

32^a

SEMANA DE TECNOLOGIA METROFERROVIÁRIA

INTEGRAÇÃO DE REDES OPERACIONAL E ADMINISTRATIVA EM AMBIENTES METROFERROVIÁRIOS

Nome dos autores

Vinicius Santos

Romolo Cyrino

INTEGRAÇÃO DE REDES OPERACIONAL E ADMINISTRATIVA EM AMBIENTES METROFERROVIÁRIOS

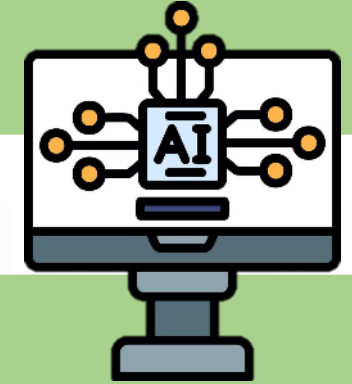


A TRANSFORMAÇÃO DIGITAL NO SETOR METROFERROVIÁRIO

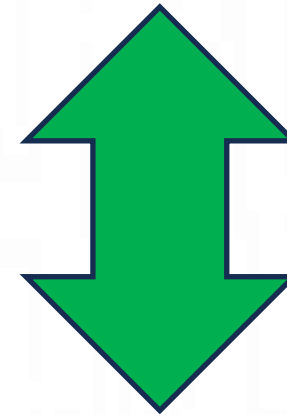
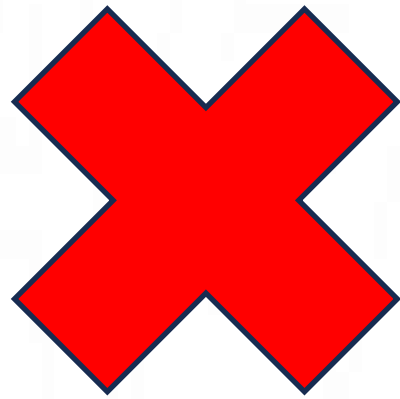
OT versus IT



Se um computador da rede administrativa fosse comprometido por ransomware, ele conseguiria alcançar os sistemas de controle da sua operação?



AMBIENTE ADMINISTRATIVO



AMBIENTE OPERACIONAL



OT – TECNOLOGIA OPERACIONAL

SERVIÇOS E SISTEMAS OPERACIONAIS



SCADA

Supervisão e controle dos processos operacionais em tempo real.



SINALIZAÇÃO FERROVIÁRIA

Controle de tráfego, intertravamentos, ATP/ATS e segurança da operação.



ENERGIA

Supervisão de subestações, distribuição elétrica e sistemas de tração.



TELECOMUNICAÇÕES

- Sistemas de comunicação de voz, rádio e dados de missão crítica.
- Automação de estações (controle de portas de plataforma, escadas rolantes, HVAC, iluminação, etc.)
- Monitoramento operacional (CFTV, detecção de incêndio, controle de acesso e monitoramento ambiental.)
- Dispositivos de campo (PLCs, IEDs, sensores, atuadores e outros dispositivos industriais.)

INTEGRAÇÃO OT ↔ IT



COMUNICAÇÃO
SEGURA



SEGMENTAÇÃO
DE REDE



CONTROLE
DE ACESSO



MONITORAMENTO
CONTÍNUO

IT – TECNOLOGIA DA INFORMAÇÃO

SERVIÇOS E SISTEMAS CORPORATIVOS



DATA LAKE / DATA WAREHOUSE

Armazenamento centralizado de dados operacionais e corporativos para análise e histórico.



PLATAFORMAS ANALÍTICAS / BI

Ferramentas de análise, dashboards, relatórios gerenciais e inteligência operacional.



CMMS (MANUTENÇÃO)

Gestão de ativos, ordens de serviço, planos de manutenção e histórico de intervenções.



ERP CORPORATIVO

Gestão de recursos empresariais: financeiro, suprimentos, contratos, estoques, RH, etc.



SERVIÇOS EM NUVEM

Hospedagem de aplicações, armazenamento, backup, escalabilidade e recuperação de desastres.



SEGURANÇA DA INFORMAÇÃO

Proteção de dados, gestão de identidades, monitoramento, SOC e conformidade.



PORTAIS E APLICAÇÕES CORPORATIVAS

Intranet, portais de gestão, sistemas administrativos e colaboração.



