ISA RIO DE JANEIRO SECTION TECH MEETING 2025

Rio de Janeiro Section

O Impacto da Transformação Digital e dos Padrões Abertos de Dados Industriais nos Negócios, Meio Ambiente e Sociedade

11 de dezembro de 2025 - das 8h às 18h

IBMEC – Campus Barra da Tijuca

Av. Armando Lombardi, 940, Rio de Janeiro / RJ

Segurança Cibernética em Tecnologia Operacional de Infraestruturas Críticas

“Só iremos nos prevenir daquilo que compreendemos como risco!”

CONTEXTUALIZAÇÃO

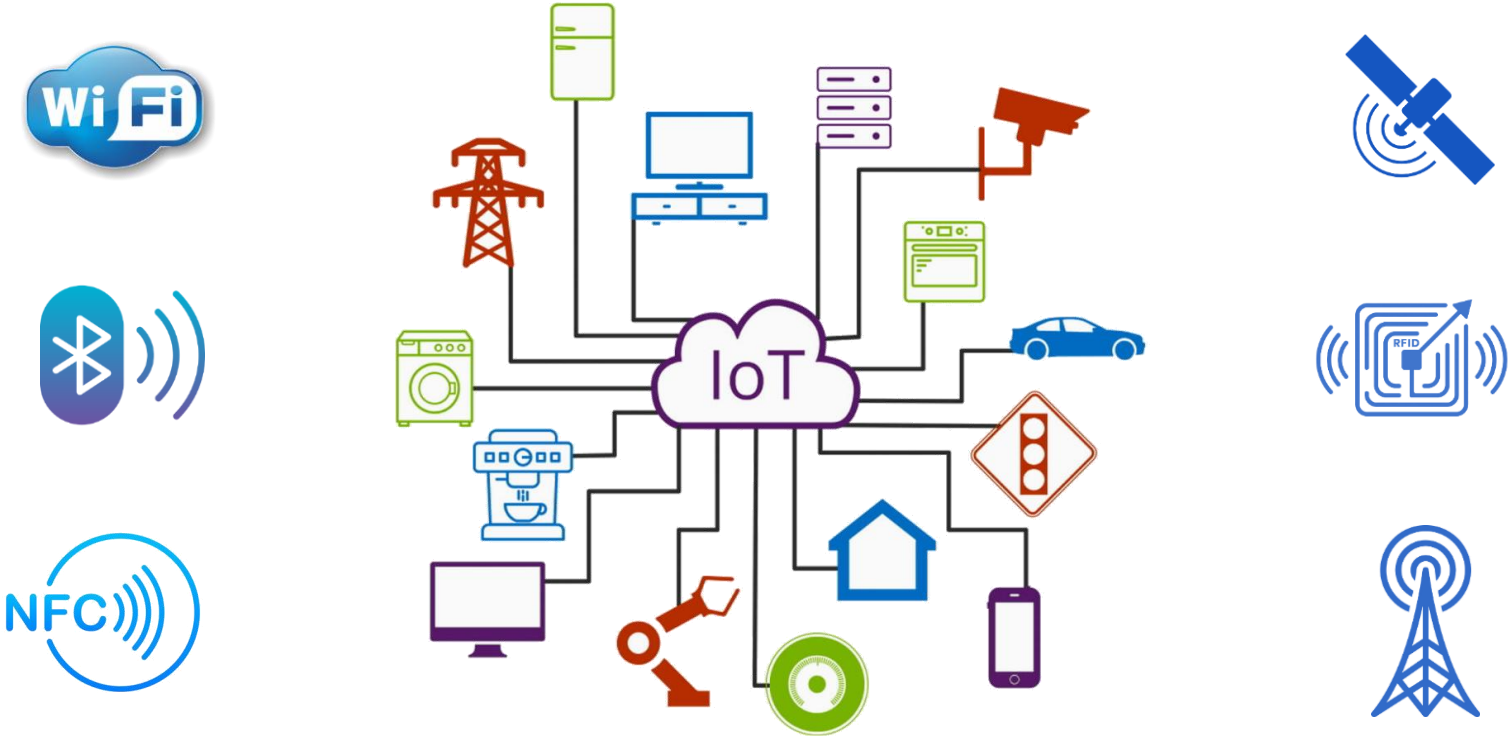
Estrutura de IT e OT

Hardwares

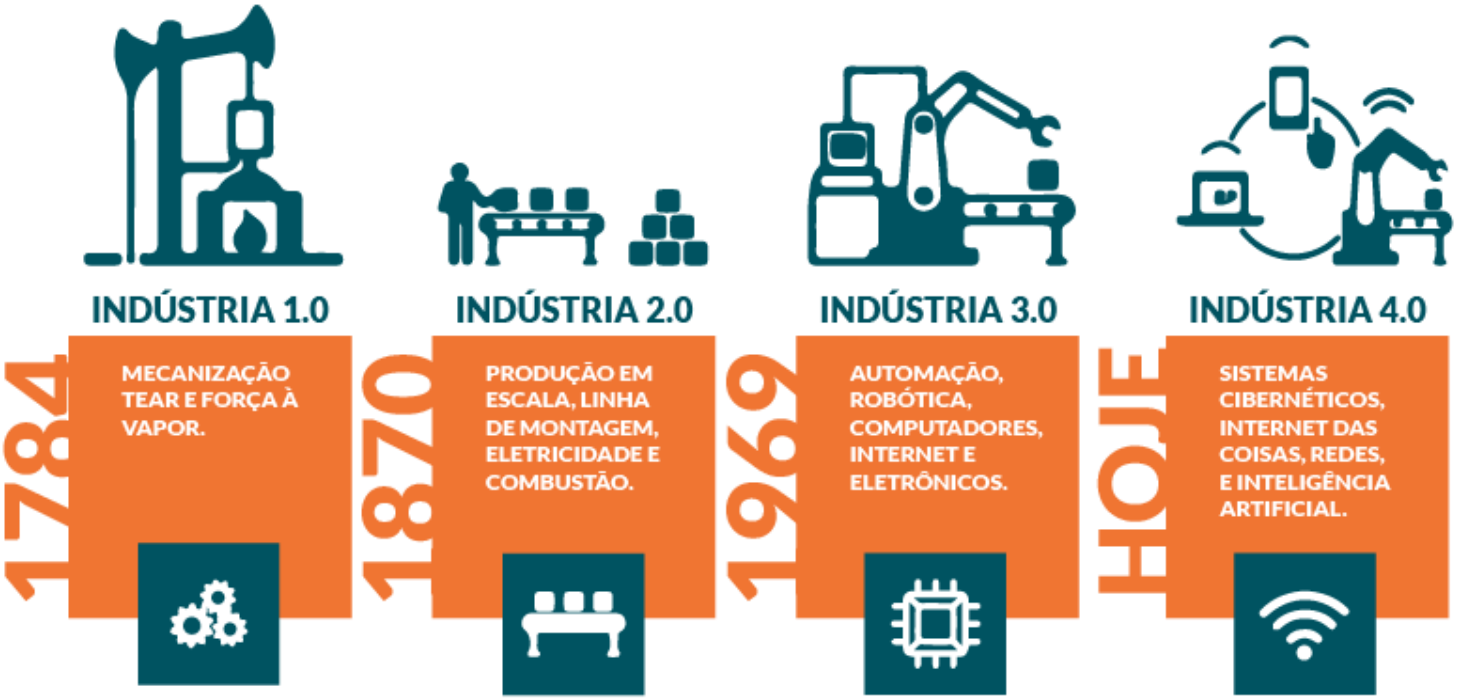
Softwares

Protocolos de Comunicação

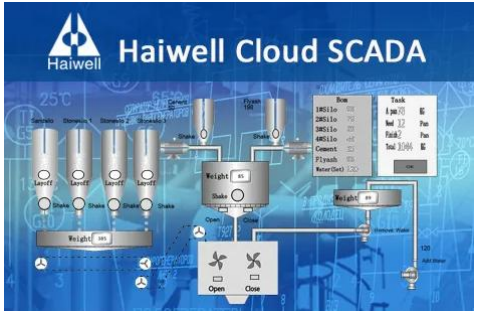
Internet das Coisas (IoT)



