SENAI

Reunião das Diretorias e Conselho do CIESP

SÃO PAULO

JUNHO 2026

MISSÃO SENAI-SP

Apoiar o aumento da competitividade da indústria por meio de ações de **educação profissional, tecnologia, inovação e empreendedorismo industrial.**

AGENDA

- Estratégia SENAI-SP para Cibersegurança
- I-ISAC - Industry Information Sharing and Analysis Center
- Exercício Guardião Cibernético
- Plataforma NEXO – Foresight industrial

CIBERSEGURANÇA

ESTRATÉGIA SENAI-SP

MISSÃO NCFTA

5 e 6 de Março 2020 - Pittsburgh - U.S.A.

NCFTA

Ministério da Justiça, FIESP E SENAI-SP.

Agenda Principal:

- **Brand and Consumer Protection (BCP)**
Combate fraudes, falsificações e riscos ao consumidor em vendas online e cadeias de suprimento..

- **Cyber Financial — CyFin**
protege o setor financeiro contra ameaças como phishing, malware, botnets e engenharia social.

- **Malware and Cyber Threat**
Monitora malwares, dark web e ameaças técnicas emergentes com inteligência acionável.

SENAI

"For the committed, not the curious" – NCFTA Law Enforcement Partner

Para os comprometidos e não os curiosos !

NCFTA®

The National Cyber-Forensics and Training Alliance

Home Careers Training Events News Resources

NCFTA


FBI
CYBER FORCE


WELCOME TO DARKORE
Operation
SHROUDED HORIZON
NCA AFP POLITI
FBI
CYBER FORCE

Escola SENAI “Paulo Antoine Skaf”

Escola SENAI “Paulo Antoine Skaf”

Arena SENAI Cyber Segurança

Arena SENAI Cyber Segurança

Arena SENAI Cyber Segurança

SEGURANÇA CIBERNÉTICA

CONSULTORIA, IMPLANTAÇÃO E AUDITORIA

SENAI

CONSULTORIA EM NORMATIVAS E REGULAMENTAÇÕES

Serviços especializados em segurança da informação, privacidade e cibersegurança, abrangendo implementação, avaliação e auditoria de práticas organizacionais, com base em referências amplamente adotadas no mercado, como.

ISO/IEC 27001, **TISAX**, **NIST** Cybersecurity Framework 2.0, **CIS** Controls e ISA **62443**

O serviço cobre desde o diagnóstico do cenário atual, passando pela definição e formalização de políticas, processos e controles, até a preparação para auditorias, certificações e exigências regulatórias.

A atuação é consultiva e especializada, com foco na estruturação e fortalecimento da segurança organizacional.

SEGURANÇA CIBERNÉTICA

CONSULTORIA, IMPLANTAÇÃO E AUDITORIA

TESTES DE VULNERABILIDADE E DE INTRUSÃO

(TESTES DE SEGURANÇA OFENSIVOS)

Teste de Intrusão (Pentest) realizado nos ambientes de chão de fábrica (TO – Tecnologia Operacional) e de Tecnologia da Informação (TI), tem como objetivo identificar falhas de segurança exploráveis em sistemas, aplicações, redes e demais ambientes tecnológicos.

A atividade simula ataques cibernéticos reais de forma controlada, autorizada e devidamente documentada. O serviço avalia o nível de exposição da organização a ameaças cibernéticas, demonstrando, de maneira prática, como vulnerabilidades podem ser exploradas e quais impactos reais podem ser gerados para o negócio.

SEGURANÇA CIBERNÉTICA

CONSULTORIA, IMPLANTAÇÃO E AUDITORIA

LABORATÓRIO INTEGRADO DE OT, IT e IIoT

Hub integrado de treinamento imersivo, experimentação aplicada e serviços especializados em segurança cibernética, voltado à proteção de ambientes IT, OT e IIoT.

Em cenários industriais realistas e de alta fidelidade,

O laboratório capacita profissionais e apoia a indústria na análise de riscos, conformidade e fortalecimento da resiliência cibernética, integrando tecnologia, governança e desenvolvimento de competências práticas para enfrentar os desafios de ambientes ciberfísicos complexos.

SEGURANÇA CIBERNÉTICA

CONSULTORIA, IMPLANTAÇÃO E AUDITORIA

SENAI

DIAGNÓSTICO GRATUITO

Avalie a maturidade de cibersegurança industrial e receba um relatório executivo com ações práticas para fortalecer a resiliência operacional (TI e TO)

- Identificação de riscos críticos e vulnerabilidades
- Recomendações priorizadas de curto e médio prazo
- Sessão de devolutiva executiva com nossos especialistas

Escaneie e faça o **diagnóstico gratuito**!

