

Pondo Inteligência em cada Acesso com Sistemas Electrónicos

***Open Intelligence, um conceito Business Control***

No ambiente de mudança permanente em que vivemos, cada organização passou a ter a necessidade de providenciar os mais elevados níveis de segurança possíveis, às suas instalações e colaboradores.

O conceito *Open Intelligence* é a resposta integrada a essa necessidade. Até muito recentemente, a segurança electrónica era demasiado associada aos universos empresarial e militar, e a tecnologias e investimentos inatingíveis. No entanto, as contínuas evoluções da tecnologia, com a aproximação da informática, permitiram, por um lado aumentar exponencialmente as capacidades dos sistemas electrónicos de segurança, por outro, fazer com que os custos a estes associados passassem a ser acessíveis à generalidade das organizações.

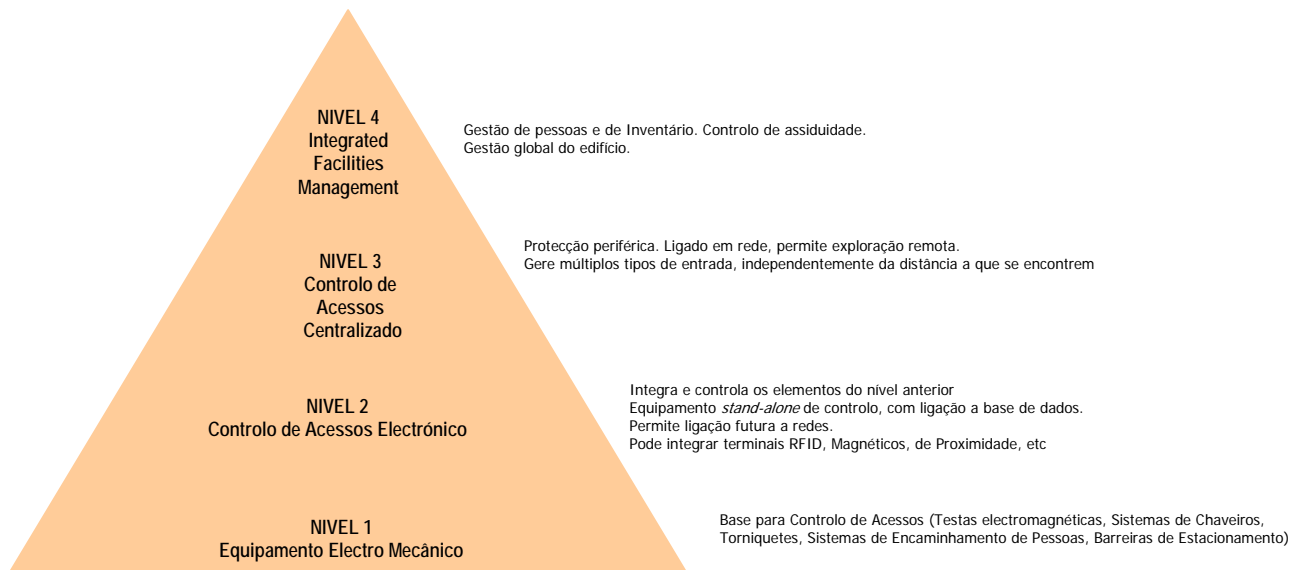
Um aspecto incontornável desta tendência é o de actualmente ser possível a criação de soluções escaláveis, em que a base do produto permite a progressão na sua complexidade, flexibilizando assim a adaptação das soluções ao quadro de necessidades e de capacidade de investimento das organizações.

O desenvolvimento do conceito *Open Intelligence* baseia-se precisamente nesta premissa. Recolhendo o melhor de todas as áreas associadas ao controlo de acessos dito "convencional", procedemos à sua integração com áreas de grande modernidade, como a identificação por radio frequência (RFID), a biometria, as redes informáticas *wireless*, ou as tecnologias de multimédia, organizando-as e hierarquizando-as de forma a construirmos um conceito sólido, inovador e tecnologicamente evoluído.