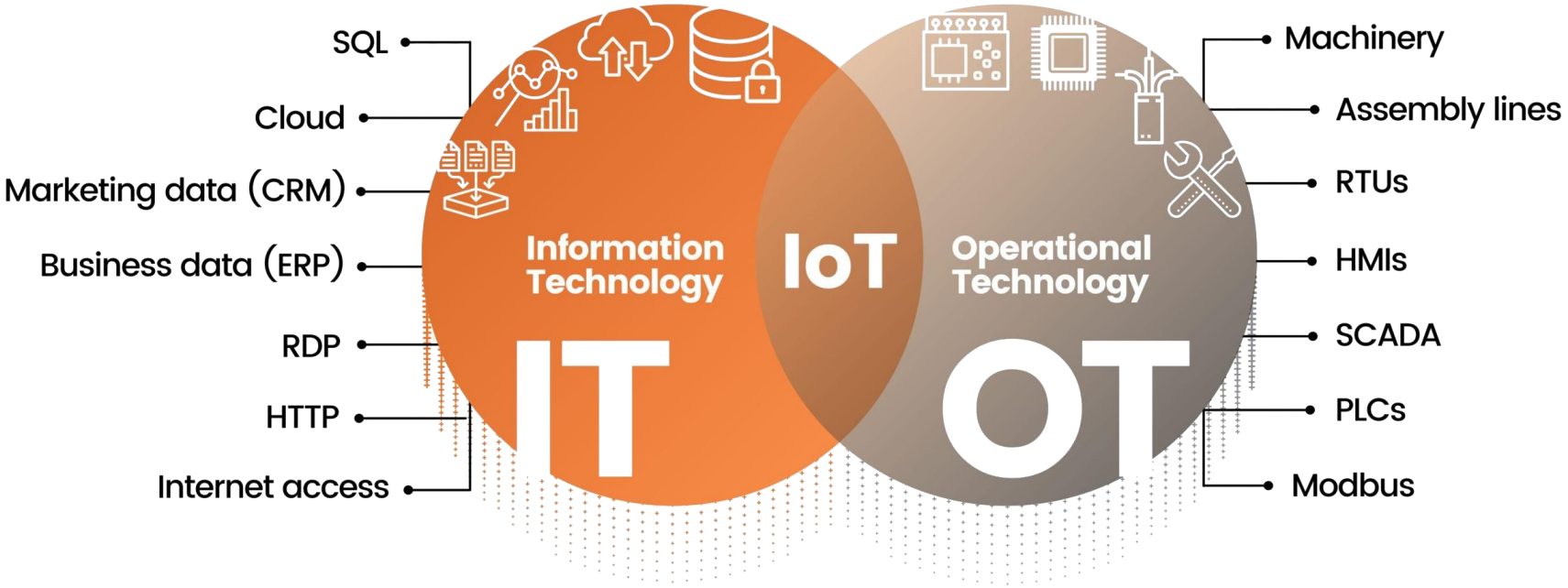
IoT e a 4ª Revolução Industrial



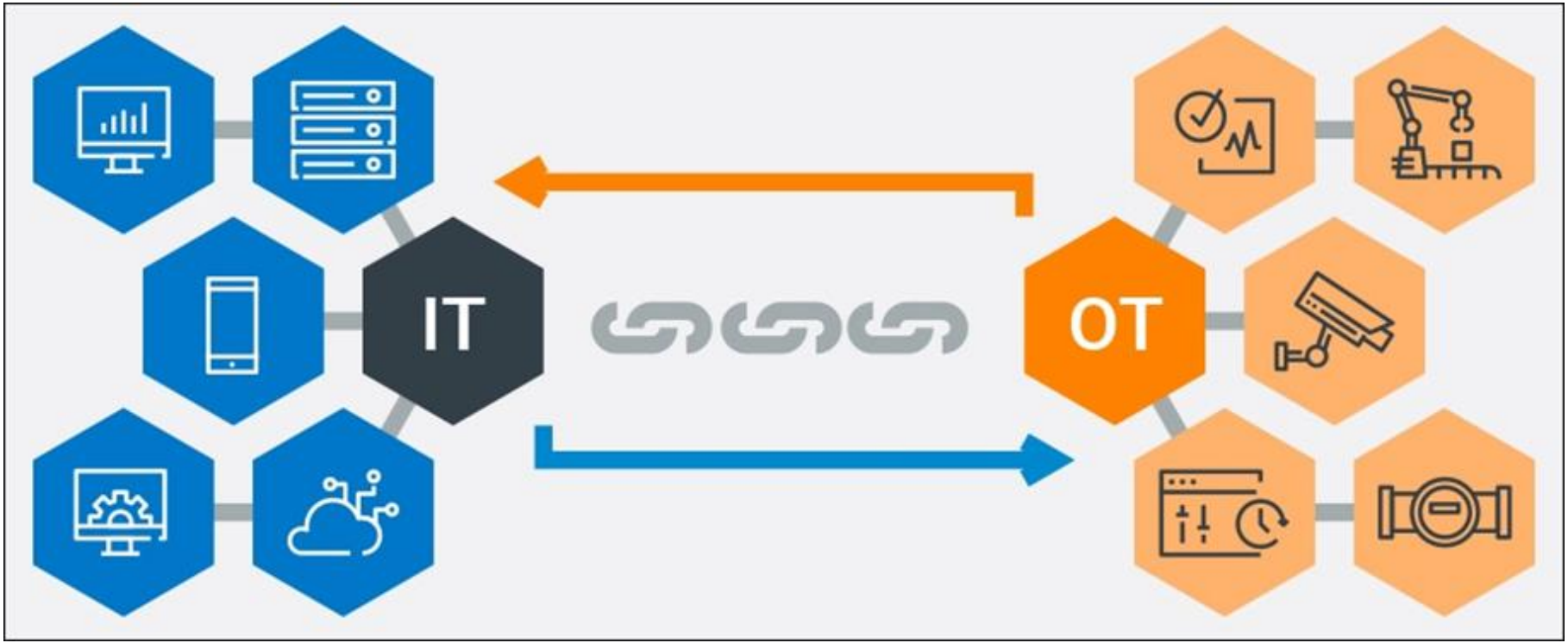
Nova Tecnologia Operacional



Integração OT e IT através de IoT

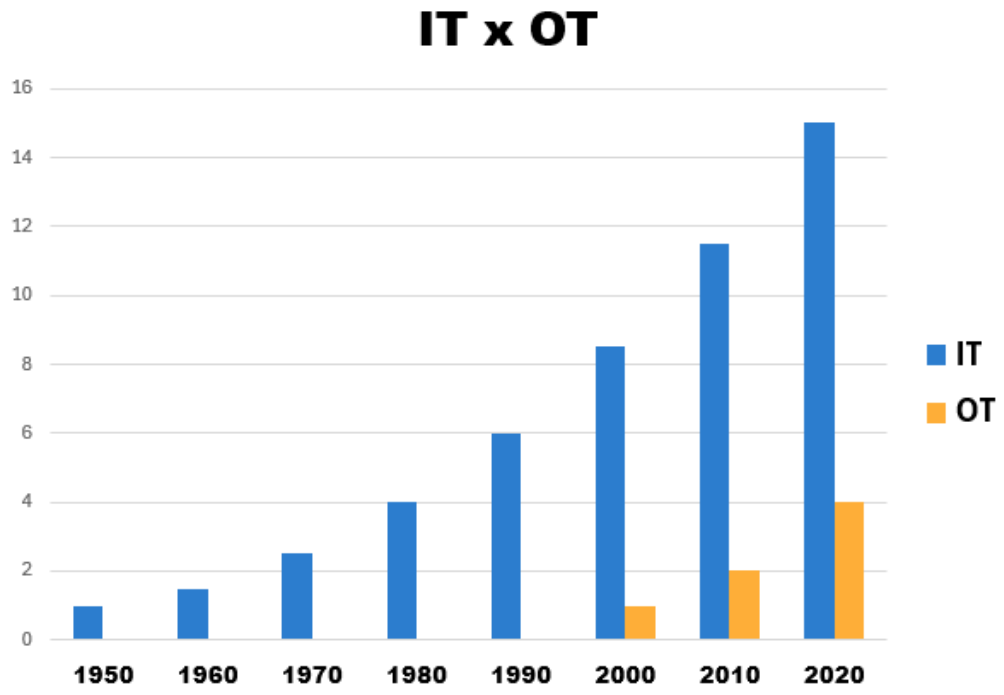


Tecnologias Diferentes e Integradas

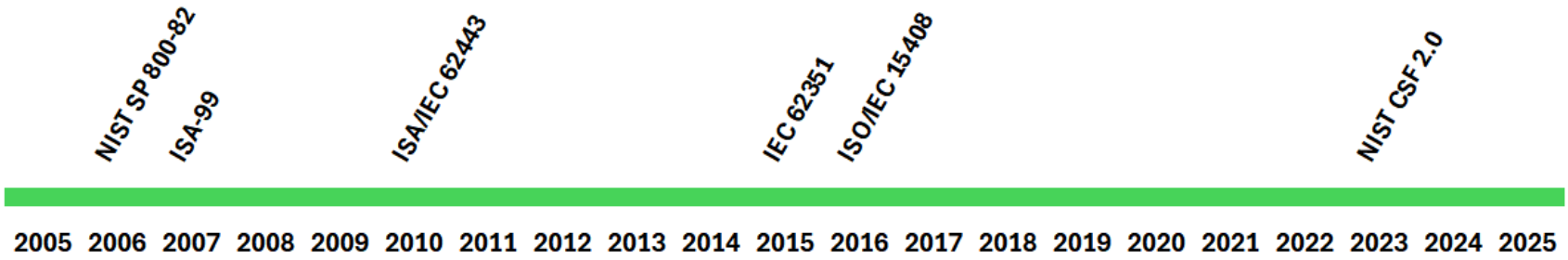


E A SEGURANÇA CIBERNÉTICA ?

Evolução da Segurança Cibernética



Evolução da Segurança Cibernética



ISA International Society of Automation
Setting the Standard for Automation™

ISO International Organization for Standardization

IEC International Electrotechnical Commission

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

POR QUE ENVOLVER SEGURANÇA CIBERNÉTICA?

