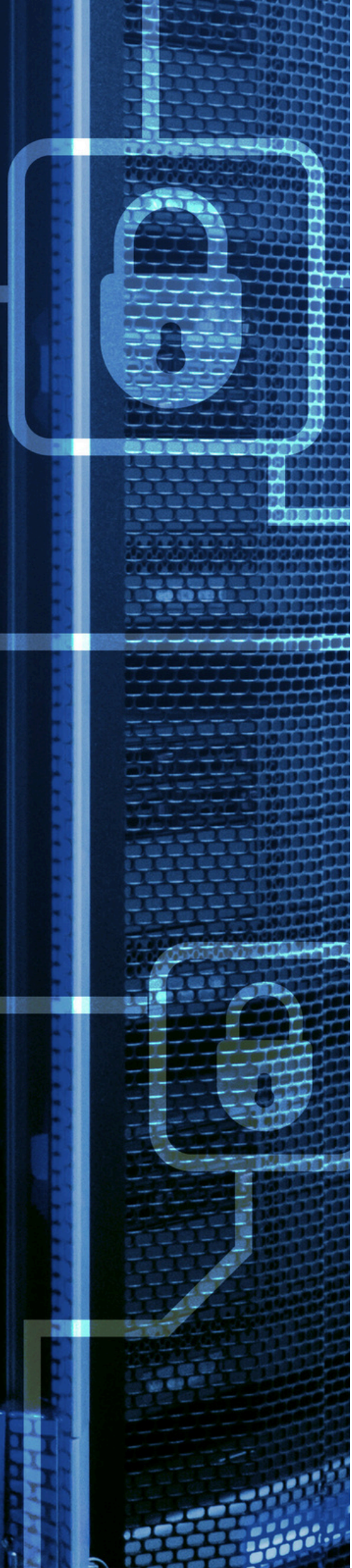
MANUAL DE *CONTINGÊNCIA,* CONTINUIDADE DE NEGÓCIOS *E CONTROLE DE ACESSOS*

PREFEITURA RIO | Administração Previ-Rio



PREVI-RIO

AUTARQUIA GESTORA DO FUNPREVI

PRESIDENTE

BERNARDO EGAS LIMA FONSECA

COORDENADORA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

FERNANDA NUNES LEIROZ

EQUIPE DA COORDENAÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (PRE/CTIC)