SEGMENTAÇÃO
DE REDE



FIREWALLS
INDUSTRIAIS



MONITORAMENTO
CONTÍNUO



CONTROLE DE ACESSO
E IDENTIDADES



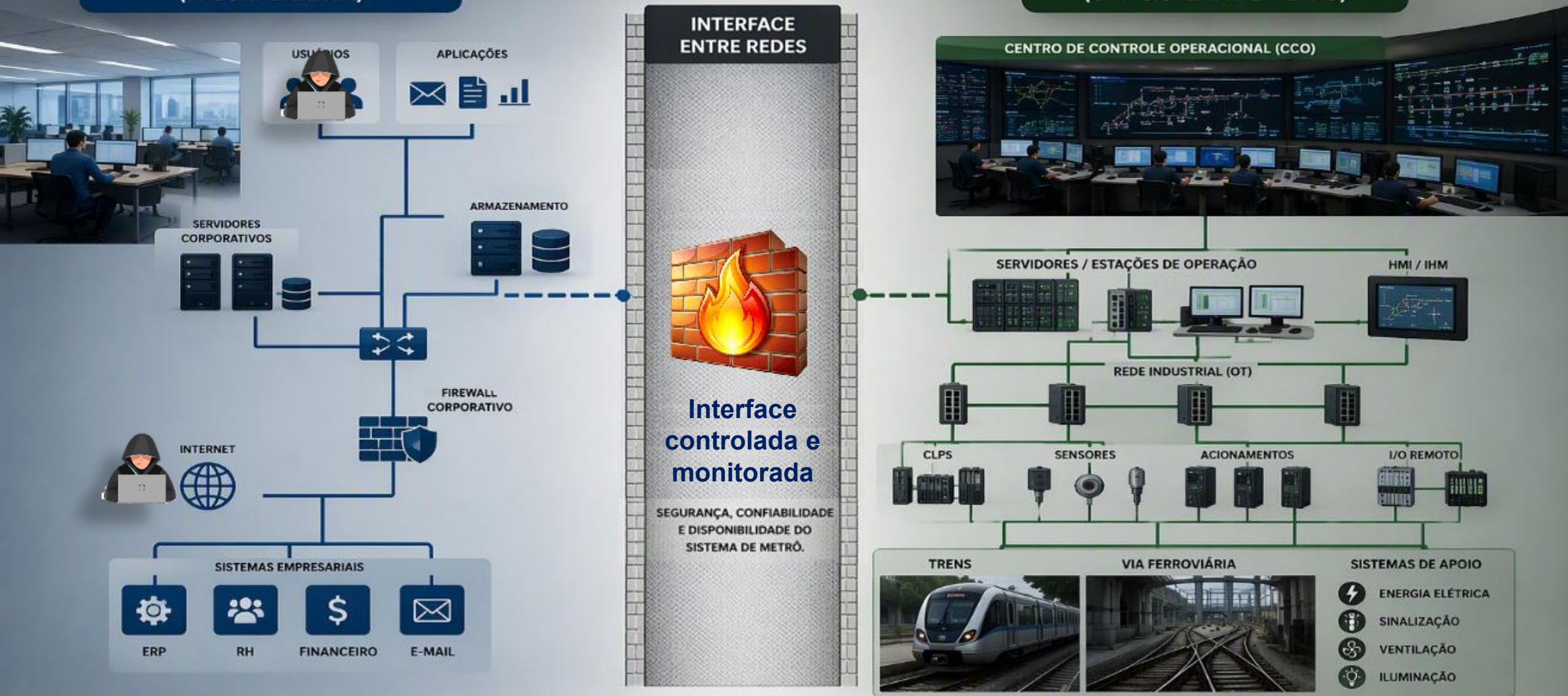
CONFORMIDADE
E NORMAS



DISPONIBILIDADE
E RESILIÊNCIA

REDE ADMINISTRATIVA (TI CORPORATIVA)

REDE OPERACIONAL (OT – SISTEMA DE METRÔ)



REDE ADMINISTRATIVA (TI)

- Dados corporativos
- Produtividade
- Acesso à internet



**SEGREGAÇÃO DE REDES
PROTEGE O SISTEMA DE METRÔ
E GARANTE SUA OPERAÇÃO SEGURA.**



REDE OPERACIONAL (OT)

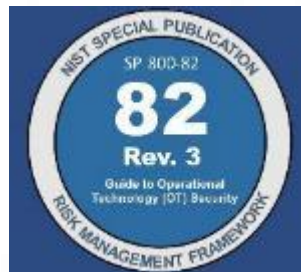
- Controle de processos
- Tempo real
- Alta disponibilidade

MODELOS DE INTEGRAÇÃO SEGUROS

Normas que Apoiam a Segurança



A IEC 62443 define requisitos de segurança para ambientes industriais.

