



A3A®
Engenharia
de Sistemas



Lenel OnGuard

Solution Overview

VISÃO GERAL

O **Lenel OnGuard** é uma plataforma corporativa LenelS2 by Honeywell para **controle de acesso físico e gerenciamento integrado de segurança eletrônica**, desenvolvida para ambientes que exigem operação centralizada, escalabilidade, rastreabilidade, alta disponibilidade e integração com sistemas externos.

A solução permite estruturar arquiteturas de segurança para edifícios corporativos, indústrias, data centers, instituições públicas, campus, hospitais, centros logísticos e infraestruturas críticas, integrando credenciais, cardholders, visitantes, alarmes, eventos, mapas, vídeo, painéis, leitores, dispositivos de campo, relatórios, dashboards, APIs e sistemas corporativos.

Em uma arquitetura de segurança eletrônica, o Lenel OnGuard pode atuar como núcleo operacional do controle de acesso, orquestrando níveis de acesso, calendários, permissões, dispositivos, integrações com VMS, gestão de visitantes, evidências e relatórios operacionais.

ESCOPO DE ATUAÇÃO

A A3A Engenharia de Sistemas atua no planejamento, implantação, integração, expansão, migração, hardening, suporte e melhoria contínua de ambientes Lenel OnGuard, conectando a plataforma aos requisitos operacionais, tecnológicos e de segurança de cada organização.

PLANEJAMENTO E ARQUITETURA LENEL ONGUARD

- Levantamento de requisitos de controle de acesso, segurança eletrônica e operação patrimonial
- Análise de sites, portas, leitores, controladoras, usuários, credenciais, visitantes e áreas críticas
- Definição de arquitetura PRO, ADV, Enterprise, Cloud, on-premises ou híbrida
- Dimensionamento de servidores, estações, browser clients, bancos de dados, regiões e segmentos
- Definição de níveis de acesso, timezones, holidays, grupos de dispositivos e grupos de lockdown
- Planejamento de integrações com VMS, RH, IAM, Active Directory, BMS, SOC e sistemas corporativos
- Definição de redundância, disponibilidade, backup, retenção, trilhas de auditoria e governança de acesso
- Planejamento de expansão futura, roadmap tecnológico e ciclo de vida da plataforma

IMPLANTAÇÃO E CONFIGURAÇÃO DO SISTEMA

- Instalação e configuração de servidores, clientes, serviços e componentes Lenel OnGuard
- Configuração de banco de dados, comunicação TCP/IP, serviços de aplicação e estações operacionais
- Cadastro e organização de painéis, leitoras, portas, sensores, entradas, saídas e dispositivos de campo
- Criação de níveis de acesso, calendários, feriados, horários, grupos, segmentos e regras operacionais
- Configuração de alarmes, eventos, mapas, notificações, relatórios, dashboards e permissões de usuários
- Configuração de clientes browser-based para operação, credenciais, visitantes, relatórios, dashboards e gestão de hardware
- Testes funcionais, validação de comunicação, validação de dispositivos, aceite operacional e documentação técnica

CONTROLE DE ACESSO CORPORATIVO

O controle de acesso Lenel OnGuard permite estruturar políticas de entrada, circulação e permanência em áreas corporativas, técnicas, industriais e críticas, com regras baseadas em usuário, grupo, localidade, horário, credencial, risco e perfil operacional.

- Gestão de portas, leitores, controladoras, sensores e atuadores
- Políticas de acesso por usuário, grupo, área, horário, segmento, site e criticidade
- Controle de acessos para funcionários, visitantes, terceiros, prestadores, equipes técnicas e operadores
- Anti-passback, lockdown, guard tour, mustering e rotinas de segurança patrimonial
- Integração com elevadores, interfonia, alarmes, vídeo, RH, IAM e sistemas corporativos
- Revisão periódica de permissões, saneamento de acessos e análise de exceções
- Governança de acessos com trilhas de auditoria, relatórios, dashboards e indicadores operacionais

GESTÃO DE CREDENCIAIS E CARDHOLDERS

A gestão de cardholders é uma das funções centrais do Lenel OnGuard. A solução pode consolidar dados de usuários, badges, fotos, credenciais móveis, níveis de acesso, registros de atividade, vínculos corporativos e informações de identificação.