Ou acesse:
https://diagnostico.sp.senai.br/

SENAI

I-ISAC

I-ISAC

SENAI

Industry Information Sharing and Analysis Center

1º Centro de Compartilhamento de Informações da Indústria Brasileira

Em São Caetano do Sul

Compartilhar

Proteger

Fortalecer

O projeto contará com centros voltados às áreas de **Finanças, Elétrica, Óleo e Gás, Saúde e atuação conjunta com GSI.**

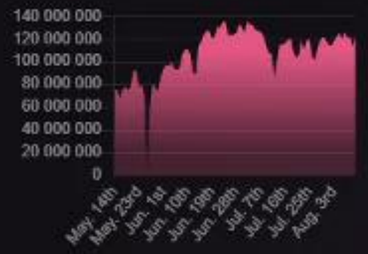
Check Point
SOFTWARE TECHNOLOGIES LTD.

THREATCLOUD

LIVE CYBER THREAT MAP

30 235 504 ATTACKS ON THIS DAY

RECENT DAILY ATTACKS



ATTACKS Current rate − 4 +

- Content Protection Violation
  11:07:36 United States → Netherlands
- Web Client Enforcement Violation
  11:07:36 Czechia → Germany
- Web Client Enforcement Violation
  11:07:36 Czechia → Germany
- Content Protection Violation
  11:07:35 United States → KY, United States
- Web Client Enforcement Violation
  11:07:35 Czechia → Germany
- Web Client Enforcement Violation
  11:07:35 Czechia → Germany
- Content Protection Violation
  11:07:35 United States → KY, United States

Malware Phishing Exploit

TOP TARGETED COUNTRIES

Highest rate of attacks per organization in the last day.

- Bolivia
- Angola
- Indonesia
- Nepal
- Taiwan

TOP TARGETED INDUSTRIES

Highest rate of attacks per organization in the last day.

- Education
- Government
- Communications

TOP MALWARE TYPES

Malware types with the highest global impact in the last day.

- Botnet
- Phishing
- Worm

SENAI

O PROBLEMA

O País Registrou, em um único ano, **60 bilhões** de tentativas de ataques cibernéticos

O MERCADO

Nesse contexto, o Brasil é o **12º maior** mercado global de segurança cibernética e deverá investir **R$104,6 bi** na área entre 2025 e 2028

**Fonte: Relatório da Associação das Empresas de Tecnologia da Informação e Comunicação*

SEGURANÇA CIBERNÉTICA

CONSULTORIA, IMPLANTAÇÃO E AUDITORIA

SENAI

I-ISAC INDUSTRIAL BRASIL

Centro de Compartilhamento e Análise de Informações de Cibersegurança do Setor Industrial Brasileiro

O ISAC é uma plataforma estratégica de inteligência cibernética para a indústria, com foco em infraestrutura crítica e ambientes industriais. Estrutura o primeiro ISAC industrial do Brasil — e um dos poucos no mundo —, criando um ambiente confiável de compartilhamento de informações sobre ameaças digitais, que permite às empresas antecipar riscos, reduzir vulnerabilidades e ampliar a resiliência operacional.

Os associados do I-ISAC são beneficiados com:

- ✓ Alerta de vulnerabilidades críticas.
- ✓ Exercícios de cibersegurança.
- ✓ Assessoria para conformidade(ISO 27001).
- ✓ Boletins de vulnerabilidades críticas em sistema ICS/SCADA e OT.
- ✓ Relatório setorial.


SENAI
CENTRO DE ANÁLISE E
COMPARTILHAMENTO DE DADOS
ISAC INDÚSTRIA
CENTROS DE ANÁLISE E COMPARTILHAMENTO DE INFORMAÇÕES (INFORMATION SHARING AND ANALYSIS CENTERS)
ÁREA DE TRABALHO – ANÁLISE


SENAI
ISAC INDÚSTRIA
ÁREA DO OBSERVATÓRIO

SENAI

EXERCÍCIO

GUARDIÃO CIBERNÉTICO

SENAI

8° Exercício Guardião Cibernético
O maior exercício do hemisfério Sul

PROCESSOS

COMUNICAÇÃO

TECNOLOGIA

SEGURANÇA CIBERNÉTICA

EVENTOS

EXERCÍCIO GUARDIÃO CIBERNÉTICO

(SETEMBRO/2026)

O Exercício Guardião Cibernético é o maior treinamento de defesa cibernética do Hemisfério Sul,

conduzido pelo Ministério da Defesa e coordenado pelo Comando de Defesa Cibernética (ComDCiber) do Exército Brasileiro.

