Instituto de Previdência dos
Servidores do Distrito Federal

PROCEDIMENTOS DE CONTROLES DE ACESSOS FÍSICOS E LÓGICOS

2026 Brasília - DF

GOVERNO DO DISTRITO FEDERAL

Governador
Ibaneis Rocha

Vice-Governadora
Celina Leão

INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO DISTRITO FEDERAL

Diretora-presidente
Raquel Galvão Rodrigues da Silva

Diretora de Governança, Projetos e Compliance
Sylvia Neves Alves

Diretora de Administração e Finanças
Elaine De Fatima De Almeida Lima

Diretor de Previdência
Pedro Henrique Araújo Nabarrete Gabini

Diretor Jurídico
Radam Nakai Nunes

Diretor de Investimentos
Thiago Mendes Rodrigues

Controladoria
Maurílio de Freitas

Unidade de Atuária
Jucelina Santana da Silva

Unidade de Comunicação Social
Hadassa da Rocha Marques

Elaboração
Filipe Silva Santos
Helber do Nascimento Soares
Coordenação de Gestão e Tecnologia da Informação

EDIÇÃO GRÁFICA

Unidade de Comunicação Social
Raphaela Satiko Reis Watanabe

Sumário

INTRODUÇÃO

Sob a ótica da governança e proteção de ativos, este manual estabelece as diretrizes para dois pilares fundamentais da segurança institucional com o controle de acesso físico que referese aos mecanismos de proteção do perímetro e das instalações sensíveis do Instituto cujo objetivo é garantir que apenas pessoas autorizadas tenham entrada e circulação em áreas críticas — como o Salas de Rack de servidores e arquivos de documentos — mitigando riscos de danos materiais, furtos ou acessos indevidos que possam comprometer a continuidade do Regime Próprio de Previdência Social (RPPS) e o controle de acesso Lógico, onde contempla as barreiras digitais que protegem os sistemas informatizados e bancos de dados. Através de protocolos de autenticação, perfis de usuários e níveis de privilégios, assegura-se que a informação seja acessada exclusivamente por quem possui a devida permissão, preservando a tríade fundamental da segurança da informação: Confidencialidade, Integridade e Disponibilidade.

OBJETIVO

O presente documento visa estabelecer as diretrizes e normas para a gestão de acessos no âmbito do IPREV-DF, desdobrando-se nos seguintes objetivos específicos:

Objetivos Gerais:

Padronizar os fluxos de concessão, alteração e revogação de acessos físicos e lógicos.

Mitigar riscos de acessos não autorizados que possam comprometer a integridade dos dados previdenciários e a segurança das instalações.

Promover a cultura de segurança entre servidores e colaboradores, definindo responsabilidades claras sobre o uso de credenciais e circulação interna.

Objetivos Específicos no Âmbito Físico:

Controlar a circulação de pessoas em áreas críticas (Salas de Tecnologia e ambiente de informática, Salas de Arquivo).

Monitorar o fluxo de visitantes e prestadores de serviço por meio de registros de identificação.

Garantir a integridade do patrimônio público e dos ativos de hardware do Instituto.

No Âmbito Lógico:

Assegurar que o acesso aos sistemas e bancos de dados seja realizado mediante autenticação única e intransferível.

Implementar a segregação de funções, evitando que um único usuário possua privilégios excessivos que possam gerar conflitos de interesse ou vulnerabilidades.
Manter trilhas de auditoria (logs) que permitam a rastreabilidade completa das operações realizadas nos sistemas do RPPS.

ABRANGÊNCIA

As diretrizes e procedimentos contidos neste manual possuem aplicação integral e obrigatória, alcançando:

1. Âmbito Pessoal aplica-se a todos os indivíduos que interagem com a infraestrutura ou com os sistemas do Instituto, independentemente do vínculo jurídico:

- Servidores Efetivos e Comissionados: Em todas as instâncias hierárquicas.
- Estagiários e Menores Aprendizes: No exercício de suas atividades de apoio.
- Prestadores de Serviço e Terceirizados: Que necessitem de acesso físico às dependências ou acesso lógico aos sistemas para manutenção e suporte.
- Consultores e Auditores Externos: Em missões específicas de avaliação e controle.

