Instituto de Previdência dos
Servidores do Distrito Federal

Manual do Processo
Gestão de Usuário de Rede

2025 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
Célia Maria Ribeiro de Sales

Diretor de Previdência
Pedro Henrique Araújo Nabarrete Gabini

Diretor Jurídico
Luiz Gustavo Barreira Muglia

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

Coordenação De Governança Gestão De Tecnologia Da Informação

EDIÇÃO GRÁFICA

Unidade de Comunicação Social
Maria Eduarda Costa Gonzaga

Sumário

MENSAGEM DA DIRETORA-PRESIDENTE

A gestão adequada dos acessos aos sistemas institucionais é um dos pilares para a segurança da informação, a continuidade dos serviços e a integridade dos dados públicos. Nesse contexto, apresento o Manual do Processo de Gestão de Usuário de Rede do Instituto de Previdência dos Servidores do Distrito Federal (Iprev-DF).

Este manual tem como objetivo padronizar os procedimentos de cadastro, alteração e desativação de usuários de rede, assegurando que todas as etapas sejam realizadas de forma controlada, rastreável e em conformidade com as normas internas, com as boas práticas de governança de tecnologia da informação e com a legislação vigente, especialmente a Lei Geral de Proteção de Dados Pessoais (LGPD).

A atuação da Coordenação de Governança e Gestão da Tecnologia da Informação, aliada à definição clara de responsabilidades, fluxos e controles, contribui para a mitigação de riscos, a prevenção de acessos indevidos e o fortalecimento da segurança do ambiente tecnológico do Instituto.

Ressalto a importância do cumprimento das orientações aqui estabelecidas por todas as áreas envolvidas, reconhecendo que a gestão responsável de usuários de rede é essencial para a proteção das informações institucionais e para a eficiência administrativa.

Agradeço às equipes técnicas pela elaboração deste manual e reafirmo o compromisso do Iprev-DF com o aprimoramento contínuo de seus processos, em consonância com os princípios da boa governança pública, da transparência e da segurança da informação.

Raquel Galvão Rodrigues da Silva

INTRODUÇÃO

Este manual tem como objetivo documentar os procedimentos para cadastro, alteração e desativação de usuários de rede no âmbito do Instituto de Previdência dos Servidores do Distrito Federal.

O processo é conduzido pela equipe da Coordenação de Governança e Gestão da Tecnologia da Informação, seguindo as diretrizes estabelecidas pela notação BPMN 2.0 (Business Process Model and Notation).

Este documento busca padronizar as práticas de gestão de usuários, garantindo consistência, segurança e rastreabilidade, além de contribuir para a integridade do ambiente de tecnologia da informação do Instituto.

DESCRIÇÃO GERAL DO PROCESSO

O processo de gestão de usuários de rede tem início a partir de uma solicitação formal, encaminhada por e-mail ou sistema, referente ao cadastro de novo usuário, alteração de dados cadastrais ou desativação de conta, geralmente motivada por mudanças funcionais ou desligamento do servidor do Instituto.

Após o recebimento, a solicitação é analisada pela equipe da Coordenação de Governança e Gestão da Tecnologia da Informação (CGTI), que valida as informações fornecidas quanto à completude e conformidade com os requisitos internos. Com base no tipo de demanda, são executadas ações específicas nos sistemas corporativos: Microsoft Active Directory, Microsoft Exchange e Sistema Eletrônico de Informações (SEI).

As atividades envolvem a criação, alteração ou desativação de contas de rede, bem como o gerenciamento de permissões de acesso, endereços de e-mail institucionais e registro formal no SEI. Ao término do atendimento, é realizada a comunicação formal com o solicitante e a devida documentação da ação executada.

Todas as etapas do processo devem ser registradas de forma íntegra e rastreável, respeitando as políticas de governança de TI e as normas legais de proteção de dados pessoais vigentes, em especial a Lei Geral de Proteção de Dados (LGPD).

