, são parametrizadas as liberações do novo usuário aos módulos e perfis de que fará uso.

Por segurança acessos especiais são liberados apenas por solicitação direta ao desenvolvimento do sistema.

Todos as movimentações no sistema são registradas nos logins de usuários, podendo ser solicitados relatórios como medidas de contingência.

5.3.2.2. Login

O Serviço pode ser acessado com login e senha únicos, pessoais e não transferíveis, que são definidos após o cadastro na Plataforma. Os Usuários são responsáveis por garantir a segurança de seu login e senha de acesso aos Serviços.

5.3.2.3. Bloqueio e cancelamento da conta de acesso

Os desligamentos devem ser comunicados para que o usuário seja bloqueado no

sistema.

6. MAPEAMENTO DAS ATIVIDADES

Os mapeamentos das atividades detalhadas neste manual, seguem conforme fluxogramas a seguir.

6.1. PROCESSO DE CÓPIAS DE SEGURANÇA DE SISTEMAS E BANCO DE DADOS

I. Procedimentos de backup - Agência Maringá de Tecnologia e Inovação: 7330982;
II. Procedimentos de backup - ACTUARY: 7330989.

6.2. PROCESSO DE CONTROLE DE ACESSO FÍSICO

I. Controle de acesso físico: 7331365.

6.3. PROCESSO DE CONCESSÃO DE ACESSO AOS SISTEMAS

I. Acesso lógico - Agência Maringá de Tecnologia e Inovação: 7331696;
II. Acesso lógico - Softprevi ACTUARY: 7331702.

Maringá, 10 de novembro de 2025.

Documento assinado eletronicamente por **Bárbara Garcia Schneider**, **Controle Interno**, em 10/11/2025, às 16:46, conforme horário oficial de Brasília, com fundamento na Medida Provisória nº 2200-2, de 24 de agosto de 2001 e Decreto Municipal nº 871, de 7 de julho de 2020.

Documento assinado eletronicamente por **Edson Paliari**, **Diretor (a)-Presidente da MGAPREV**, em 11/11/2025, às 07:08, conforme horário oficial de Brasília, com fundamento na Medida Provisória nº 2200-2, de 24 de agosto de 2001 e Decreto Municipal nº 871, de 7 de julho de 2020.

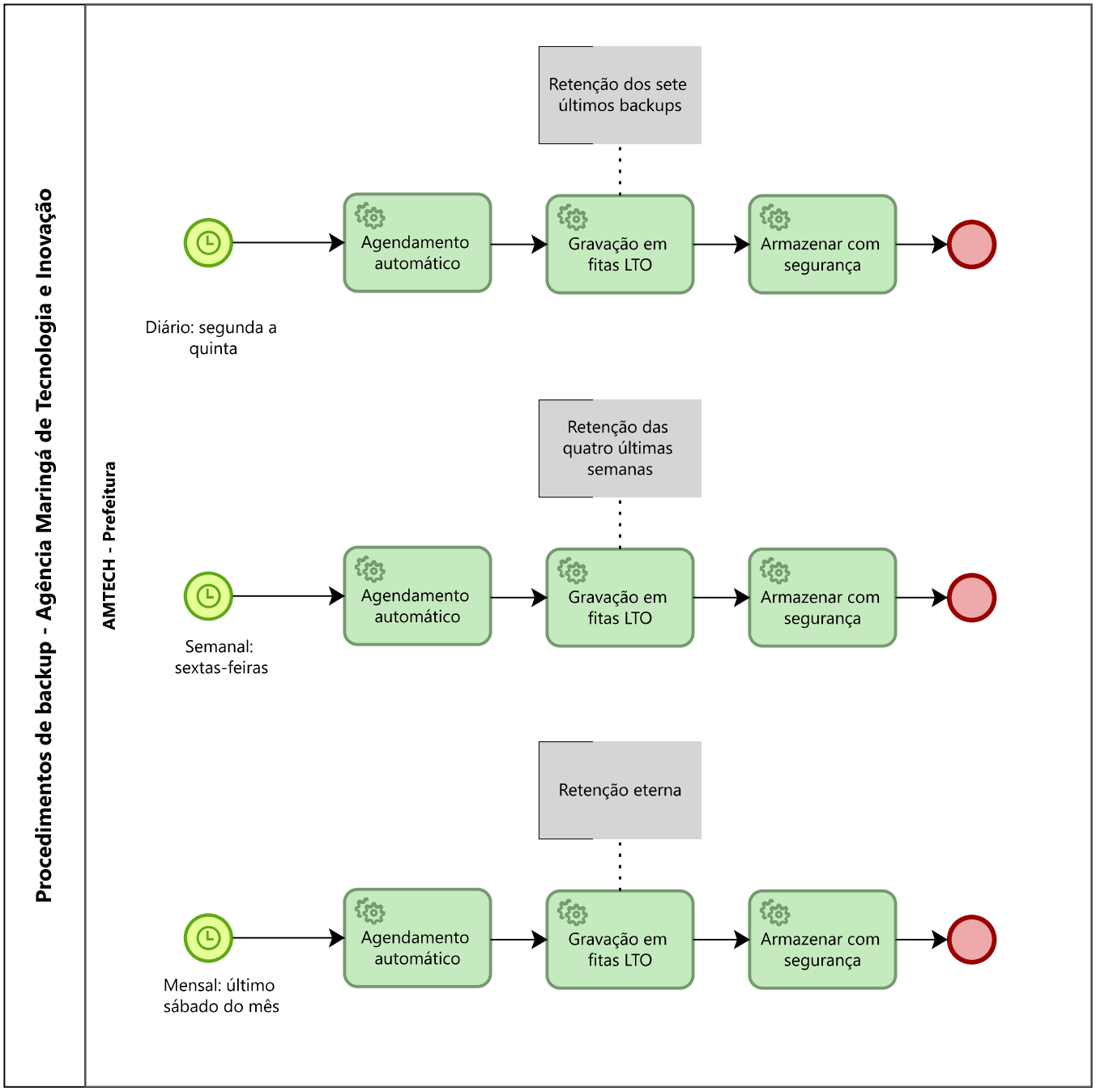
A autenticidade deste documento pode ser conferida no site https://sei.maringa.pr.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7319548** e o código CRC **619692B3**.

