CONTROL ROOM RIO

PIPELINE SUMMIT 2026

Avanço no nível NIST do Ambiente OT e Processos CyberOT da NTS

Henrique Costa | Coordenador SCADA
Marcos Costa | Especialista CyberOT

NTS – Nova Transportadora do Sudeste

PIPELINE BRAZIL

RIO DE JANEIRO, 21 E 22 DE OUTUBRO DE 2026

Dimensão/Dimension: IV. Dimensão Operacional
Tema/Theme: SCADA e Cybersegurança

Sumário / Agenda

1. Introdução – Cibersegurança OT
2. Evolução dos Ataques Cibernéticos
3. Nova Fase em CyberOT
4. NIST Cybersecurity
5. Assessment – Framework Cybersecurity 2.0
6. Do Framework à Rotina Operacional

CONTROL ROOM RIO

PIPELINE SUMMIT 2026

21 e 22/10/2026

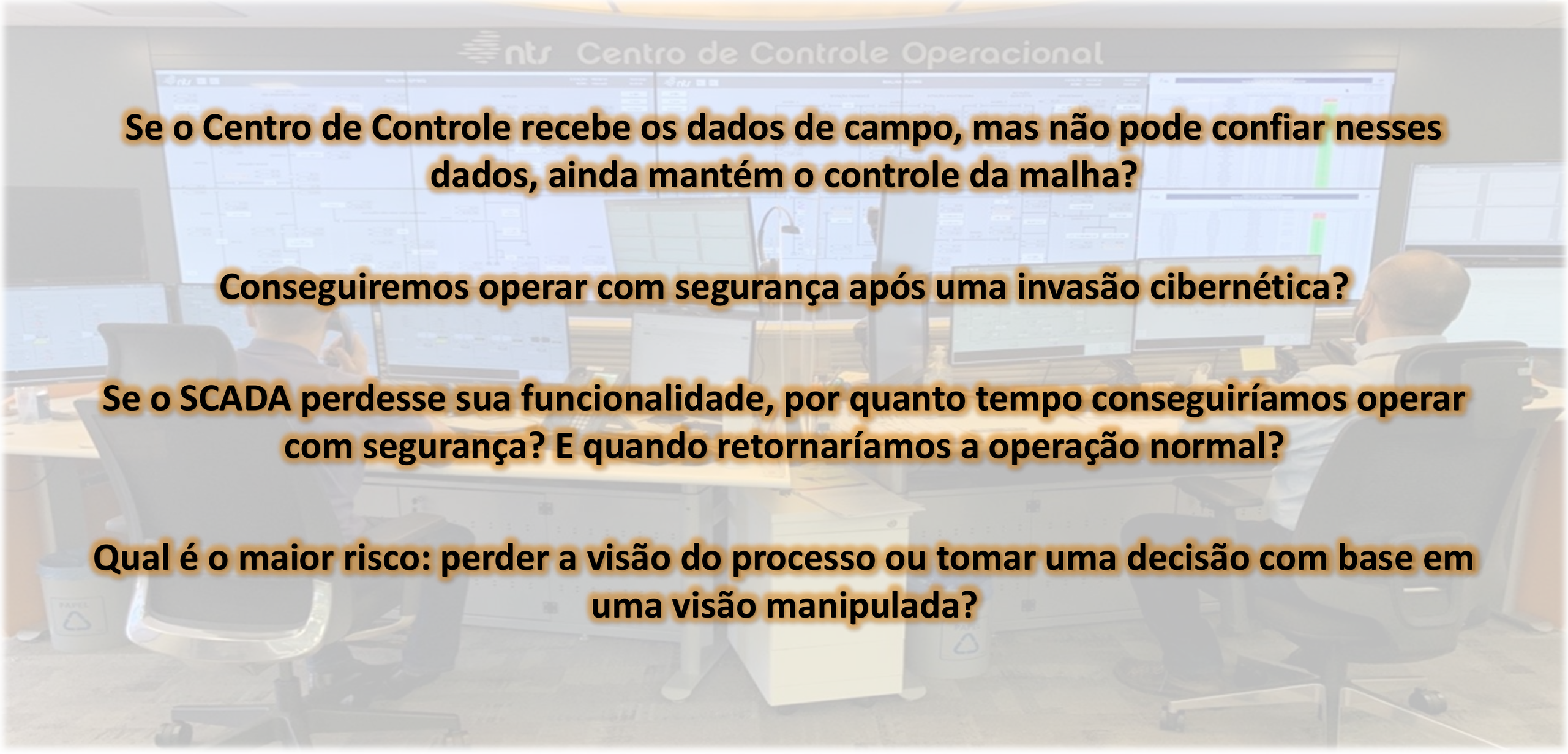
Hotel Florida, Rio de Janeiro

1. Introdução

Os 40 passos para implementar Programa de Cibersegurança OT de Classe Mundial:

1) Obter patrocínio executivo.
2) Definir política de cibersegurança OT.
3) Definir responsabilidades para TI e OT.
4) Criar Comitê de Cybersecurity.
5) Realizar inventário dos ativos OT.
6) Inventariar softwares e sistemas OT.
7) Mapear comunicação e protocolos.
8) Elaborar diagnóstico de maturidade NIST.
9) Realizar assessment de risco OT.
10) Realizar Gap Analysis.
11) Elaborar governança e política OT.
12) Segmentar rede (Zones & Conduits).
13) Criar DMZ Industrial.
14) Monitorar acessos remotos.
15) Controlar acessos privilegiados.
16) Configurar MFA para acessos remotos.
17) Elaborar hardening dos ativos críticos.
18) Constituir gestão de vulnerabilidades.
19) Monitoramento OT (SOC/SIEM).
20) Executar backups periódicos.
21) Manter cópias offline.
22) Testar restauração regularmente.
23) Criar plano de recuperação OT.
24) Criar plano de continuidade operacional.
25) Definir RTO e RPO.
26) Realizar gerenciamento de terceiros.
27) Criar programa contínuo de treinamento.
28) Definir processo de comunicação.
29) Integrar equipes OT e TI.
30) Registrar lições aprendidas.