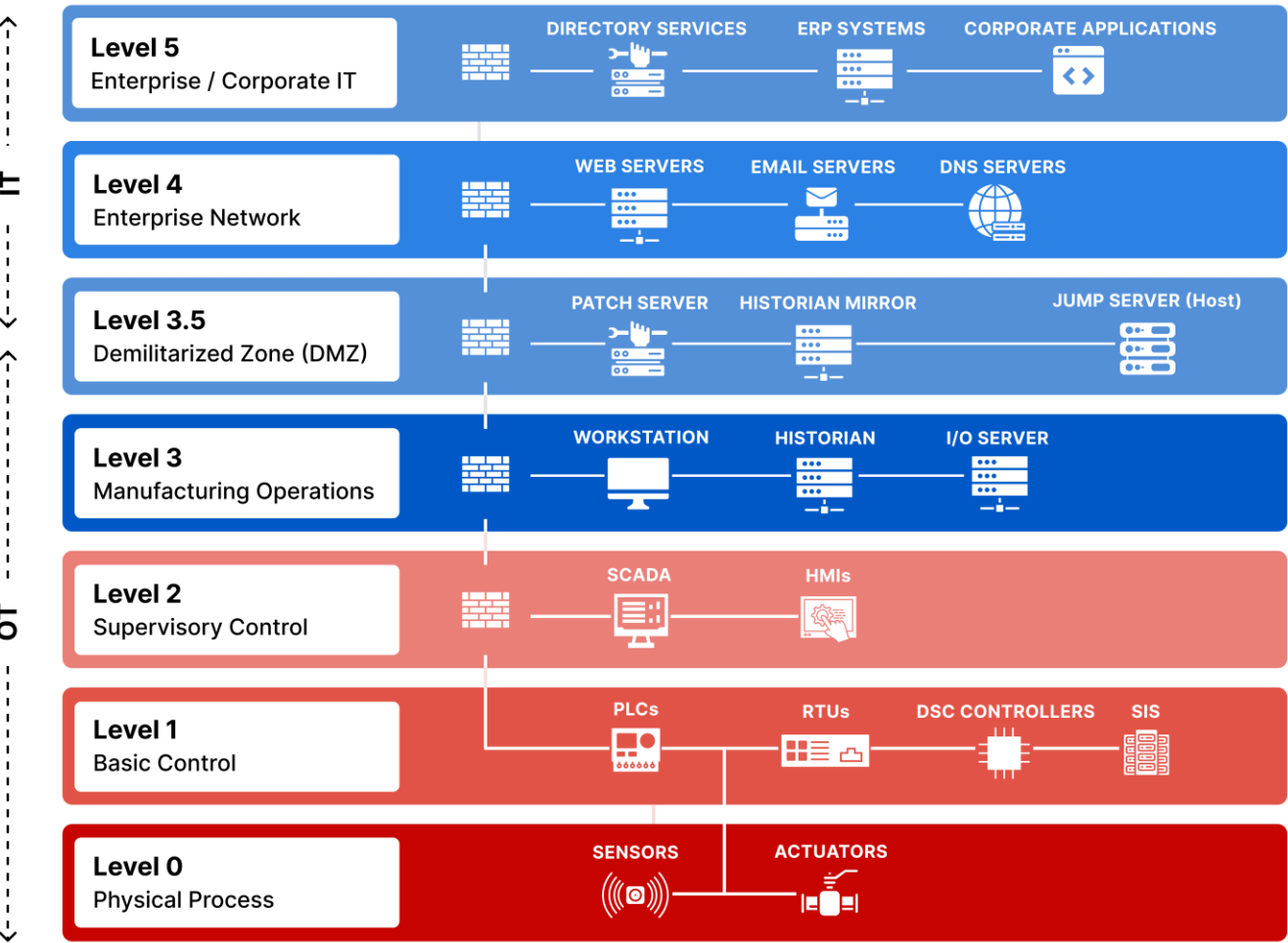


O NIST SP 800-82 apresenta boas práticas para proteção de sistemas OT.

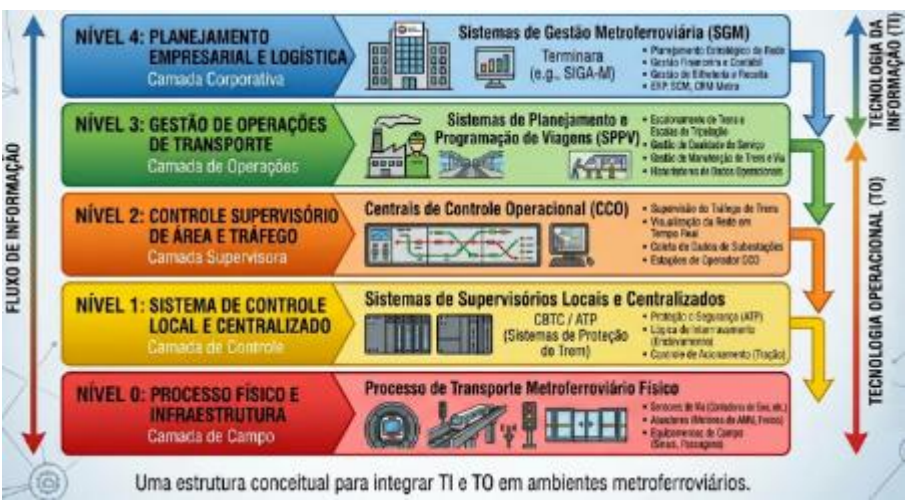


A ISA-95 estabelece modelos para integração entre sistemas industriais e corporativos.

