



Fernando Cunha

HoD IT · Vigent Group | Metalogalva

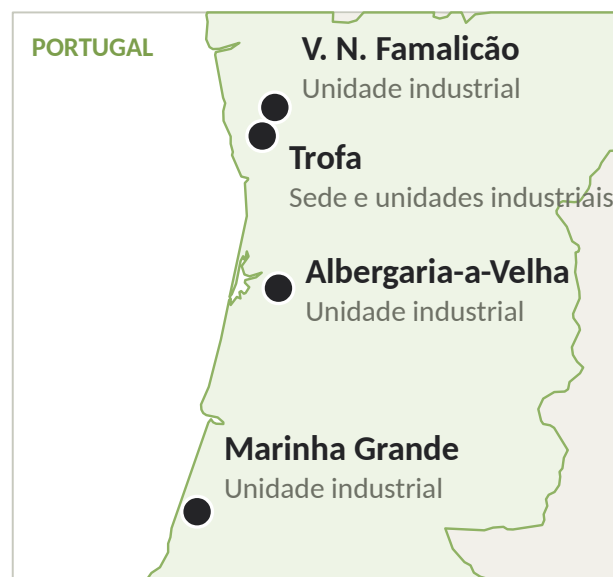
SEGURANÇA DA OPERAÇÃO INDUSTRIAL

Da rede ao SOC: quatro fases para proteger uma operação industrial distribuída

Metalogalva: uma operação industrial distribuída

Estruturas metálicas e galvanização • fundada em 1971, na Trofa • Vigent Group

- 308 equipamentos de rede e segurança, distribuídos por 14 localizações e dois datacenters
- Unidades industriais em Portugal e localizações no estrangeiro
- A produção depende das comunicações e dos sistemas centrais
- Ambientes empresariais e industriais, com necessidades de proteção distintas
- Com a NOSHUT, evoluímos a infraestrutura e o modelo de operação em quatro fases



● Unidade industrial

■ País abrangido pelo projeto

Sistemas centrais e perímetro em dois datacenters de prestadores externos (não representados)

