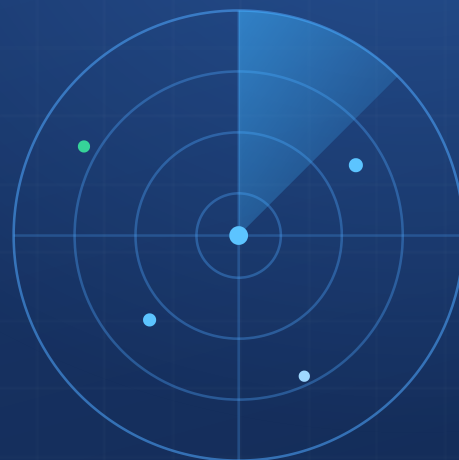




## INTRODUÇÃO EXECUTIVA AO ITSM

# GrandLinks ITSM

Um centro de comando para **visibilidade, governação, segurança, continuidade do serviço e soberania dos dados.**

**OBJECTIVO**

O **GrandLinks ITSM** dá à liderança visibilidade e controlo centralizados sobre toda a infraestrutura digital da organização — activos, serviços, utilizadores, localizações, operações de suporte, postura de segurança e processos de governação.

## TEMAS EXECUTIVOS PRINCIPAIS



Comando e Controlo



Visibilidade



Governação



Segurança



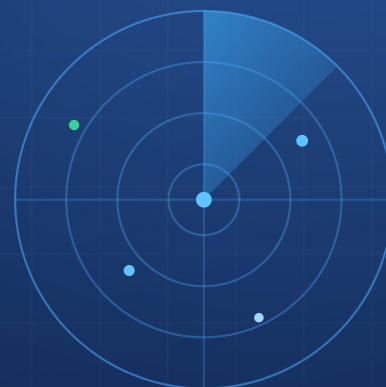
Soberania

O GRANDLINKS ITSM NUMA PÁGINA

## Visão Executiva

UMA VISÃO CONTROLADA DAS OPERAÇÕES DIGITAIS

O GrandLinks ITSM dá à liderança uma visão controlada das operações digitais na sede, nos departamentos, nas províncias e nos escritórios remotos. Reúne pedidos de serviço, incidentes, activos, utilizadores, localizações, indicadores de segurança e histórico de auditoria numa única plataforma operacional.



### O VALOR PARA A LIDERANÇA

Um único centro de comando para ver o que está a acontecer, saber que equipamento existe, atribuir responsabilidades, reduzir atrasos operacionais, detectar riscos cedo e manter o controlo sobre os dados institucionais.

| PERGUNTA DA LIDERANÇA   | O QUE O GRANDLINKS ITSM TORNA VISÍVEL                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------|
| Controlo nas províncias | O que está a acontecer, onde e quem é o responsável?                                                         |
| Confiança nos activos   | Que equipamento e software temos, e onde está?                                                               |
| Suporte remoto          | As equipas conseguem apoiar os escritórios sem deslocações desnecessárias?                                   |
| Supervisão da segurança | Os sistemas estão protegidos, actualizados, monitorizados e alinhados com a política?                        |
| Detecção precoce        | É possível ver os problemas recorrentes e os pontos fracos antes de o serviço parar?                         |
| Soberania dos dados     | A instituição controla os dados operacionais, os acessos, os registos de auditoria e as cópias de segurança? |

Não é apenas um helpdesk. É uma **camada de controlo institucional** para os serviços digitais.

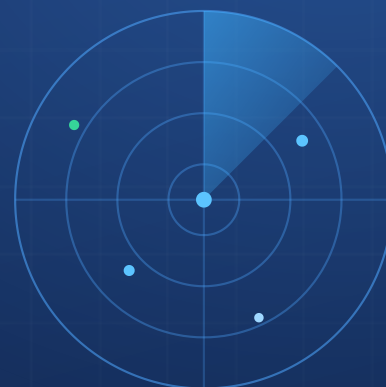


AS OPERAÇÕES DIGITAIS CRESCEM MAIS DEPRESSA DO QUE A VISIBILIDADE DA LIDERANÇA

## O Desafio Institucional

A LIDERANÇA PRECISA DE CONTROLO OPERACIONAL, NÃO APENAS DE RELATÓRIOS

As grandes organizações dependem da tecnologia em cada província, agência, departamento e ponto de atendimento. À medida que o ambiente cresce, a liderança precisa de mais do que relatórios técnicos — precisa de um controlo operacional claro.