TABELA DE ATIVIDADES

Atividade	Descrição	Responsável
Receber solicitação	Recebimento de solicitação via e-mail ou sistema.	CGTI
Diferenciar tipo de solicitação	Alterar, Excluir ou cadastrar usuário.	CGTI
Alterar dados de usuário	Acessar usuário no A.D. ou Exchange	CGTI
Excluir usuário	Acessar usuário no A.D.	CGTI
Cadastrar usuário no Active Directory	Criação de conta de usuário na rede.	CGTI
Verificar se informações mínimas cumprem o requisito	Análise da documentação recebida.	CGTI
Acessar Microsoft Exchange	Acesso para conferência e cadastro de e-mail.	CGTI
Pesquisar usuário cadastrado	Verificação de duplicidade.	CGTI
Verificar duplicidade e SMTP	Confirmação de dados técnicos no Exchange.	CGTI
Informar cadastro realizado	Envio de confirmação ao solicitante.	CGTI
Responder à solicitação	Retorno formal com os dados de acesso.	CGTI
Encaminhar mensagem de orientações	Instruções sobre uso inicial da conta.	CGTI
Receber e-mail para cadastro no SEI	Registro formal da solicitação	Protocolo
Informar conta de usuário e e-mail	Envio dos dados ao usuário.	CGTI
Informar senha de acesso inicial	Definição de critérios e envio de senha temporária.	CGTI

Orientar sobre cadastro biométrico	Orientações sobre acesso facial e digital.	CGTI
Finaliza cadastro	Confirmação de encerramento do processo.	CGTI

TECNOLOGIAS E FERRAMENTAS UTILIZADAS

- Microsoft Active Directory
- Microsoft Exchange
- Outlook (e-mail institucional)
- Sistema Eletrônico de Informações - SEI
- Editor de fluxoBPMN 2.0 (ex: Bizagi)

ETAPAS DETALHADAS DO PROCESSO

ETAPA 1: RECEBIMENTO DA SOLICITAÇÃO

- Origem: DIGEP ou outro setor demandante.
- Meio de comunicação: E-mail institucional enviado à Coordenação de Governança e Gestão da Tecnologia da Informação (CGTI).
- Ações: Verificação da completude das informações obrigatórias: nome completo, CPF, setor de lotação, telefone de contato e tipo de acesso solicitado

ETAPA 2: VERIFICAR TIPO DE SOLICITAÇÃO

- Identificação do tipo de solicitação: cadastro, alteração ou exclusão de usuário.
- Registro inicial da solicitação no sistema interno ou planilha de controle.
- Esta é uma atividade manual, realizada pela equipe da CGTI.

ETAPA 3: ALTERAR USUÁRIO

- Acesso ao Active Directory (AD) e/ou MicrosoftExchange.
- Verificação de grupos, permissões e dados vinculados.
- Atualização de informações conforme solicitação.

ETAPA 3.1: ANÁLISE DE DADOS PARA ALTERAÇÃO DE USUÁRIO

- Validação das informações fornecidas.
- Ajustes em campos específicos conforme diretrizes internas.
- Registro da atividade para controle e auditoria.

ETAPA 4: EXCLUIR USUÁRIO

- Acesso ao Active Directory para desabilitação ou exclusão da conta.
- Cancelamento de acessos vinculados (e-mail, grupos, sistemas internos).

ETAPA 4.1: ANÁLISE DE DADOS PARA EXCLUSÃO DE USUÁRIO

- Conferência final dos dados antes da desativação.
- Garantia de que a conta está fora de uso e sem impacto em processos internos.

ETAPA 5: ANÁLISE E VALIDAÇÃO PARA CADASTRO DE USUÁRIO

- Verificação dos requisitos mínimos para criação da conta (dados pessoais, função, setor, autorização formal).
- Esta etapa antecede a automação do cadastro e visa garantir conformidade.

ETAPA 5.1: CADASTRO NO ACTIVE DIRECTORY (AD)

- Criação de login e senha provisória.
- Atribuição de grupos, permissões e políticas de acesso.
- Registro técnico da conta no sistema de controle de TI.
- Atividade automatizada, com revisão técnica pela equipe.

ETAPA 5.2: CADASTRO DE E-MAIL NO MICROSOFT EXCHANGE

- Verificação da existência prévia de conta.
- Geração de endereço SMTP e vinculação ao AD.
- Atividade automatizada, monitorada pela equipe técnica.

ETAPA 5.3: COMUNICAÇÃO AO USUÁRIO

- Envio de dados de acesso ao usuário contendo login, endereço de e-mail e senha provisória.
- Instruções sobre troca de senha, uso seguro da conta e diretrizes de acesso.