O objetivo do exercício é testar, integrar e fortalecer a capacidade de resposta do Brasil frente a incidentes e ataques cibernéticos, especialmente aqueles que impactam infraestruturas críticas nacionais, como energia, água, transporte, comunicações, finanças e serviços essenciais.

ComDCyber

Comando de Defesa Cibernética

- Responsável por **proteger as infraestruturas críticas** e a soberania digital do Brasil.
- Atua como escudo estratégico no ambiente cibernético, garantindo **prontidão, dissuasão e resposta a ameaças digitais**.
- Participa de exercícios internacionais com a **OTAN**
- Comando **General Ivan de Souza Corrêa Filho**

Acordo de Cooperação Técnica

HUB VOLTADO À PROTEÇÃO DIGITAL DA INDÚSTRIA

Proposta do Primeiro Hub em São Paulo

Setembro de 2026

- Participação das Simulações com Indústrias em São Paulo

- Possibilidade de Ação Paralela ao Exercício Guardião Cibernético em 5 unidades do SENAI

- 1.602 Empresas com Ciso - Diretor de Segurança da Informação

2026 - EGC 8.0

HUB Central
Brasília - DF

HUB Manaus - AM

HUB Belém-PA

HUB São Paulo-SP

HUB Recife-PE

HUB Curitiba-PR

HUB Rio de Janeiro - RJ

EXERCÍCIO GUARDIÃO CIBERNÉTICO
COOPERAR - INTEGRAR

O maior exercício de Ciber-resiliência do Hemisfério Sul

240 Organizações e 2000 Participantes

Simulação Construtiva

Cenário - *IC Brasileiras – Ataques reais ocorridos

** Incidente cibernético*

APTs Reais que atuam no Brasil e no mundo

Ameaça Persistente Avançada

EGC 8.0 – Simulação Virtual

SENAI

HUB CENTRAL – BRASÍLIA DF

HUBS REGIONAIS

RED TEAM

GOLD TEAM

SETOR IC

BLUE TEAM

SETOR IC

BLUE TEAM

SETOR IC

BLUE TEAM

SETOR IC

BLUE TEAM

Empresas Estratégicas de Defesa, Comércio, Indústria e Serviços

SETOR IC

BLUE TEAM

Empresas Estratégicas de Defesa, Comércio, Indústria e Serviços

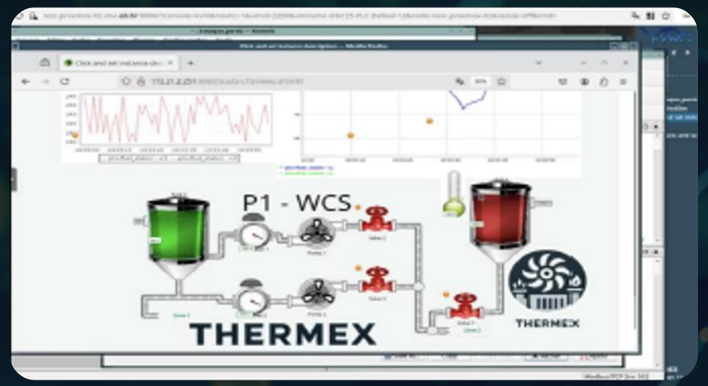
SETOR IC

BLUE TEAM

Simulação Virtual – Sistemas de Controle Industrial (SCADA) customizados por Setor Estratégico

