

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

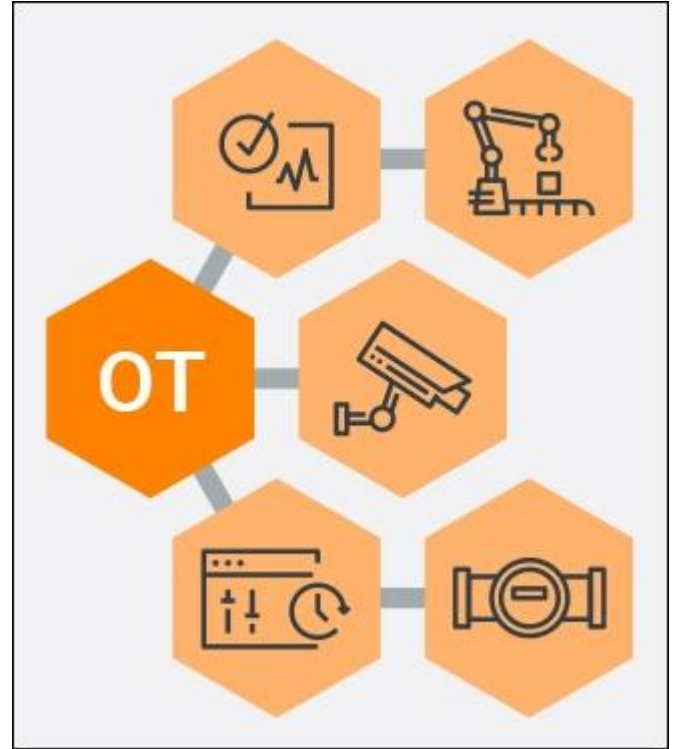
Estrutura de IT e OT



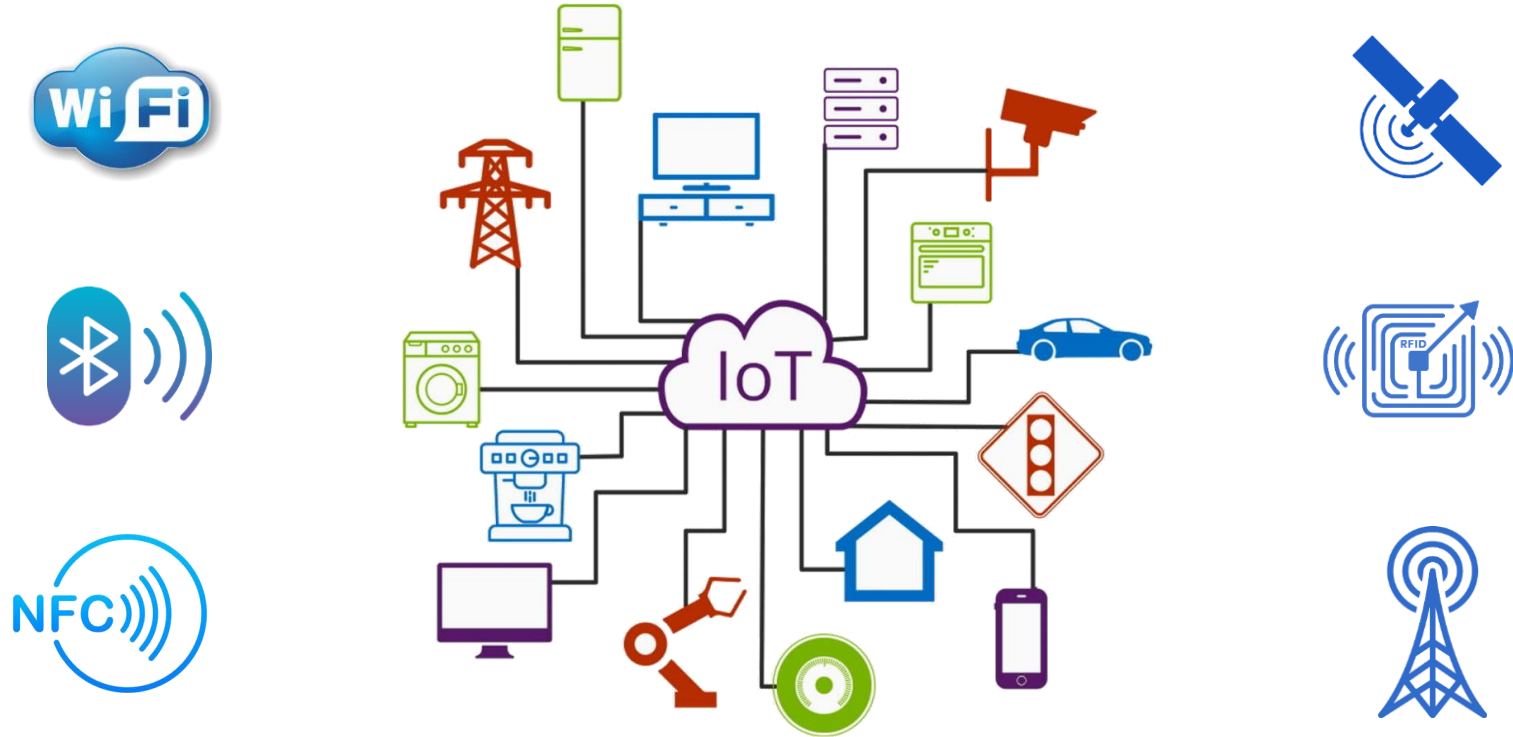
Hardwares

Softwares

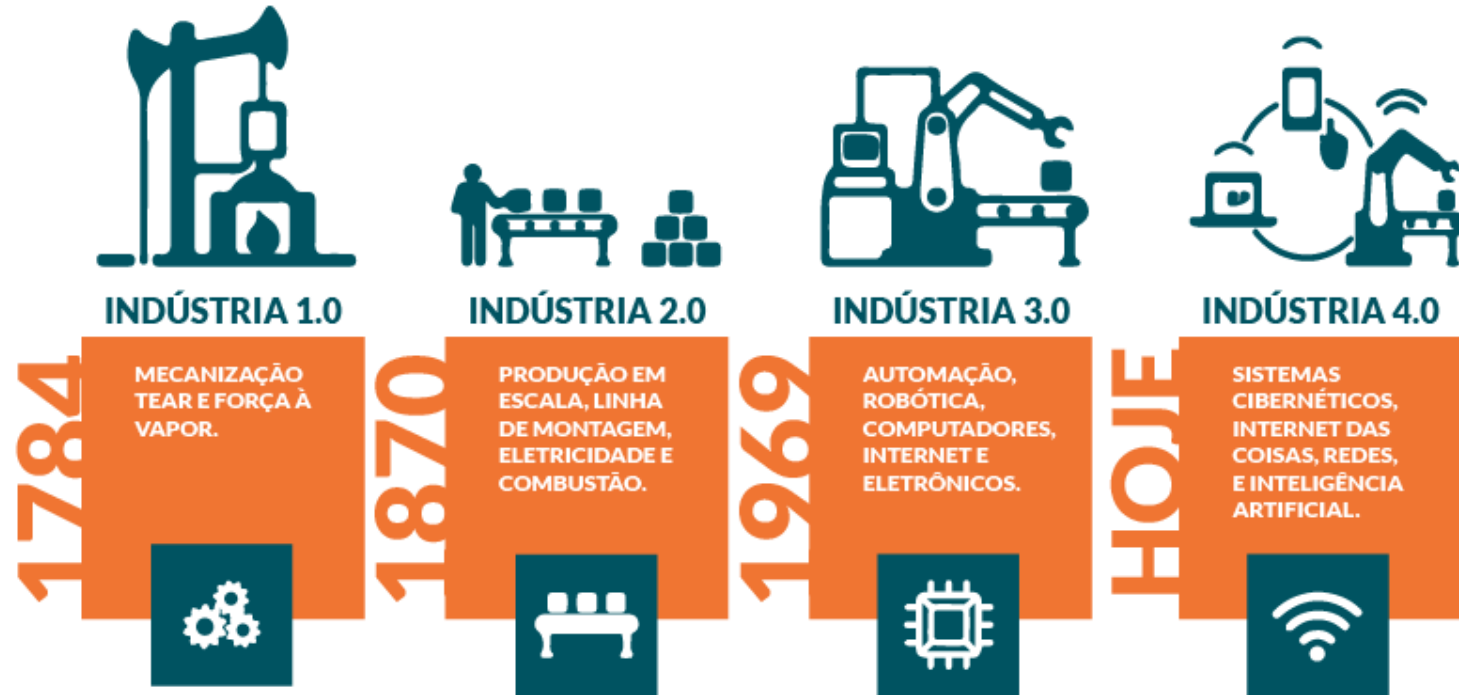
**Protocolos de
Comunicação**



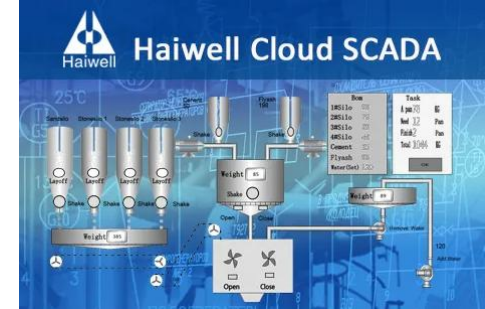
Internet das Coisas (IoT)