ALEXANDRE FERREIRA TAVARES

CESAR AUGUSTO PEREIRA PEIXOTO

DENISE MARIANO CORRÊA

FABIO LUIZ LOPES FERREIRA

GILSON VAGUINER DOS SANTOS JUNIOR

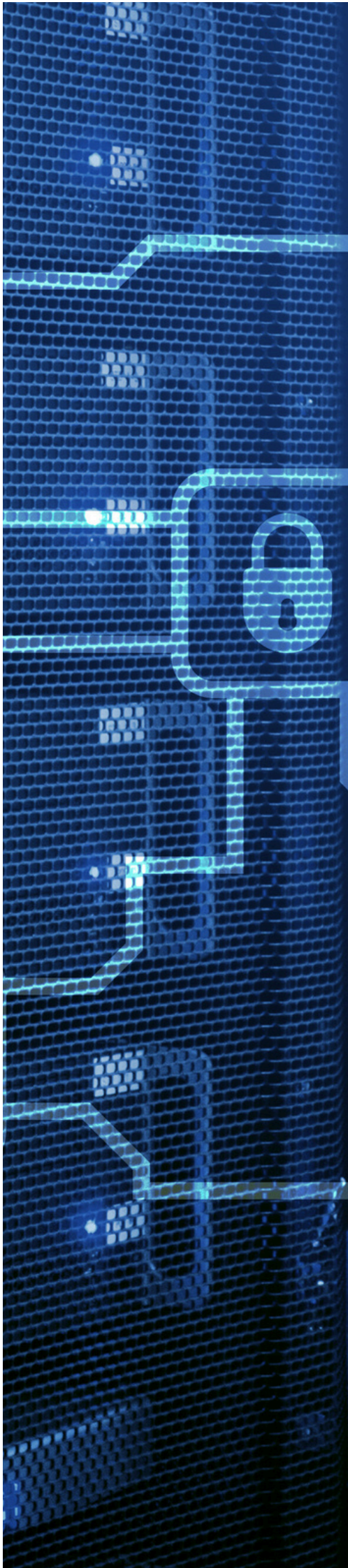
JACKELINE FERNANDA DE OLIVEIRA

MARCELO MOTA DAS VIRGENS

PAULO ROBERTO RODRIGUES MARIM JUNIOR

PAULO ROBERTO XAVIER DE CARVALHO

Índice



1. INTRODUÇÃO E OBJETIVOS

Este manual tem por objetivo orientar sobre as ações necessárias para a realização do controle de acesso (físico e lógico) e dos procedimentos de contingência.

As diretrizes aqui descritas baseiam-se nos princípios fundamentais da Segurança da Informação:

- **Confidencialidade**: garantia de que as informações sejam acessadas apenas por indivíduos autorizados.
- **Integridade**: manutenção da precisão e completude das informações, protegidas contra perda, dano ou modificação não autorizada.
- **Disponibilidade**: garantia de que as informações e os processos autorizados estejam acessíveis sempre que necessários.
- **Autenticidade**: garantia de que os ativos da informação identificados como remetentes ou destinatários sejam, de fato, quem afirmam ser. Refere-se à veracidade das identidades envolvidas em um processo de comunicação.

A Continuidade de Negócios é um objetivo central deste manual. Refere-se à capacidade estratégica e tática do PREVI-RIO de planejar e responder a incidentes que possam causar interrupções, visando minimizar impactos e manter as operações em níveis aceitáveis de disponibilidade previamente definidos.

2. APLICAÇÃO E ABRANGÊNCIA

Este manual é dirigido às seguintes pessoas:

• Agente Público (independentemente de sua função, cargo ou vínculo empregatício).

• Prestador de Serviço.

• Estagiário.

• Qualquer pessoa física ou jurídica autorizada a tratar informações do PREVI-RIO, FUNPREVI e FASS em quaisquer meios (físicos ou digitais).

3. COMPETÊNCIAS E RESPONSABILIDADES

3.1. ÁREAS RESPONSÁVEIS

São responsáveis pelo processo de controle de acesso e contingência:

- **PREVI-RIO/PRE/CTIC** — Coordenação de Tecnologia da Informação e Comunicação**;**
- **IPLANRIO** — Empresa Municipal de Informática, prestadora de serviços de administração dos recursos de Tecnologia da Informação e Comunicação (TIC).

A IPLANRIO também é responsável por instituir e coordenar o Grupo de Prevenção, Tratamento e Resposta a Incidentes, bem como elaborar, implantar e gerenciar o Programa de Continuidade de Negócios dos serviços corporativos..

3.2. RESPONSABILIDADE DO USUÁRIO

Compete aos usuários dos ativos de informação:

- Tratar a informação de acordo com sua classificação, adotando as medidas de proteção correspondentes.
- Comunicar imediatamente ao chefe imediato, ou ao preposto (no caso de prestadores de serviço), quaisquer desvios ou incidentes de segurança.
- Manter-se atualizado quanto às políticas e normas de segurança vigentes.

4. CONTROLES DE ACESSO

O controle de acesso aos ativos da informação deve ser regido por um processo formal, que contemple a criação, manutenção, suspensão e exclusão de acessos.

4.1. ACESSO LÓGICO

O acesso aos sistemas e à rede corporativa deve ocorrer mediante identificação individual, com credenciais de uso pessoal e intransferível.

4.1.1. Procedimento de Logon

No PREVI-RIO, o logon é realizado em rede, com autenticação por servidor.

É criado um login e uma senha individual, que deve ser obrigatoriamente alterada no primeiro acesso.