ETAPA 5.4: ENCAMINHAR PARA CADASTRO E REGISTRO NO SEI

- Encaminhamento da solicitação e resposta ao setor de Protocolo, para formalização no SEI (Sistema Eletrônico de Informações).
- Arquivamento da comunicação e documentação de respaldo.

ETAPA 5.5: ORIENTAÇÃO SOBRE BIOMETRIA E ACESSO FÍSICO

- Encaminhamento de orientações para o cadastro de biometria facial e digital, quando aplicável.
- Instruções para uso de sistemas de controle de acesso físico.
- Esta atividade ocorre em paralelo e é realizada manualmente.

ETAPA 6: FINALIZAÇÃO

- Confirmação de que todas as etapas foram concluídas com sucesso.
- Atualização dos registros interno se fechamento da demanda.

ETAPA 7: RESPOSTA AO DEMANDANTE E OUTRAS ÁREAS

- Comunicação ao setor solicitante informando a conclusão do processo (cadastro, alteração ou exclusão).
- Encaminhamento ao Protocolo das atividades realizadas.
- Fechamento formal da solicitação.

PROCESSOS PARALELOS E COMPLEMENTARES

Além do fluxo principal de cadastro, alteração e desativação de usuários, existem atividades que podem ocorrer de forma paralela ou complementar ao processo principal. A adequada coordenação dessas ações é essencial para evitar inconsistências, atrasos ou retrabalho.

Recomenda-se atenção especial aos seguintes processos:

- Alteração de permissões de acesso: Pode ser executada paralelamente ao cadastro de novos usuários, principalmente em situações emergenciais em que é necessário conceder acessos temporários ou adicionais. Deve ser acompanhada de autorização formal e registrada adequadamente.

- Desativação de contas por desligamento funcional: A desativação de contas ocorre mediante solicitação da Divisão de Gestão de Pessoas (DIGEP), com base em processos de desligamento, aposentadoria, exoneração ou movimentação interna. A solicitação deve ser clara quanto ao prazo e tipo de desligamento, e deve conter a documentação de respaldo.
- Solicitações de acesso a sistemas específicos: Algumas solicitações envolvem permissões específicas para sistemas internos ou ferramentas de gestão. Nestes casos, o processo de gestão de usuários pode ser complementado por fluxos adicionais de homologação e validação junto às áreas responsáveis pelos sistemas.
- Cadastro biométrico e liberação de acesso físico: Após a criação da conta de rede e validação dos dados, o usuário poderá ser orientado a realizar o cadastro de biometria facial e/ou digital. Este processo é conduzido por área específica e deve ocorrer somente após a confirmação do cadastro eletrônico pela CGTI.
- Manutenção e sincronização de contas: Em alguns casos, a equipe técnica realiza rotinas periódicas de sincronização entre o Active Directory e demais sistemas institucionais, assegurando a integridade dos dados e a continuidade do acesso.
- Monitoramento de contas inativas: Contas sem uso por períodos prolongados devem ser identificadas, analisadas e, se necessário, desativadas conforme critérios de segurança e política de uso aceitável de recursos de TI.

Esses processos devem ser acompanhados com atenção e devidamente integrados ao fluxo principal para assegurar a conformidade com as políticas internas e com a legislação vigente, incluindo a Lei Geral de Proteção de Dados (LGPD) e normas de segurança da informação.

PONTOS CRÍTICOS (GARGALOS)

PROCESSO

- Criação e exclusão de usuários manualmente: pode gerar lentidão, retrabalho e falhas humanas.
- Falta de padronização de procedimentos: diferentes responsáveis podem seguir fluxos distintos, o que compromete a segurança e a rastreabilidade.

SEGURANÇA

- Atraso na revogação de acessos de ex-servidores ou usuários inativos: representa risco grave de segurança.
- Permissões excessivas (privilégios não mínimos): usuários mantêm acessos desnecessários por falta de revisão periódica.
- Controle deficiente de grupos de acesso: grupos mal organizados geram confusão e erros de atribuição.