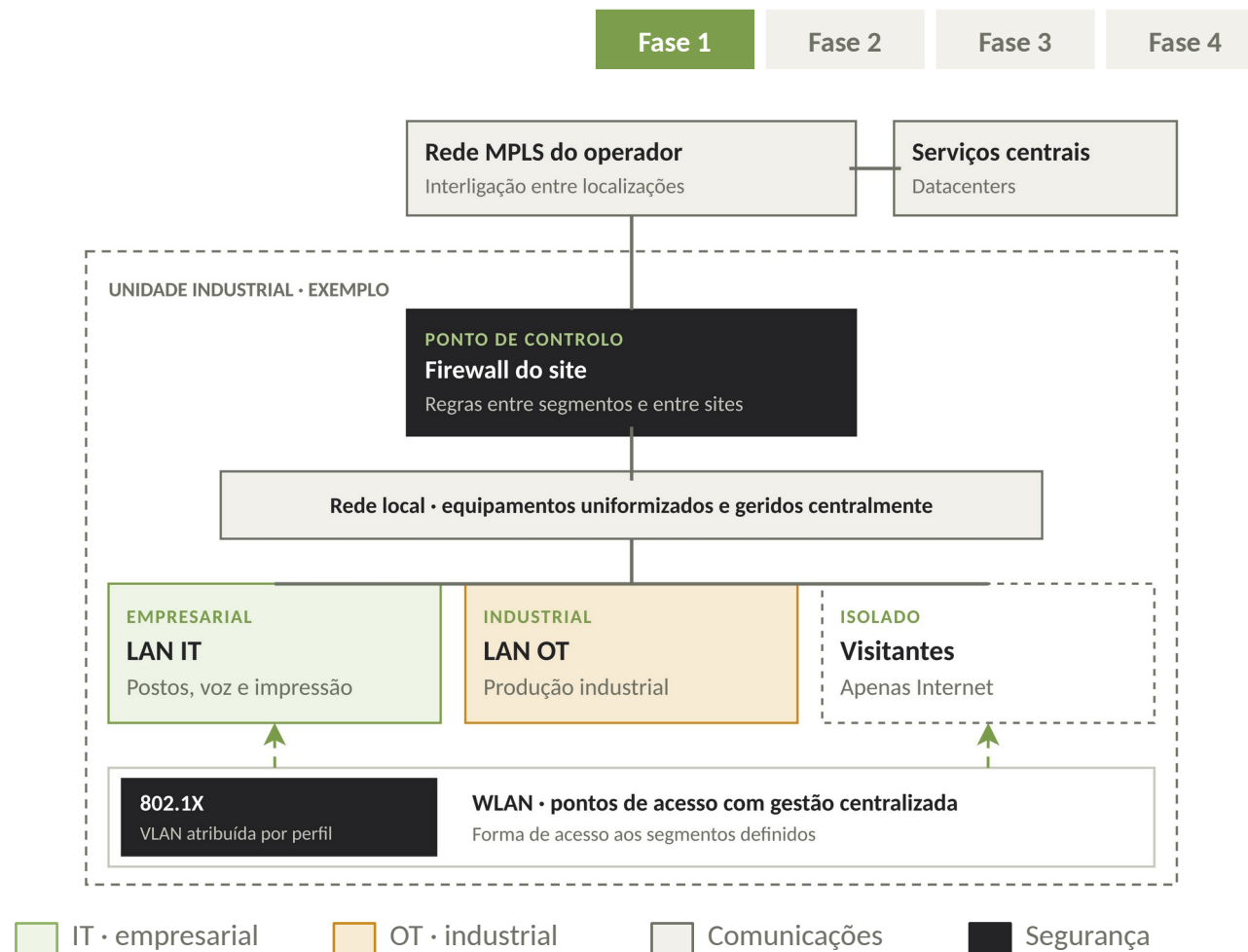


Organizar a rede e estabelecer a segurança local

Criou a base comum sobre a qual assentam as fases seguintes.

Ponto de partida: Rede pouco segmentada, circuitos de acesso e interligação entre sites geridos pelo operador, sem firewalls locais na maioria das localizações.

- **Arquitetura comum a todos os sites**
→ Gestão consistente entre localizações
- **Segmentação funcional e separação IT/OT**
→ Ambientes empresariais e industriais segregados
- **Segurança (firewall) por site**
→ Limita comunicações e propagação de ameaças
- **Equipamentos uniformizados, gestão central**
→ Menos variantes a gerir e a manter
- **WLAN consolidada, 802.1X e VLAN por perfil**
→ Controlo sobre quem acede a cada recurso



Reforçar os serviços centrais e os acessos

Estendeu a arquitetura aos sistemas centrais, ao perímetro e aos acessos.