2. Âmbito Físico estende-se a todas as unidades e espaços físicos sob responsabilidade do IPREV-DF, com especial atenção a:

- Áreas Comuns e Administrativas: Recepções, gabinetes e postos de atendimento.
- Áreas Restritas: Data Center (Sala de Cofre), salas de servidores, centrais de monitoramento e depósitos de suprimentos tecnológicos.
- Arquivos e Depósitos: Locais de guarda de documentos sensíveis e processos físicos do Regime Próprio de Previdência Social (RPPS).

3. Âmbito Lógico e Tecnológico abrange todo o ecossistema digital gerido pelo Instituto, incluindo:

- Redes de Dados: Conexões cabeadas e redes Wi-Fi institucionais.
- Sistemas Finalísticos: Softwares de gestão previdenciária, bancos de dados e sistemas de folha de pagamento.
- Ativos de Hardware: Computadores, notebooks, tablets, servidores e dispositivos de armazenamento (storages).
- Serviços em Nuvem: E-mails institucionais, ferramentas de colaboração e repositórios digitais oficiais.

BASE NORMATIVA

Lei Complementar nº 840/2011: Regime jurídico dos servidores do DF.

Lei nº 13.709/2018: Lei Geral de Proteção de Dados Pessoais (LGPD).

Lei nº 12.737/2012: Tipificação criminal de delitos informáticos. Resolução nº 01/2024: Política de Segurança da Informação e Comunicação (POSIC) do GDF.

Decreto Distrital nº 40.015/2019: Centralização da rede GDFNet e CeTIC-DF.

RESPONSABILIDADES

A eficácia dos controles de acesso físico e lógico depende do comprometimento conjunto de diferentes níveis hierárquicos e áreas do Instituto. As responsabilidades são distribuídas da seguinte forma:

1. Alta Gestão

- Prover recursos necessários para a manutenção das tecnologias de segurança (biometria, sistemas de vigilância, firewalls).
- Fomentar a cultura de segurança, assegurando que as diretrizes de acesso sejam respeitadas por todos os níveis da autarquia.

2. Da Unidade de Tecnologia da Informação (TI)

- Administrar o acesso lógico, criando, alterando e revogando perfis de usuários conforme as solicitações autorizadas.
- Monitorar trilhas de auditoria (logs) para identificar tentativas de acesso indevido ou comportamentos anômalos nos sistemas.
- Garantir a segurança das redes, implementando criptografia, autenticação multifator e firewalls.

3. Da Coordenação de Administração Geral (Segurança Física)

- Gerir o acesso físico, controlando a entrega de crachás, chaves e o registro de visitantes.
- Fiscalizar o acesso a áreas restritas (como o Data Center e almoxarifados sensíveis).

4. Gestão de Pessoas (Cadastros)

- Solicitar cadastro físico e lógico para novos servidores ou mudanças de lotação.
- Comunicar imediatamente o desligamento ou transferência de servidores para que os acessos físicos e lógicos sejam revogados no mesmo dia.

5. Das Chefias Imediatas (Gerências e Diretorias)

- Solicitar acessos para seus subordinados com base estritamente na necessidade do serviço (Princípio do Privilégio Mínimo).
- Comunicar imediatamente o desligamento ou transferência de servidores.
- Revisar periodicamente os níveis de permissão de sua equipe.

6. De Todos os Usuários (Servidores, Terceirizados e Estagiários)

- Zelar pelas credenciais: Manter senhas de sistemas e crachás de identificação como itens de uso pessoal e intransferível.
- Reportar incidentes: Informar imediatamente à TI ou à Segurança sobre a perda de cartões de acesso, suspeita de vazamento de senhas ou presença de estranhos em áreas restritas.
- Uso Ético: Utilizar os recursos tecnológicos e físicos exclusivamente para finalidades institucionais, respeitando as normas de sigilo e ética pública.