- Cadastro, importação, manutenção e saneamento de cardholders
- Associação de badges, credenciais físicas, credenciais móveis, access levels e perfis de acesso
- Impressão de crachás, captura de fotos, edição de imagens e gestão de informações de identificação
- Gestão em massa de acessos, badges, cardholders e registros inativos
- Busca, filtros, listas customizadas, relatórios e exportação de dados
- Suporte a segmentação, campos personalizados e regras específicas por unidade ou grupo
- Integração com RH, diretórios, IAM, sistemas de visitantes, sistemas de terceiros e fluxos corporativos

ACCESS MANAGER E GESTÃO DESCENTRALIZADA DE PERMISSÕES

Em ambientes grandes, a gestão de permissões pode ser distribuída para responsáveis por áreas, departamentos ou unidades. O Lenel OnGuard permite estruturar fluxos de solicitação, aprovação, negação, atribuição e revisão de acessos conforme as regras de

negócio da organização.

- Gestão de direitos de acesso por gestores autorizados
- Aprovação, negação ou retenção de solicitações de acesso
- Visualização de access levels disponíveis e leitores associados
- Gestão de badges ativos e inativos com indicadores visuais
- Definição de áreas de controle e limites de atuação para cada gestor
- Suporte a fluxos com Cardholder Self Service e workflows internos
- Redução da dependência da equipe central para alterações simples e recorrentes

GESTÃO DE VISITANTES

O Lenel OnGuard pode apoiar processos completos de gestão de visitantes, desde o pré-cadastro até o check-in, emissão de crachá, atribuição de acesso temporário, notificação ao anfitrião, registro de evidências e check-out.

- Pré-cadastro de visitantes por anfitriões ou equipe de recepção
- Check-in e check-out em recepção assistida ou modelo self-service
- Impressão de crachás temporários, captura de fotos e emissão de credenciais temporárias
- Atribuição de credenciais descartáveis, plásticas ou móveis
- Notificações automáticas para hosts e co-hosts
- Aceite de documentos, termos, políticas, NDAs e requisitos de compliance
- Controle de visitas por agenda, visitante, anfitrião, localidade, horário e tipo de visita
- Rastreabilidade de presença, permanência, acesso concedido e histórico de visitas

MONITORAMENTO DE ALARMES, MAPAS E EVENTOS

O ambiente de operação Lenel OnGuard pode concentrar alarmes, eventos, dispositivos, mapas, status de hardware, imagens, vídeos e ações contextuais, permitindo que operadores acompanhem e respondam a ocorrências em tempo real.

- Monitoramento em tempo real de alarmes, eventos, dispositivos e zonas operacionais
- Reconhecimento, tratamento, escalonamento, marcação em progresso e encerramento de alarmes
- Mapas interativos com status de dispositivos, notificações visuais e ações contextuais
- Listas filtradas por operador, severidade, área, zona, tipo de evento ou criticidade
- Visualização de vídeo ao vivo e gravado associado a eventos de acesso ou alarmes
- Layouts personalizados por zona de monitoramento, operador, site ou equipe

- Suporte a respostas operacionais, abertura de portas, verificação de cardholder e investigação de eventos

INTEGRAÇÃO COM VÍDEO E VMS

A integração entre Lenel OnGuard e sistemas de vídeo permite associar eventos de controle de acesso a imagens ao vivo, gravações, snapshots, clipes e investigação visual, aumentando a consciência situacional da equipe de segurança.

- Integração com LenelS2 NVR, Milestone XProtect e plataformas de vídeo compatíveis
- Visualização de vídeo ao vivo e gravado em contexto de eventos de acesso, alarmes e mapas
- Associação de câmeras, portas, alarmes, áreas, dispositivos e zonas de monitoramento
- Criação de layouts de vídeo, visualização por múltiplas câmeras e operação em monitores dedicados
- Controle PTZ, zoom digital, busca por data e hora, snapshots e exportação de clipes
- Integração entre VMS, storage, permissões, rede, retenção e operação de segurança
- Suporte à investigação de eventos, análise pós-incidente e preservação de evidências

RELATÓRIOS, DASHBOARDS E AUDITORIA

Relatórios e dashboards transformam os dados do Lenel OnGuard em informações úteis para operação, auditoria, gestão de riscos, conformidade, revisão de permissões e melhoria contínua da segurança.