Fase 1

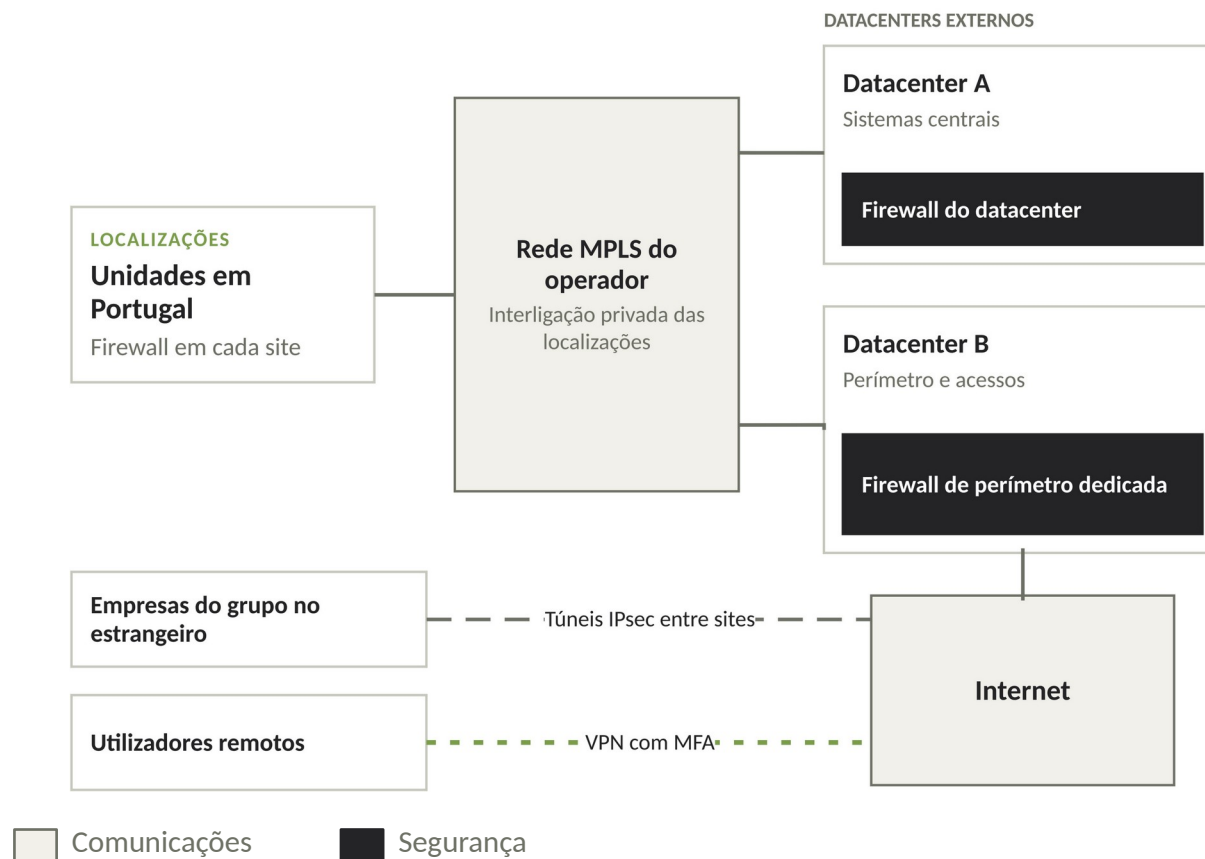
Fase 2

Fase 3

Fase 4

- **Datacenters com rede e segurança reforçadas**
→ Proteção dos sistemas centrais
- **Firewall de perímetro dedicada**
→ Políticas próprias, coerentes com a arquitetura comum
- **VPN remota com autenticação multifator (MFA)**
→ Validação reforçada dos acessos de utilizadores
- **Princípios Zero Trust (ZTNA) na rede local**
→ Acesso condicionado ao estado do dispositivo
- **Túneis IPsec com os sites no estrangeiro**
→ Ligações entre sites cifradas e controladas

Contribui para os objetivos de redução de risco da NIS2. Não equivale a conformidade integral.



Assegurar a operação contínua da infraestrutura

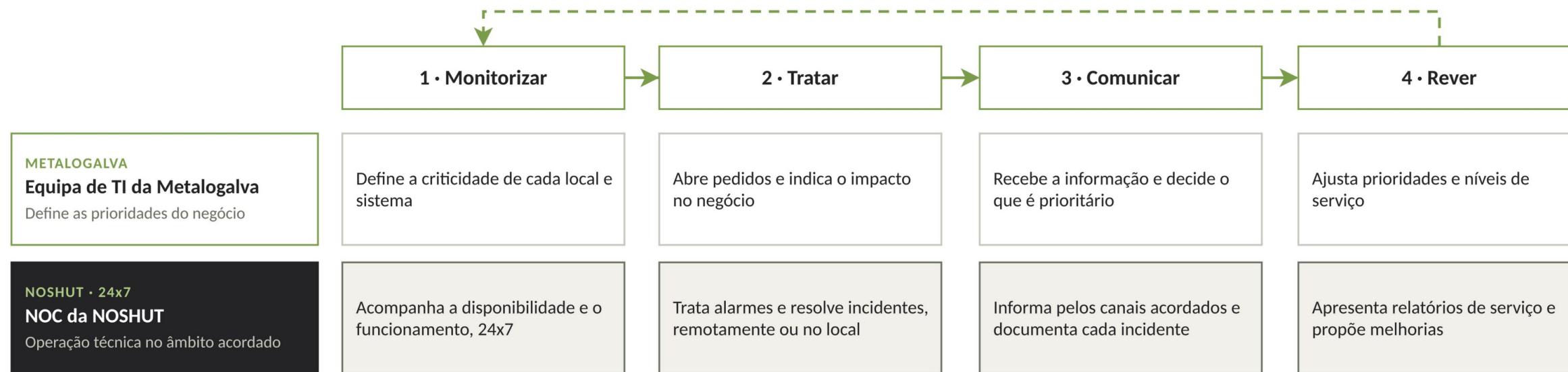
A infraestrutura passou de projeto a serviço, com acompanhamento permanente.