Ciberataques à Infraestrutura Crítica

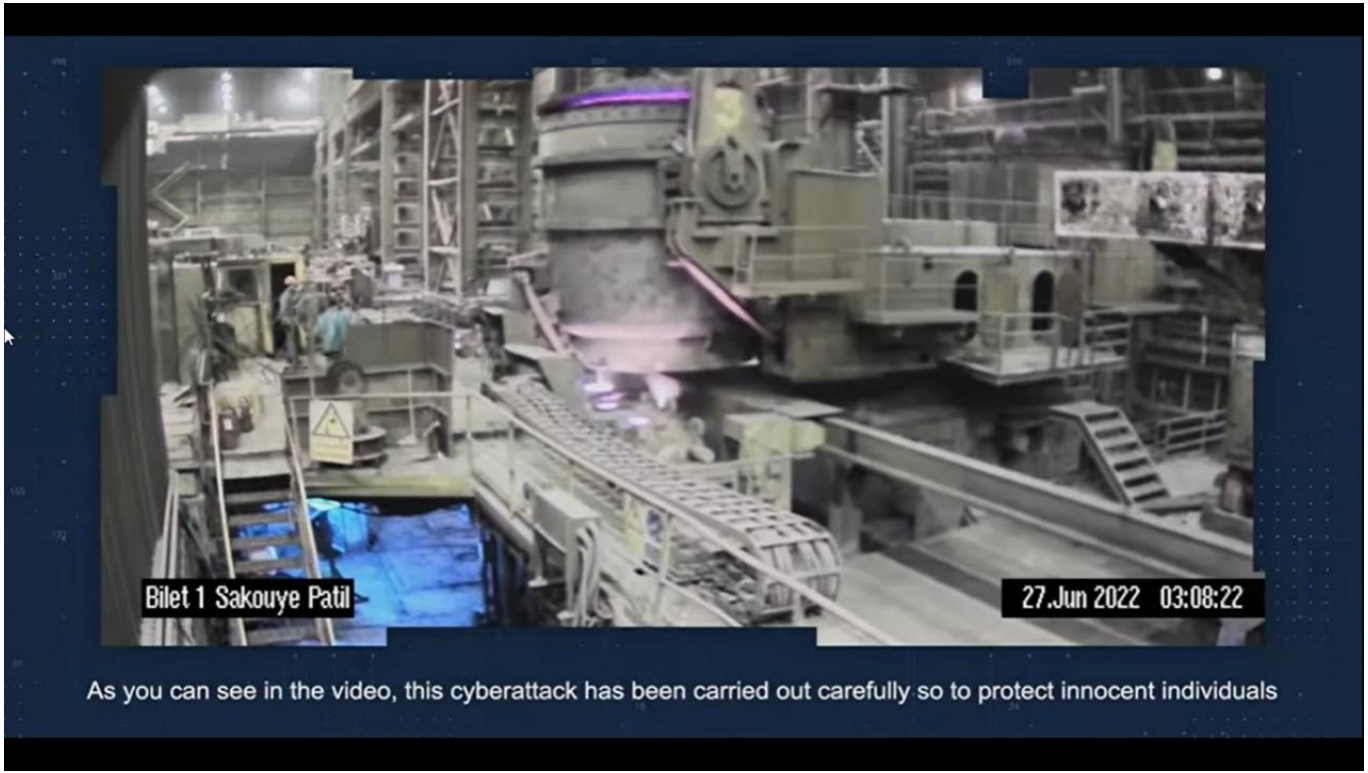
Junho/2022

Ciberataque paralisa companhia siderúrgica no Irã
Grupo responsável pelo ataque é o mesmo que já havia paralisado algumas infraestruturas críticas como ferrovias, radiodifusão e postos de gasolinas iranianos no ano passado

Fevereiro/2024

Gigante siderúrgica ThyssenKrupp sofre ciberataque e paralisa divisão automotiva
Uma das maiores produtoras de aço do mundo sofreu grande impacto devido a ataque ao se sistema de TI

Ciberataques à Infraestrutura Crítica



Ciberataques à Infraestrutura Crítica

Maio/2024

Rockwell pede desconexão de Internet para redes IoT

Fabricante de equipamentos industriais Rockwell pediu a seus clientes que desconectassem os dispositivos ICS da Internet devido ao aumento da atividade cibernética maliciosa. A empresa citou o aumento no número de atores de ameaças que visam infraestruturas críticas

Ciberataques à Infraestrutura Crítica

Agosto/2025

Ataque cibernético à Jaguar Land Rover gera prejuízo estimado de US$ 2,5 bilhões no Reino Unido

Paralisação afetou mais de 5 mil empresas e levou o governo britânico a oferecer US$ 2 bilhões em garantias de crédito à montadora

Ciberataques à Infraestrutura Crítica

CASOS DE ALTO IMPACTO NO SANEAMENTO

Ciberataques ao Saneamento

Novembro/2023

Instalação de água da Pensilvânia atingida por hackers ligados ao Irã

Um grupo hacker anti-Israel com ligações ao Irã forçou uma estação de tratamento de água na Pensilvânia a entrar em operação manual

Fevereiro/2024

Hacker invade e altera tratamento de água na Flórida

Invasão ao sistema ocorreu através do software de acesso remoto que os operadores usavam para manutenção e alterou o nível de hidróxido de sódio de 100 para 11.100 partes por milhão

Ciberataques ao Saneamento

Ciberataques ao Saneamento

Fevereiro/2024

Infraestrutura crítica está em risco real e imediato

*A Agência de Segurança Cibernética e de Infraestruturas (**CISA**), a Agência de Segurança Nacional (**NSA**) e o Departamento Federal de Investigação (**FBI**), em conjunto com as principais agências internacionais e governamentais do EUA, como a Agência de Proteção Ambiental (**EPA**), publicaram um **Aviso Conjunto de Segurança Cibernética** em 7 de fevereiro sobre atividades maliciosas de um grupo de ataque conhecido como Volt Typhoon que é patrocinado pela China*

Ciberataques ao Saneamento

Ciberataques ao Saneamento

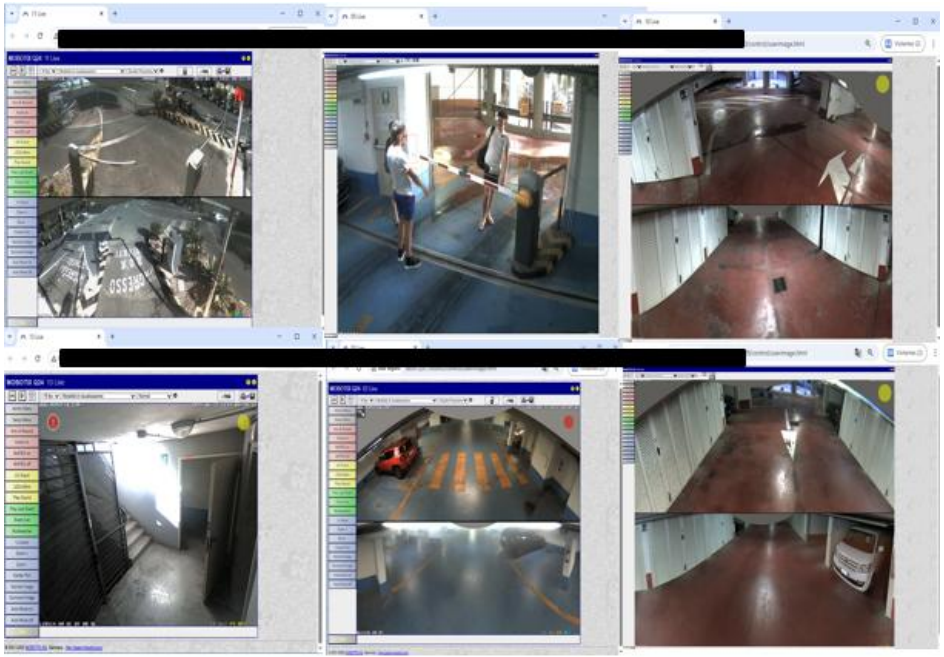
Julho/2024

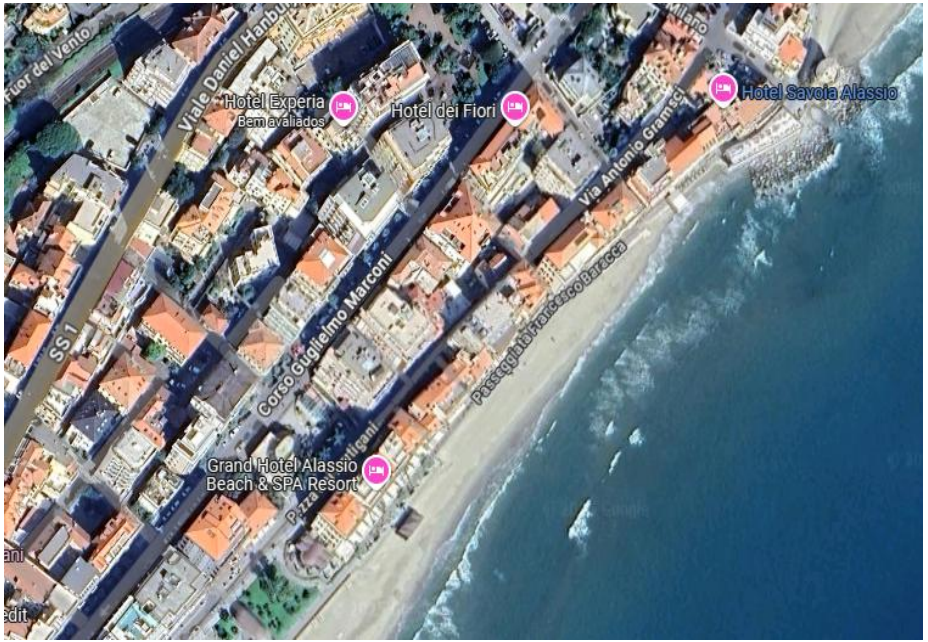
Prioridade Máxima: EUA declaram guerra total aos ciberataques chineses

A China tem sido acusada de realizar inúmeros ataques cibernéticos contra infraestruturas críticas dos EUA, com um foco particular em endpoints expostos à Internet em instalações de água. Estes ataques não só comprometem a segurança de sistemas, mas também ***colocam em risco a saúde pública e a segurança nacional***

Ativos Expostos na Internet

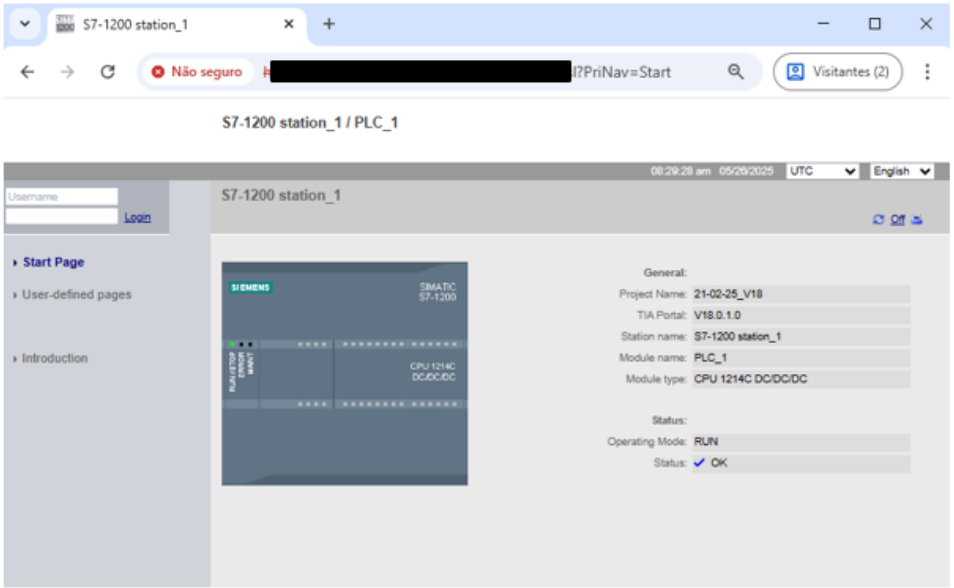
Sistema de videomonitoramento em hotel na Itália