Matriz de Responsabilidade (Resumo)

Atividade	Responsável Primário	Apoio
Definição de perfis de acesso	Chefia do Setor	TI
Manutenção de portas, e travas	Setor de Patrimônio	Setor de Patrimônio
Reset de senhas e bloqueios	TI	Usuário
Cancelamento de acesso (desligamento)	Gestão de Pessoas (RH)	TI e Logística

CONTINGÊNCIA

DIRETRIZES GERAIS

As diretrizes abaixo fundamentam a política de controle de acesso do IPREV-DF e devem ser observadas em todos os procedimentos operacionais:

1. Privilégio Mínimo

O acesso aos recursos (físicos ou lógicos) será concedido apenas no nível estritamente necessário para o exercício das atribuições do cargo ou função. Nenhum usuário deverá possuir privilégios além daqueles essenciais para a execução de suas tarefas rotineiras.

2. Identificação Única e Intransferível

Todo acesso deve ser individualizado. É terminantemente proibido o compartilhamento de senhas, crachás, tokens ou qualquer outro meio de autenticação. A responsabilidade por qualquer ação realizada sob uma credencial é de seu titular.

3. Segregação de Funções

Os processos devem ser desenhados para que as responsabilidades de autorização, execução e revisão sejam distribuídas entre pessoas diferentes. No IPREV-DF, isso evita que um único servidor tenha controle total sobre um processo sensível (como a concessão de benefício e a liberação do pagamento no sistema).

4. Rastreabilidade e Auditoria (Compliance)

Todas as tentativas de acesso, bem como as ações executadas dentro dos sistemas e a circulação em áreas restritas, devem ser registradas em logs. Estes registros devem ser protegidos contra alteração e estar disponíveis para auditorias internas e externas.

5. Revogação Imediata de Acesso

Em casos de desligamento, exoneração, término de contrato ou alteração de função que não exija mais o acesso prévio, as permissões físicas e lógicas devem ser revogadas imediatamente (em tempo real ou em até 24 horas úteis).

6. Proteção de Dados Sensíveis (LGPD)

O controle de acesso é a principal barreira de proteção dos dados pessoais e previdenciários dos segurados. Todo acesso a bancos de dados contendo informações sensíveis deve seguir critérios rigorosos de confidencialidade, conforme a Lei Geral de Proteção de Dados.

7. Periodicidade de Revisão

Os perfis de acesso e as permissões de entrada física não são permanentes. Serão realizadas revisões semestrais para validar se os níveis de acesso concedidos ainda são compatíveis com as atividades exercidas pelos colaboradores.