Procedimentos de backup - AMTECH

Autor: Maringá Previdência

Versão: 3.0

Descrição: Processo de cópias de segurança de sistema e banco de dados

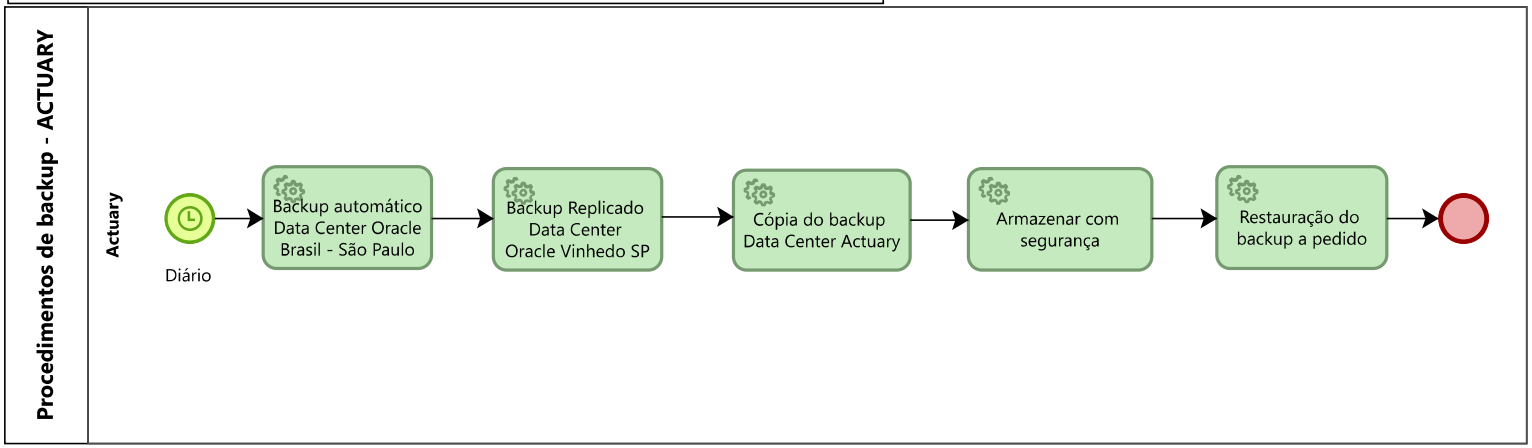


Procedimentos de backup - ACTUARY

Autor: Maringá Previdência

Versão: 3.0

Descrição: Processo de cópias de segurança de sistema e banco de dados - Actuary

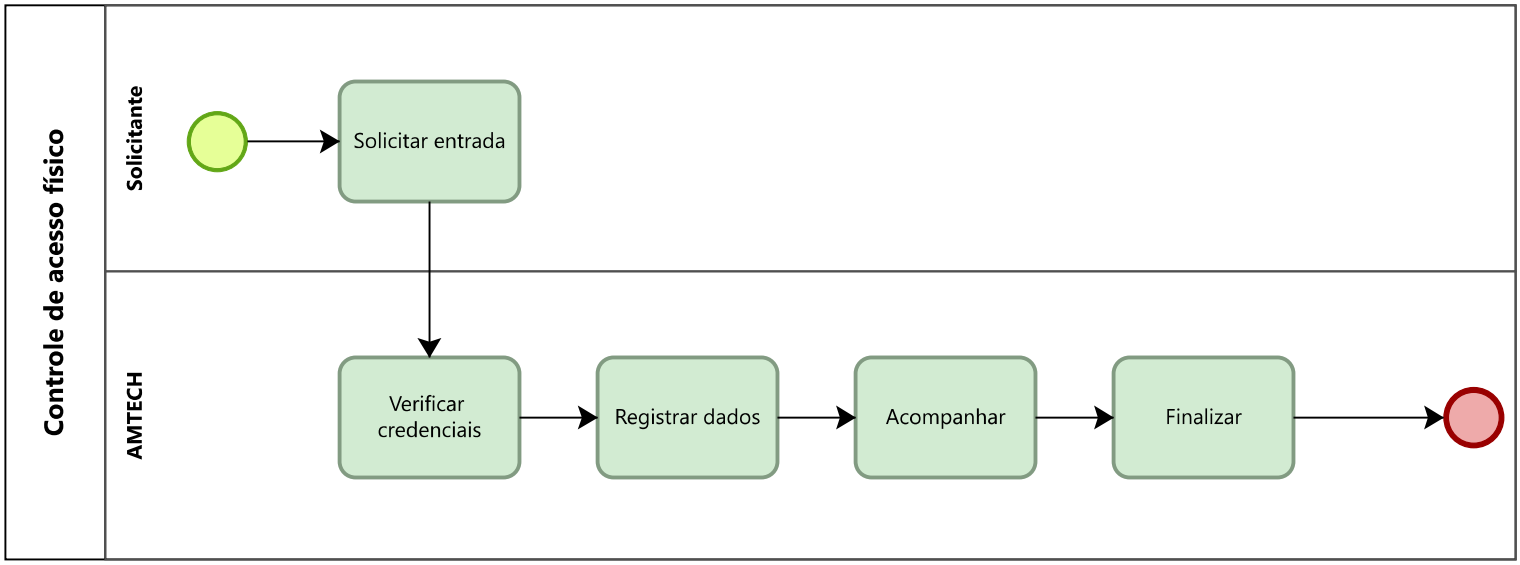


Controle de acesso físico AMTECH