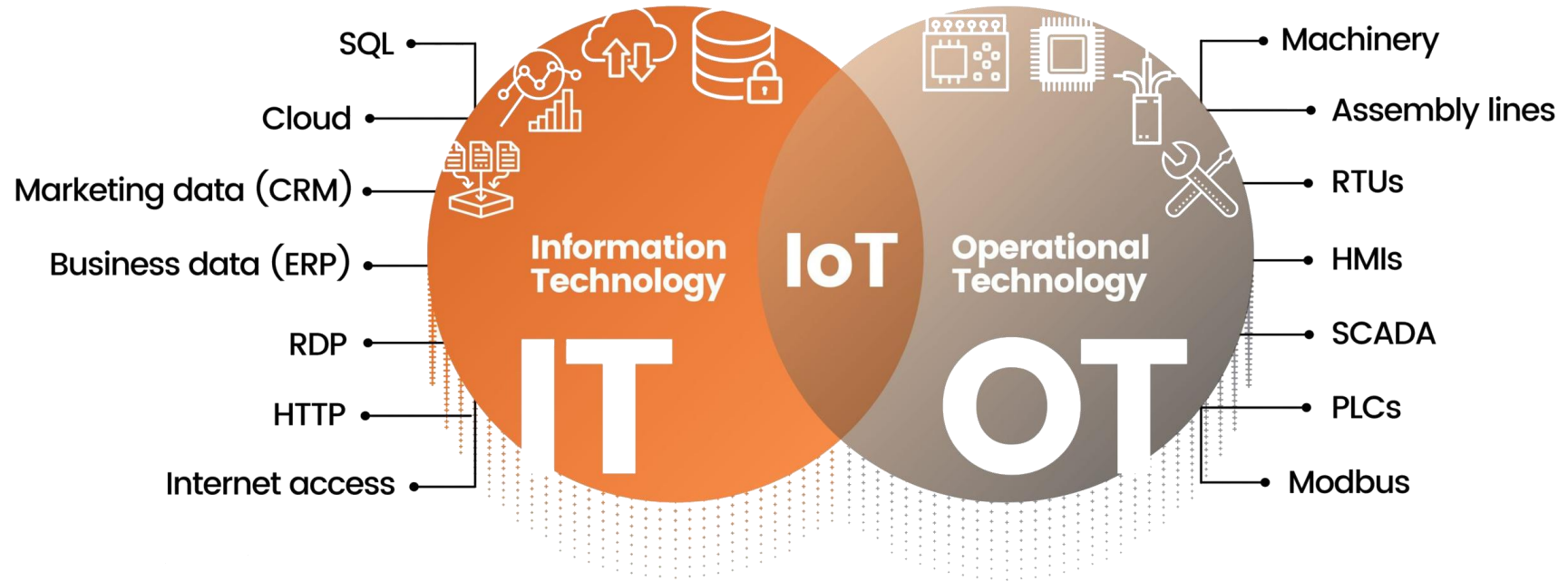
IoT e a 4ª Revolução Industrial



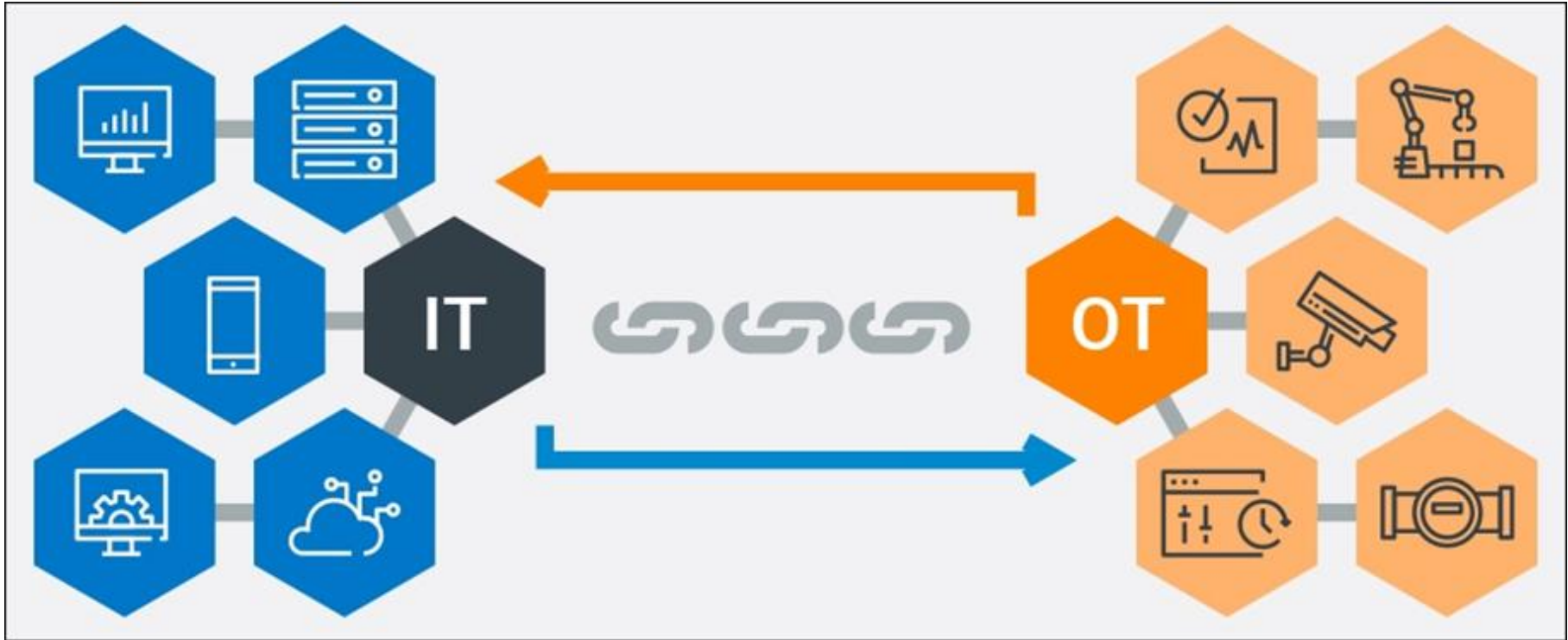
Nova Tecnologia Operacional



Integração OT e IT através de IoT

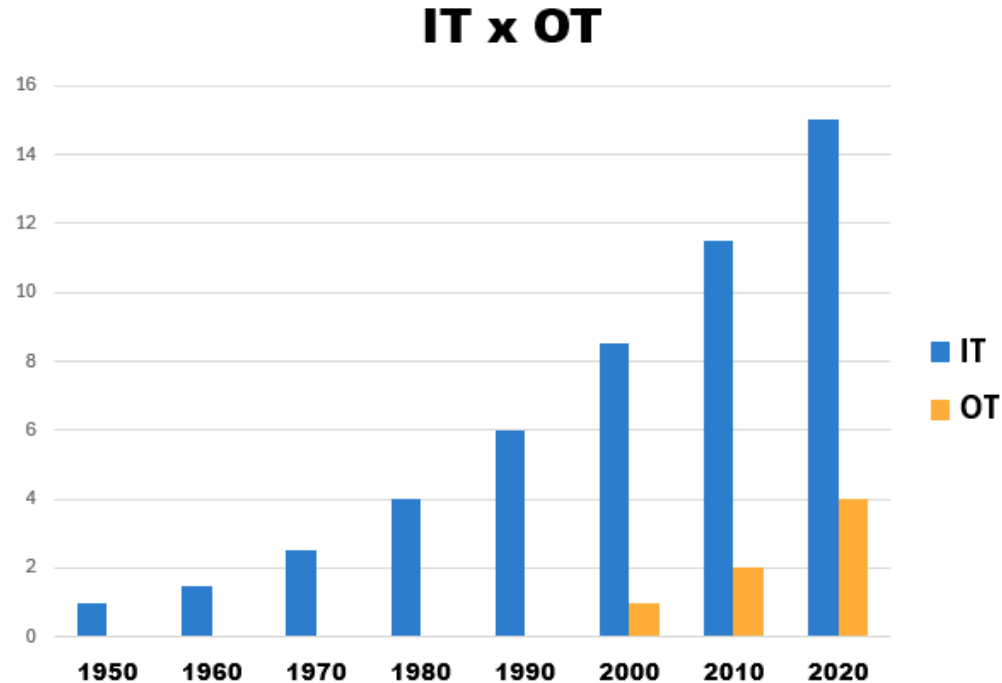


Tecnologias Diferentes e Integradas

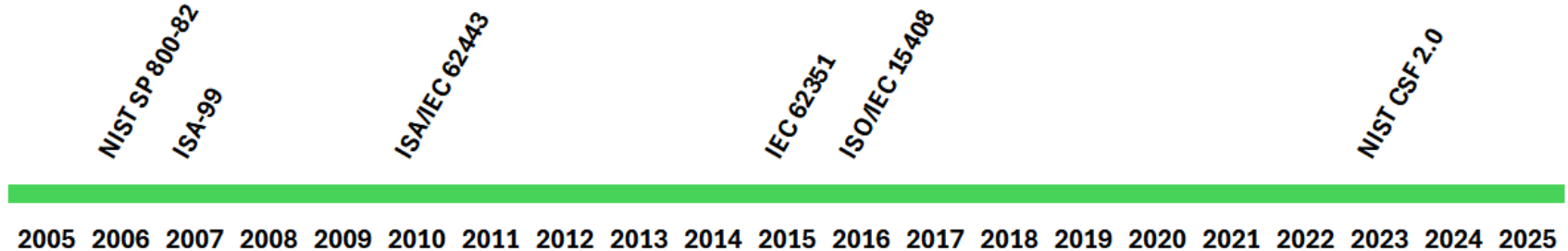


E A SEGURANÇA CIBERNÉTICA ?

Evolução da Segurança Cibernética



Evolução da Segurança Cibernética



International Society of Automation
Setting the Standard for Automation™