- Relatórios de eventos, cardholders, acessos, alarmes, usuários e transações
- Dashboards gráficos para operação, segurança, auditoria e gestão
- Agendamento de relatórios recorrentes e publicação controlada de informações
- Exportação em formatos como Excel, PDF, HTML e texto delimitado
- Filtros, ordenações, relatórios favoritos e visões personalizadas
- Indicadores de uso, alarmes, credenciais, exceções operacionais, permissões e conformidade
- Suporte a auditorias, investigações, governança de acesso e revisão periódica de acessos

SAÚDE DO SISTEMA, MANUTENÇÃO E WATCH

Ambientes Lenel OnGuard com operação crítica exigem monitoramento contínuo da saúde do sistema, incluindo servidores, banco de dados, serviços, backups, capacidade, contagens de dispositivos, logs e desempenho operacional.

- Monitoramento de servidores, banco de dados, serviços, versões e indicadores de performance
- Acompanhamento de contagens de segmentos, painéis, leitores, entradas, saídas, cardholders, badges e visitantes
- Verificação de status de serviços, tamanho de logs, backups, archive/purge e rotinas críticas
- Dashboards de saúde, capacidade, desempenho, utilização de áreas e indicadores de sistema
- Identificação de riscos operacionais antes que se tornem falhas críticas
- Suporte a manutenção preventiva, revisão de configuração e recomendações de melhoria
- Apoio à operação de ambientes enterprise, multi-site e de alta disponibilidade

HARDWARE, CONTROLADORAS MERCURY E SEGURANÇA DA COMUNICAÇÃO

A infraestrutura Lenel OnGuard depende de dispositivos de campo, controladoras, leitores, sensores, atuadores e comunicação segura. A gestão adequada desses elementos é essencial para disponibilidade, conformidade e segurança operacional.

- Gestão de controladoras LenelS2/Mercury e dispositivos de campo
- Administração remota de senhas, usuários e parâmetros de controladoras
- Aplicação de políticas fortes de senha e controle granular de usuários
- Gestão de certificados TLS, validade, expiração, renovação e cadeia de confiança
- Suporte a autenticação mútua, comunicação segura e alinhamento com políticas de TI/InfoSec
- Atualização simultânea de múltiplas controladoras para redução de esforço operacional
- Redução de downtime e maior rastreabilidade sobre mudanças de configuração

INTEGRAÇÕES CORPORATIVAS E CUSTOMIZAÇÕES

O Lenel OnGuard pode ser integrado a sistemas corporativos, operacionais e prediais para reduzir retrabalho, automatizar fluxos, aumentar rastreabilidade e conectar segurança física aos processos de negócio.

- Integração com RH, IDMS, Active Directory, IAM, ERP, BMS e plataformas corporativas
- Sincronização de cardholders, admissões, desligamentos, alterações cadastrais e credenciais
- Integração com elevadores, estacionamento, sistemas de reserva, recepção, visitantes e facilities

- Integração com alarmes, SOC, VMS, interfonia, automação, painéis e sistemas de terceiros
- Desenvolvimento de interfaces, workflows, regras customizadas e automações específicas
- Integrações via APIs, DataConduIT, conectores, importações e exportações controladas
- Fluxos para terceiros, contratadas, certificações, treinamentos, acessos temporários e áreas restritas

ONGUARD CLOUD E MIGRAÇÃO PARA NUVEM

O Lenel OnGuard pode ser planejado em arquitetura on-premises, cloud ou híbrida, conforme requisitos de conectividade, governança, disponibilidade, segurança, operação, suporte e estratégia de TI da organização.

- Análise de viabilidade para OnGuard Cloud, implantação local ou arquitetura híbrida
- Avaliação de cloud readiness, conectividade, requisitos de segurança e dependências operacionais
- Planejamento de migração de ambientes existentes para cloud ou modernização gradual
- Estratégia de backups, atualizações, suporte, monitoramento, disponibilidade e continuidade
- Redução de esforço local de infraestrutura, quando o modelo cloud for aderente aos requisitos do cliente
- Integração com clientes browser-based, sistemas corporativos, dispositivos de campo e operação remota
- Plano de transição com minimização de downtime, validação funcional e operação assistida

UPGRADES, MIGRAÇÕES E ALTA DISPONIBILIDADE

Ambientes Lenel OnGuard frequentemente exigem upgrade de versão, migração de sistemas legados, consolidação de bases, conversões de arquitetura, hardening, clustering, revisão de permissões e implantação de alta disponibilidade.