31) Registrar sessões remotas.
32) Realizar auditorias periódicas.
33) Revisar riscos anualmente.
34) Atualizar arquitetura OT.
35) Atualizar políticas e procedimentos.
36) Reavaliar maturidade anualmente.
37) Executar pentests OT controlados.
38) Comparar-se com benchmarks do setor.
39) Atualizar roadmap de evolução.
40) Buscar excelência operacional contínua.

Implementar Cibersegurança, em um ambiente OT cada vez mais conectado à TI, é uma jornada contínua para manter o controle e preservar a resiliência da operação das infraestruturas críticas.



Se o Centro de Controle recebe os dados de campo, mas não pode confiar nesses dados, ainda mantém o controle da malha?

Conseguiremos operar com segurança após uma invasão cibernética?

Se o SCADA perdesse sua funcionalidade, por quanto tempo conseguiríamos operar com segurança? E quando retornaríamos a operação normal?

Qual é o maior risco: perder a visão do processo ou tomar uma decisão com base em uma visão manipulada?

2. Evolução dos Ataques Cibernéticos

1º Ataque a OT

2010 – Instalações Nucleares Iranianas
STUXNET – mais de quinze instalações iranianas foram atacadas e infiltradas pelo vírus Stuxnet. Acredita-se que esse ataque foi iniciado pelo pendrive de um funcionário aleatório.

Surgimento do Ransoware

2017 – WannaCry Ransomware
Um dos ataques de dados mais conhecidos envolvendo ransomware (sequestro de dados). Este ataque visou diversos computadores que usavam o Sistema operacional Microsoft Windows. Os usuários tiveram seus dados criptografados e os criminosos exigiram pagamento em Bitcoin.

Vazamento de Dados

2024 – Transport for London (TfL)
TfL sofreu um ataque cibernético que causou interrupções em seus serviços. O ataque comprometeu os dados pessoais de aprox. 5.000 clientes, incluindo informações sensíveis, como endereços residenciais e dados bancários.