Purdue Model for ICS Security: Layers and Zones of Defense



Modelo Purdue para ambientes Metroferroviários



ARQUITETURA DE REFERÊNCIA DE EMPRESA METROFERROVIÁRIA (AREM)

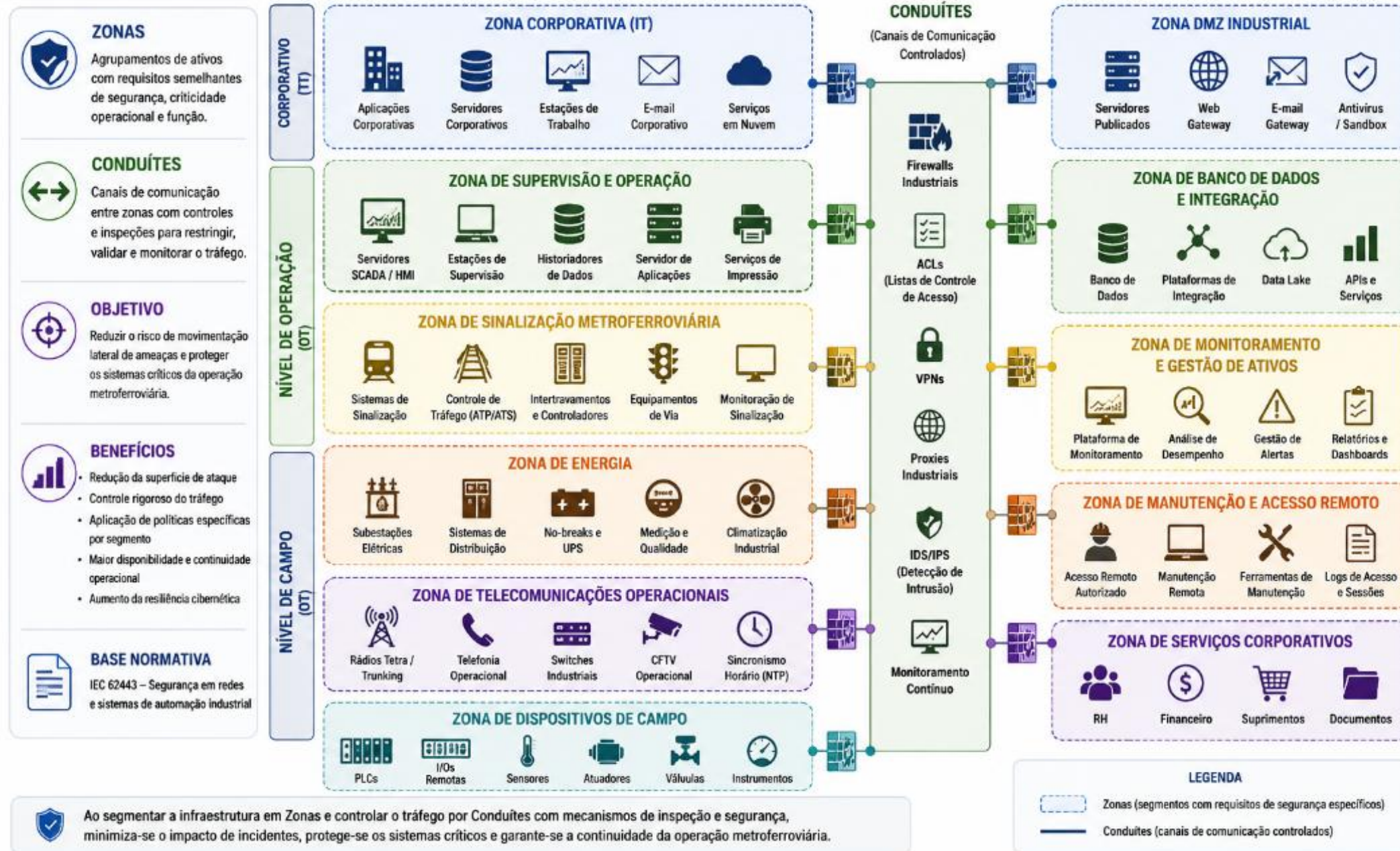
AS CAMADAS ISA-95 (Contexto Metroferroviário)



Uma estrutura conceitual para integrar TI e TO em ambientes metroferroviários.

Modelo Zones and Conduits – IEC 62443

Segmentação lógica e controle de comunicação para ambientes OT metroferroviários



Ao segmentar a infraestrutura em Zonas e controlar o tráfego por Conduítes com mecanismos de inspeção e segurança, minimiza-se o impacto de incidentes, protege-se os sistemas críticos e garante-se a continuidade da operação metroferroviária.

INDUSTRIAL DMZ (IDMZ)

Zona intermediária entre a rede corporativa (IT) e a rede operacional (OT)



OBJETIVO

Impedir comunicação direta entre os ambientes IT e OT, funcionando como uma camada de proteção e monitoramento.



FUNÇÃO

Controlar, inspecionar e registrar o tráfego entre as redes, permitindo apenas comunicações necessárias e autorizadas.



BENEFÍCIO

Reduz significativamente o risco de propagação de ataques vindos da rede corporativa.