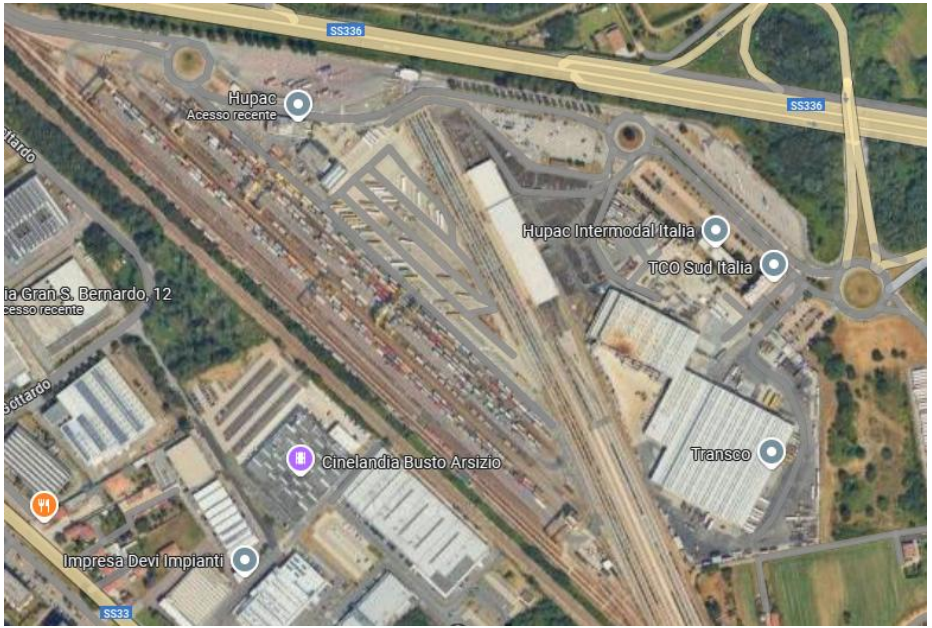




Ativos Expostos na Internet

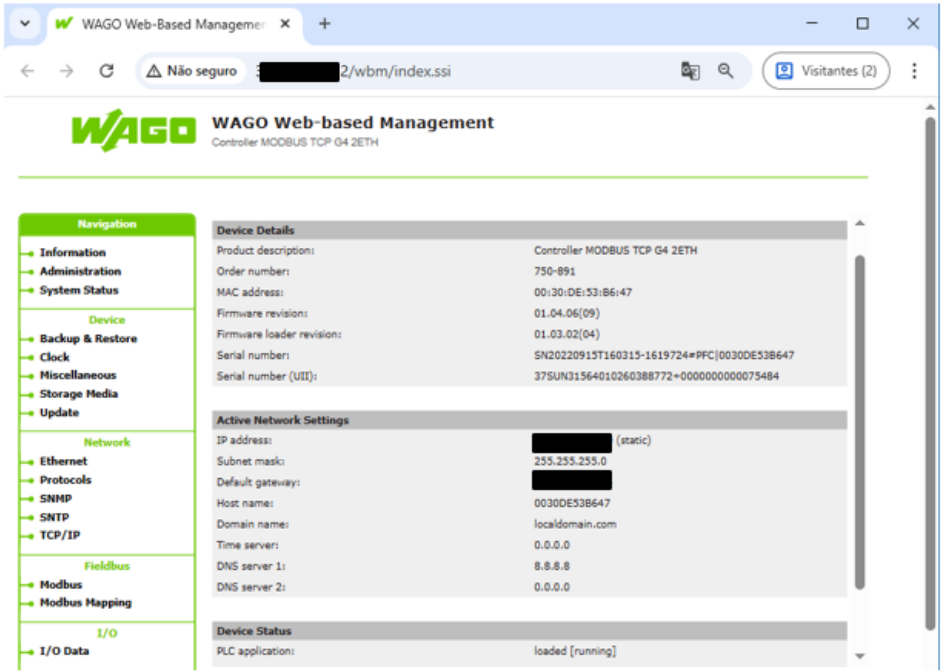
PLC de empresa ferroviária na Itália





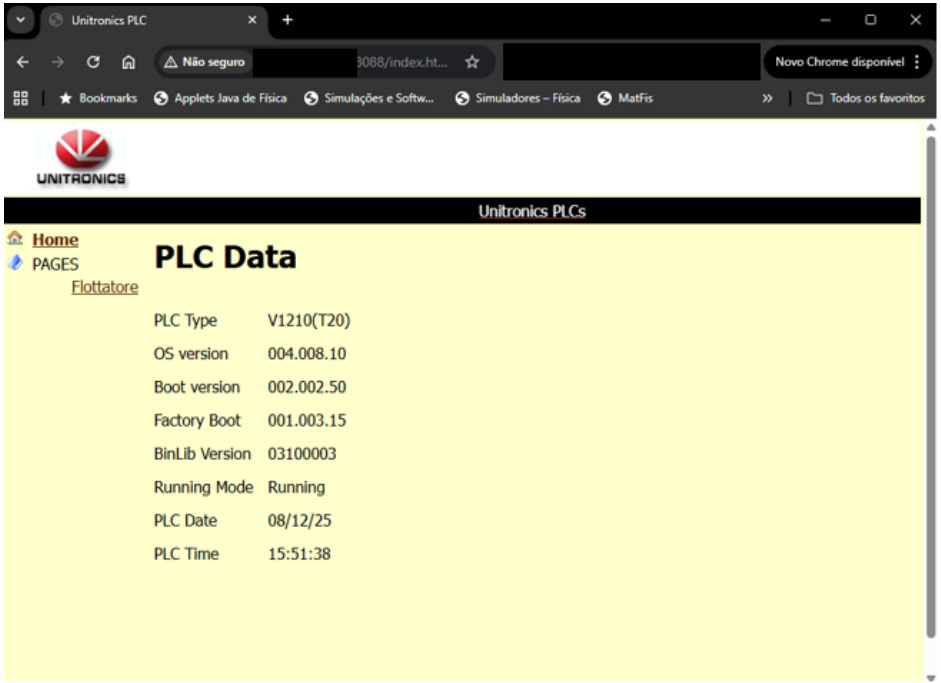
Ativos Expostos na Internet

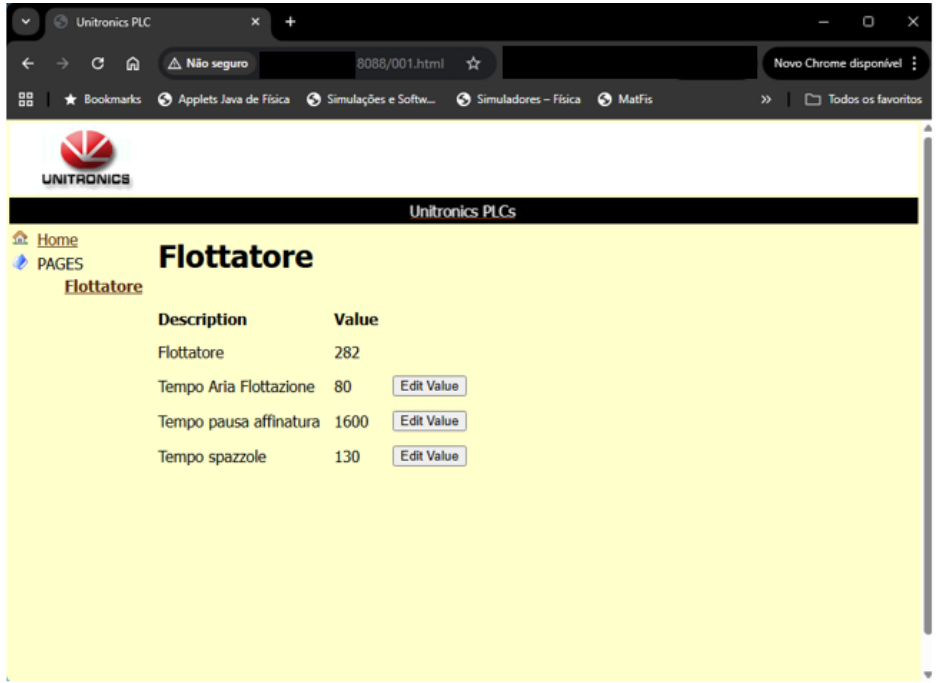
Controlador Modbus em empresa de saneamento na Suíça



Ativos Expostos na Internet

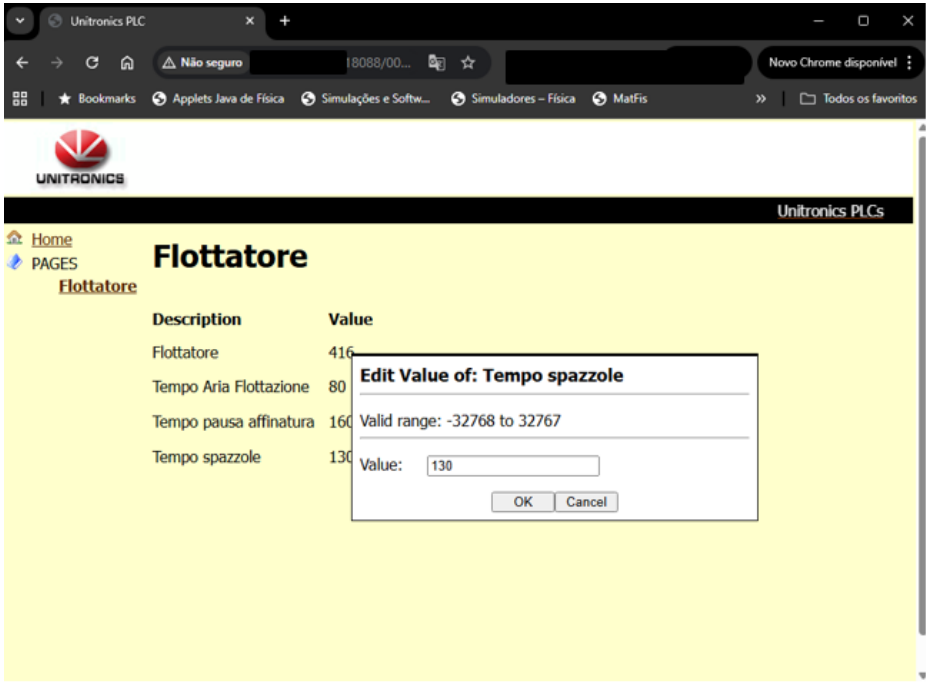
PLC + HMI em empresa de saneamento na Itália