O processo é efetuado pressionando **"Ctrl + Alt + Delete"** e digitando o Login e a Senha, confirmando a entrada no domínio "RIO".

4.1.2. Requisitos de Senha

A senha deve atender aos seguintes requisitos mínimos:

- Mínimo de 10 caracteres.
- Pelo menos 1 letra maiúscula.
- Pelo menos 1 letra minúscula.
- Pelo menos 1 número.

4.1.3. Diretrizes de Segurança

As autorizações de acesso devem ser restritas aos privilégios mínimos necessários para o desempenho das funções do usuário.

Recomenda-se:

- Utilizar senhas fortes e únicas.
- Não compartilhar credenciais.
- Bloquear a estação de trabalho ao se ausentar (atalho: Windows + L).

4.2. ACESSO FÍSICO

As medidas de proteção adotadas pelo PREVI-RIO devem ser proporcionais aos riscos identificados.

Os recursos de informação essenciais às atividades são armazenados em áreas de acesso restrito, protegidas contra ameaças naturais e humanas, com controle biométrico de acesso.

O acesso de visitantes às áreas que abrigam recursos críticos é autorizado por agente competente e supervisionado por representante designado.

5. PROCEDIMENTOS DE CONTINGÊNCIA E RECUPERAÇÃO

Este manual formaliza os procedimentos de contingência e continuidade, cobrindo possíveis falhas e assegurando a manutenção das operações essenciais.

5.1. GESTÃO DE INCIDENTES

A gestão de incidentes deve seguir processo formal que inclua detecção, triagem, análise e resposta.

O objetivo do Plano de Gerenciamento de Incidentes é restabelecer os sistemas à normalidade dentro dos prazos previstos.

5.1.1. Tratamento de Falhas no Logon

PROBLEMA	PROCEDIMENTO	RESPONSÁVEL
Senha Incorreta	Verificar maiúsculas/minúsculas, usuário e domínio; caso a senha tenha sido atualizada recentemente, testar novamente. Se o problema persistir, abrir chamado para o suporte.	Usuário/ CTIC
Falha na relação de Segurança	Acionar o suporte, pois o computador perdeu a relação de confiança com o servidor de autenticação.	CTIC/ Suporte
Servidor de domínio indisponível	Verificar conexão física do cabo de rede (luzes acesas); se apagadas, acionar o suporte; se acesas, reiniciar o computador. Caso o servidor de autenticação esteja fora do ar, abrir chamado para reparo.	Usuário/ CTIC
Usuário bloqueado	Solicitar o desbloqueio junto ao suporte técnico.	CTIC/ Suporte
Senha não atende aos requisitos mínimos / falha na alteração	Verificar se a nova senha cumpre os requisitos mínimos (10 caracteres, letras maiúsculas e minúsculas, números) e se a senha antiga foi digitada corretamente.	Usuário

5.1.2. Resposta a Ataques de Vírus

Todos os computadores do Instituto possuem antivírus instalado.

Em caso de detecção e aviso na tela:

- **Não interagir com o computador.**
- **Contatar imediatamente a CTIC para a resolução do problema.**

5.1.3. Contato e Suporte

Em caso de dúvidas ou necessidade de auxílio, o usuário deve abrir um chamado junto ao suporte de TI, por meio do portal: http://iplanfacil.prefeitura.rio.

5.2. GUARDA E RECUPERAÇÃO DE INFORMAÇÕES (BACKUPS)

O sistema de informação do PREVI-RIO deve ser coberto por um processo formal e estruturado de guarda e recuperação, garantindo disponibilidade e integridade dos dados.

- As estratégias de backup devem assegurar níveis de disponibilidade, capacidade e agilidade de recuperação compatíveis com a criticidade das informações.
- A integridade dos backups e da infraestrutura de armazenamento deve ser testada periodicamente.
- Em casos de alienação ou descarte de ativos, os procedimentos devem respeitar a classificação da informação neles contida, prevenindo vazamentos ou perdas de dados sensíveis.