**International
Organization for
Standardization**



**International
Electrotechnical
Commission**



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

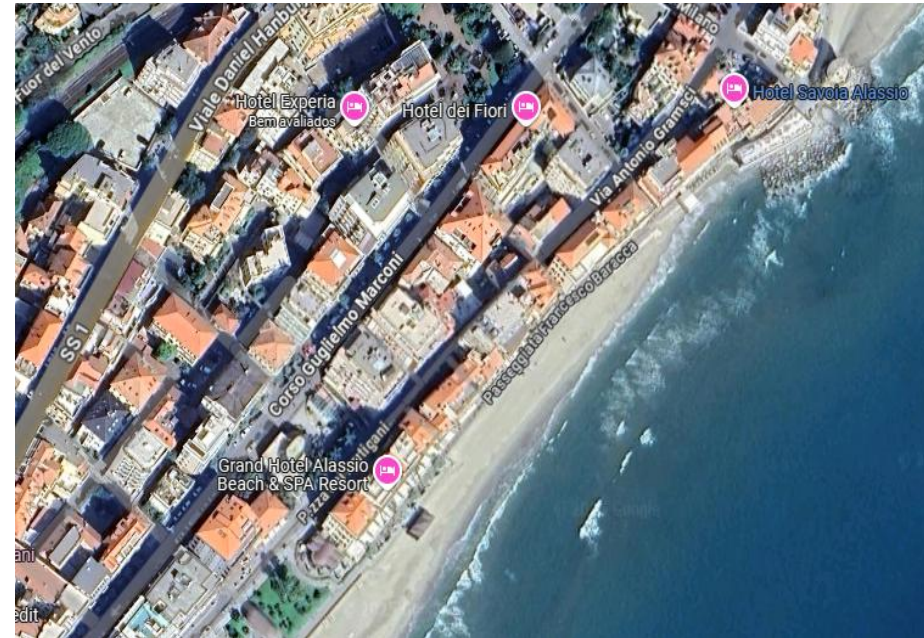
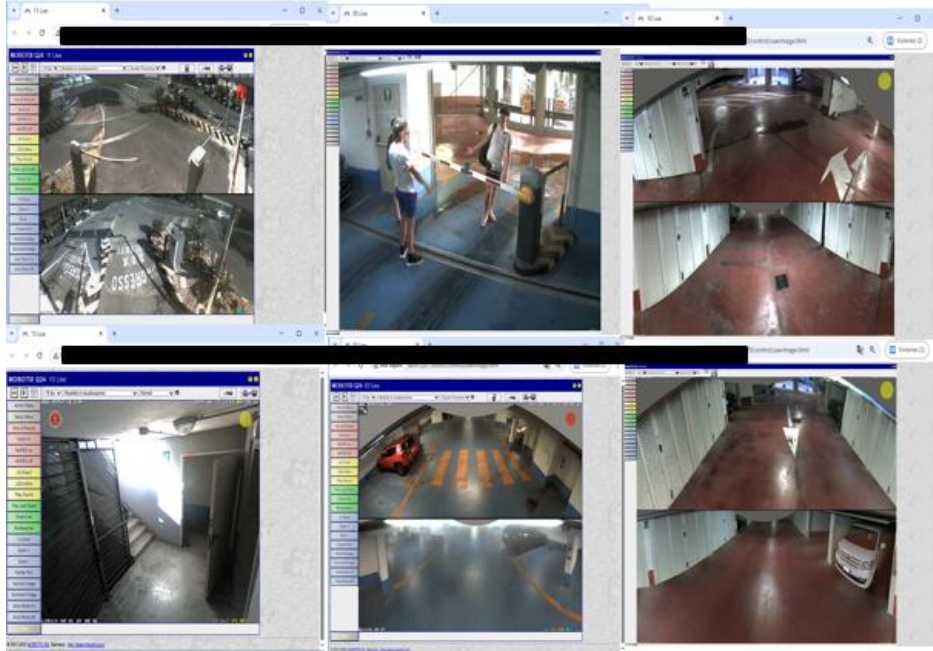
Prioridade Máxima: EUA declaram guerra total aos ciberataques chineses

*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***



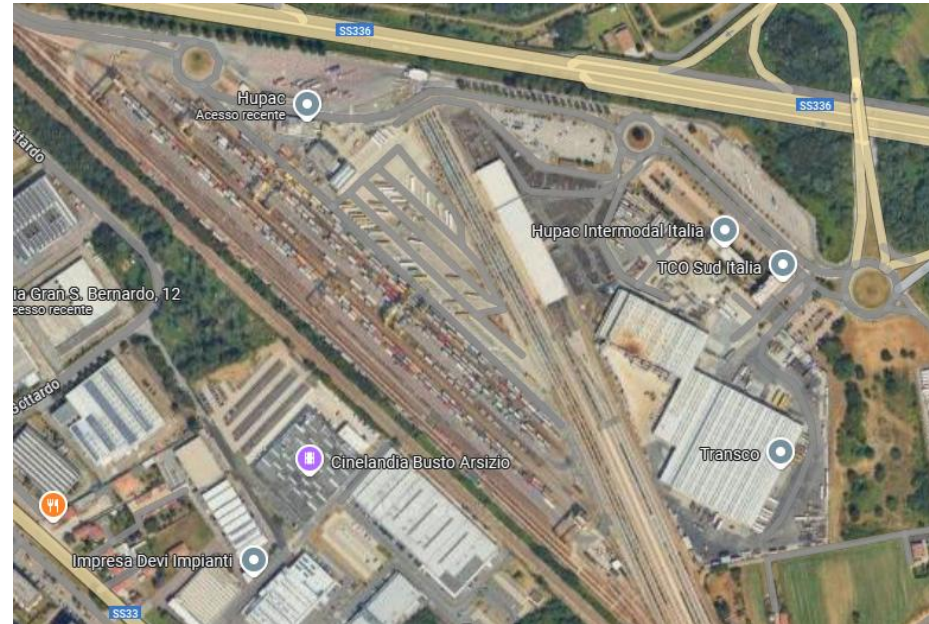
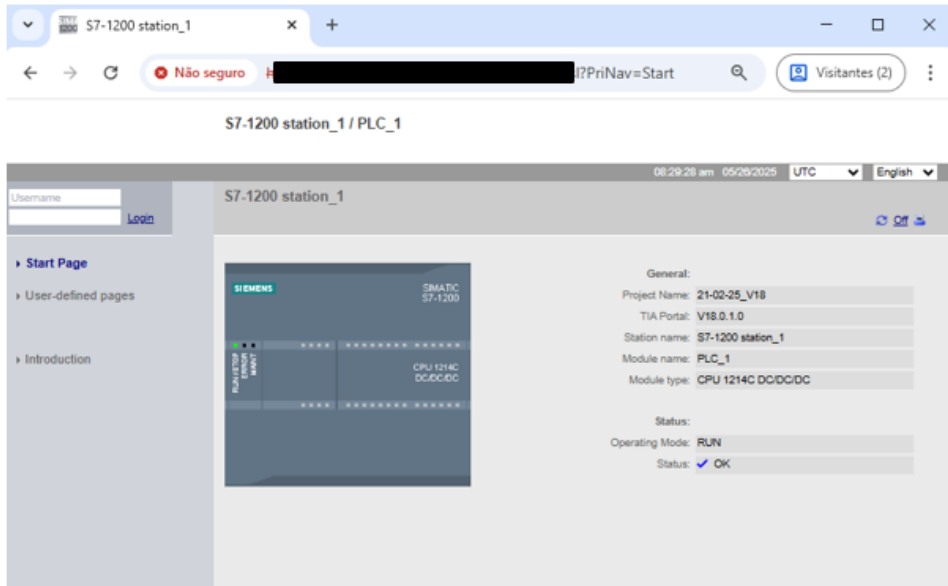
Ativos Expostos na Internet

