

UNIDADE GESTORA: Instituto de Previdência Social dos Servidores Públicos do Município de Balneário Camboriú.

DIRETORIA EXECUTIVA

Diretor-Presidente: João Olindino Koeddermann

Diretor Financeiro: Jackson Fernando de Medeiros

Diretor de Benefícios: Robson Luiz de Moraes Ortiz

Manual de Controle de Acesso Físico e Lógico

1. Objetivo

Garantir a segurança das informações e dos ambientes físicos.

Padronizar procedimentos de acesso físico (instalações, documentos, visitantes) e lógico (sistemas, senhas, credenciais).

Assegurar conformidade com legislações e políticas de segurança da informação.

2. Regulamentação e Referências

Política de Segurança da Informação (PSI/PPSI).

Leis municipais e portarias ministeriais aplicáveis (ex.: Lei 9.717/1998, EC 103/2019).

Normas internas de cada RPPS.

Código de Ética institucional.

Planos de Contingência e Backup.

3. Responsabilidades

Setor/Órgão	Responsabilidades
Recepção/Protocolo	Identificação de pessoas e documentos, registro de entrada/saída, encaminhamento.
Assessoria de	Criação e gestão de credenciais, monitoramento de

Setor/Órgão	Responsabilidades
Informática / TI	acessos, suporte técnico.
Controle Interno	Declaração de conformidade, auditoria de processos.
Diretoria Executiva	Deliberação e autorização final.
Jurídico	Pareceres em caso de não conformidade.
Usuários/Servidores	Uso responsável das credenciais, participação em treinamentos, comunicação de incidentes.

4. Processo de Acesso Físico

1. Identificação do visitante na recepção.
2. Registro em livro ou sistema de controle.
3. Direcionamento ao setor competente.
4. Acompanhamento até a área indicada, respeitando protocolos de segurança.
5. Atendimento cordial e objetivo.
6. Encerramento com registro de saída.

-Indicadores de desempenho: tempo de atendimento, registros completos, ausência de incidentes.

5. Processo de Acesso Lógico

1. Solicitação de acesso via ficha cadastral ou abertura de chamado.
2. Conferência e validação dos dados pelo setor responsável.
3. Criação de credenciais (login e senha provisória).
4. Primeiro acesso com troca obrigatória de senha.
5. Definição de perfil de acesso conforme necessidade de conhecer.
6. Monitoramento contínuo (logs, auditorias).
7. Bloqueio ou exclusão de acesso em caso de desligamento ou não conformidade.

- **Indicadores de desempenho:** tempo de liberação, conformidade com perfis, incidentes reportados.

6. Gestão de Riscos

Legal: conformidade com legislação vigente.

Operacional: falhas humanas ou técnicas.

Reputacional: conduta ética e transparente.

Tecnológico: vulnerabilidades de sistemas e equipamentos.

7. Contingência e Backup

Cópias de segurança automáticas em nuvem e/ou servidores locais.

Backups manuais sob responsabilidade dos usuários.

Plano de contingência ativado em caso de falhas críticas.

Acompanhamento por TI em manutenções externas.

8. Disposições Finais

O manual deve ser atualizado sempre que houver mudanças legais ou tecnológicas.

Alterações propostas pela TI, Controle Interno ou Comissão de Segurança devem ser submetidas à Diretoria Executiva.

O cumprimento das etapas é obrigatório e auditável.