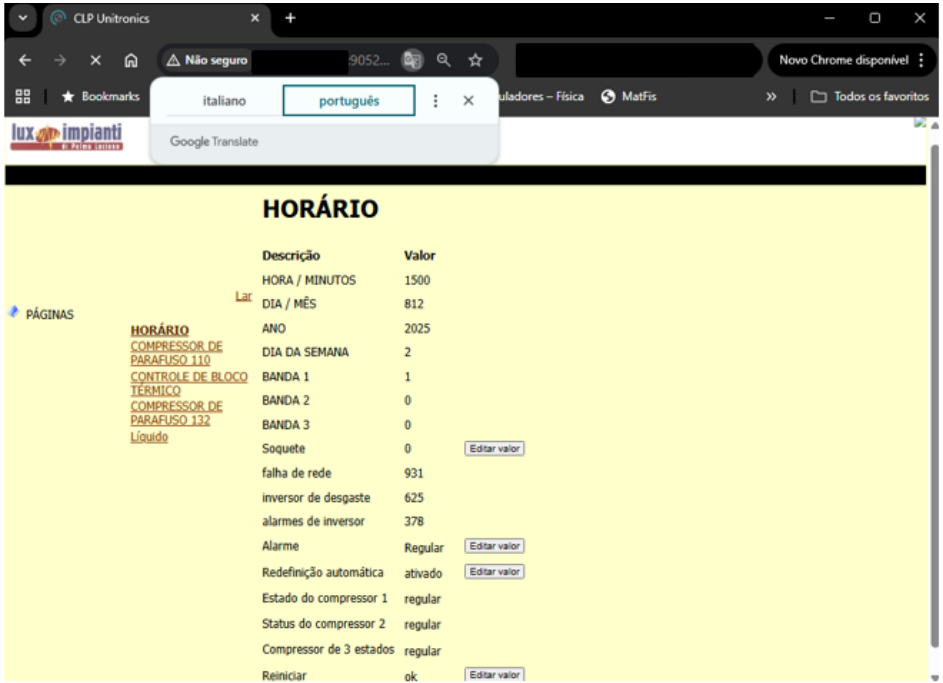




Ativos Expostos na Internet

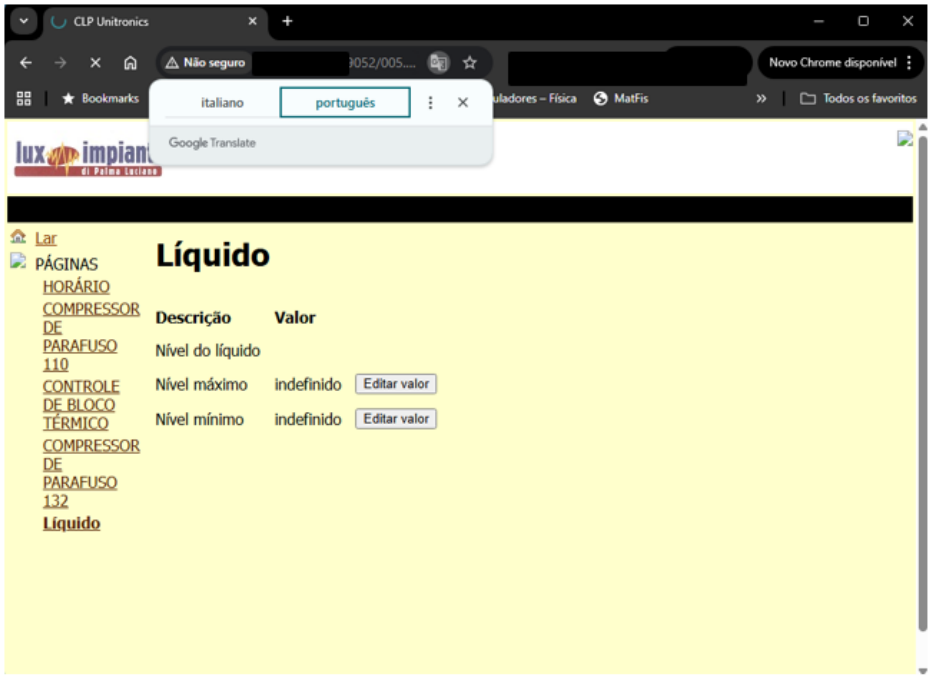
PLC + HMI em empresa de saneamento na Itália





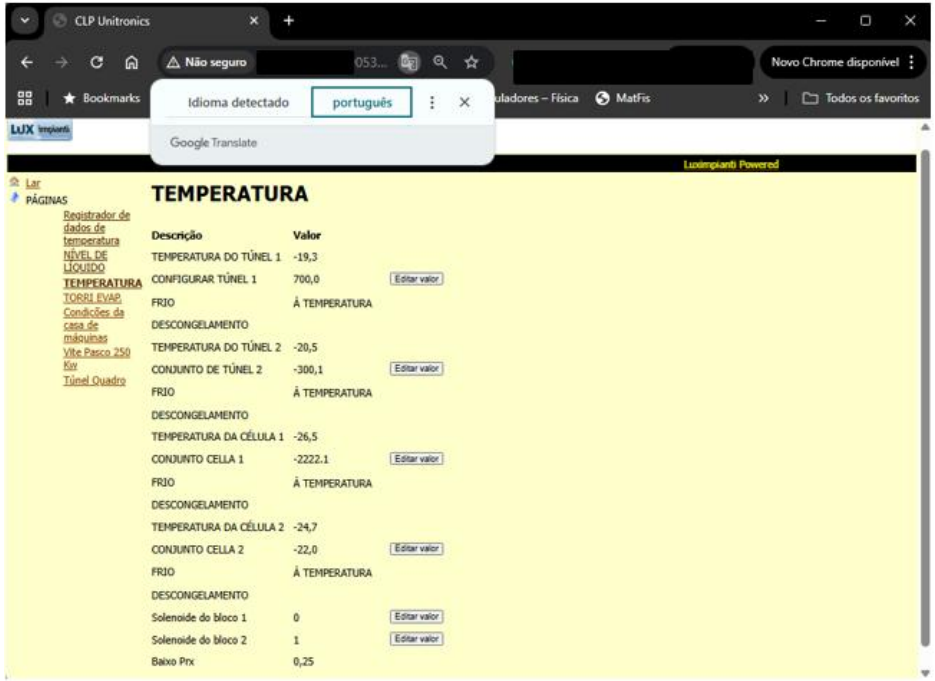
Ativos Expostos na Internet

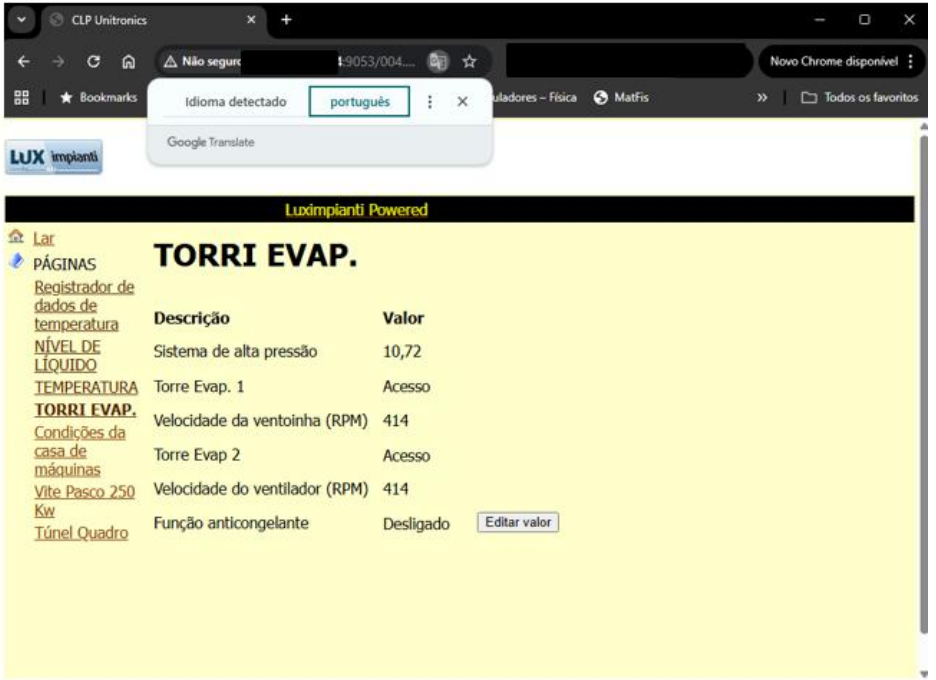
PLC + HMI em empresa de saneamento na Itália