### Activos dispersos

Equipamento, software, utilizadores e serviços estão espalhados por muitas localizações, muitas vezes com registos incompletos de propriedade e de ciclo de vida.



### Suporte fragmentado

Os pedidos chegam por chamadas, mensagens, emails e canais informais, o que dificulta a priorização e o acompanhamento.



### Visibilidade tardia do risco

Falhas de segurança, sistemas desactualizados, incidentes recorrentes e activos frágeis só são muitas vezes detectados depois de afectarem o serviço.



### Responsabilização limitada

Sem um fluxo de trabalho governado, é difícil provar quem agiu, quando, o que atrasou e porquê.

### O RISCO PARA A LIDERANÇA

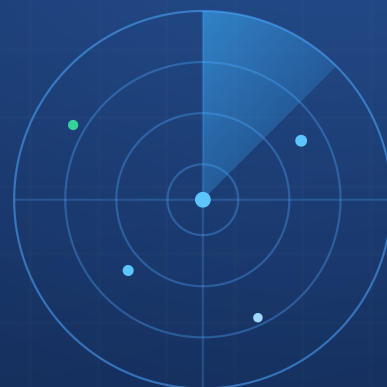
Quando a informação operacional está dispersa, as decisões tornam-se reactivas. Orçamentos, segurança, aquisições, qualidade do serviço e continuidade são geridos com factos incompletos.

UM CENTRO DE COMANDO PARA AS OPERAÇÕES DIGITAIS

## O Que É o GrandLinks ITSM

UMA PLATAFORMA QUE LIGA SEIS DISCIPLINAS

O GrandLinks ITSM é uma plataforma de gestão integrada que liga a gestão de serviços, a inteligência de activos, a visibilidade da segurança, o suporte remoto, os fluxos de governação e os relatórios executivos.



### Operações de serviço

Gerir incidentes, pedidos, itens do catálogo, prioridades, atribuições, escalonamentos e histórico de encerramento.



### Inteligência de activos

Manter uma CMDB fiável com hardware, software, propriedade, localização, estado, ciclo de vida e dependências.



### Relatórios executivos

Ver o desempenho do serviço, os pedidos pendentes, o cumprimento dos SLA, as tendências de risco, a cobertura de activos e os indicadores de responsabilização.

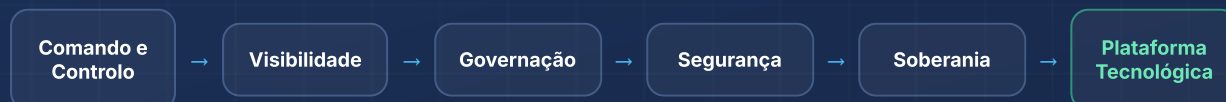


### Segurança e continuidade

Ligar a saúde dos endpoints, os indicadores de segurança, as falhas recorrentes e o risco operacional aos activos e serviços afectados.

#### MODELO OPERACIONAL EXECUTIVO — DA VISIBILIDADE AO CONTROLO

As operações digitais seguem uma cadeia executiva clara, do comando e controlo até à plataforma tecnológica que o torna possível.



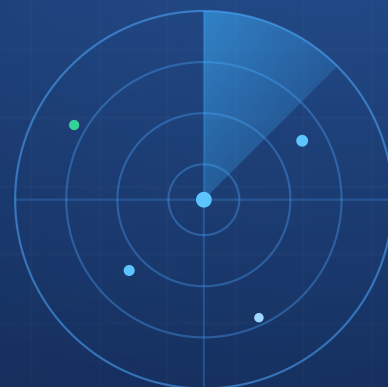
O resultado é um sistema que a liderança utiliza para gerir a tecnologia como um serviço institucional — e não um conjunto de ferramentas desligadas.