8. Cultura de "Mesa Limpa e Tela Bloqueada"

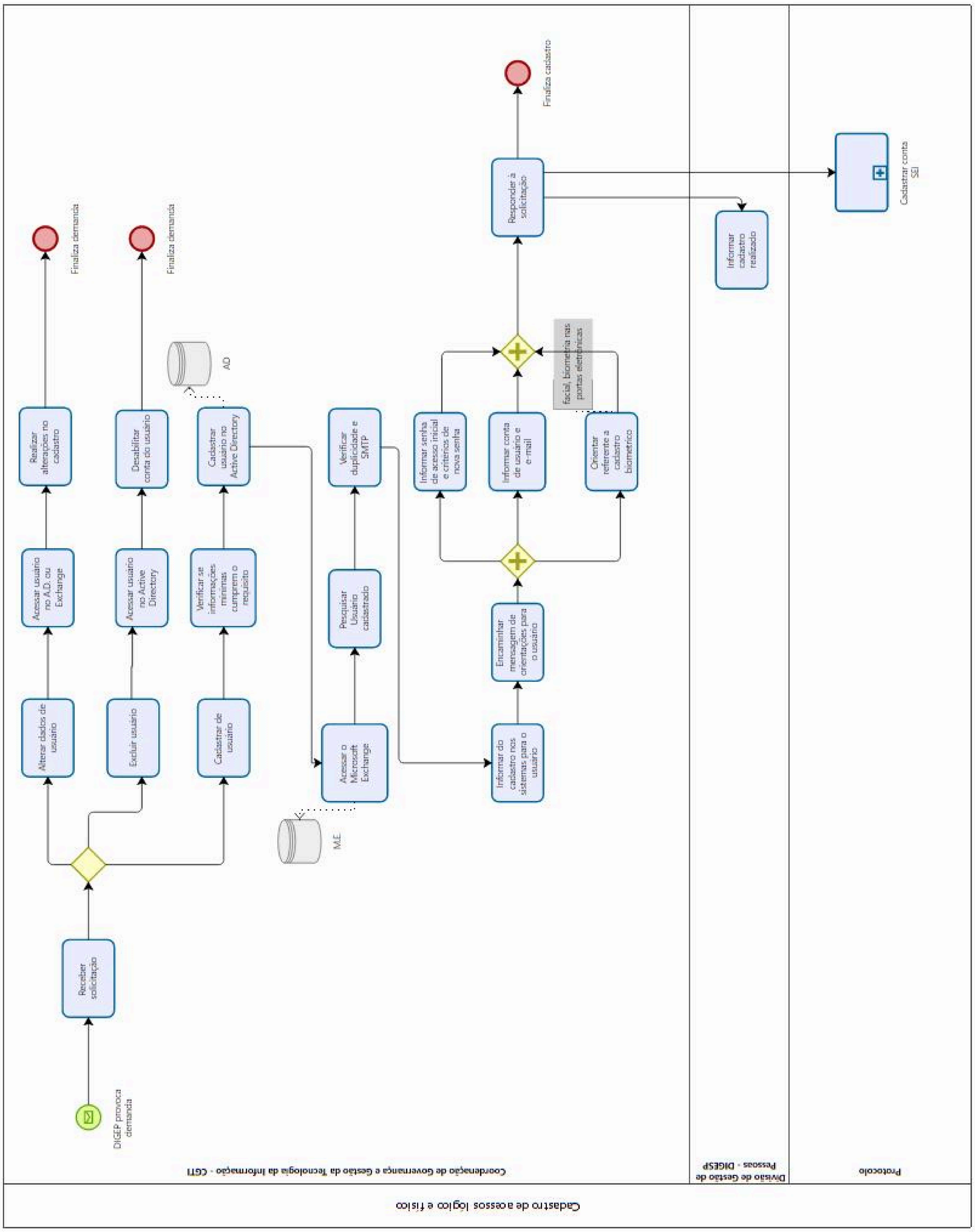
É diretriz do IPREV-DF que servidores e colaboradores bloqueiem suas estações de trabalho sempre que se ausentarem da mesa (mesmo que por poucos minutos) e não deixem documentos sensíveis ou senhas anotadas expostas fisicamente.

9. Regime Disciplinar e Sanções

- **Falsa Identidade:** O uso de senhas ou dispositivos de terceiros configura crime de falsa identidade (Art. 307 do Código Penal).
- **Uso de Software:** A instalação de softwares não licenciados é infração grave com consequências legais e financeiras.
- **Sanções Administrativas:** O uso inadequado de recursos de TIC ou violação das normas de segurança pode resultar em advertências e sanções disciplinares, além de responsabilidade civil e criminal.
- **Sigilo Funcional:** Divulgar dados obtidos nos sistemas para terceiros não envolvidos na atividade constitui quebra de sigilo funcional.

Diretriz de Contingência: Em situações de emergência (incêndio, sinistros ou falhas críticas de sistema), os controles de acesso físico devem priorizar a **segurança da vida** (saída livre), enquanto os controles lógicos devem acionar os protocolos de backup e recuperação previstos no Plano de Continuidade de Negócios.

FLUXOGRAMA



Cadastro de acesso lógico e físico		
Protocolo	Divisão de Gestão de Pessoas - DIGESP	Coordenação de Governança e Gestão da Tecnologia da Informação - CGTI

DISPOSIÇÕES FINAIS

Este manual formaliza o controle de acesso físico e lógico para proteger os ativos de informação do IPREV-DF.

Objetiva garantir a confidencialidade, integridade e disponibilidade dos dados previdenciários dos segurados.

Aplica-se a todos os servidores, estagiários e prestadores de serviço com acesso aos sistemas.

Estabelece restrições em áreas sensíveis com uso de biometria e registros de monitoramento.

Define senhas pessoais intransferíveis e acesso limitado ao menor privilégio necessário na rede.

Obriga a notificação imediata de incidentes de segurança para contenção e resposta rápida. Regula o acesso remoto via VPN e exige requisitos mínimos de segurança em dispositivos particulares.

Mudanças em sistemas devem ser formalmente aprovadas para mitigar riscos operacionais.

A conformidade assegura a proteção da privacidade e a continuidade dos serviços institucionais.

IPREV DF

Instituto de Previdência dos
Servidores do Distrito Federal