Ativos Expostos na Internet

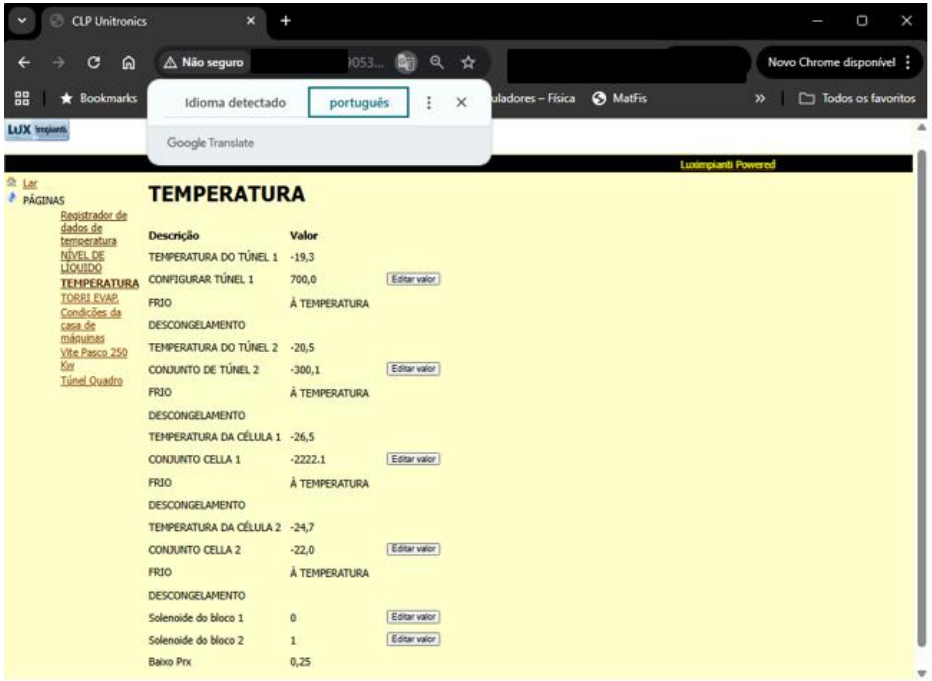
PLC + HMI em empresa de saneamento na Itália





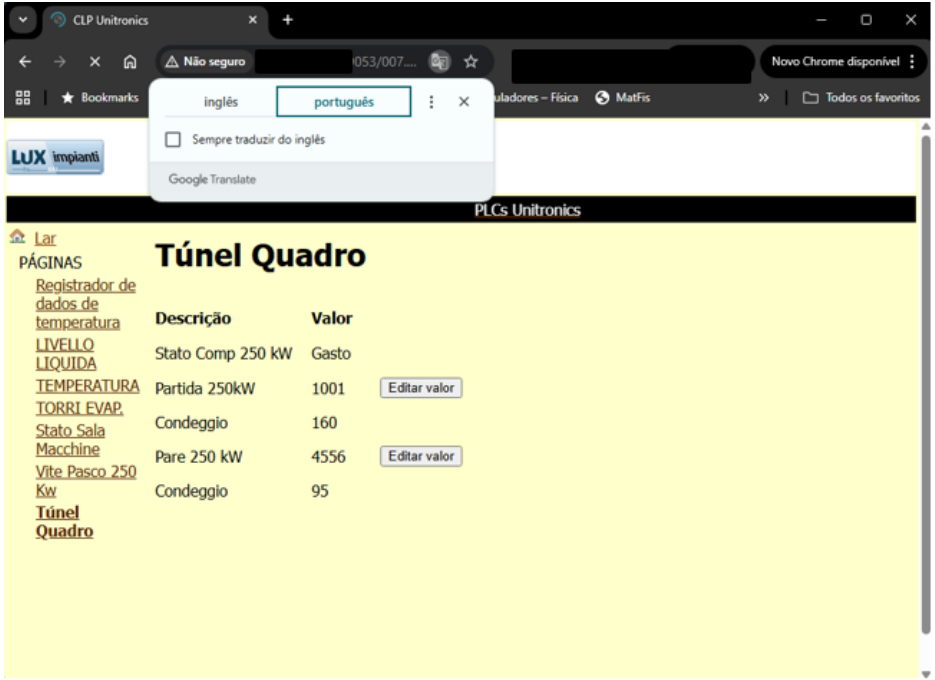
Ativos Expostos na Internet

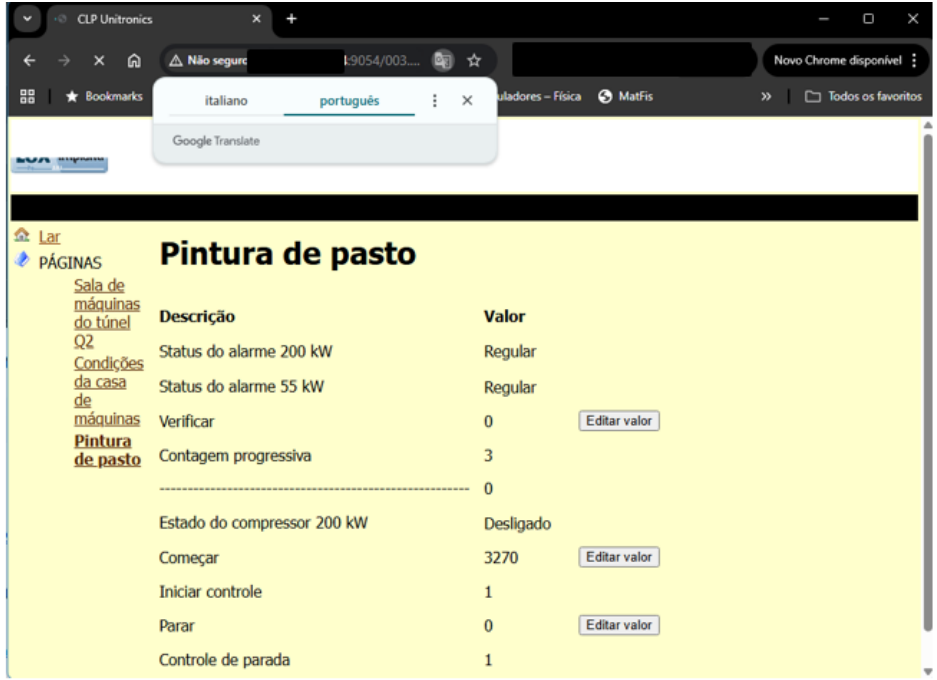
PLC + HMI em empresa de saneamento na Itália



Ativos Expostos na Internet

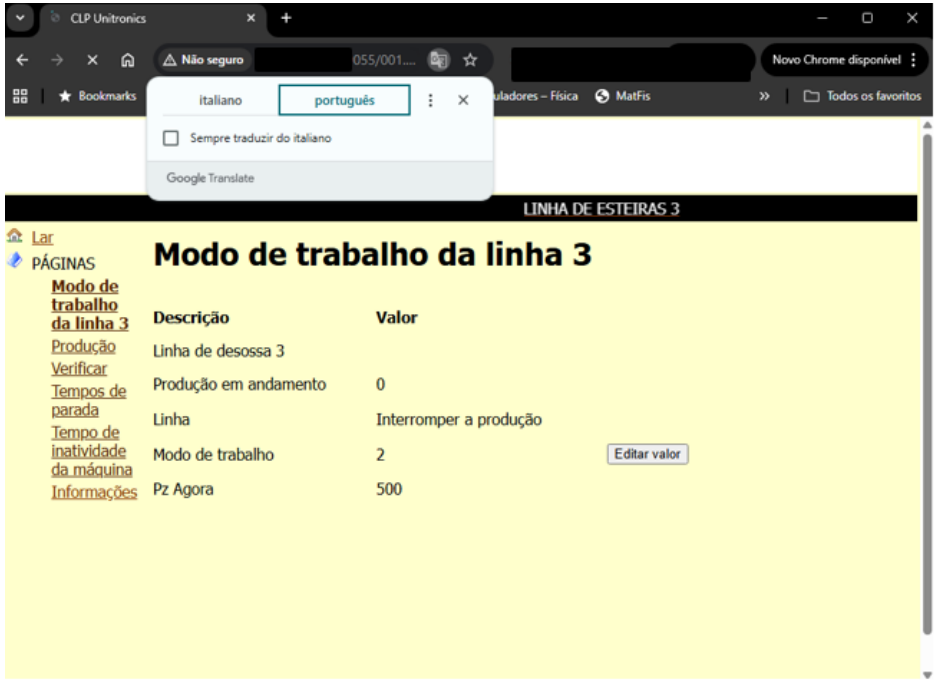
PLC + HMI em empresa de saneamento na Itália