Sistema de videomonitoramento em hotel na Itália



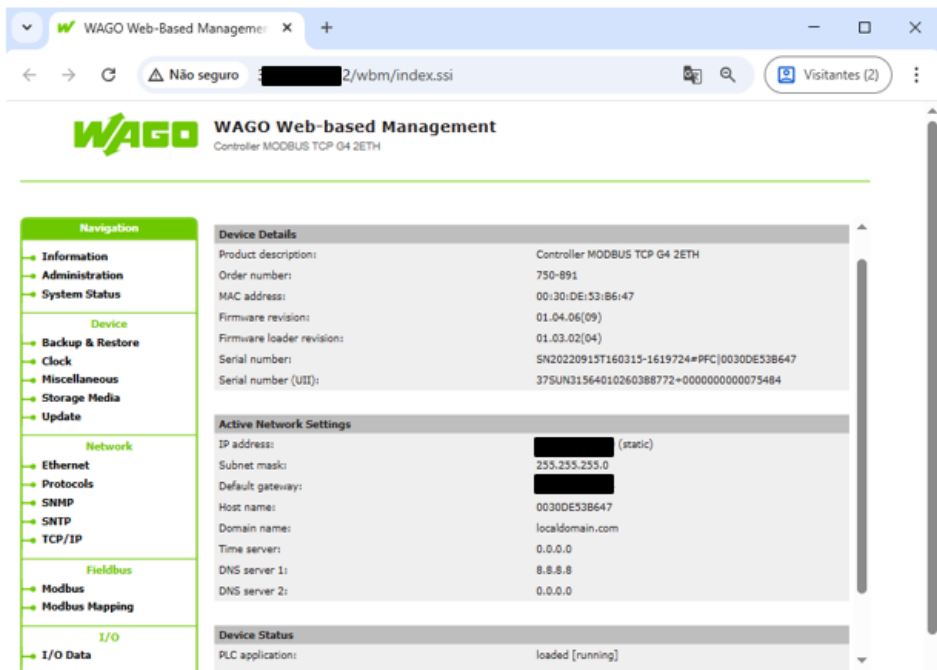
Ativos Expostos na Internet

PLC de empresa ferroviária na Itália



Ativos Expostos na Internet

Controlador Modbus em empresa de saneamento na Suíça

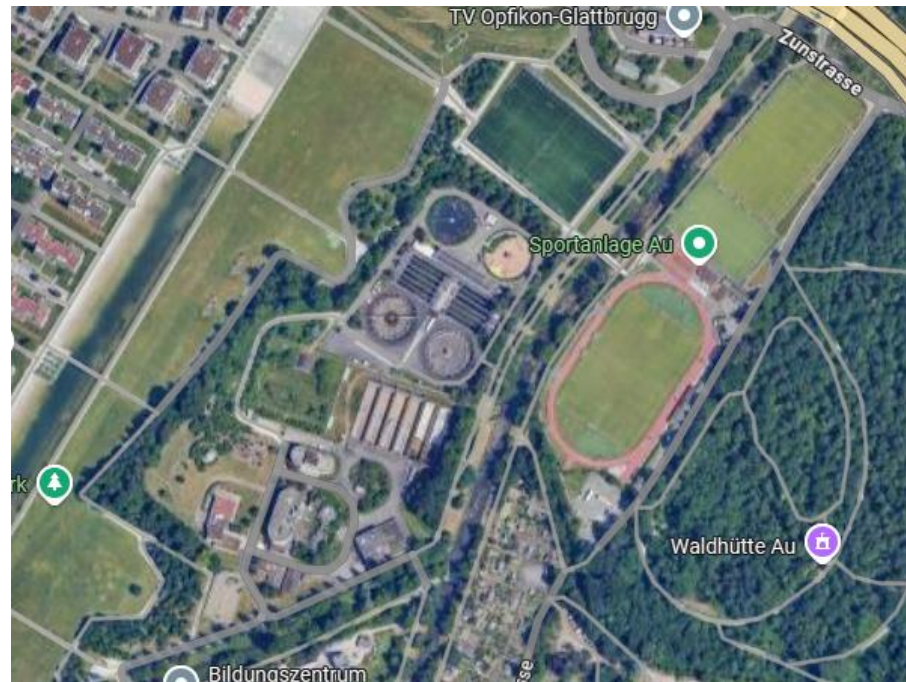


The screenshot shows a web browser window with the address `2/wbm/index.ssi`. The page title is "WAGO Web-based Management" and the subtitle is "Controller MODBUS TCP G4 2ETH". The left sidebar contains a navigation menu with categories: Information, Administration, System Status, Device, Backup & Restore, Clock, Miscellaneous, Storage Media, Update, Network, Ethernet, Protocols, SNMP, SNTP, TCP/IP, Fieldbus, Modbus, Modbus Mapping, and I/O Data. The main content area displays the following details:

Device Details	
Product description:	Controller MODBUS TCP G4 2ETH
Order number:	750-891
MAC address:	00:30:DE:53:B6:47
Firmware revision:	01.04.06(09)
Firmware loader revision:	01.03.02(04)
Serial number:	SN20220915T160315-1619724#PFC0030DE53B647
Serial number (UII):	375UN31564010260388772#0000000000075484

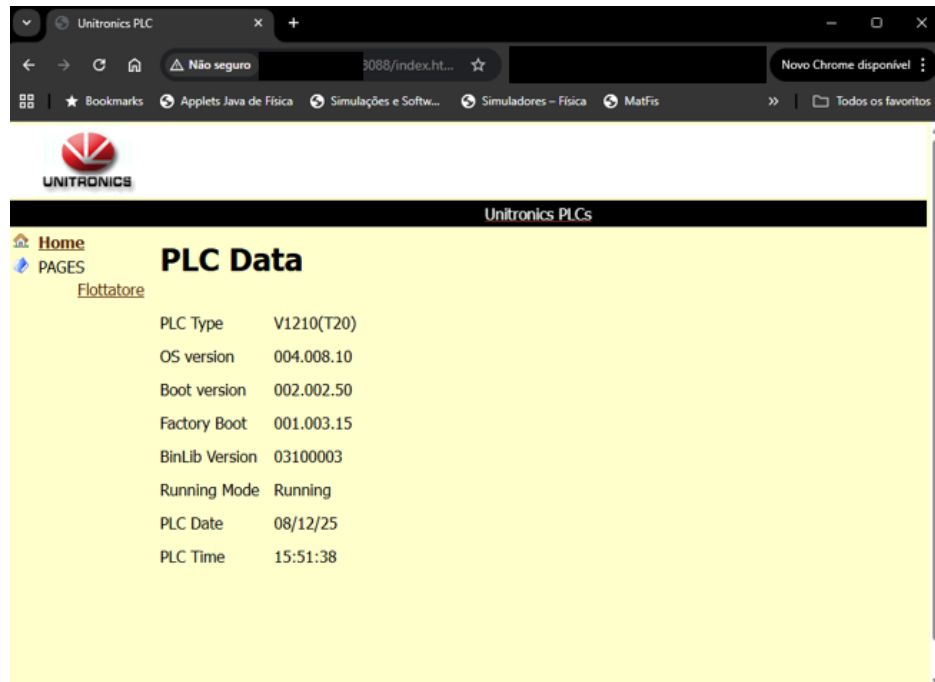
Active Network Settings	
IP address:	[REDACTED] (static)
Subnet mask:	255.255.255.0
Default gateway:	[REDACTED]
Host name:	0030DE53B647
Domain name:	localdomain.com
Time server:	0.0.0.0
DNS server 1:	8.8.8.8
DNS server 2:	0.0.0.0