- Planejamento e execução de upgrades de versão com controle de risco e redução de downtime
- Migração de sistemas legados para Lenel OnGuard
- Conversões PRO, ADV e Enterprise conforme escala, capacidade e necessidade de expansão

- Integração, consolidação ou saneamento de bases de cardholders, badges e access levels
- Implementação de ambientes redundantes, clusters, backup, contingência e planos de recuperação
- Factory acceptance testing, testes de regressão, validação funcional e rollback planejado
- Hardening, revisão de permissões, cleanup de acessos e alinhamento com políticas de TI/InfoSec

SUPORTE, SUSP E SERVIÇOS GERENCIADOS

A sustentação de um ambiente Lenel OnGuard deve considerar atualizações, patches, suporte técnico, revisão periódica, manutenção preventiva, monitoramento de saúde, documentação e suporte à equipe operacional.

- Apoio à gestão do Software Upgrade and Support Plan (SUSP)
- Planejamento de atualizações, patches, upgrades e release notes
- Revisão de ambiente, arquitetura, versões, banco de dados, backups e logs
- Monitoramento de replicação, falhas de RPC, serviços, archive/purge e contagens de registros
- Suporte a ambientes de teste, homologação, produção e contingência
- Treinamento, documentação, base de conhecimento e capacitação de operadores e administradores
- Manutenção preventiva, recomendações de melhoria e acompanhamento de saúde da plataforma

APLICAÇÕES E AMBIENTES

A solução Lenel OnGuard é indicada para organizações que precisam controlar acessos físicos, credenciais, visitantes, alarmes, eventos e integrações em ambientes com múltiplas áreas, usuários, níveis de criticidade e requisitos de governança.

- Edifícios corporativos e sedes administrativas
- Indústrias, utilities, plantas operacionais e ambientes IT/OT
- Data centers, salas críticas e infraestruturas de missão crítica
- Hospitais, universidades, centros de pesquisa e instituições de ensino
- Instituições financeiras, bancos, seguradoras e ambientes regulados
- Centros logísticos, condomínios empresariais, shopping centers e instalações multiusuário
- Órgãos públicos, aeroportos, portos, terminais, campus e infraestruturas críticas
- Ambientes enterprise com múltiplas unidades, regiões, segmentos e integrações corporativas

Em todos esses contextos, o objetivo é aplicar o Lenel OnGuard como plataforma central de segurança eletrônica, com regras de acesso bem definidas, operação rastreável, integração com sistemas adjacentes e capacidade de expansão ao longo do ciclo de vida da organização.

CRITÉRIOS TÉCNICOS DE PROJETO

O projeto de uma solução Lenel OnGuard deve considerar escala, arquitetura, integração, disponibilidade, governança, cibersegurança, operação, manutenção e requisitos de expansão.

ESCALA E ARQUITETURA

- Número de cardholders, badges, leitores, portas, painéis, alarmes, entradas e saídas
- Número de sites, regiões, segmentos, estações de trabalho, browser clients e operadores
- Arquitetura PRO, ADV, Enterprise, Cloud, on-premises ou híbrida
- Servidores, bancos de dados, storage, rede, estações, clientes e sistemas integrados
- Capacidade atual, capacidade futura, expansão planejada e requisitos de continuidade

DISPONIBILIDADE E CONTINUIDADE

- Redundância de servidores, banco de dados, serviços, rede, energia e armazenamento
- Failover, cluster, backup, contingência, recuperação e tolerância a falhas
- Plano de manutenção, janelas operacionais, testes de recuperação e documentação
- Monitoramento de saúde, logs, backups, archive/purge, serviços e performance
- Critérios de disponibilidade compatíveis com a criticidade da operação de segurança

SEGURANÇA, HARDENING E GOVERNANÇA

- Perfis administrativos, permissões, segregação de funções e trilhas de auditoria
- Senhas fortes, certificados, TLS, autenticação, comunicação segura e gestão de controladoras
- Atualização de software, patches, revisão de versões e alinhamento com políticas de TI/InfoSec
- Revisão periódica de access levels, cardholders inativos, badges inativos e acessos temporários
- Governança de dados, retenção, relatórios, evidências e conformidade com políticas internas

INTEGRAÇÃO COM SISTEMAS EXTERNOS

- Integração com VMS, NVR, vídeo, interfonia, elevadores, estacionamento e alarmes
- Integração com RH, IAM, Active Directory, ERP, BMS, SOC e sistemas de gestão
- Integração por APIs, DataConduIT, conectores, importações, exportações e automações