Fase 1

Fase 2

Fase 3

Fase 4



Acompanhamento 24x7

Rede, Wi-Fi e segurança de todas as localizações

Especialização

Equipa técnica especializada, complementar à nossa

Tratamento de falhas

Alarmes, incidentes e atualizações com procedimentos definidos

Previsibilidade

Níveis de serviço por criticidade e revisão periódica

Aprofundar a proteção e organizar a resposta

Sobre uma base protegida e operada, organizamos a deteção e a resposta.

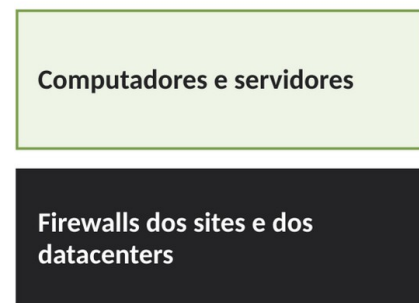
Fase 1

Fase 2

Fase 3

Fase 4

FONTES DE EVENTOS



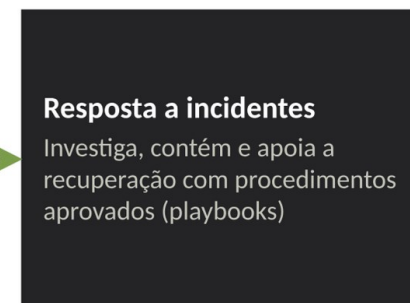
PLATAFORMAS



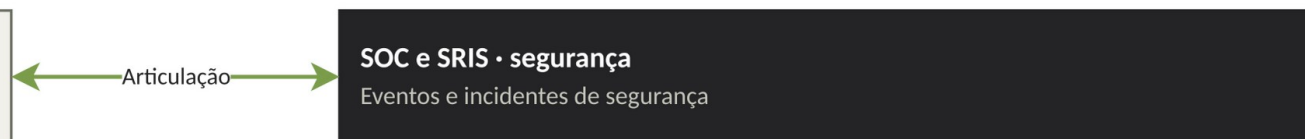
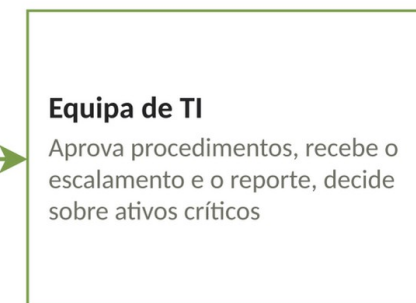
SERVIÇO DO FABRICANTE



SRIS • NOSHUT



METALOGALVA



Visibilidade

Postos, servidores e firewalls analisados em conjunto

Análise especializada

Alertas qualificados e investigados

Resposta organizada

Procedimentos acordados com a nossa equipa

Enquadramento NIS2

Reforça prevenção, deteção e resposta; não esgota a NIS2

O valor para a operação industrial e para a equipa de TI

Os contributos das quatro fases no quotidiano da Metalgalva.

Fase 1

Fase 2

Fase 3

Fase 4

Operação industrial

Comunicações IT/OT com pontos de controlo e regras

Fase 1

Serviços que suportam a atividade protegidos nos datacenters e no perímetro

Fase 2

Ocorrências analisadas segundo a criticidade operacional

Fases 3-4

Resposta coordenada para limitar o impacto de incidentes

Fase 4

Equipa interna de TI

Apoio especializado em rede e segurança

Fases 3-4

Responsabilidades e escalamentos definidos

Fases 3-4

Melhor articulação entre deteção e intervenção técnica

Fase 4

Mais capacidade para acompanhar a evolução do negócio

Fases 1-4

Principais aprendizagens

O que levamos deste percurso.

Fase 1

Fase 2

Fase 3

Fase 4

01

Arquitetura consistente

Uma base comum facilita a proteção e a operação de todas as localizações.

02

Operação contínua

Mantém essa base e acompanha a sua evolução.

03

Contexto industrial

A resposta de segurança beneficia do conhecimento da realidade industrial.

04

Colaboração

A articulação entre a nossa equipa e o parceiro sustenta o modelo.

O valor de um SOC está em compreender a operação que protege e em coordenar, com quem a conhece, a resposta adequada.



Obrigado.

Questões e contactos

Fernando Cunha • HoD IT, Metalogalva

wireless-meeting.com