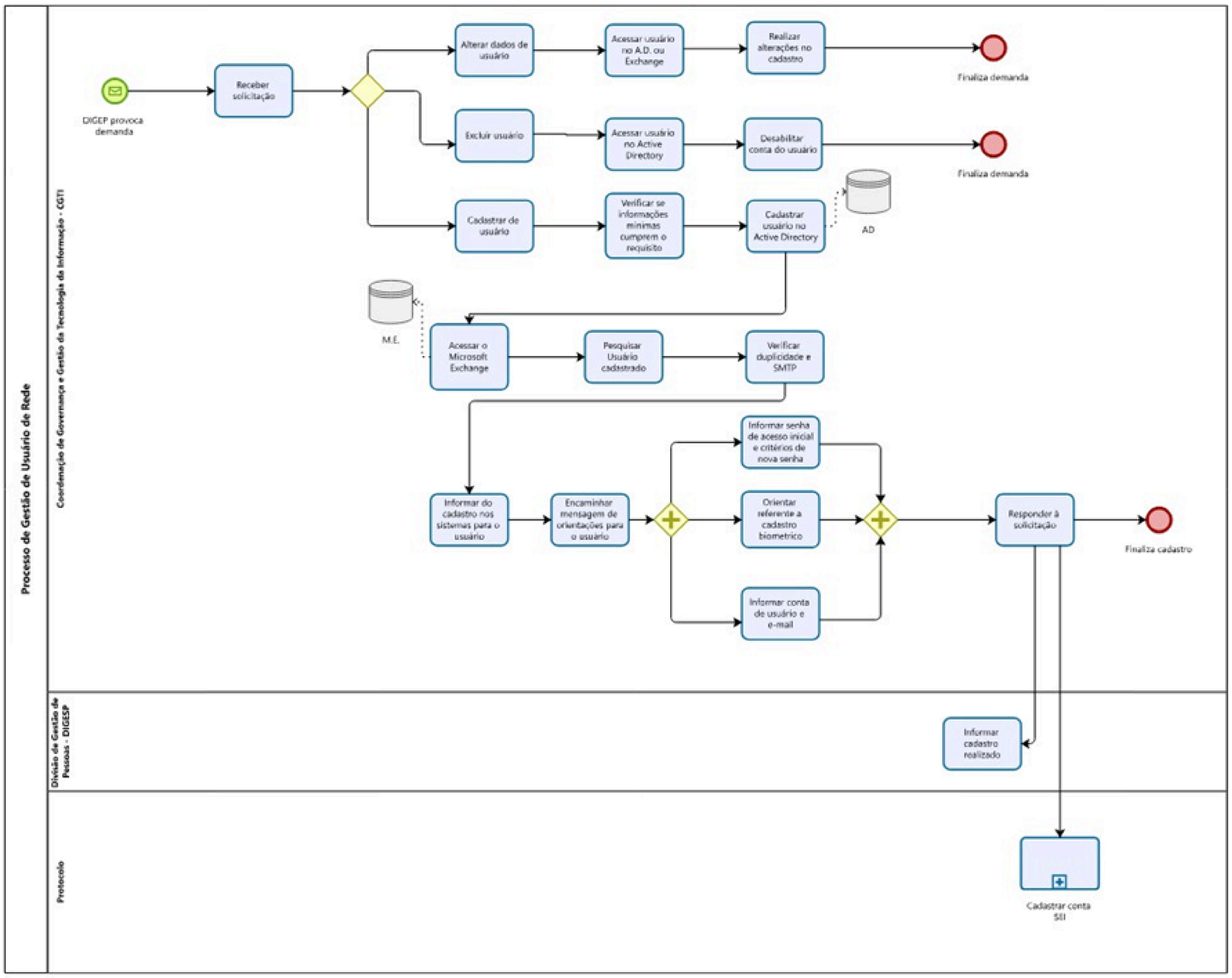
OBSERVAÇÕES E BOAS PRÁTICAS

Para garantir a segurança, eficiência e integridade do processo de gestão de usuários, recomenda-se a adoção das seguintes boas práticas:

