



# Norma Gestão de Acesso Físico

## SUMÁRIO

1. Objetivo .....	3
2. Campo de aplicação .....	3
3. Definições .....	3
4. PAPÉIS E RESPONSABILIDADES.....	4
4.1. Recepção.....	4
4.2. Departamento Pessoal .....	4
4.3. Equipe de Infraestrutura de TI.....	4
4.4. Equipe de Manutenção / Brigada de Incêndio .....	4
5. DESCRIÇÃO .....	5
5.1. Procedimentos e Controles de Acesso Físico .....	5
5.1.1. Áreas comuns de circulação .....	5
5.1.2. Ambientes de acesso restrito .....	5
5.2. Proteção dos Ambientes Restritos .....	5
5.2.1. Proteção física dos ativos de informação.....	5
5.2.2. Controles ambientais.....	6
5.2.3. Continuidade dos ativos de informação .....	6
5.3. Revisões e Testes Periódicos .....	7
6. Evidências geradas .....	7
7. DOCUMENTOS DE REFERÊNCIA.....	8
8. REGISTRO DE ALTERAÇÕES.....	8
9. FORMALIZAÇÃO .....	8

## 1. OBJETIVO

Esta Norma descreve as regras e os controles aplicáveis à gestão de acesso físico, tanto dos ambientes comuns quanto dos ambientes restritos de processamento de informações. Inclui medidas e mecanismos para garantir a segurança física, a continuidade dos ativos de informação e seus respectivos controles ambientais.

## 2. CAMPO DE APLICAÇÃO

Aplicável a todos os colaboradores, próprios ou terceiros, que utilizam recursos de TI fornecidos pelo **Grupo Benner\*** para o exercício de suas atividades.

\* Denominação utilizada para designar as empresas: Benner Sistemas S.A., Benner Tecnologia e Sistemas em Saúde Ltda., Benner Tecnologia e Serviços em Saúde Ltda., Otto HX Tecnologia e Sistemas Ltda e Itessa Tecnologia e Serviços S.A.

## 3. DEFINIÇÕES

- **Ativos de Informação:** Toda e qualquer pessoa, processo, tecnologia ou ambiente que manipule, processe, armazene, transporte, transmita e descarte informações corporativas.
- **Ativos de Infraestrutura de TI:** Servidores, switches, roteadores e outros equipamentos que fazem parte da infraestrutura que suporta os recursos de TI utilizados na Empresa
- **Computador:** Todo equipamento que possua dispositivos de processamento e armazenamento de dados e conexão à rede e/ou internet, tais como: servidores, estações de trabalho (desktops), notebooks, tablets e smartphones.
- **CPD:** Centro de processamento de dados. Ambiente de acesso restrito, no qual são armazenados os ativos críticos da infraestrutura de TI.
- **Recurso de TI:** Todo hardware, software, infraestrutura de rede e internet disponibilizados pela Empresa aos seus colaboradores, para desempenho das atividades a que foram designados.

- **Siscon:** Sistema utilizado para registro e atendimento de chamados relativos à infraestrutura de TI do Grupo Benner. Acessível por meio do endereço: <https://siscon.benner.com.br/>.

Outros termos e definições utilizados no contexto da Segurança da Informação podem ser consultados no MSI - Manual de Segurança da Informação.

## **4. PAPÉIS E RESPONSABILIDADES**

### **4.1. Recepção**

Acionar o colaborador anfitrião para validar o acesso de visitantes, registrar os acessos e providenciar crachá de identificação para visitantes.

### **4.2. Departamento Pessoal**

Providenciar o crachá de identificação para colaboradores internos e manter as permissões de acesso dos colaboradores atualizadas nos sistemas de controle de acesso.

Manter o registro atualizado dos colaboradores da equipe de Infraestrutura de TI, únicos com acesso autorizado aos ambientes restritos. Quando algum membro deixar a equipe, solicitar imediatamente o bloqueio do seu acesso biométrico e crachá magnético.

### **4.3. Equipe de Infraestrutura de TI**

Monitorar os controles ambientais, acompanhar visitantes e prestadores de serviço nos ambientes de acesso restrito;

Registrar o chamado no Siscon para as manutenções necessárias e acompanhar as atividades até a conclusão do atendimento.

### **4.4. Equipe de Manutenção / Brigada de Incêndio**

Monitorar os ambientes e acionar as equipes responsáveis, em caso de acionamento de alarmes.

Outras definições de papéis, atividades e responsabilidades no contexto de segurança da informação estão detalhadas na Seção 6 da PSI - Política de Segurança da Informação.

## 5. DESCRIÇÃO

### 5.1. Procedimentos e Controles de Acesso Físico

#### 5.1.1. Áreas comuns de circulação

Para acessar às áreas comuns de circulação, os colaboradores e visitantes devem portar um crachá de identificação.

O crachá é fornecido e controlado pelo Departamento Pessoal para os colaboradores próprios e pela Recepção para terceiros e visitantes.

Os visitantes devem ser acompanhados pelo Colaborador anfitrião, durante todo o período em que permanecer nas dependências da Empresa.

#### 5.1.2. Ambientes de acesso restrito

O CPD e demais dependências que possuem ativos de infraestrutura de TI possuem acesso restrito. Somente a Equipe de Infraestrutura de TI da Benner deve possuir acesso a estes ambientes. Inspeções e manutenções preventivas ou corretivas nos ambientes de acesso restrito serão realizadas mediante abertura de um chamado no sistema Siscon.