COMO A IDMZ PROTEGE

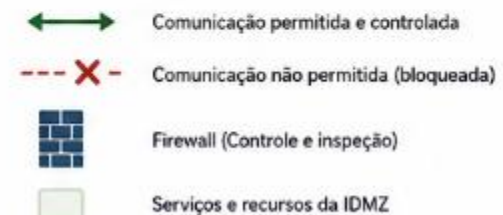
Evita comunicação direta entre IT e OT

- Permite apenas fluxos específicos e autorizados
- Inspecciona, registra e monitora todo o tráfego
- Limita o alcance de ataques e movimentação lateral
- Aumenta a visibilidade e o controle sobre integrações

EXEMPLOS DE FLUXOS PERMITIDOS ATRAVÉS DA IDMZ



LEGENDA



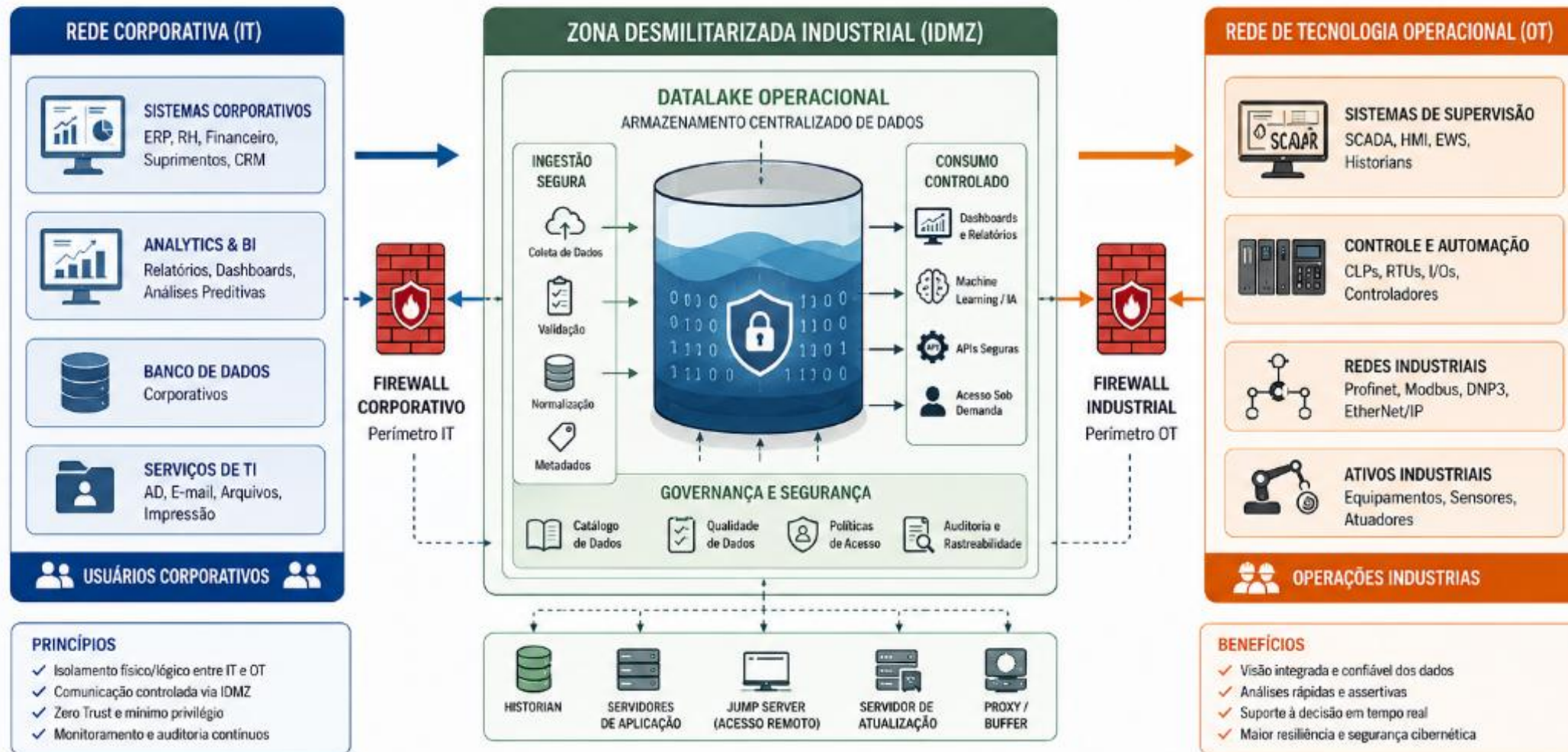
BENEFICIOS OPERACIONAIS

Consolidação e Tratamento dos Dados



ARQUITETURA DE DADOS SEGURA: ISOLAMENTO OT-IT COM DATALAKE NA IDMZ

Integração segura, governança e valor dos dados com isolamento entre ambientes



FLUXO DE DADOS CONTROLADO

IT → IDMZ: Requisições, Consultas, Configurações

IDMZ: Coleta, Processamento, Armazenamento, Distribuição

OT → IDMZ: Telemetria, Eventos, Alarmes, Logs



ISOLAMENTO