SENAI

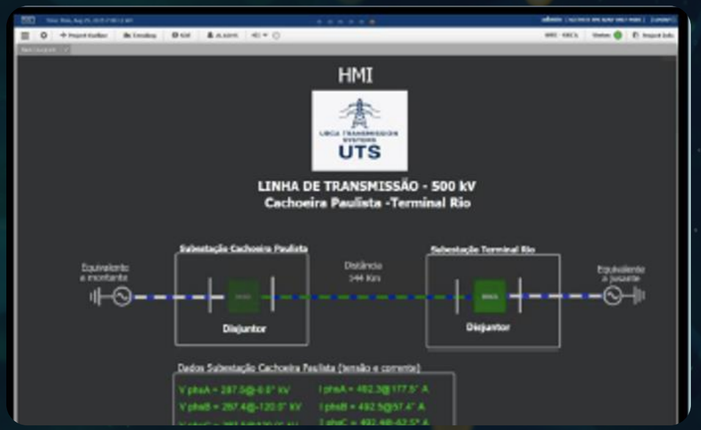
Setor Defesa - Thermex



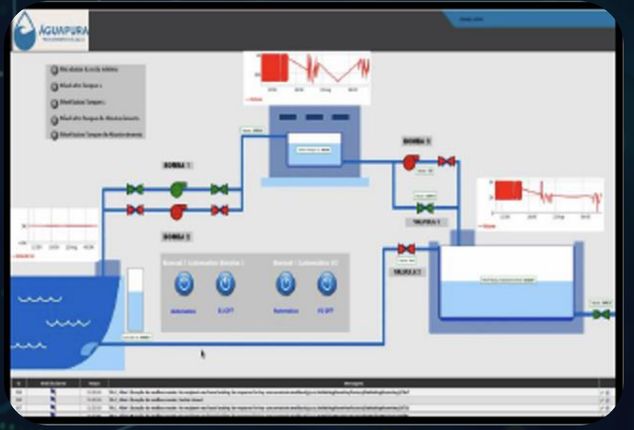
Setor Defesa – Sistema de Defesa Aérea

Setor Transportes – C2 Drone

Setor Energia – Simulador Digital Em Tempo Real



Setor Água, e-Gov, Biossegurança e Bioproteção – Tratamento de Água



Setor Financeiro e Comunicações – Controle de Temperatura e Baterias de Site E Data Center

Jogo Cibernético

SENAI

Capture The Flag (CTF) – 2000 vagas
- 1400 civis/300 militres/300 Cooperação Internacional;

GoHacking
CYBER SECURITY TRAININGS

COOPERAÇÃO INTERNACIONAL

Países convidados


SENAI
FORESIGHT
PLATAFORMA NEXO
DISTRITO
TECNOLÓGICO
SENAI·SP

NEXO EXPERIENCE

PROPÓSITO

Apoiar empresas em seus **processos de inovação**, oferecendo um plano integrado de facilitação de ponta a ponta — **desde a identificação dos desafios até a construção de *roadmaps* de soluções,** conduzidos e executados tecnicamente pelo próprio Distrito.

JUSTIFICATIVA

Ampliar as ações colaborativas, práticas e **escalonáveis** para fomentar a inovação nas empresas e indústrias do estado de São Paulo

A TRILHA

Entendendo fases do método

1

FOCO DO ESTUDO

Objetivo de investigação

O que a empresa deseja estudar?

Horizonte temporal

Qual o tempo a se considerar? 5, 10, 20 anos?

Megatendências mais relevantes

Quais as tendências globais que mais se conectam com o segmento e objetivo do estudo?

2

DADOS DE MERCADO

Scanning: Levantamento de forças tecnológicas, tendências do setor, patentes, sinais e eventos improváveis de grande impacto.

3

FUTUROS DA EMPRESA

Construção em workshop de cenários possíveis que poderão moldar o futuro da empresa. Exploramos possibilidades e enxergamos caminhos.

4

HORIZONTES DE INOVAÇÃO E DECISÃO

Desenho de projetos de inovação em **H1, H2 e H3** Decisão sobre onde inovar e como alocar os esforços.

5

ROADMAP DE PROJETOS

Plano de ação necessário para transformar o futuro escolhido em realidade. Conexão com linhas de fomento com maior sinergia aos projetos.

Data Driven

Bancos de dados que baseam a sala e o método

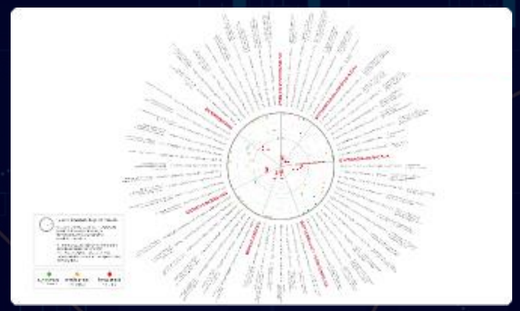
PLATAFORMA ORION

IF FORESIGHT INSTITUTE
*ITONICS**

Acesso a mais de 2.800 forças motrizes em 20 dimensões: Tendências, sinais e wild cards para scanning e workshop de foresight.
**Acesso solicitado*

BANCO DE DADOS

Patentes, Artigos Científicos,
Análise de potenciais mercado

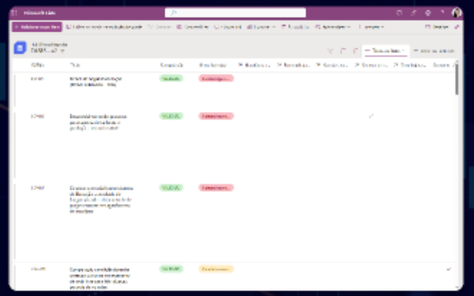


Acesso ao banco de dados de patentes e rotas tecnológicas para alimentar os dados gerados pela sala.