UMA VISÃO OPERACIONAL ÚNICA DE AMBIENTES  
DISTRIBUÍDOS

## Controlo nas Províncias e nos Escritórios

GERIR A PROCURA, OS ACTIVOS E O SUPORTE POR LOCALIZAÇÃO

O GrandLinks ITSM apoia instituições que operam em várias províncias, agências, pontos de atendimento e escritórios remotos. Dá à liderança uma visão estruturada da procura, dos incidentes, dos activos, dos riscos e da actividade de suporte por localização.



### Visibilidade por localização

Ver tickets, activos, departamentos, utilizadores e trabalho pendente por província, escritório, piso, departamento ou área de serviço.



### Priorização do serviço

Concentrar a atenção da gestão nas localizações críticas, nas falhas repetidas, nos pedidos em atraso e nas interrupções de maior impacto.



### Suporte remoto facilitado

Dar às equipas de suporte os dados dos activos, o histórico, o contexto do utilizador e a informação dos incidentes para resolver mais problemas à distância.



### Responsabilização operacional

Saber quem recebeu o pedido, quem é responsável pela tarefa, o que mudou e quando o serviço foi restabelecido.

#### ANTES DO GRANDLINKS ITSM

A informação depende de chamadas, mensagens e acompanhamento manual.

Os técnicos são enviados sem diagnóstico completo nem histórico.

Os relatórios são preparados depois dos factos.

#### DEPOIS DO GRANDLINKS ITSM

A liderança vê o estado, a localização, o responsável, a prioridade e o impacto no serviço numa única plataforma.

O diagnóstico remoto começa pelos registos dos activos, pelos incidentes anteriores e pelo contexto da localização.

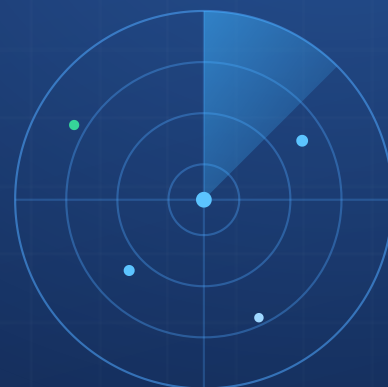
Os painéis e os registos de auditoria estão disponíveis para uma governação contínua.

A FONTE DE VERDADE SOBRE EQUIPAMENTO, SOFTWARE E CONTEXTO DE SERVIÇO

## Inteligência de Activos e CMDB

FACTOS FIÁVEIS POR TRÁS DE CADA DECISÃO

A CMDB é a camada de inteligência de activos do GrandLinks ITSM. Mantém registos estruturados dos itens de configuração — computadores, dispositivos, software, aplicações, serviços, localizações, utilizadores, propriedade e histórico do ciclo de vida.



### Saber o que existe

Manter um inventário controlado de hardware, software, aplicações, activos relacionados e registos de propriedade.



### Saber onde está

Associar os activos a províncias, localizações, departamentos, utilizadores, salas e responsabilidades operacionais.



### Conhecer o ciclo de vida

Acompanhar o estado, a configuração, a garantia, a informação de inventário, o histórico e as alterações ao longo do tempo.



### Conhecer o impacto

Perceber como se ligam activos, serviços, incidentes e dependências antes de tomar decisões.

### ✓ RESULTADO PARA A LIDERANÇA

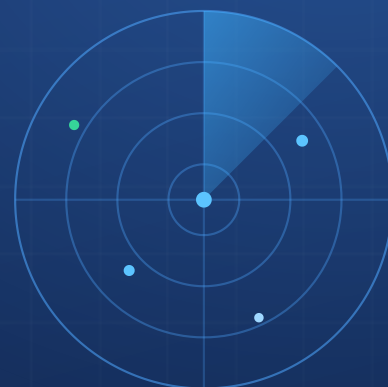
As aquisições, os orçamentos, as auditorias, a renovação de equipamento, a avaliação de riscos e as decisões de suporte passam a basear-se em factos operacionais fiáveis.