- **Verificar a autenticidade da solicitação:** Confirmar as informações diretamente com o solicitante ou responsável pela unidade antes de iniciar o processo, a fim de evitar fraudes, erros ou retrabalho.
- **Assegurar a completude dos dados recebidos:** Conferir se a solicitação contém todas as informações obrigatórias, como nome completo, CPF, setor de lotação, tipo de acesso, e autorização formal.
- **Adaptar o processo conforme a infraestrutura disponível:** Ajustar procedimentos de acordo com os recursos tecnológicos da instituição, sem comprometer os critérios de segurança e padronização.
- **Revisar periodicamente scripts e automações:** Monitorar ferramentas automatizadas (como scripts de provisionamento ou sincronização de contas) para prevenir falhas ou comportamentos indevidos.
- **Manter controle de acessos e permissões:** Revisar periodicamente os acessos concedidos aos usuários, evitando privilégios excessivos ou desnecessários, conforme o princípio do menor privilégio.
- **Aplicar políticas de senha seguras:** Garantir que as senhas provisórias respeitem critérios mínimos de complexidade e expirem em prazo adequado, orientando o usuário quanto à troca imediata.
- **Capacitar a equipe técnica regularmente:** Promover treinamentos contínuos sobre ferramentas utilizadas, normas internas e legislações aplicáveis, como a LGPD.
- **Atualizar o manual conforme mudanças tecnológicas ou normativas:** Manter este documento sempre alinhado com as práticas mais recentes, revisando-o sempre que houver alterações relevantes nos sistemas ou nas diretrizes institucionais.

FLUXOGRAMA BPMN DO PROCESSO

Abaixo está o fluxograma do processo conforme as regras do BPMN 2.0



Gestão de usuário de rede	
Autor:	CGTI
Versão:	1.0
Descrição:	Processo SEI: 00413-00000520/2025-81

REFERÊNCIAS

FONTES NORMATIVAS E INSTITUCIONAIS

- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais – LGPD. Diário Oficial da União: Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.
- BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. Estabelece regras sobre governança no compartilhamento de dados no setor público. Diário Oficial da União: Brasília, DF, 10 out. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm.
- BRASIL. Lei nº 14.133, de 1º de abril de 2021. Nova Lei de Licitações e Contratos Administrativos. Diário Oficial da União: Brasília, DF, 1 abr. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14133.htm.

BOAS PRÁTICAS E PADRÕES TÉCNICOS

- ALLWEYER, Thomas. BPMN – Modelagem de Processos de Negócio com BPMN. 2. ed. Rio de Janeiro: Brasport, 2016.
- ISO/IEC. Norma 27001:2022 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Genebra: International Organization for Standardization, 2022.
- ISO/IEC. Norma 27002:2022 – Código de práticas para controles de segurança da informação. Genebra: International Organization for Standardization, 2022.
- ISACA. COBIT 2019 Framework: Governance and Management Objectives. Rolling Meadows: ISACA, 2019.
- OGC. ITIL Foundation – IT Infrastructure Library. Londres: The Stationery Office, 2019.

PLATAFORMAS E FERRAMENTAS

- MICROSOFT. Active Directory Domain Services Overview. Redmond, WA: Microsoft, 2024. Disponível em: https://learn.microsoft.com/en-us/windows-server/identity/active-directory-domain-services.
- MICROSOFT. Exchange Server Documentation. Redmond, WA: Microsoft, 2024. Disponível em: https://learn.microsoft.com/en-us/exchange/.
- MICROSOFT. Exchange Online PowerShell. Redmond, WA: Microsoft, 2024. Disponível em: https://learn.microsoft.com/en-us/powershell/exchange/exchange-online-powershell.

GDF, SEI E ÓRGÃOS LOCAIS

- GOVERNO DO DISTRITO FEDERAL. Portal Institucional do GDF. Brasília, DF: GDF, 2025. Disponível em: https://www.df.gov.br/.
- SEPLAD – SECRETARIA DE ESTADO DE PLANEJAMENTO, ORÇAMENTOE
- ADMINISTRAÇÃO DO DF. Portal Institucional. Brasília, DF: SEPLAD,2025. Disponível em: https://www.seplad.df.gov.br/.
- GOVERNO DO DISTRITO FEDERAL. Sistema Eletrônico de Informações – SEI/DF. Brasília, DF: GDF, 2025. Disponível em: https://www.sei.df.gov.br/.

MODELAGEM DE PROCESSOS (BPMN)

- OMG – OBJECT MANAGEMENT GROUP. BPMN 2.0 Specification – Business Process Model and Notation. Needham, MA: OMG, 2014. Disponível em: https://www.omg.org/spec/BPMN/2.0/.
- ·ABPMP BRASIL. Guia BPM CBOK – Guia de Conhecimento em Gerenciamento de Processos de Negócio. São Paulo: ABPMP Brasil, 2017. Disponível em: https://www.abpmp-br.org/.

IPREV DF

Instituto de Previdência dos
Servidores do Distrito Federal