Bases Internacionais de patentes: ESPACENET, Google Patents e Lens
Busca e definição de classes de patentes - IPC, CPC
Análise bibliométrica (VOSviewer)
Banco de dados de base científica : Scopus/Web of Science/ScienceDirect
Anlálise e potenciais mercados: GENiP

CASES DISTRITO

LEVANTAMENTO DE CASES POR VERTICAL



Cruzamento de dados de tendências e forças de mudanças com os cases e linhas de pesquisa desenvolvidas por cada vertical do Distrito.

O Método

Método proprietário de *FORESIGHT*

O método atua como uma inteligência estratégica que conecta o presente às forças que estão moldando o futuro para definir onde e como inovar.

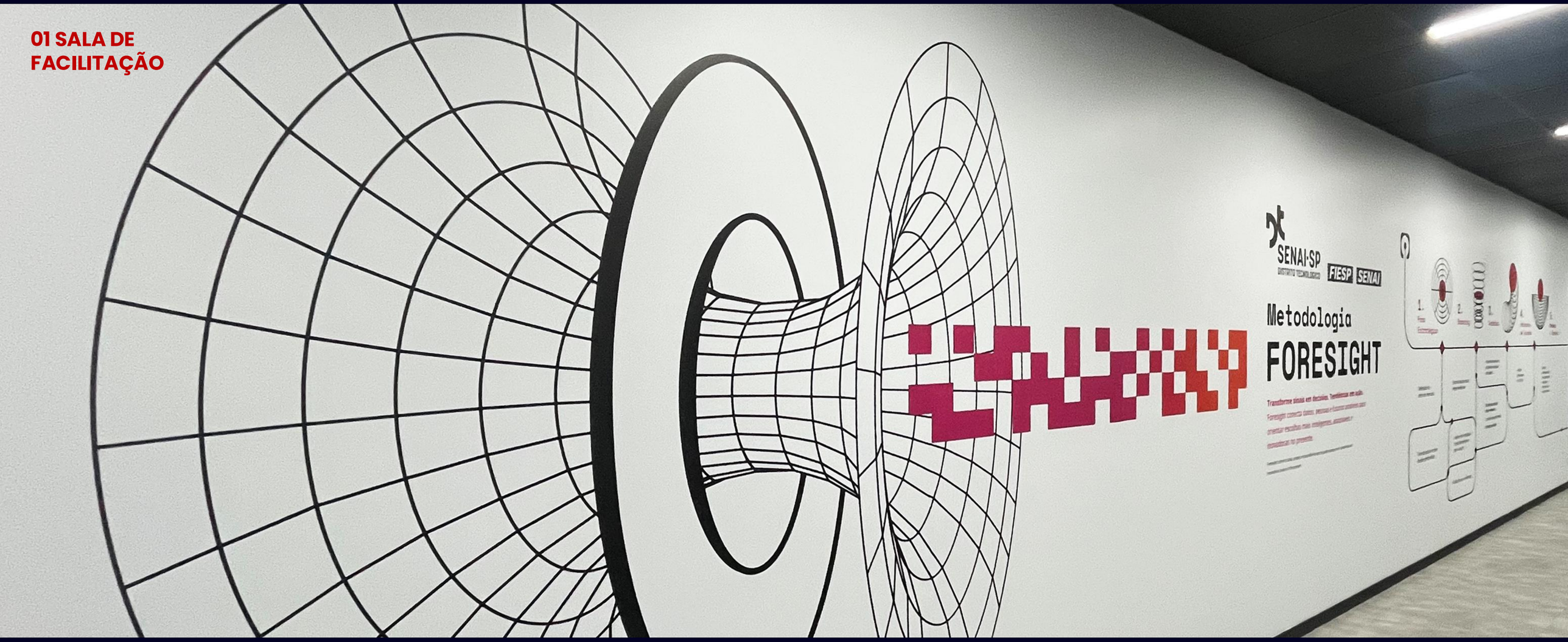
O Resultado:

Roadmap de projetos de inovação: ações práticas para começar a executar **hoje**, com direção estratégica clara para os próximos anos.

ESPAÇO NEXO

SENAI

01 SALA DE FACILITAÇÃO



ESPAÇO NEXO

Fotos do ambiente

SENAI

DEPARTAMENTO REGIONAL
DE **SÃO PAULO**

OSVALDO LAHOZ MAIA

DIRETORIA REGIONAL SENAI SÃO PAULO