TPRM

2025 – Ataque à Terceirizada da Petrobras
Grupo hacker “Everest” roubou entre 90 GB e 190 GB de dados confidenciais de logística e prospecção de petróleo de uma empresa prestadora de serviços à Petrobras.

Novas Modalidades

2026 – Tecnologia Médica Stryker
Grupo hacker “Handala” realizou ataque do tipo *wiper* destruindo dados e comprometendo operação. Estima-se que 50Tb de dados foram apagados, e não houve nenhum pedido de resgate desses dados.

2000 2010 2015 2017 2021 2024 2025 2026

2000 Ciber Segurança

2015 – Ataque à rede elétrica na Ucrânia
O ataque a rede elétrica da Ucrânia foi o primeiro ataque cibernético contra uma rede elétrica. Por consequência do ataque, aproximadamente metade das residências na região de Ivano-Frankisvsk, na Ucrânia, ficaram sem energia por algumas horas.

Ataque a OT Remoto

2021 – Incidente Colonial Pipeline
Um dos maiores gasoduto dos EUA, responsável por fornecer mais de 45% da gasolina, diesel e combustível de aviação da Costa Leste, foi forçado a desligar completamente suas operações.

Ransoware as SaaS

2025 – Setor elétrico nacional – Tentativas de ataques (1º sem)
ANEEL e o ONS divulgaram que o setor elétrico brasileiro sofreu mais de 500 mil tentativas de ataques cibernéticos apenas no primeiro semestre de 2025, todas bloqueadas antes de causar impacto operacional.

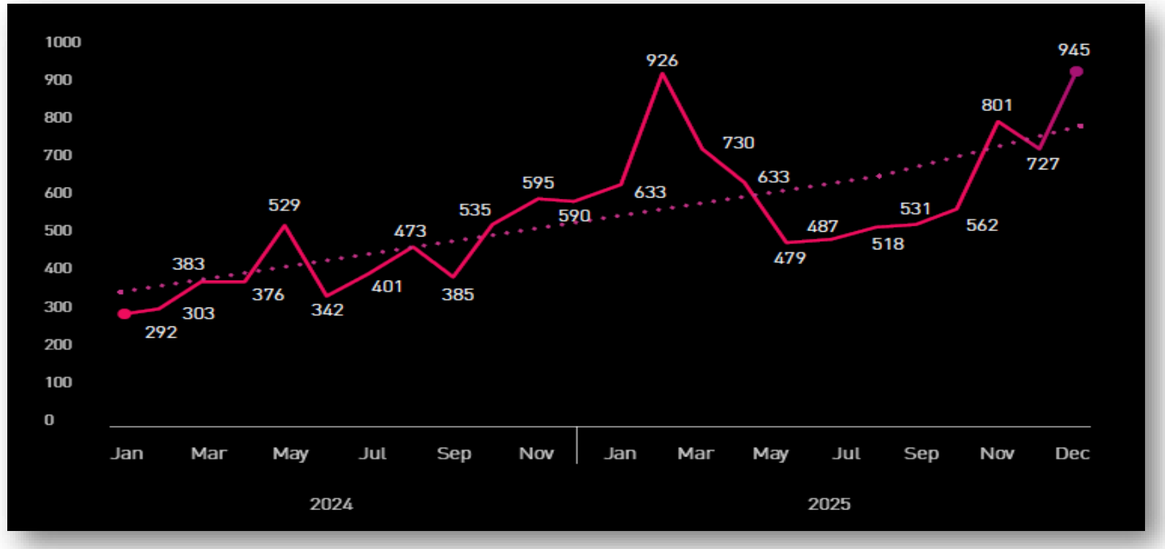
Escalada de Eventos

2026 – França: Ataque a supermercados
Hackers invadiram remotamente os controladores de refrigeração alterando os parâmetros de degelo e temperatura, fazendo com que geladeiras e freezers chegassem a 50°C ~ 80°C o que provocou pequenos incêndios e a perda total de alimentos perecíveis e congelados.