- Sincronização de usuários, visitantes, desligamentos, alterações cadastrais e credenciais
- Compatibilização entre requisitos de segurança física, TI, facilities, compliance e operação

OPERAÇÃO, AUDITORIA E MELHORIA CONTÍNUA

- Fluxos de atendimento, alarmes, eventos, reconhecimento, escalonamento e encerramento
- Relatórios e dashboards para operação, auditoria, segurança patrimonial e gestão
- KPIs de alarmes, acessos, visitantes, exceções, falhas, credenciais e disponibilidade
- Treinamento de operadores, administradores, recepção, segurança patrimonial e equipe técnica
- Revisão de regras, limpeza de cadastros, tuning de alarmes e evolução da plataforma

ARQUITETURA DO SISTEMA

A escolha entre Lenel OnGuard on-premises, OnGuard Cloud ou arquitetura híbrida depende da estratégia de TI, criticidade operacional, conectividade, requisitos de segurança, governança de dados, disponibilidade, suporte, custo de infraestrutura e modelo de gestão da organização.

Ambientes on-premises podem ser indicados quando a organização precisa manter controle direto sobre servidores, banco de dados, rede, integrações locais e políticas internas de infraestrutura. Já a nuvem pode ser considerada quando há interesse em reduzir carga operacional de infraestrutura, simplificar atualizações, ampliar acesso web e adotar um modelo gerenciado.

Em muitos cenários, a melhor estratégia pode ser híbrida ou gradual, com avaliação de dependências, requisitos de rede, dispositivos de campo, integrações, janelas de migração, planos de contingência e operação assistida.

IMPLEMENTAÇÃO

Implementar ou modernizar um ambiente Lenel OnGuard exige mais do que instalação de software. A solução envolve engenharia de segurança eletrônica, redes, servidores, banco de dados, dispositivos de campo, integração com sistemas corporativos, governança de acessos, cibersegurança e operação contínua.

A A3A Engenharia de Sistemas conduz soluções Lenel OnGuard por meio de uma metodologia orientada a diagnóstico, engenharia, implantação, integração, validação, documentação e melhoria contínua.

DIAGNÓSTICO

- Levantamento de portas, leitores, painéis, servidores, estações, usuários, credenciais e integrações
- Análise da arquitetura atual, versão, banco de dados, SUSP, infraestrutura e capacidade
- Inventário de cardholders, badges, access levels, timezones, holidays, alarmes e eventos
- Avaliação de riscos, lacunas, obsolescência, gargalos, falhas operacionais e requisitos futuros
- Verificação de documentação, permissões, políticas, governança, relatórios e suporte atual

ENGENHARIA

- Definição de arquitetura lógica, física, operacional e de integração
- Especificação de servidores, clientes, rede, banco de dados, disponibilidade e retenção
- Desenho de matriz de acesso, política de credenciais, visitantes, relatórios e auditoria
- Planejamento de integrações com VMS, RH, IAM, AD, BMS, SOC e sistemas corporativos
- Elaboração de plano de migração, upgrade, implantação, contingência, rollback e aceite

IMPLANTAÇÃO E INTEGRAÇÃO

- Instalação e configuração de componentes Lenel OnGuard
- Cadastro ou migração de hardware, cardholders, badges, perfis, grupos e níveis de acesso
- Configuração de alarmes, mapas, eventos, visitantes, relatórios, dashboards e clientes web

- Integração com vídeo, controladoras, diretórios, RH, sistemas corporativos e plataformas externas
- Execução de mudanças em janela operacional, com controle de risco e acompanhamento técnico

VALIDAÇÃO E COMISSIONAMENTO

- Testes de leitores, portas, controladoras, alarmes, mapas, eventos e credenciais
- Testes de access levels, timezones, holidays, visitantes, relatórios e dashboards
- Testes de vídeo, VMS, snapshots, clipes, retenção e evidências
- Testes de integração, failover, backup, recuperação, permissões e operação
- Registro de pendências, correções, aceite operacional e documentação de entrega

OPERAÇÃO ASSISTIDA E MELHORIA CONTÍNUA

- Treinamento de operadores, administradores, recepção, equipe técnica e gestores
- Acompanhamento inicial da operação, suporte a dúvidas e ajustes finos
- Revisão de alarmes, permissões, relatórios, dashboards, cadastros e integrações
- Documentação as built, manuais operacionais, matriz de responsabilidades e recomendações
- Plano de manutenção, upgrades, SUSP, hardening, revisão periódica e evolução da plataforma

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.