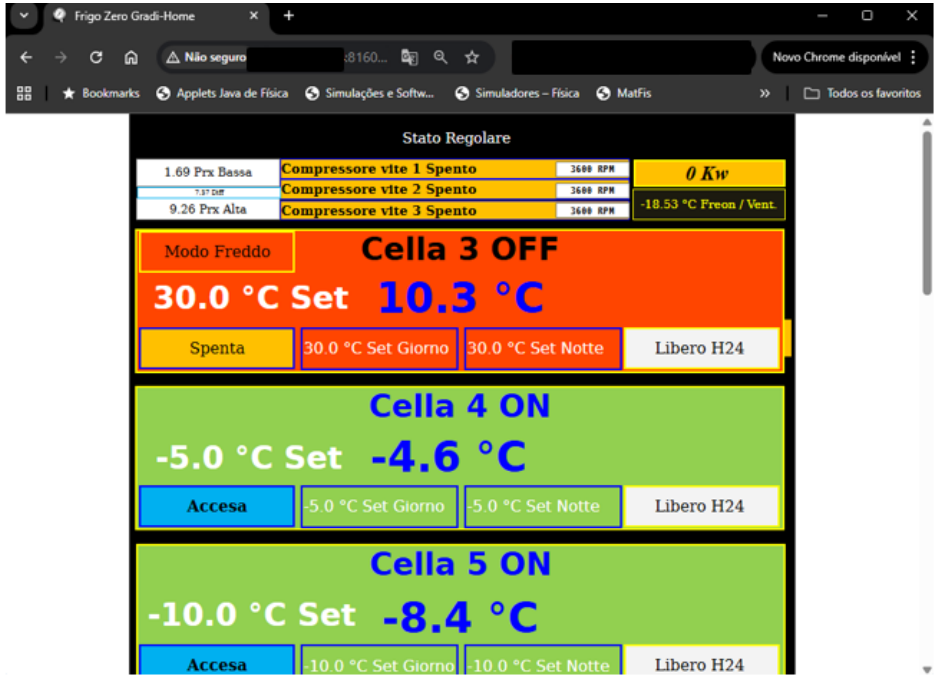




Ativos Expostos na Internet

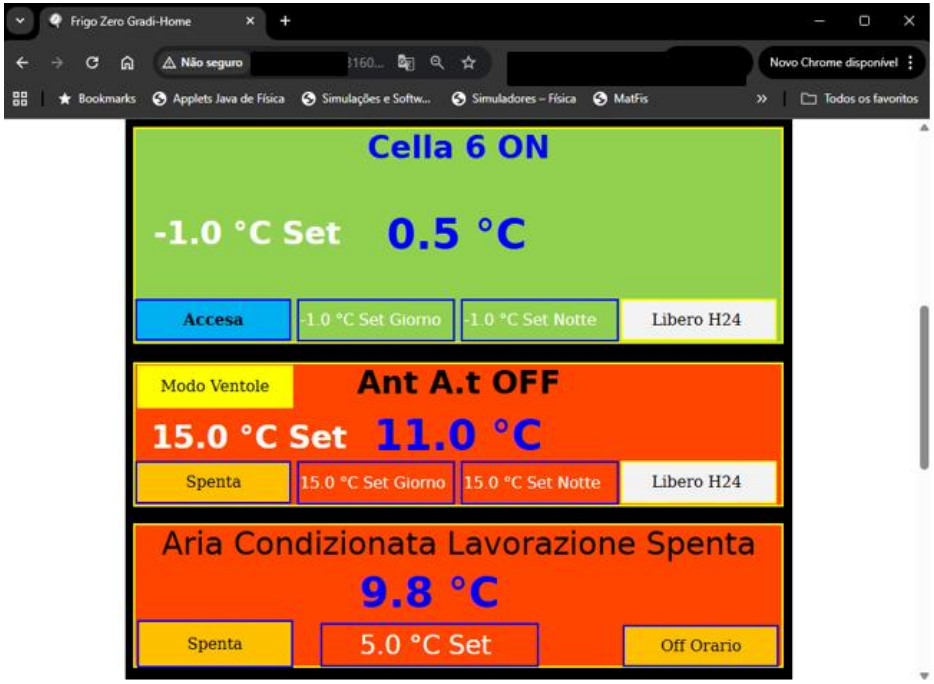
PLC + HMI em empresa de saneamento na Itália

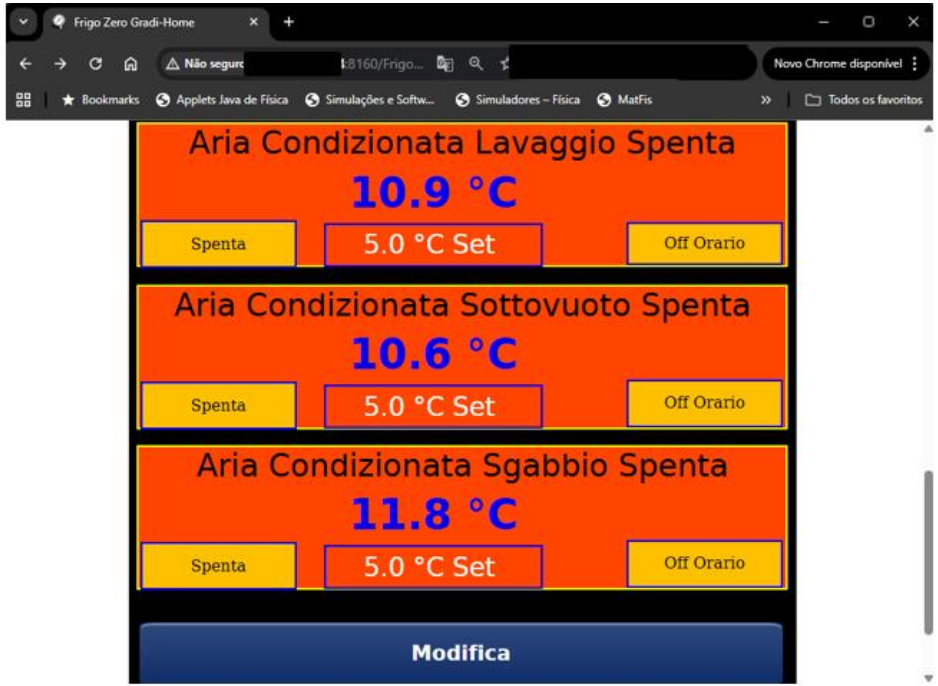




Ativos Expostos na Internet

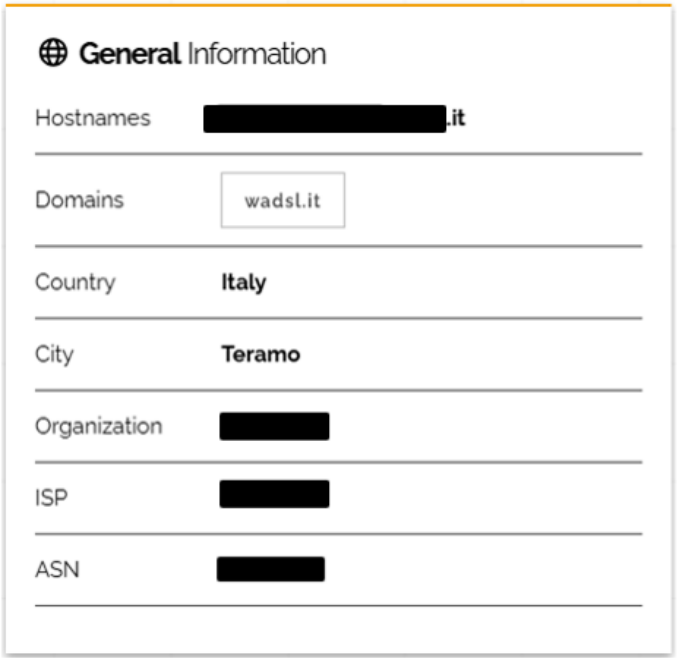
PLC + HMI em empresa de saneamento na Itália

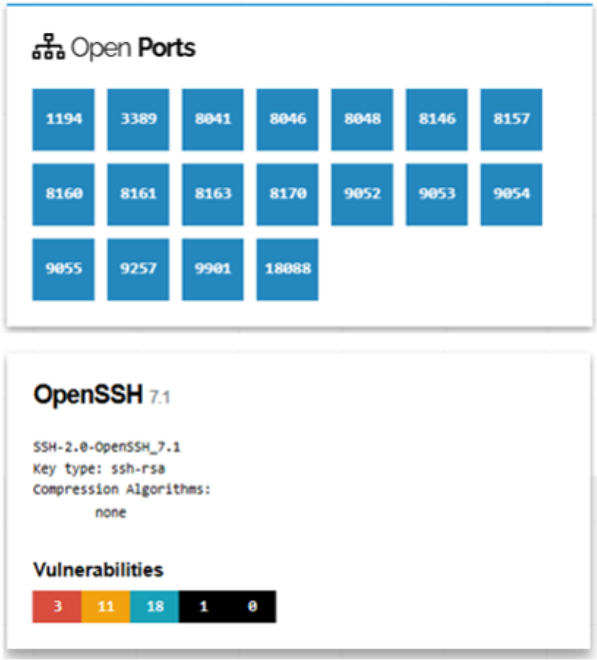




Ativos Expostos na Internet

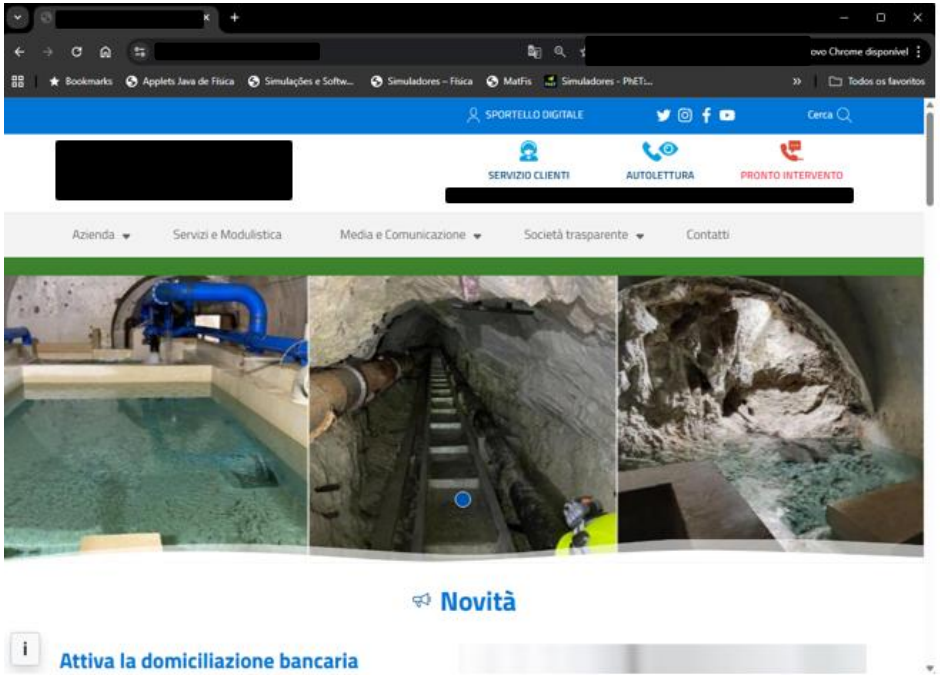
PLC + HMI em empresa de saneamento na Itália

