


| | | | |
|---|--|----------------|--|
|  | INSTRUÇÃO DE OPERAÇÃO | | ITO-276 |
| | Título: | | Revisão: B |
| | SEGURANÇA FÍSICA DO DATA CENTER | | Página: 1 de 2 |
| | Departamento: T.I | | Data de efetivação: 12/02/25 |
| Elaborador | Revisor | Aprovador | |
| Vitor Faustino | André Munerato | Carina Affonso | |

1. OBJETIVO

A Segurança Física do Data Center da ORGANIZAÇÃO tem como objetivo estabelecer diretrizes rigorosas para proteger as instalações críticas do data center, garantindo a integridade, disponibilidade e confidencialidade dos sistemas e dados armazenados.

2. REFERÊNCIAS

- NBR ISO/IEC 27001.
- NBR ISO/IEC 27002.
- NBR ISO/IEC 27005.
- ITO-185 Portaria.
- ITO-259 Classificação da informação.
- PO-15 Política de Proteção de dados Pessoais.
- PO-16 Incidentes de Segurança.

3. ABRANGÊNCIA

A todos os usuários (sócios, prepostos, empregados, estagiários, aprendizes e contratados, prestadores de serviço) que tem acesso ao data center da ORGANIZAÇÃO

4. RESPONSABILIDADES

Área de segurança da informação: Garantir que os requisitos de segurança da informação sejam considerados quando do desenvolvimento, implantação e uso de sistemas de informação.

A área de segurança da informação coordenará as áreas técnicas, as áreas de apoio e as áreas de negócio para desenvolvimento e implantação de projetos, procedimentos, ações, instruções e normativos que possibilitem a operacionalização e manutenção desta instrução.

5. AUTORIDADE

O superior imediato tem autoridade definida para assegurar o cumprimento das normas de segurança, das instruções de operação e das normas e legislação em geral.

6. DEFINIÇÕES

- **Usuário:** Agentes externos ao sistema ou pessoas que se utilizam dos recursos, serviços e/ou estruturas de tecnologia.
- **Senha/Autenticação:** palavra-passe, ou ainda palavra-chave ou password, é uma palavra ou código secreto previamente convencionado entre as partes como forma de reconhecimento. Em sistemas de computação, senhas são amplamente utilizadas para autenticar usuários e conceder-lhes privilégios para agir como administradores de um sistema, por exemplo ou permitir-lhes o acesso a informações personalizadas armazenadas no sistema.
- **Gestor da Informação (GI):** Cada informação deverá ter seu Gestor que será indicado formalmente pela diretoria responsável pelos sistemas que acessam a informação. O Gestor da Informação é o responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação.


7. EPI

N/A

8. DESCRIÇÃO DA ATIVIDADE

8.1. Controle de Acesso ao Data Center

- **Acesso Autorizado:** O acesso ao data center será concedido somente a funcionários autorizados com necessidade de acesso para cumprir suas funções.

| | | | |
|--|--|--|-----------------------|
|  | INSTRUÇÃO DE OPERAÇÃO | | ITO-276 |
| | Título: | | Revisão: B |
| | SEGURANÇA FÍSICA DO DATA CENTER | | Página: 2 de 2 |

- **Autenticação e Autorização:** O acesso será controlado por sistemas de autenticação e autorização rigorosos, incluindo cartões de acesso, senhas e biometria.

- **Registro de Acesso:** Todos os acessos ao data center serão registrados e monitorados.

8.2. Monitoramento de segurança

- **Câmeras de Segurança:** Câmeras de segurança de alta resolução serão instaladas em todas as áreas críticas do data center.
- **Deteção de Intrusão:** Sistemas de detecção de intrusão serão implementados para monitorar acessos não autorizados.

8.3. Proteção física do data center

- **Controle de Temperatura e Umidade:** Os parâmetros de temperatura e umidade serão mantidos dentro dos limites ideais para equipamentos de TI.
- **Alimentação de Energia Redundante:** Fontes de energia redundantes e sistemas de backup de energia estão implementados para garantir a disponibilidade contínua.

8.4. Segurança das instalações

- **Controle de Acesso Físico:** A entrada no data center será restrita a pessoal autorizado, e todas as entradas serão monitoradas.
- **Armazenamento Seguro:** Equipamentos sensíveis e dados críticos serão armazenados em armários corta fogo e gabinetes trancados.

8.5. Planos de contingência e recuperação de desastres

- **Planos de Contingência:** Planos de contingência detalhados foram desenvolvidos para lidar com interrupções e emergências no data center.
- **Testes e Simulações:** Exercícios regulares serão conduzidos para testar a eficácia dos planos de recuperação de desastres.

8.6. Treinamento e conscientização

- **Treinamento de Pessoal:** Todos os funcionários que têm acesso ao data center passarão por treinamento em segurança física e procedimentos operacionais seguros.

8.7. Relatórios de incidentes

- **Relatórios e Investigação:** Todos os incidentes de segurança física no data center devem ser relatados imediatamente. Uma investigação completa será conduzida, e ações corretivas serão implementadas.

9. REGISTRO DE ALTERAÇÕES

| Revisão | Alteração | Data | Responsável |
|---------|----------------------------------|----------|----------------|
| A | Criação | 25/01/23 | Vitor Faustino |
| B | Revisão periódica a cada 02 anos | 12/02/25 | Vitor Faustino |