Estas soluções são hoje adaptáveis, com igual fiabilidade, a ambientes tão distintos como aeroportos, edifícios públicos, centrais nucleares, hospitais, fábricas, universidades, estaleiros de obras, condomínios, ginásios, parques de estacionamento, etc. As enormes diferenças na tipologia, quer das necessidades, quer da natureza arquitectónica destes locais poderia fazer crer exactamente o contrário: que seria impossível fazer uso das mesmas tecnologias para dar resposta aos problemas de Controlo de Acessos aí levantados.

O conceito *Open Intelligence* oferece a resposta a estas questões, através de uma filosofia de integração de Controlo de Acessos de multi-nível, em que as soluções progridem numa lógica de camada (*MultiLayer*), sendo a camada de equipamentos e serviços anterior, base para a camada seguinte.

O objectivo final pretende ser a gestão global dos edifícios ou campus, no que diz respeito à circulação das pessoas e bens. O software e as bases de dados que surgem no topo da pirâmide do sistema inicial tornam-se a base para um novo sistema, onde para o surgimento do controlo electrónico de ponto, do inventário automático de bens ou da gestão das operações de manutenção do edifício passam a ser necessários pouco mais que a utilização um conjunto de periféricos específicos, que integram com *plug-ins* e *suites* adicionais de software no sistema base.



## A Base de um Controlo de Acessos

Apesar de se tratar de uma área onde a tecnologia se tem mostrado pródiga em desenvolver soluções, o objectivo básico de um Sistema de Controlo de Acessos é extremamente simples: controlar **quem pode estar num dado momento, num determinado local** (*who goes where and when*).

O conceito *Open Intelligence* procura ir mais longe: pode não bastar para as exigências de segurança de uma organização, controlar segundo este modelo. Frequentemente, a organização precisará saber quem tentou entrar num dado local utilizando um cartão falso ou furtado; se o colaborador da empresa, com autorização de acesso, o fez acompanhado de um estranho; se, ainda que autorizado, o fez fora das horas normais de serviço – a lista de excepções dependerá apenas do grau de exigência.

Para que estas excepções possam ser endereçadas, a integração de sistemas torna-se vital, e o conceito deve inevitavelmente evoluir do Controlo de Acessos para o Controlo Integrado de Instalações (Integrated Facilities Management). Torna-se necessária a integração de tecnologias multimédia para a interligação de sistemas de Circuito Fechado de Televisão (CCTV), de tecnologias wireless para a obtenção de dados a partir de locais remotos ou

simplesmente para a sua redundância, de tecnologias de reconhecimento biométrico e/ou de RFID para a *certificação incrementalmente mais apurada da identidade do indivíduo*.

Esta progressiva tendência - conceptual e física - de integração, potencia a criação de sistemas globais de gestão, na medida em que os pontos de contacto (comuns) das tecnologias empregues, são cada vez mais numerosos e de grande fiabilidade de utilização.

Exemplo deste tipo de abordagem são os ambientes de condomínio “cash free”.

Este conceito apoia-se na possibilidade de, a partir de um identificador de RFID – um cartão, tag, pulseira, etc. – atribuído a um dado cliente, este ter a possibilidade de aceder a todos os serviços de um condomínio fechado, quer se trate de ver a sua entrada franqueada no Health Club, ou utilizar a crédito da sua conta no condomínio, os serviços de Bar ou Restaurante.

A partir de um único elemento identificador (RFID), um condómino pode aceder ao interior do condomínio com a sua viatura; abrir todas as portas até ao seu apartamento, incluindo esta; marcar hora no corte de ténis ou golfe; reservar mesa no restaurante; aceder à infraestrutura de telecomunicações comum do empreendimento para utilizar a internet; identificar-se perante o sistema de domótica para alterar as especificações de climatização do seu apartamento – e ver debitadas automaticamente na sua conta crédito (ou débito) de condómino todas as acções que impliquem despesas, que lhe chegarão num único extracto de conta.

Os benefícios de um sistema RFID são inúmeros. A partir do momento em que a integração de diferentes sistemas de serviço a clientes se tornou possível sob um único elemento de identificação, o limite é o adequação do potencial às realidades específicas de cada caso.