



Boas Práticas de Proteção Inteligente Global

Rangel Logistics Solutions

O projeto de Boas Práticas de Segurança Física e Tecnológica visa reforçar a proteção integrada das operações de transporte e logística contratual, promovendo um modelo moderno, resiliente e alinhado com os desafios atuais. Assente nos princípios de proteção, inovação, confiança e visão sistémica, estabelece políticas, procedimentos e soluções que garantem a segurança de pessoas, bens, infraestruturas e informação ao longo de toda a cadeia logística. Na vertente física, inclui controlo de acessos, vigilância, proteção perimetral e gestão de incidentes, suportados por metodologias de avaliação de risco que permitem identificar vulnerabilidades e implementar medidas preventivas eficazes. Na componente tecnológica, aposta na digitalização e integração de sistemas inteligentes, como videovigilância avançada, monitorização remota e análise de dados, assegurando uma visão em tempo real das operações. A convergência entre segurança física e tecnológica elimina silos, aumenta a eficiência e melhora a capacidade de resposta. O projeto valoriza também o fator humano, promovendo formação contínua e uma cultura organizacional orientada para a segurança como um elemento central na gestão das operações de transporte e logística contratual, promovendo uma abordagem integrada, inovadora e orientada para resultados. Tecnologia, processos e pessoas, estabelecem as bases para um modelo de segurança robusto, adaptável e sustentável, capaz de responder aos desafios atuais e futuros do setor.

O projeto de Boas Práticas de Segurança Física e Tecnológica constitui uma iniciativa estratégica orientada para reforçar a proteção integrada das operações de transporte e logística contratual, promovendo um modelo de segurança moderno, resiliente e alinhado com os desafios contemporâneos. Tem como principal objetivo garantir a segurança de pessoas, bens, infraestruturas e informação ao longo de toda a cadeia logística, através da definição de um quadro estruturado de políticas, procedimentos e soluções tecnológicas. Paralelamente, visa reduzir riscos operacionais, prevenir incidentes e perdas, e assegurar a continuidade do negócio, mesmo em contextos adversos. Entre os objetivos centrais destaca-se ainda a integração eficaz entre segurança física e tecnológica, eliminando redundâncias e promovendo uma visão global e em tempo real das operações.

O projeto pretende também aumentar a eficiência operacional, otimizar recursos e melhorar a capacidade de resposta a incidentes, suportando a tomada de decisão com base em informação fiável e atualizada. No domínio da segurança física, o objetivo passa pela implementação de práticas normalizadas de controlo de acessos, vigilância, proteção perimetral e gestão de incidentes, suportadas por metodologias de avaliação de risco que permitam identificar vulnerabilidades e adotar medidas preventivas eficazes. Já na componente tecnológica, pretende-se potenciar a digitalização das operações, através da integração de sistemas inteligentes, como videovigilância, monitorização remota e análise de dados. Outro objetivo estratégico consiste em promover uma cultura organizacional de segurança, valorizando o fator humano através da formação contínua, sensibilização e desenvolvimento de competências, reforçando o compromisso coletivo com a prevenção e a melhoria contínua.

O projeto visa igualmente assegurar o cumprimento normativo e o alinhamento com boas práticas internacionais, reforçando a confiança, a transparência e a credibilidade junto de clientes, parceiros e



stakeholders. Simultaneamente, procura posicionar a segurança como um investimento estratégico, com impacto direto na reputação, sustentabilidade e competitividade das organizações. Em síntese, este projeto tem como objetivo central transformar a segurança num pilar estruturante da gestão logística, através de uma abordagem integrada, inovadora e orientada para resultados, capaz de responder de forma eficaz aos desafios atuais e futuros do setor.