Perímetros e firewalls dedicados entre IT, IDMZ e OT



INTEGRAÇÃO SEGURA
Troca de dados unidirecional e controlada



DATALAKE NA IDMZ
Centraliza, organiza e disponibiliza dados com segurança

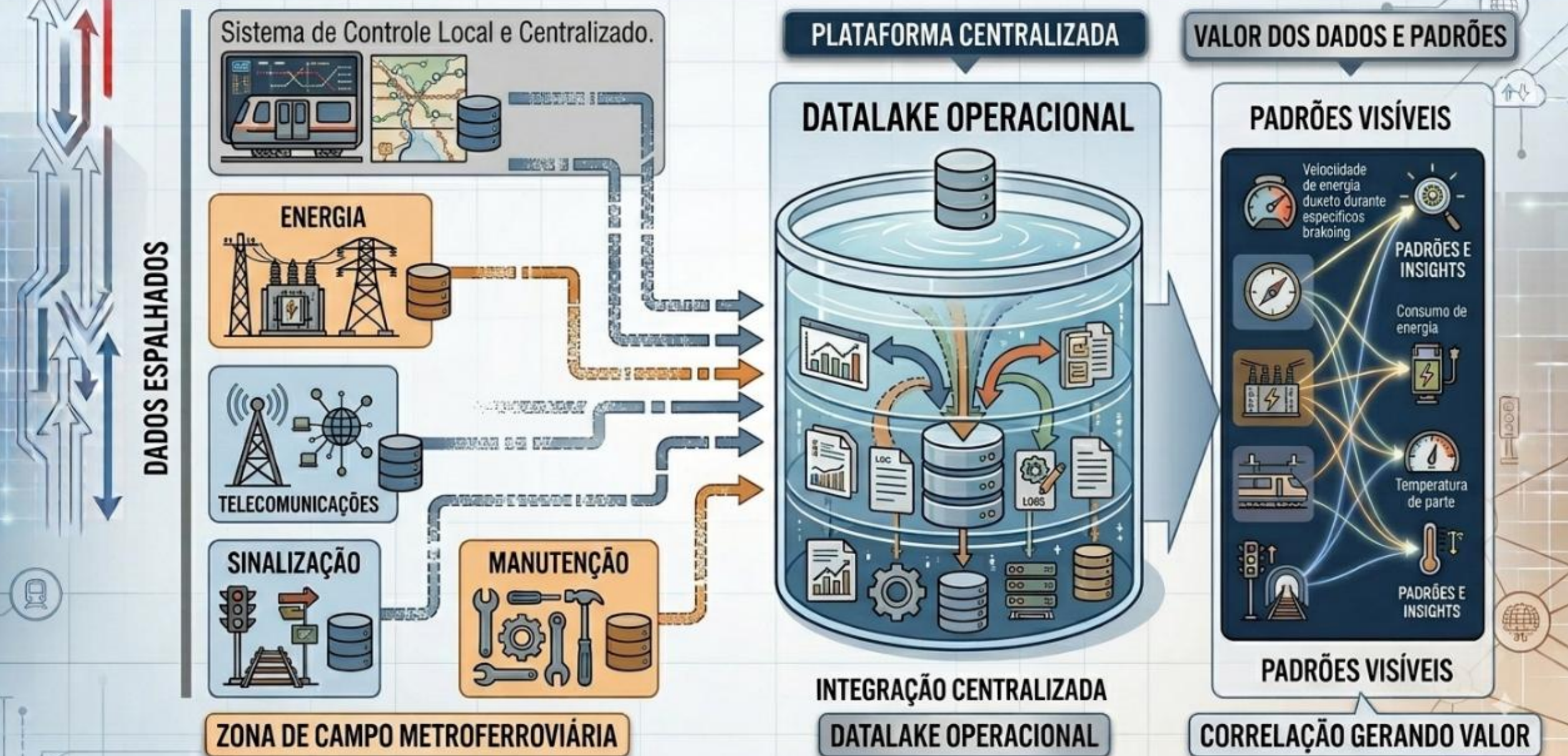


GOVERNANÇA
Políticas, qualidade e rastreabilidade de ponta a ponta



VALOR AO NEGÓCIO
Inteligência operacional, eficiência e inovação

DATALAKE OPERACIONAL: INTEGRANDO SISTEMAS METROFERROVIÁRIOS



MANUTENÇÃO AUTOMATIZADA E PRESCRITIVA

PADRÕES VISÍVEIS



GERAÇÃO AUTOMÁTICA DE O.S. (SAP)



Triagem IA e Agendamento

Dispatch Para Técnico (Mobile)

Action

PADRÕES VISÍVEIS



GATILHO DE INSIGHT (do Datalake) 100% Automatizada

SAP CRIAÇÃO DE ORDEM DE SERVIÇO

Nº da O.S.	(Automático)
Tipo:	Manutenção
Equipamento	
Local	
Sinal de Falha	
Responsável	

PROCESSADO COM SUCESSO

O.S. ID:

DADOS ESPALHADOS



INTEGRAÇÃO CENTRALIZADA DATALAKE OPERACIONAL

ENERGIA



SINALIZAÇÃO



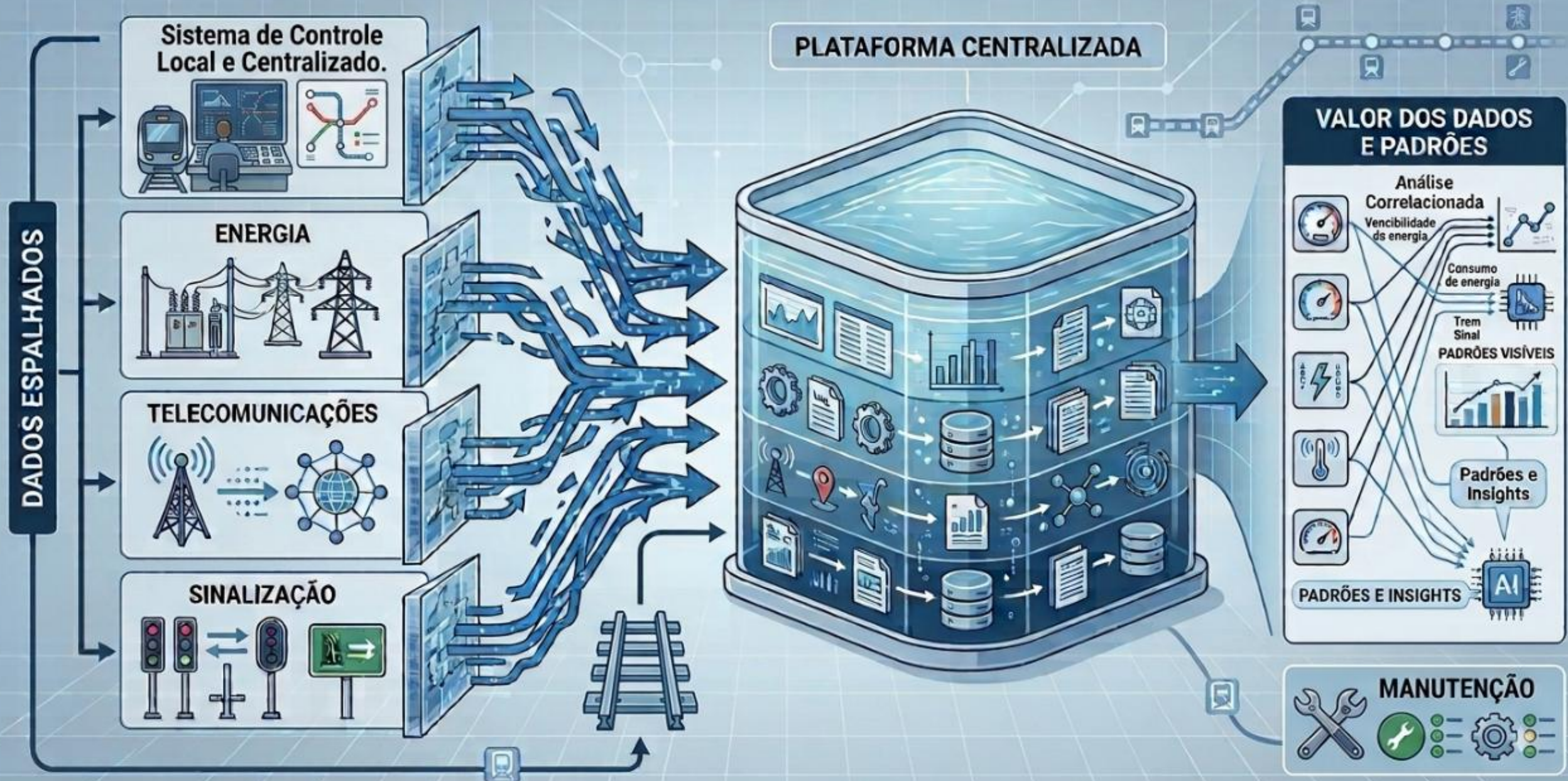
Sistema de Controle Local



MANUTENÇÃO



DATA DRIVEN OPERATION: OPERAÇÃO ORIENTADA A DADOS



CONCLUSÃO

A integração OT/IT é inevitável



INTEGRAÇÃO SEGURA ENTRE REDES OT E IT EM AMBIENTES METROFERROVIÁRIOS

Arquitetura baseada em IEC 62443, NIST SP 800-82, ISA-95, Purdue Model e Zones & Conduits

1. NORMAS E REFERÊNCIAS

- IEC 62443 – Segurança em Sistemas de Automação e Controle
- NIST SP 800-82 – Guia de Segurança para Sistemas OT
- ISA-95 – Integração entre Sistemas Empresariais e de Controle
- Purdue Model – Arquitetura por Níveis
- Zones & Conduits – Segmentação e Comunicação Controlada

2. PRINCÍPIOS APLICADOS

- Segmentação de Redes (Zones & Conduits)
- Defesa em Profundidade
- Princípio do Menor Privilégio
- Monitoramento Contínuo
- Alta Disponibilidade e Redundância
- Segurança sem comprometer a operação (Safety + Security)

3. BENEFÍCIOS

- Redução de riscos cibernéticos
- Maior disponibilidade dos sistemas
- Continuidade operacional
- Conformidade com normas internacionais
- Integração segura entre negócio e operação