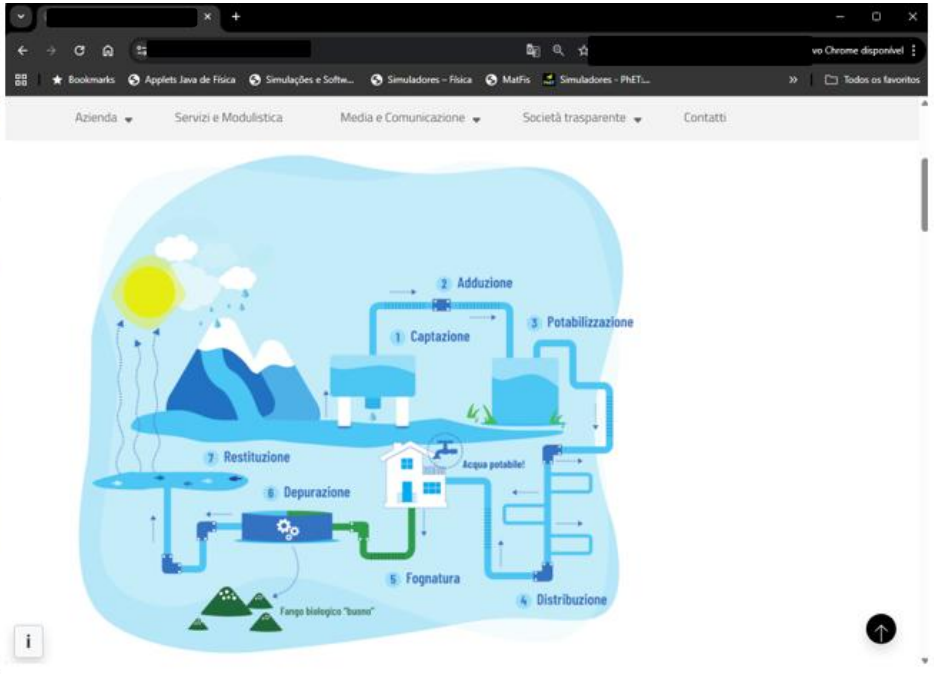




Ativos Expostos na Internet

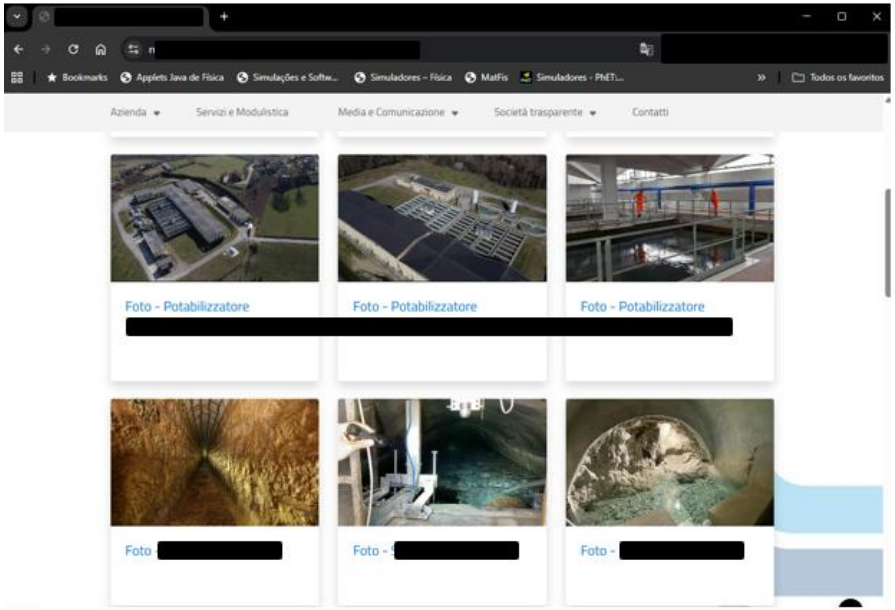
PLC + HMI em empresa de saneamento na Itália





Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália



E NO BRASIL ?

Ciberataques no Brasil

Março/2024

Grupo Dark Storm anuncia ataques a infraestruturas críticas do Brasil

Ameaça visa backbones de Internet, aeroportos, hospitais, serviços e sites do Governo, como represália a nações que apoiam Israel contra o Hamas

Abril/2024

Infraestrutura crítica brasileira está sob ciberataques

Brasil sofreu 61 ciberataques em infraestruturas críticas em 2023, trazendo impactos em setores diversos, incluindo tecnologia, saúde, agricultura e governo

Ciberataques no Brasil

Abril/2025

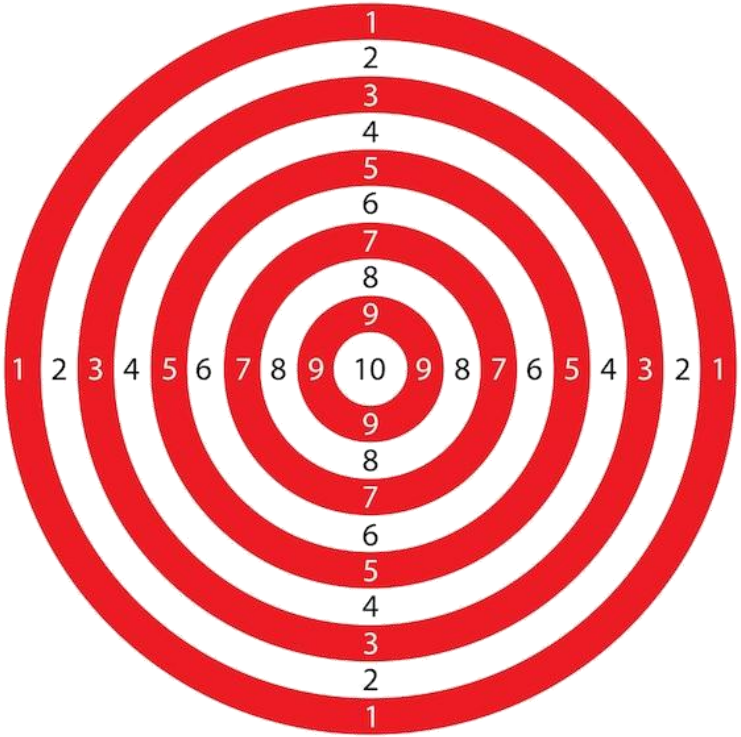
Ataque hacker suspende atividades do IPEN, um dos principais produtores de fármacos contra o câncer do Brasil

Ação foi classificada como altamente sofisticada e organizada, segundo a Comissão Nacional de Energia Nuclear (CNEN) e paralisou a linha de produção por vários dias

Ciberataques no Brasil

QUAIS SÃO AS MOTIVAÇÕES?

Motivações de Ciberataques



- **Motivação Financeira**
- **Espionagem Industrial**
- **Hacktivismo Político**
- **Vingança**
- **Sabotagem**
- **Desafio e Notoriedade**
- **Curiosidade e Pesquisa**
- **Terrorismo**

Componente Geopolítico

COMO INTEGRAR OT, IT E SEGURANÇA CIBERNÉTICA ?

Plano Estratégico - Etapas

Fase 1 - Diagnóstico e Avaliação Inicial

- Inventário de ativos OT/ICS
- Mapeamento de topologias físicas e lógicas
- Risk Assessment em OT
- Análise de vulnerabilidades técnicas
- Gap Analysis em relação à ISA/IEC 62443 e NIST SP 800-82

Fase 2 - Definição de Políticas e Arquitetura Segura

- Criação e/ou revisão de política de segurança OT
- Definição de zonas e conduítes de segurança
- Definição de controles de acesso físico e lógico
- Revisão de protocolos industriais
- Gestão de vulnerabilidades, patches e mudanças

Fase 3 - Implementação de Controles Técnicos

- Segmentação de redes IT/OT com firewalls industriais
- Controle de acesso a dispositivos OT
- Whitelisting de aplicações em HMIs e servidores
- Monitoramento contínuo de tráfego OT
- Hardening de PLC, switches industriais, estações
- Controle de mídias removíveis e acesso remoto seguro

Fase 4 - Capacitação e Conscientização

- Treinamento para operadores sobre segurança OT
- Simulações de resposta a incidentes OT

Fase 5 - Monitoramento Contínuo e Resposta a Incidentes

- Implantação de SOC OT ou integração com SOC IT
- Configuração de SIEM com fontes OT
- Resposta a Incidentes OT com playbooks específicos
- Integração Threat Intelligence para ambientes industriais

Fase 6 - Melhoria Contínua

- Revisão periódica de riscos
- Atualização de patches/firmware em ciclo de manutenção
- Auditorias técnicas anuais de segurança OT
- Testes de penetração não-invasivos (PenTest OT)
- Simulações anuais de crises cibernéticas OT

Plano Estratégico - Fontes

Normas e Frameworks

ISA International Society of Automation
Setting the Standard for Automation™

IEC International Electrotechnical Commission

ISO International Organization for Standardization

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Consultorias

Gartner

Fornecedores

CLAROTY

FORTINET

Honeywell

NOZOMI NETWORKS

Rockwell Automation

westcon

ISA 99 – ISA/IEC 62443

Geral	IEC 62443-1-1	IEC 62443-1-2	IEC 62443-1-3	IEC 62443-1-4	
	Conceitos e Modelos	Glossário Mestre de Termos e Abreviações	Métricas de conformidade de segurança do sistema	Ciclo de vida de segurança e casos de uso do IACS	
Políticas e Procedimentos	IEC 62443-2-1	IEC 62443-2-2	IEC 62443-2-3	IEC 62443-2-4	IEC 62443-2-5
	Requisitos do programa de segurança para proprietários de ativos do IACS	Guia de implementação para um sistema de gerenciamento de segurança IACS	Gerenciamento de patches no ambiente IACS	Requisitos para Fornecedores de Soluções IACS	Orientação de implementação para proprietários de ativos do IACS
Sistema	IEC 62443-3-1	IEC 62443-3-2	IEC 62443-3-3		
	Tecnologias de Segurança para IACS	Avaliação de Riscos de Segurança e Projeto de Sistemas	Requisitos de segurança do sistema e níveis de segurança		
Componente	IEC 62443-4-1	IEC 62443-4-2			
	Requisitos do ciclo de vida de desenvolvimento de produtos seguros	Requisitos técnicos de segurança para componentes IACS			

Normas Internacionais para Segurança de Sistemas de Automação e Controle Industrial (IACS) e Redes de Tecnologia Operacional (OT)

Integração IT, OT e Cibersegurança

Obrigado!

Paulo Santos
Chefe de Departamento de Infraestrutura e Segurança da Informação - CEDAE

E-mail: psantos@cedae.com.br
Tel.: (21) 2562-6070
(21) 98736-9854