Foram implementados: Sistemas de Segurança Física ⌘ Controlo de acessos electrónico (cartões RFID, biometria, QR Code) para gestão de entradas/saídas ⌘ Videovigilância (CCTV/IP) com gravação digital e analytics (deteção de movimento, reconhecimento de padrões) ⌘ Sistemas de intrusão (sensores, alarmes, detecção perimetral) ⌘ Barreiras físicas inteligentes (torniquetes, portões automatizados, bollards) ⌘ Sistemas de gestão de visitantes com registo e rastreabilidade Tecnologias de Segurança Inteligente ⌘ Plataformas PSIM (Physical Security Information Management) para integração e centralização de todos os sistemas ⌘ VMS (Video Management Systems) avançados para gestão de vídeo em tempo real ⌘ Análise de vídeo com IA (deteção de comportamentos suspeitos, objetos abandonados, controlo de multidões) ⌘ Dashboards operacionais com KPIs e monitorização em tempo real Tecnologias aplicadas à Logística e Transporte ⌘ Sistemas de geolocalização (GPS/GNSS) em veículos e activos ⌘ Telemetria e IoT para monitorização de condições (temperatura, abertura de portas, rotas) ⌘ Sistemas de gestão de frotas (FMS) com controlo de rotas e comportamento do condutor ⌘ Selos electrónicos e sensores inteligentes para protecção de carga Segurança da Informação e Cibersegurança ⌘ Sistemas SIEM (Security Information and Event Management) para monitorização de eventos ⌘ Controlo de acessos lógico (IAM) ⌘ Firewalls, EDR/XDR e protecção de endpoints ⌘ Encriptação de dados e backups seguros Comunicação e Coordenação Operacional ⌘ Centros de controlo (SOC/CSO) com monitorização 24/7 ⌘ Sistemas de comunicação crítica (rádio digital, apps seguras) ⌘ Plataformas de gestão de incidentes com workflows automatizados Inovação e Tecnologias Emergentes ⌘ Inteligência Artificial e análise preditiva para antecipação de riscos ⌘ Big Data e Business Intelligence para apoio à decisão ⌘ Drones e robótica para vigilância de perímetros extensos ⌘ Integração com plataformas digitais de logística Em síntese Foram implementadas tecnologias que permitem prevenir, detectar, analisar e responder a riscos em tempo real, garantindo uma visão integrada da segurança e aumentando significativamente a eficiência e resiliência das operações.

O desenvolvimento do projecto de Boas Práticas de Segurança Física e Tecnológica foi motivado pela crescente complexidade e criticidade das operações de transporte e logística contratual, num contexto marcado pela globalização, digitalização e aumento das exigências regulatórias e operacionais. A evolução das cadeias logísticas, cada vez mais interligadas e dependentes de sistemas tecnológicos, expôs as organizações a novos riscos, incluindo ameaças físicas, intrusões, furtos, sabotagem, bem como vulnerabilidades digitais e ciberataques. Paralelamente, verificou-se uma maior exigência por parte de clientes e parceiros relativamente à segurança, rastreabilidade e fiabilidade dos serviços prestados.

Adicionalmente, a fragmentação entre sistemas de segurança física e tecnológica, muitas vezes geridos de forma isolada, evidenciou ineficiências, redundâncias e limitações na capacidade de resposta a incidentes. Esta realidade reforçou a necessidade de uma abordagem integrada, capaz de proporcionar uma visão global e em tempo real das operações.

Outro factor determinante foi a necessidade de garantir a continuidade do negócio e a resiliência operacional, especialmente em cenários de disrupção, como falhas tecnológicas, incidentes de segurança



ou eventos externos imprevistos. Tornou-se essencial evoluir de uma lógica reactiva para uma abordagem preventiva e preditiva, suportada por tecnologia e análise de dados. Por fim, o projecto surge também como resposta à necessidade de promover uma cultura organizacional de segurança, valorizando o factor humano, a formação contínua e a responsabilização dos diversos intervenientes. Neste contexto, o projecto foi concebido como uma iniciativa estratégica para alinhar processos, tecnologias e pessoas, reforçando a protecção, a eficiência e a confiança nas operações de transporte e logística, e posicionando a segurança como um verdadeiro pilar de valor e competitividade.