Device Status	
PLC application:	loaded [running]



Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália



Unitronics PLC

Não seguro 8088/index.ht... Novo Chrome disponível

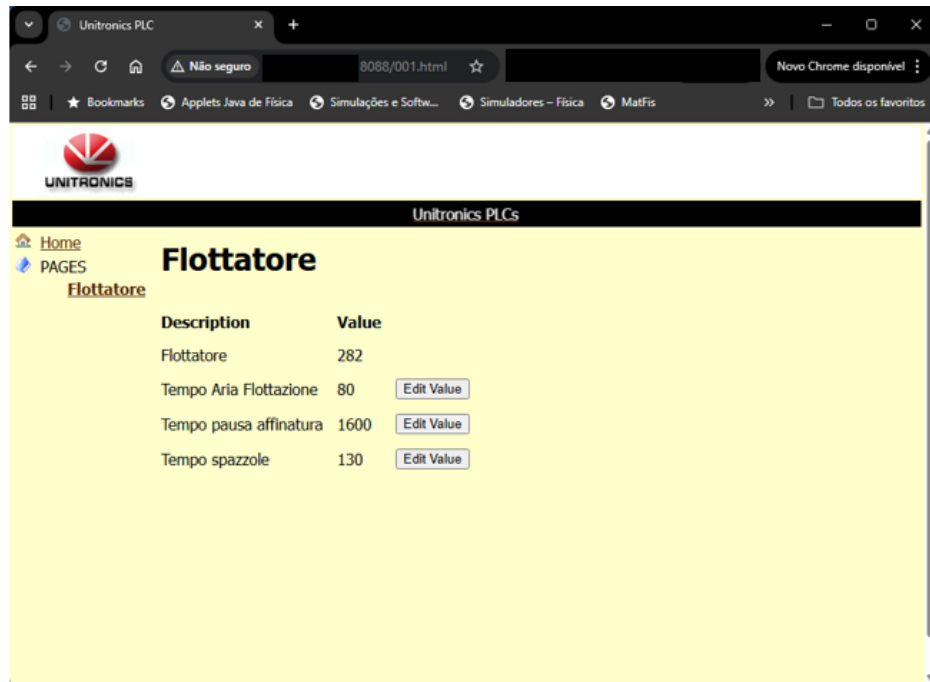
Unitronics

Unitronics PLCs

Home
PAGES
Flottatore

PLC Data

PLC Type	V1210(T20)
OS version	004.008.10
Boot version	002.002.50
Factory Boot	001.003.15
BinLib Version	03100003
Running Mode	Running
PLC Date	08/12/25
PLC Time	15:51:38



Unitronics PLC

Não seguro 8088/001.html Novo Chrome disponível

Unitronics

Unitronics PLCs

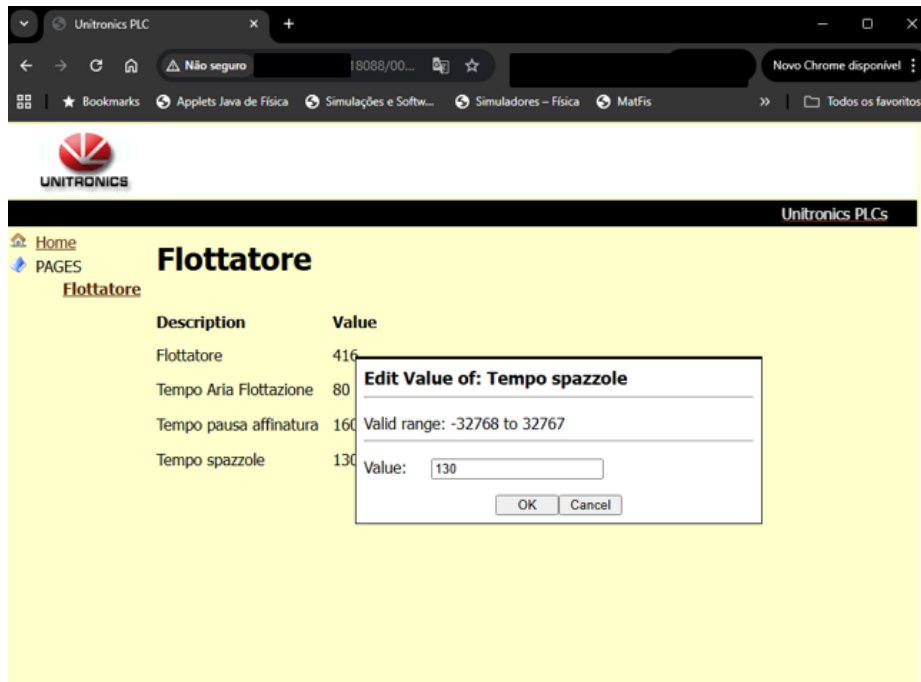
Home
PAGES
Flottatore

Flottatore

Description	Value	
Flottatore	282	
Tempo Aria Flottazione	80	Edit Value
Tempo pausa affinatura	1600	Edit Value
Tempo spazzole	130	Edit Value

Ativos Expostos na Internet

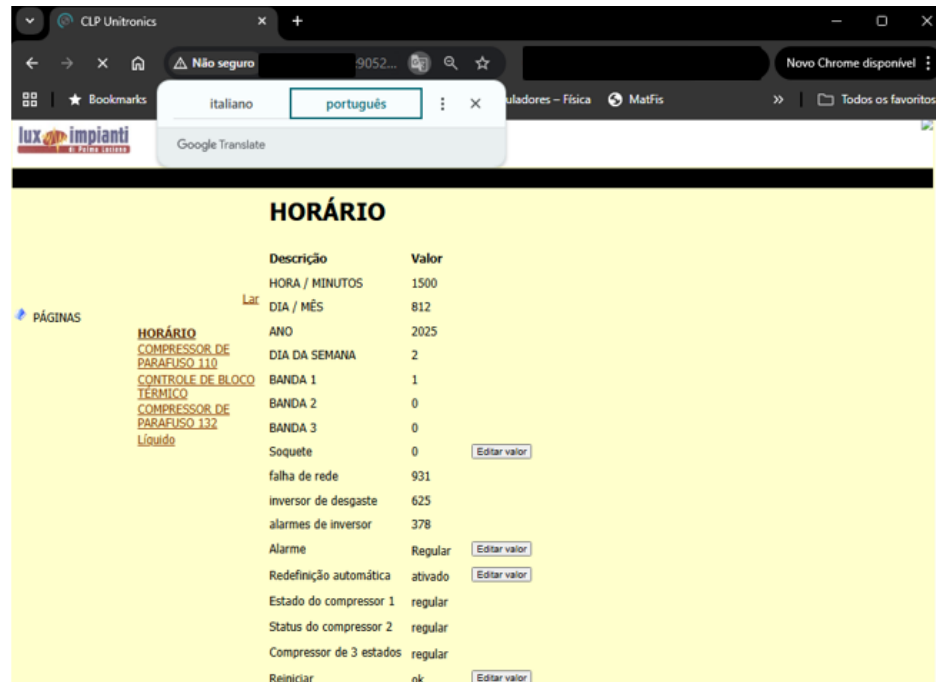
PLC + HMI em empresa de saneamento na Itália



The screenshot shows the Unitronics PLC web interface. The browser address bar displays "18088/00...". The page title is "Unitronics PLCs". The main content area is titled "Flottatore" and contains a table with the following data:

Description	Value
Flottatore	416
Tempo Aria Flottazione	80
Tempo pausa affinatura	160
Tempo spazzole	130

An "Edit Value of: Tempo spazzole" dialog box is open, showing a "Valid range: -32768 to 32767" and a "Value:" input field containing "130". The dialog has "OK" and "Cancel" buttons.