A IPLANRIO, em coordenação com a CTIC/PREVI-RIO, é responsável por garantir e manter o Programa de Continuidade de Negócios, incluindo as estratégias de recuperação.

6. REVISÃO E APRIMORAMENTO CONTÍNUO

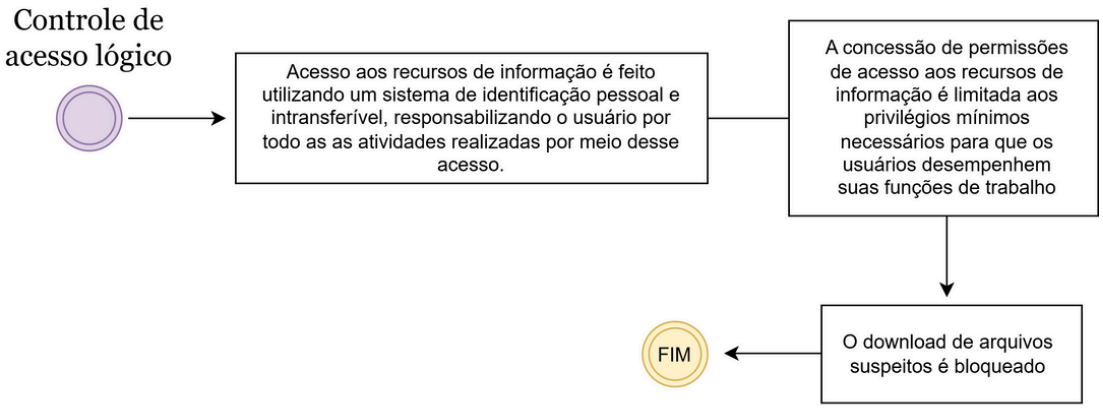
Para assegurar a melhoria contínua da gestão, o Plano de Gerenciamento de Incidentes deve ser documentado, revisado e testado periodicamente.
Além disso, programas permanentes de sensibilização e conscientização em Segurança da Informação devem ser oferecidos aos agentes públicos.

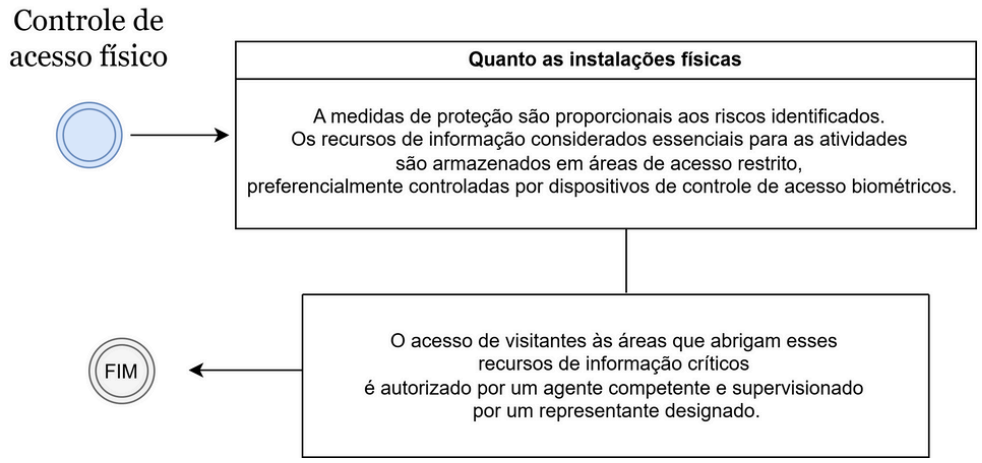
7. LEGISLAÇÃO APLICÁVEL

- Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais (LGPD)
- Decreto Rio n.º 53.700, de 8 de dezembro de 2023
- Resolução CVL n.º 216, de 15 de dezembro de 2023
- NBR ISO/IEC 17799.

8. MAPEAMENTO

8.1. CONTROLES DE ACESSO FÍSICO E DE ACESSO LÓGICO





8.2. PROCEDIMENTO DE CONTINGÊNCIA