6. IMPACTOS DA INTEGRAÇÃO OT/IT (COM ARQUITETURA ADEQUADA)

SEGURANÇA CIBERNÉTICA

- ✓ Redução da superfície de ataque
- ✓ Segmentação rápida e movimentação lateral
- ✓ Monitoramento e detecção de ameaças
- ✓ Conformidade com IEC 62443 e NIST SP 800-82

DISPONIBILIDADE

- ✓ Redundância de servidores e comunicação
- ✓ Segmentação evita falhas em cascata
- ✓ Monitoramento proativo
- ✓ Manutenção sem impacto na operação

CONTINUIDADE OPERACIONAL

- ✓ Processos críticos isolados e protegidos
- ✓ Resposta rápida a incidentes
- ✓ Integração segura para tomada de decisão
- ✓ Operação contínua e resiliente

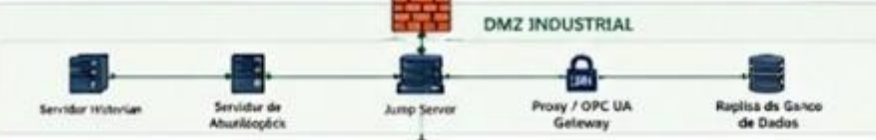
NÍVEL 5 CORPORATIVO (IT)



NÍVEL 4 NEGÓCIO (IT)



DMZ INDUSTRIAL



NÍVEL 3 OPERAÇÕES (OT)



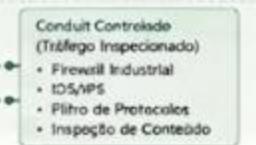
NÍVEL 2 SUPERVISÃO (OT)



NÍVEL 1 CONTROLE (OT)



NÍVEL 0 PROCESSO (OT)



4. ZONES & CONDUITS

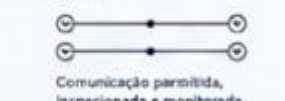
ZONES (Zonas)

Agrupamentos lógicos de ativos com requisitos de segurança semelhantes.



CONDUITS (Conduites)

Canais controlados que permitem a comunicação segura entre as zonas.



5. PRÁTICAS DE SEGURANÇA APLICADAS

- Autenticação forte (MFA, RBAC)
- Controle de Acesso Baseado em Função
- Gestão de Patches (Windows / Linux / OT)
- Monitoramento Contínuo (SIEM / SOC)
- Backup e Recuperação
- Resposta a Incidentes (Plano de Contingência)

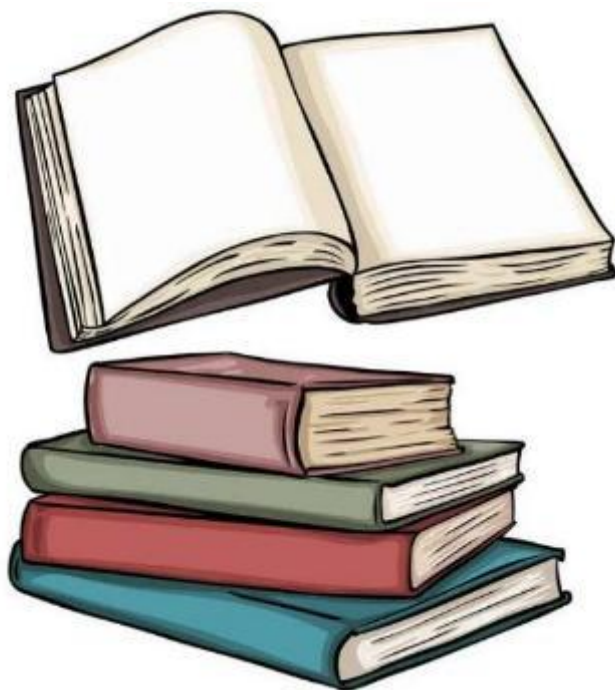
LEGENDA

— Rede IT — Rede OT --- Conduit (Comunicação Controlada) Firewall Industrial Switch Industrial

7. EXEMPLO DE FLUXO DE DADOS SEGURO



Fluxo controlado, inspecionado e autorizado



Bruce Schneier — *Secrets and Lies: Digital Security in a Networked World* (2000).

Ross Anderson — *Security Engineering*.

A segurança de uma rede não depende exclusivamente de seus controles tecnológicos, mas também do comportamento, das credenciais e das práticas de seus usuários.

A rede pode possuir as melhores tecnologias de segurança, mas continuará vulnerável se seus usuários forem o elo mais fraco.

O objetivo final não é conectar redes. É transformar dados operacionais em inteligência para o negócio.

32^a

SEMANA DE TECNOLOGIA METROFERROVIÁRIA

OBRIGADO(A)!

Vinicius Santos
Romolo Cyrino

vinicius.santos@linhauni.com.br

Romolo.Cyrino@linhauni.com.br



13ª Edição
Prêmio
Tecnologia &
Desenvolvimento
Metroferroviários

ANP TRILHOS
Associação Nacional dos Transportadores
de Passageiros sobre Trilhos

TIC TRENS

 **AEAMESP**
ASSOCIAÇÃO DOS ENGENHEIROS E ARQUITETOS DE METRÔ