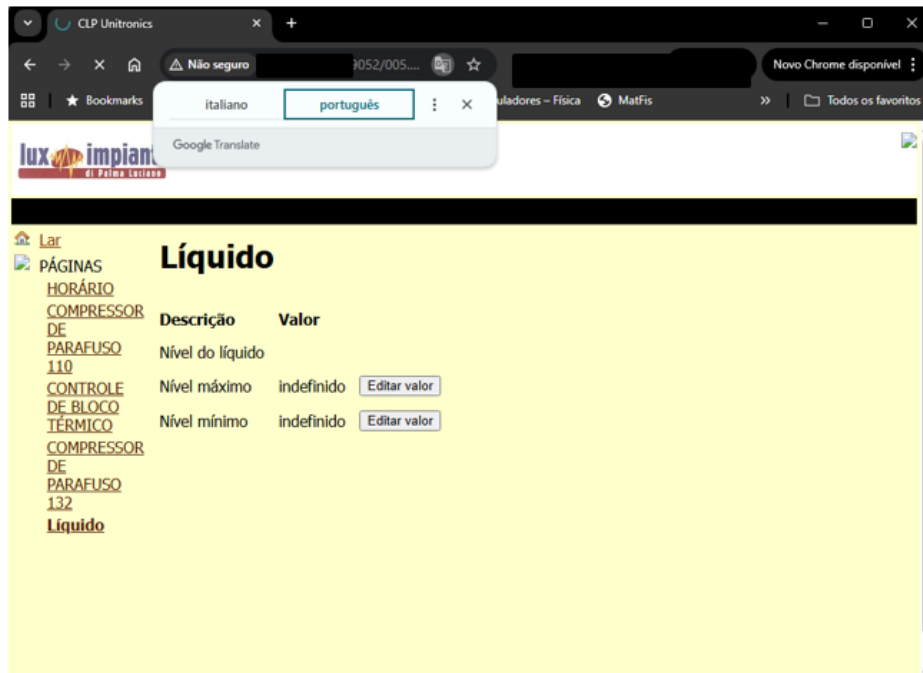
The screenshot shows the CLP Unitronics web interface. The browser address bar displays "9052...". The page title is "CLP Unitronics". The main content area is titled "HORÁRIO" and contains a table with the following data:

Descrição	Valor
HORA / MINUTOS	1500
DIA / MÊS	812
ANO	2025
DIA DA SEMANA	2
BANDA 1	1
BANDA 2	0
BANDA 3	0
Soquete	0
falha de rede	931
inversor de desgaste	625
alarmes de inversor	378
Alarme	Regular
Redefinição automática	ativado
Estado do compressor 1	regular
Status do compressor 2	regular
Compressor de 3 estados	regular
Reiniciar	ok

Each row in the table has an "Editar valor" button next to it. The page is in Portuguese, as indicated by the "português" language selection in the browser's address bar.

Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália



CLP Unitronics

Não seguro 1052/005...

Idioma detectado: italiano | **português**

Google Translate

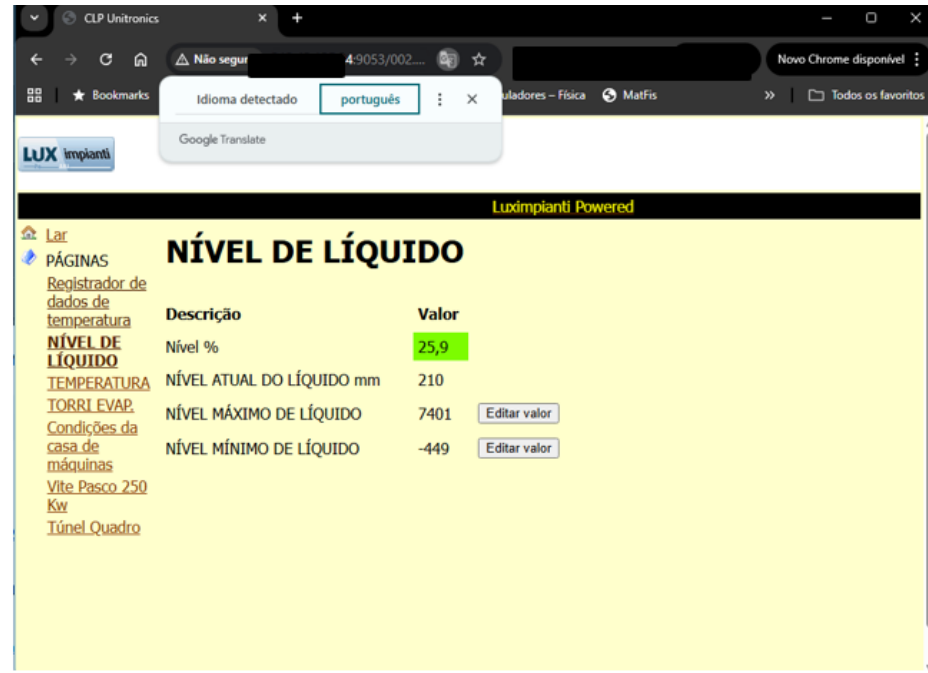
LUX impianti

Líquido

Descrição **Valor**

Nível do líquido	
Nível máximo	indefinido Editar valor
Nível mínimo	indefinido Editar valor

[Lar](#)
[PÁGINAS](#)
[HORÁRIO](#)
[COMPRESSOR DE PARAFUSO 110](#)
[CONTROLE DE BLOCO TÉRMICO](#)
[COMPRESSOR DE PARAFUSO 132](#)
[Líquido](#)



CLP Unitronics

Não seguro 4:9053/002...

Idioma detectado: italiano | **português**

Google Translate

LUX impianti

Luximpianti Powered

NÍVEL DE LÍQUIDO

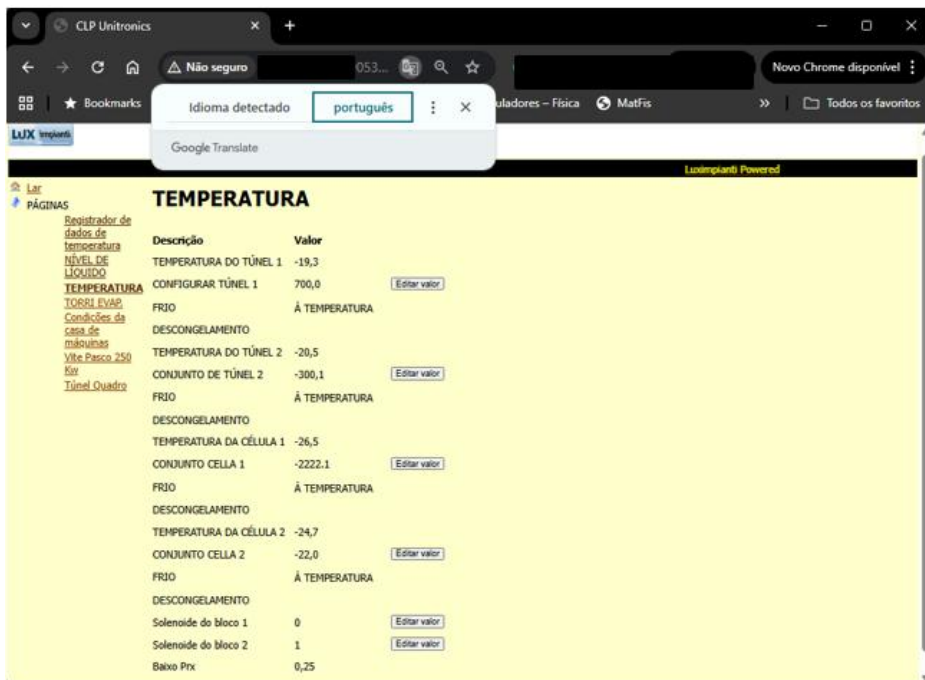
Descrição **Valor**

Nível %	25,9
NÍVEL ATUAL DO LÍQUIDO mm	210
NÍVEL MÁXIMO DE LÍQUIDO	7401 Editar valor
NÍVEL MÍNIMO DE LÍQUIDO	-449 Editar valor

[Lar](#)
[PÁGINAS](#)
[Registrador de dados de temperatura](#)
[NÍVEL DE LÍQUIDO](#)
[TEMPERATURA TORRI EVAP](#)
[Condições da casa de máquinas](#)
[Vite Pasco 250 Kw](#)
[Túnel Quadro](#)

Ativos Expostos na Internet

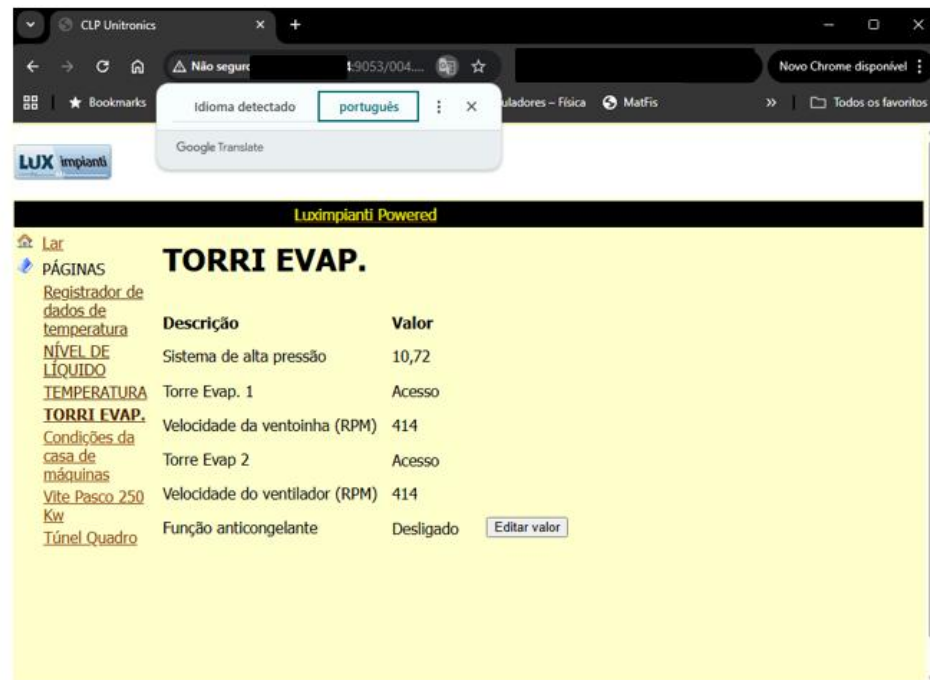
PLC + HMI em empresa de saneamento na Itália