Os resultados do projecto de Boas Práticas de Segurança Física e Tecnológica devem ser apresentados com base em indicadores objectivos, demonstrando impacto directo na redução de riscos, eficiência operacional e reforço da resiliência organizacional.

Destacam-se os seguintes: Resultados mensuráveis alcançados 1. Redução de incidentes e perdas ⇨ Diminuição significativa de furtos, intrusões e acessos não autorizados ⇨ Redução de incidentes operacionais relacionados com falhas de segurança ⇨ Menor número de ocorrências com impacto financeiro directo 2. Melhoria dos tempos de resposta ⇨ Redução do tempo médio de detecção e resposta a incidentes (MTTD/MTTR) ⇨ Maior capacidade de actuação preventiva através de alertas em tempo real ⇨ Resolução mais rápida e eficaz de situações críticas 3. Aumento da visibilidade e controlo operacional ⇨ Monitorização em tempo real de operações, ativos e infraestruturas ⇨ Rastreabilidade completa de veículos, cargas e acessos ⇨ Centralização da informação em plataformas integradas 4. Eficiência operacional e optimização de recursos ⇨ Redução de redundâncias entre sistemas físicos e tecnológicos ⇨ Optimização de equipas de segurança e vigilância ⇨ Diminuição de custos operacionais associados a falhas ou incidentes 5. Cumprimento normativo e auditorias ⇨ Maior conformidade com requisitos legais e standards internacionais ⇨ Melhoria dos resultados em auditorias internas e externas ⇨ Reforço da governação e controlo interno 6. Desenvolvimento de cultura de segurança ⇨ Aumento da adesão dos colaboradores a práticas seguras ⇨ Melhoria dos níveis de formação e sensibilização ⇨ Redução de erros humanos associados a falhas de segurança Contributo para a segurança da organização

O projecto contribuiu de forma estruturante para a segurança organizacional, ao transformar um conjunto disperso de medidas num sistema integrado, proactivo e orientado para resultados. Em primeiro lugar, permitiu a transição de um modelo reactivo para uma abordagem preventiva e preditiva, baseada em análise de risco e utilização de tecnologia. Esta evolução reduziu significativamente a exposição a ameaças e aumentou a capacidade de antecipação. Em segundo lugar, a integração entre segurança física e tecnológica proporcionou uma visão global das operações, melhorando a coordenação entre equipas e sistemas, e eliminando lacunas que anteriormente poderiam ser exploradas. Adicionalmente, o projecto reforçou a resiliência operacional, assegurando a continuidade do negócio mesmo em cenários adversos, através de planos de contingência, monitorização contínua e capacidade de resposta rápida. Importa ainda destacar o impacto ao nível da confiança e reputação institucional, uma vez que o reforço da segurança aumentou a credibilidade junto de clientes, parceiros e stakeholders, constituindo um factor diferenciador no mercado. Por fim, ao valorizar o factor humano e promover uma cultura de segurança, o projecto garantiu que as soluções implementadas são sustentáveis no tempo, assegurando não apenas a protecção dos activos, mas também a evolução contínua das práticas organizacionais. Os resultados demonstram que o projecto não só reduziu riscos e incidentes, como também elevou a segurança a um nível estratégico, contribuindo directamente para a eficiência, sustentabilidade e competitividade da organização.



PRÉMIOS DE SEGURANÇA

SECURITY MAGAZINE | REVISTA DOS PROFISSIONAIS DE SEGURANÇA

Os principais desafios de segurança da organização decorrem da crescente complexidade das operações de transporte e logística contratual, num contexto marcado pela digitalização, interconectividade e elevada exigência operacional. Um dos desafios centrais prende-se com a protecção integrada de pessoas, bens e infraestruturas ao longo de toda a cadeia logística, frequentemente dispersa geograficamente e sujeita a múltiplos intervenientes. Esta dispersão aumenta a exposição a riscos como furtos, intrusões, sabotagem e acessos não autorizados.