Autor: Maringá Previdência

Versão: 3.0

Descrição: Procedimentos de controle de acesso físico

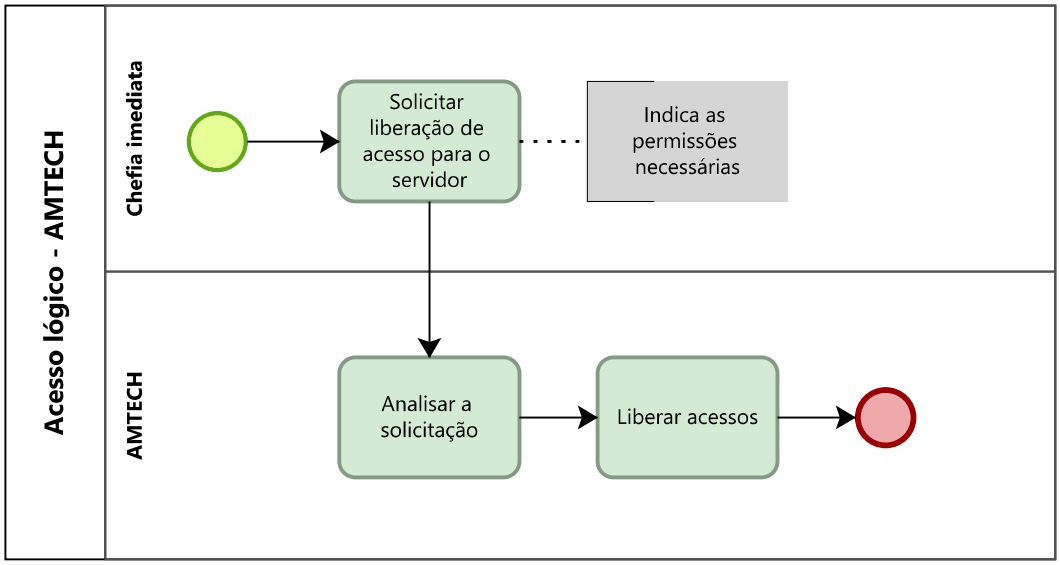


Processo de concessão de acesso aos sistemas AMTECH

Autor: Maringá Previdência

Versão: 3.0

Descrição: Procedimentos de controle de acesso lógico



Processo de concessão de acesso ao Softprevi - Actuary

Autor: Maringá Previdência

Versão: 3.0

Descrição: Procedimentos de controle de acesso lógico