MEDIDO, AUDITADO E PROTEGIDO

# Governança, Segurança e Continuidade

UM PROCESSO DE SERVIÇO GOVERNADO, COM GESTÃO PROACTIVA DO RISCO

O GrandLinks ITSM normaliza a forma como os pedidos são criados, atribuídos, priorizados, escalonados, resolvidos e revistos — e liga os indicadores de segurança e de saúde aos activos, localizações, utilizadores e incidentes que a liderança tem de governar.



## Processo de serviço governado

O catálogo de serviços, o controlo dos SLA, a disciplina na atribuição e um histórico pronto para auditoria dão uma responsabilidade clara e a resposta esperada.



## Responsabilização e auditoria

Cada pedido tem um responsável, um estado, uma prioridade e um histórico registado; os gestores revêem os pedidos pendentes, o cumprimento dos SLA e a carga de trabalho.



## Postura de segurança e saúde

Acompanhar o antivírus, a firewall, as actualizações, a encriptação, o arranque seguro e a saúde dos endpoints; identificar activos frágeis e falhas recorrentes.



## Risco e continuidade

Ligar os sinais de risco aos serviços e responsáveis afectados, e usar o histórico de incidentes e as ligações entre activos para responder mais depressa em caso de perturbação.

### ✓ RESULTADO PARA A LIDERANÇA

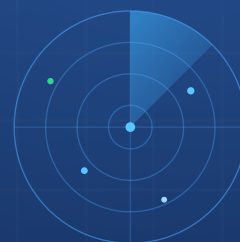
O suporte torna-se um processo governado e a instituição passa de um suporte reactivo para uma gestão proactiva do risco — menos surpresas, intervenção mais rápida e evidências prontas para auditoria.

A INTELIGÊNCIA OPERACIONAL FICA SOB GOVERNAÇÃO

# Soberania dos Dados e Benefícios para a Liderança

CONTROLO INSTITUCIONAL HOJE, VALOR ESCALÁVEL AMANHÃ

As instituições responsáveis por operações críticas têm de manter a autoridade sobre os dados operacionais, o histórico do serviço, os registos de segurança e as evidências de auditoria. O GrandLinks ITSM mantém a total propriedade e governação da inteligência operacional e suporta modelos de implementação alinhados com os requisitos institucionais de segurança e de soberania.



## Implementação controlada

Infraestrutura interna ou ambientes privados, alinhados com a política da instituição.



## Acesso por funções

Acessos de executivos, gestores, técnicos e utilizadores separados por responsabilidade.



## Auditoria e rastreabilidade

Registos da actividade de serviço, das alterações aos activos, das atribuições, das aprovações e do encerramento.



## Preparação para cópias de segurança e recuperação

Registos de serviço, inteligência de activos e evidências de governação protegidos como informação institucional.

## BENEFÍCIOS PARA A LIDERANÇA

### ● Visibilidade unificada

Um único lugar para activos, serviços, incidentes, sinais de segurança e responsabilidades.

### ● Melhores decisões

Planeamento, aquisições, orçamentos e gestão do risco com base em informação verificada.

### ● Eficiência operacional

Menos esforço duplicado, acompanhamento informal, deslocações e pedidos pendentes.

### ● Redução do risco

Activos frágeis, sistemas desactualizados e incidentes recorrentes são detectados mais cedo.

### ● Governação e conformidade

Registos, aprovações, controlo de acessos e registos de auditoria apoiam a responsabilização.

### ● Preparação para o futuro

Um modelo escalável para expansão, integração e modernização.

O GrandLinks ITSM transforma a actividade de TI dispersa em **operações digitais governadas** — a camada de controlo para **ver, governar e proteger** os serviços institucionais.

PULSAR