Outro desafio relevante é a convergência entre segurança física e tecnológica. A coexistência de sistemas distintos, nem sempre integrados, dificulta a obtenção de uma visão global e em tempo real das operações, limitando a capacidade de detecção precoce e resposta eficaz a incidentes. A cibersegurança assume também um papel crítico, face à crescente digitalização dos processos e à utilização de plataformas tecnológicas interligadas. A protecção de dados, sistemas e comunicações contra ciberameaças tornou-se essencial para garantir a continuidade do negócio e a confiança dos stakeholders.

Adicionalmente, destaca-se a necessidade de gestão eficiente do risco em ambiente dinâmico, com exigência de adaptação constante a novas ameaças, alterações regulatórias e evolução tecnológica. A antecipação de riscos e a transição de uma abordagem reactiva para preventiva constituem desafios permanentes. O factor humano representa igualmente um ponto crítico, exigindo investimento contínuo em formação, sensibilização e criação de uma cultura organizacional orientada para a segurança, de forma a minimizar erros e comportamentos de risco. Por fim, a organização enfrenta o desafio de garantir a continuidade operacional e a resiliência, assegurando a capacidade de resposta a incidentes e a rápida recuperação perante eventuais disrupções, mantendo níveis elevados de serviço e confiança.

O projecto envolveu uma equipa multidisciplinar de aproximadamente 25 colaboradores, reflectindo a sua natureza transversal e estratégica. Estiveram directamente envolvidos os seguintes departamentos-chave: • Segurança (física e corporativa) – coordenação global do projecto, definição de políticas, análise de risco e implementação de medidas • Tecnologias de Informação (IT) – integração de sistemas, cibersegurança, infraestrutura tecnológica e suporte às plataformas digitais • Operações / Logística – articulação com as actividades de transporte, definição de procedimentos operacionais e validação de soluções no terreno • Gestão de Frota / Transportes – implementação de sistemas de monitorização, rastreabilidade e controlo de activos móveis • Recursos Humanos – desenvolvimento de programas de formação, sensibilização e promoção da cultura de segurança • Compliance / Jurídico – garantia de conformidade legal, regulamentar e alinhamento com boas práticas e standards internacionais. Adicionalmente, contou-se com o contributo de parceiros externos especializados, nomeadamente fornecedores de tecnologia, consultores de segurança e entidades certificadoras, que apoiaram a implementação de soluções e a validação técnica do projecto. Esta abordagem colaborativa permitiu assegurar uma integração eficaz entre áreas, promovendo uma visão holística da segurança e garantindo a adopção consistente das boas práticas em toda a organização.

O que torna este projeto diferenciador face às práticas comuns no mercado é a sua abordagem integrada, preventiva e estratégica da segurança, particularmente relevante no contexto dos transportes e da logística contratual, ainda marcados por modelos reativos e fragmentados. Este projeto rompe com essa lógica ao implementar um modelo preditivo, suportado por análise contínua de risco e tecnologias inteligentes, que permitem antecipar ameaças e reduzir vulnerabilidades. A integração de sistemas, a centralização da informação e a monitorização em tempo real proporcionam uma visão global das operações, melhorando significativamente a capacidade de decisão e resposta. Adicionalmente, posiciona a segurança como um



pilar estratégico do negócio, diretamente ligado à continuidade operacional, à proteção de pessoas e mercadorias e à confiança dos clientes. A valorização do fator humano e a promoção de uma cultura de segurança reforçam a eficácia e sustentabilidade das medidas implementadas. Assim, o projeto distingue-se por transformar a segurança de uma função reativa num modelo proativo, inteligente e orientado para resultados, aumentando a eficiência, resiliência e competitividade da organização.

Nota: A informação contida neste documento destina-se exclusivamente à divulgação dos Prémios de Segurança da Security Magazine. Qualquer utilização para outros fins requer autorização prévia da Security Magazine e dos respetivos intervenientes.