LUX impianti

TEMPERATURA

Descrição	Valor
TEMPERATURA DO TÚNEL 1	-19,3
CONFIGURAR TÚNEL 1	700,0 Editar valor
FRIO	À TEMPERATURA
DESCONGELAMENTO	
TEMPERATURA DO TÚNEL 2	-20,5
CONJUNTO DE TÚNEL 2	-300,1 Editar valor
FRIO	À TEMPERATURA
DESCONGELAMENTO	
TEMPERATURA DA CÉLULA 1	-26,5
CONJUNTO CELLA 1	-2222,1 Editar valor
FRIO	À TEMPERATURA
DESCONGELAMENTO	
TEMPERATURA DA CÉLULA 2	-24,7
CONJUNTO CELLA 2	-22,0 Editar valor
FRIO	À TEMPERATURA
DESCONGELAMENTO	
Solenóide do bloco 1	0 Editar valor
Solenóide do bloco 2	1 Editar valor
Baixo Pnx	0,25



LUX impianti

TORRI EVAP.

Descrição	Valor
Sistema de alta pressão	10,72
Torre Evap. 1	Acesso
Velocidade da ventoinha (RPM)	414
Torre Evap 2	Acesso
Velocidade do ventilador (RPM)	414
Função anticongelante	Desligado Editar valor

Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália

CLP Unitronics

Não seguro 1053...

Idioma detectado português

Google Translate

LUX impianti

Lar

PÁGINAS

Registador de dados de temperatura

NÍVEL DE LÍQUIDO

TEMPERATURA

TORRE EVAP.

Condições da casa de máquinas

Vite Pasco 250 Kw

Túnel Quadro

Luximpianti Powered

Descrição	Valor
TEMPERATURA DO TÚNEL 1	-19,3
CONFIGURAR TÚNEL 1	700,0 Editar valor
FRIO	À TEMPERATURA
DESCONGELAMENTO	
TEMPERATURA DO TÚNEL 2	-20,5
CONJUNTO DE TÚNEL 2	-300,1 Editar valor
FRIO	À TEMPERATURA
DESCONGELAMENTO	
TEMPERATURA DA CÉLULA 1	-26,5
CONJUNTO CELLA 1	-2222,1 Editar valor
FRIO	À TEMPERATURA
DESCONGELAMENTO	
TEMPERATURA DA CÉLULA 2	-24,7
CONJUNTO CELLA 2	-22,0 Editar valor
FRIO	À TEMPERATURA
DESCONGELAMENTO	
Solenóide do bloco 1	0 Editar valor
Solenóide do bloco 2	1 Editar valor
Baixo Pnx	0,25

CLP Unitronics

Não seguro 4:9053/004...

Idioma detectado português

Google Translate

LUX impianti

Lar

PÁGINAS

Registador de dados de temperatura

NÍVEL DE LÍQUIDO

TEMPERATURA

TORRE EVAP.

Condições da casa de máquinas

Vite Pasco 250 Kw

Túnel Quadro

Luximpianti Powered

Descrição	Valor
Sistema de alta pressão	10,72
Torre Evap. 1	Acesso
Velocidade da ventoinha (RPM)	414
Torre Evap 2	Acesso
Velocidade do ventilador (RPM)	414
Função anticongelante	Desligado Editar valor

Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália

The screenshot shows a web browser window with the URL '1053/007...'. A Google Translate popup is visible, showing the translation from English to Portuguese. The page title is 'PLCs Unitronics'. The main heading is 'Túnel Quadro'. Below it, there is a sidebar with a list of links: 'Lar', 'PÁGINAS', 'Registrador de dados de temperatura', 'LIVELLO LIQUIDA', 'TEMPERATURA TORRI EVAP', 'Stato Sala Macchine', 'Vite Pasco 250 Kw', 'Túnel Quadro'. The main content area displays a table with two columns: 'Descrição' and 'Valor'. The table has three rows of data, each with an 'Editar valor' button.

Descrição	Valor
Stato Comp 250 kW	Gasto
Partida 250kW	1001
Condeggio	160

The screenshot shows a web browser window with the URL '1-9054/003...'. A Google Translate popup is visible, showing the translation from Italian to Portuguese. The page title is 'PLCs Unitronics'. The main heading is 'Pintura de pasto'. Below it, there is a sidebar with a list of links: 'Lar', 'PÁGINAS', 'Sala de máquinas do túnel', 'Q2', 'Condições da casa de máquinas', 'Pintura de pasto'. The main content area displays a table with two columns: 'Descrição' and 'Valor'. The table has six rows of data, each with an 'Editar valor' button.

Descrição	Valor
Status do alarme 200 kW	Regular
Status do alarme 55 kW	Regular
Verificar	0
Contagem progressiva	3
Estado do compressor 200 kW	Desligado
Começar	3270

Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália

CLP Unित्रonics

Não seguro 055/001... Novo Chrome disponível

italiano português

☐ Sempre traduzir do italiano

Google Translate

Linha de Esteiras 3

Modo de trabalho da linha 3

Descrição	Valor
Produção	Linha de desossa 3
Verificar	Produção em andamento 0
Tempos de parada	Linha Interromper a produção
Tempo de inatividade da máquina	Modo de trabalho 2
Informações	Pz Agora 500

Editar valor

Frigo Zero Gradi-Home

Não seguro 83160... Novo Chrome disponível

Applets Java de Física Simulações e Softw... Simuladores - Física MatFis

Stato Regolare

1.69 Prx Basso	Compressore vite 1 Spento	3600 RPM	0 Kw
7.17 Prx	Compressore vite 2 Spento	3600 RPM	
9.26 Prx Alta	Compressore vite 3 Spento	3600 RPM	-18.53 °C Freon / Vent.

Modo Freddo

Cella 3 OFF

30.0 °C Set 10.3 °C

Spenta 30.0 °C Set Giorno 30.0 °C Set Notte Libero H24

Cella 4 ON

-5.0 °C Set -4.6 °C

Accesa -5.0 °C Set Giorno -5.0 °C Set Notte Libero H24

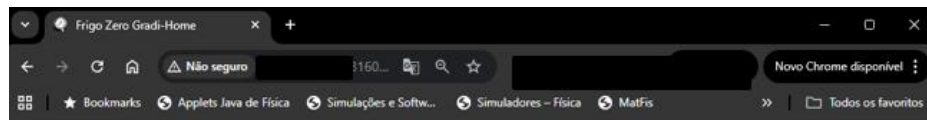
Cella 5 ON

-10.0 °C Set -8.4 °C

Accesa -10.0 °C Set Giorno -10.0 °C Set Notte Libero H24


Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália



Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália

 **General Information**

Hostnames

██████████.it

Domains

wadsl.it

Country

Italy

City

Teramo

Organization


██████████

ISP

██████████

ASN

██████████

 **Open Ports**

1194	3389	8041	8046	8048	8146	8157
8160	8161	8163	8170	9052	9053	9054
9055	9257	9901	18088			

OpenSSH 7.1

SSH-2.0-OpenSSH_7.1
Key type: ssh-rsa
Compression Algorithms:
none


Vulnerabilities

3	11	18	1	0
---	----	----	---	---

VNC

RFB 003.000
Authentication disabled

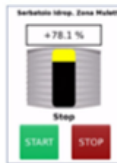
Serbatoio Idrop. Zona Muletta Serbatoio Idrop. Zona Mole



VNC:
Protocol Version: 3.8
Security Types:
1: None
Server Name: Unitronics
Geometry: 800x400