Quaisquer necessidades de acesso de outros colaboradores – próprios ou terceiros – somente será permitida com a presença de um colaborador da Equipe de Infraestrutura de TI, que deverá preencher o formulário RAC - Registro de Acesso Controlado, descrevendo: o período da visita, os dados do visitante, colaborador responsável e motivo da visita.

O acesso é individual e intransferível. É terminantemente proibido compartilhar ou permitir o uso das credenciais de acesso pessoais (crachá, biometria etc.) por outro colaborador.

### 5.2. Proteção dos Ambientes Restritos

#### 5.2.1. Proteção física dos ativos de informação

As áreas que possuem acesso restrito são identificadas e protegidas por mecanismo adicional de controle de acesso por biometria. Todo o ambiente restrito é monitorado por

câmeras de segurança, as quais geram imagens (em tempo real ou mediante sensores de acionamento) que são acessíveis (ou ficam gravadas) pela Equipe de Infraestrutura de TI.

### **5.2.2. Controles ambientais**

O CPD possui os seguintes controles para assegurar a adequada proteção do ambiente e seus ativos críticos:

- Sistema de detecção de incêndio - detectores de fumaça e fogo, com alarme visual e sonoro monitorado 24 horas; portas corta-fogo.
- Sistema de climatização, com sensores de temperatura. Em caso de falhas ou variações significativas nas temperaturas monitoradas, sensores acionam um alarme visual e sonoro, inicialmente disparando o alerta para a segurança do condomínio. O sistema também envia um alerta remoto para a empresa terceirizada de segurança, que então envia uma pessoa à nossa empresa para verificar se é início de incêndio ou problemas no sensor.

Em caso de acionamento dos alarmes, os profissionais de vigilância e segurança estão orientados a contactar as Equipes de Infraestrutura de TI e/ou Brigada de Incêndio.

### **5.2.3. Continuidade dos ativos de informação**

Os ambientes de acesso restrito possuem os seguintes mecanismos para assegurar a continuidade dos ativos de informação:

- Equipamentos com fontes redundantes, com circuito alternativo de fornecimento de energia.
- Fornecimento alternativo de energia por meio de Nobreaks e Geradores em caso de interrupção da fonte primária de energia elétrica.
- Links redundantes de dados (primário e secundário), por fibra óptica e ADSL, com balanceamento de cargas.

- Estrutura de backup local, com armazenamento local em disco e cópias em mídias magnéticas mantidas em local distinto do ambiente do CPD. Adicionalmente, realiza-se a replicação dos backups em nuvem, provendo resiliência e disponibilidade dos dados.
- Sistemas utilizados para o monitoramento dos ativos de rede (servidores, switches, links de internet, VPN).
- EDR (*end point detection and response*) – Ferramenta de análise avançada de ameaças cibernéticas de todos os dispositivos ligados na rede corporativa.
- MDR (Managed Detection and Response) – Serviço gerenciado de monitoramento contínuo e resposta a incidentes de segurança, provido por consultoria especializada em operações de segurança cibernética.

### 5.3. Revisões e Testes Periódicos

Os testes em sistemas e dispositivos e as revisões dos controles existentes são realizados a partir do agendamento de chamados no sistema Siscon, nos itens:

- Manutenção elétrica geral, limpeza do ar-condicionado; verificação de baterias dos nobreaks, testes de backup e restore; teste de desligamento do CPD para checar o acionamento e desempenho dos nobreaks, testes de funcionamento dos geradores; testes gerais e simulações de continuidade do CPD;

## 6. EVIDÊNCIAS GERADAS

- Sistema Siscon: registro dos incidentes e das manutenções programadas relativas aos ativos de infraestrutura de TI e dos ambientes de acesso restrito.
- Sistema de Acesso Biométrico: registro dos colaboradores com acesso biométrico aos ambientes de acesso restrito.
- Cadastro de Chaves: avaliar a criação de um controle das chaves que dão acesso ao CPD (atualmente em poder dos colaboradores da Equipe de Infraestrutura de TI).
- RAC - Registro de Acesso Controlado - Registro de visitantes ao ambiente de CPD.

## 7. DOCUMENTOS DE REFERÊNCIA

- PSI - Política de Segurança da Informação
- MSI - Manual de Segurança da Informação
- NAL – Norma Gestão de Acesso Lógico

## 8. REGISTRO DE ALTERAÇÕES

Versão	Data	Etapa	Responsável
00	07/06/2022	Emissão do documento	Jane Glauce R. Coimbra (DM11)
01	02/03/2023	Revisão	Jorge Espinhara (BENNER)
02	03/01/2024	Revisão	Jorge Espinhara (BENNER)

## 9. FORMALIZAÇÃO

ELABORAÇÃO/REVISÃO		APROVAÇÃO	
Jorge Espinhara – Governança de TI		Severino Benner - CEO	
09/01/2024	<small>DocuSigned by:</small> <i>Jorge Luiz Carvalho Espinhara</i> <small>#8FC1E7A18DC49D...</small>	09/01/2024	<small>DocuSigned by:</small> <i>Severino Benner</i> <small>B5112A47CD594F7...</small>