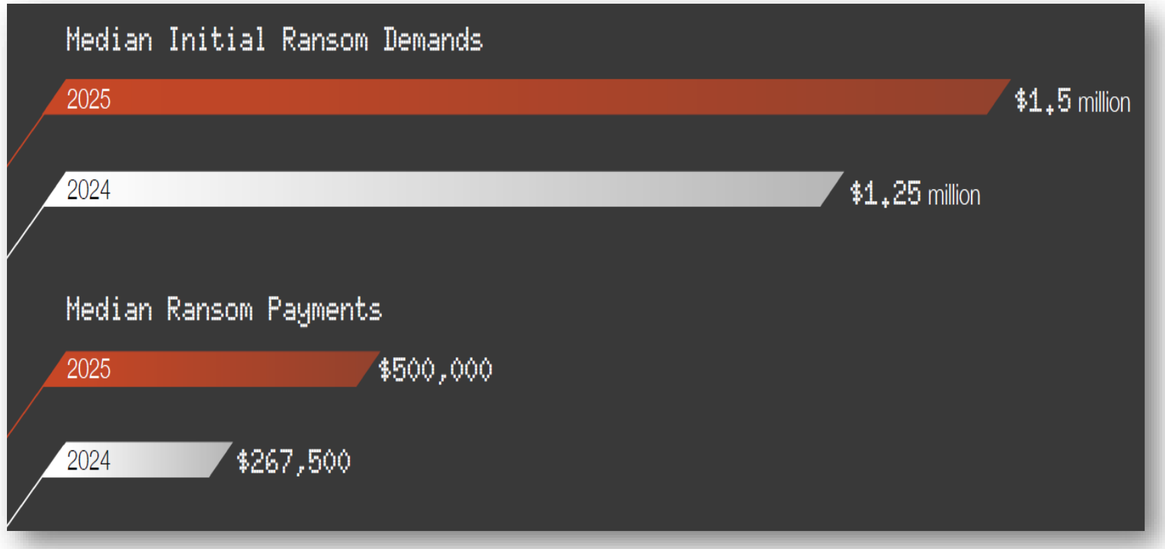
END-OF-LIFE

3. Nova Fase em CyberOT

Crescimento de Ransoware



Serviço de Ransoware cada vez mais lucrativo



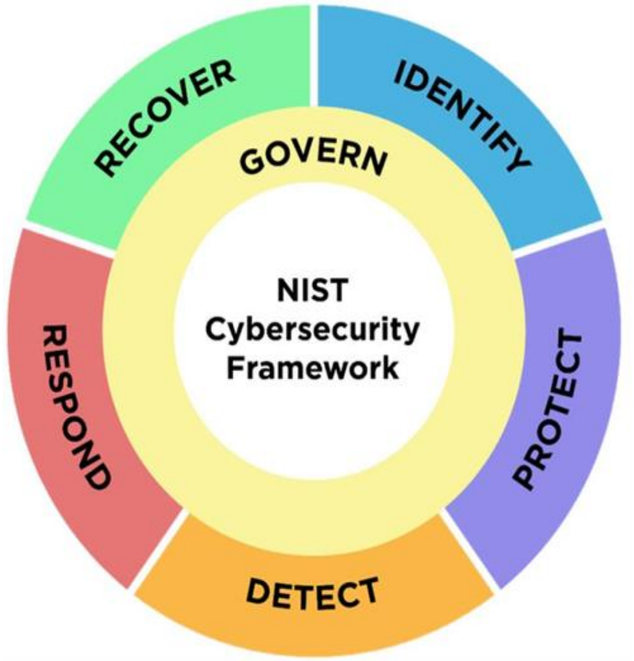


Modelos de IA utilizados para (lista não exaustiva):

- Identificar vulnerabilidades.
- Gerar malwares personalizados.
- Acelerar o ciclo de movimentação lateral.
- Reduzir tempo de exfiltração de dados.
- Controlar e gerenciar cadeias de ataque completas.
- Ampliar a escala de ataques de phishing e engenharia social.