Serbatoio Idrop. Zona Muletta

+78.1 %



START STOP

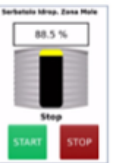
Ev Chiusa



START STOP

Serbatoio Idrop. Zona Mole

88.5 %



START STOP

00:00 1 MAX POWER

START STOP

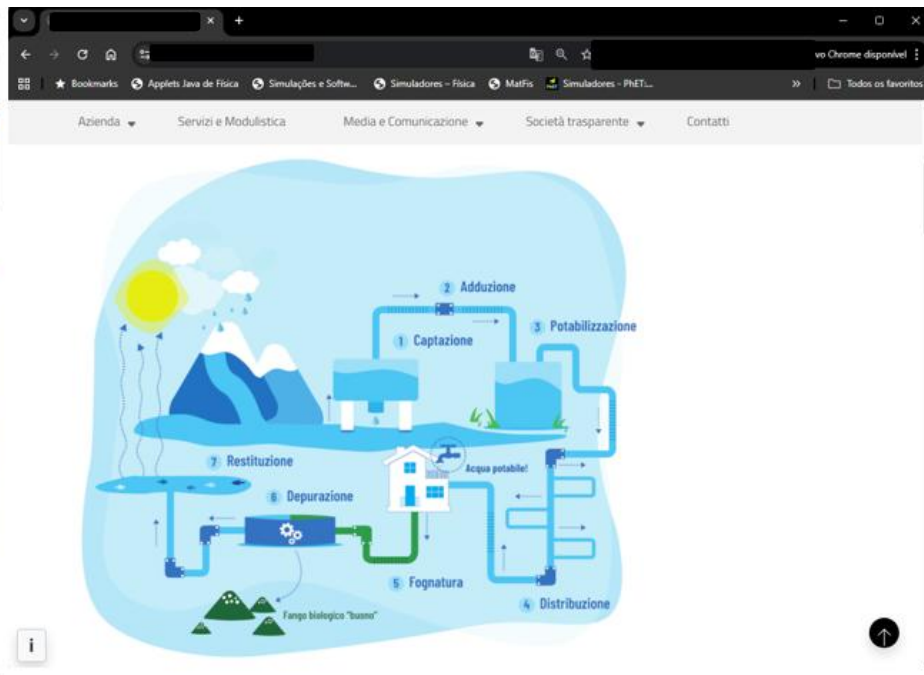
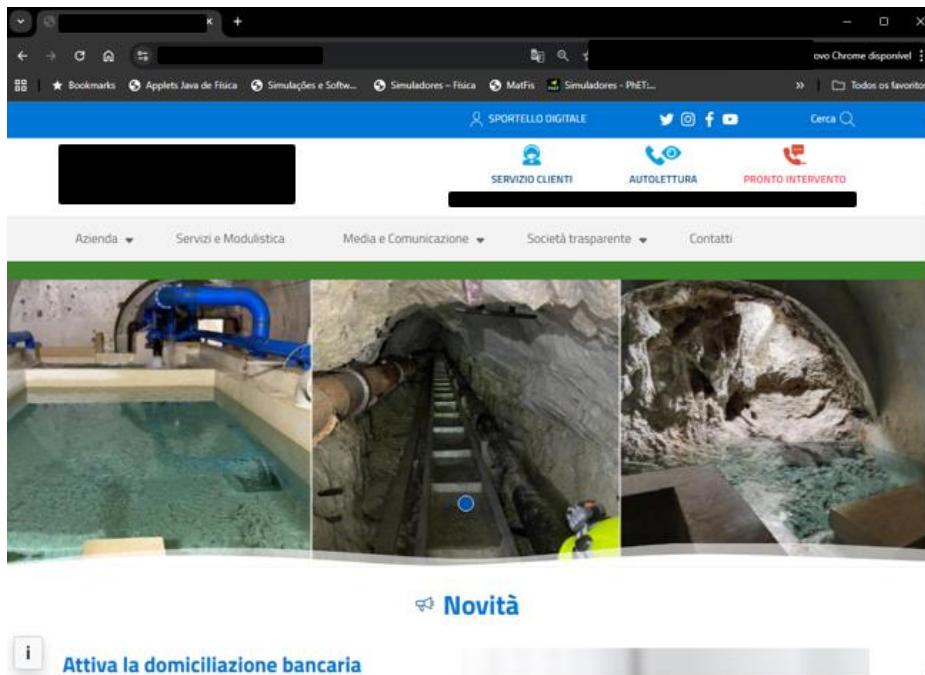
00:00

0

Password Stop

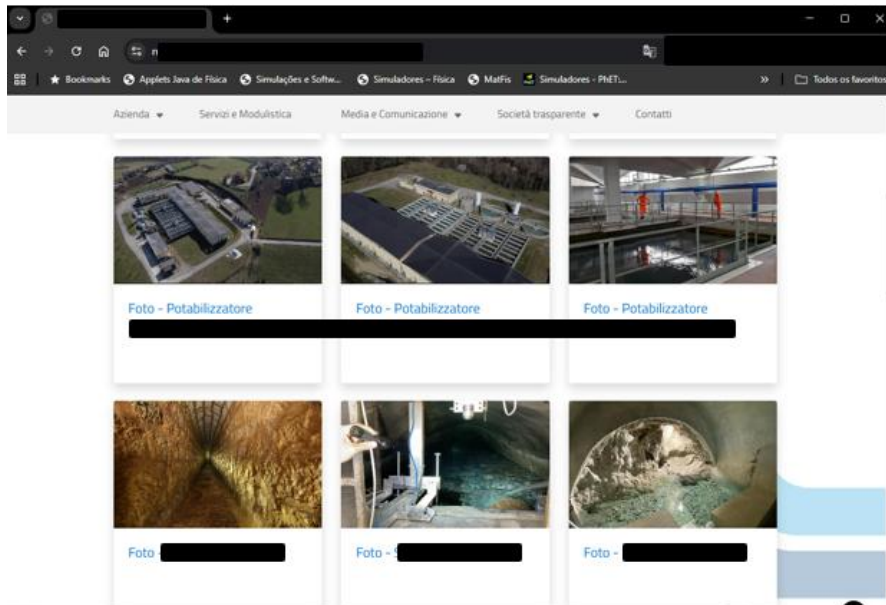
Ativos Expostos na Internet

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

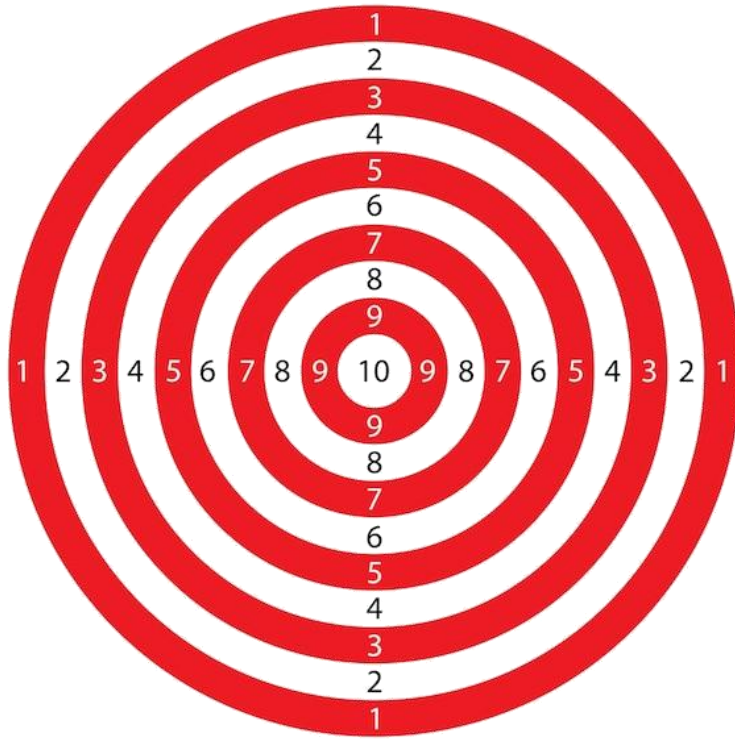


Ciberataques no Brasil



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

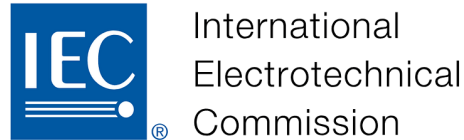
- Implantação de SOC OT ou integração com SOC IT
- Configuração de SIEM com fontes OT
- Resposta a Incidentes OT com playbooks específicos
- Integração Threat Intelligence para ambientes industriais

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



Consultorias



Fornecedores



ISA 99 – ISA/IEC 62443



	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				
Geral	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		
Políticas e Procedimentos	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						
Sistema	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								
Componente											

Normas Internacionais de Segurança de Automação e Controle (IACS) e Redes Operacionais

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