4. NIST Cybersecurity

O NIST CSF 2.0 (*National Institute of Standards and Technology Cybersecurity Framework*, versão 2.0) é um guia desenvolvido pelo governo dos EUA em fev/2024 para ajudar organizações a gerenciar, reduzir e comunicar riscos de cibersegurança. Essa atualização permite que o framework deixe de ser focado apenas em infraestruturas críticas e passe a ser aplicável a qualquer tipo de organização, de qualquer porte ou setor.



GOVERNAR	IDENTIFICAR	PROTEGER	DETECTAR	RESPONDER	RECUPERAR
A estratégia, as expectativas e a política de gerenciamento de riscos de segurança cibernética da organização são estabelecidas, comunicadas e monitoradas	Os riscos atuais de segurança cibernética da organização são compreendidos	Controles e salvaguardas relacionadas para assegurar a entrega de serviços críticos de infraestrutura	Ferramentas, técnicas e atividades para identificar a ocorrência de eventos de *cybersecurity*	Planos, processos e procedimentos para a tomada de ações relacionadas a eventos de *cybersecurity* detectados	Manter planos para a resiliência e para a recuperação de quaisquer capacidades ou serviços impactados por eventos de *cybersecurity*

5. Assessment – Framework Cybersecurity 2.0

Function Description	Function	Category	Score by Category
The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored	GOVERN (GV)	Organizational Context (GV.OC)	
		Risk Management Strategy (GV.RM)	
		Roles, Responsibilities, and Authorities (GV.RR)	
		Policy (GV.PO)	
		Oversight (GV.OV)	
		Cybersecurity Supply Chain Risk Management (GV.SC)	
The organization's current cybersecurity risks are understood	IDENTIFY (ID)	Asset Management (ID.AM)	
		Risk Assessment (ID.RA)	
		Improvement (ID.IM)	
Safeguards to manage the organization's cybersecurity risks are used	PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AA)	
		Awareness and Training (PR.AT)	
		Data Security (PR.DS)	
		Platform Security (PR.PS)	
		Technology Infrastructure Resilience (PR.IR)	
Possible cybersecurity attacks and compromises are found and analyzed	DETECT (DE)	Continuous Monitoring (DE.CM)	
		Adverse Event Analysis (DE.AE)	
Actions regarding a detected cybersecurity incident are taken	RESPOND (RS)	Incident Management (RS.MA)	
		Incident Analysis (RS.AN)	
		Incident Response Reporting and Communication (RS.CO)	
		Incident Mitigation (RS.MI)	
Assets and operations affected by a cybersecurity incident are restored	RECOVERY (RC)	Improvements (RC.IM)	
		Incident Recovery Communication (RC.CO)	

O assessment destina-se a conhecer as diretrizes, os processos, procedimentos, tecnologia adotada, entre outros, e resulta em uma nota que varia 1 a 5 para cada quesito do framework.

Passo seguinte é desenvolver plano de ação para tratamento de *gap analysis*, adquirindo maturidade e aderência as recomendações de cibersegurança.

6. Do Framework à Rotina Operacional

1. Envolvimento e comunicação da Alta Direção e Time Operacional.
2. Capacitar, alinhar e definir ambientes de TI e de OT.
3. Conhecer e segregar os Ativos do Ambiente OT.
4. Riscos Cibernéticos X Riscos Operacionais.
5. Planos de Backup e Restore estruturados e testados.



Plano de Resposta a Incidentes Cibernéticos precisa funcionar às 2horas da manhã de um domingo

pipelinebrazil.com/

linkedin.com/company/pipelinebrazil

instagram.com/pipelinebrazil

Obrigado/Thanks

Nome/Name: Henrique Costa | Marcos Costa

Empresa/Company: NTS – Nova Transportadora do Sudeste

Email: henrique.costa@ntsbrasil.com | marcos.costa@ntsbrasil.com

Tel/Mobil: +55 21 99509-3728