b&a
BRASILIANO & ASSOCIADOS

REVISTA ELETRÔNICA 39ª

www.brasiliano.com.br

ROUBO DE INFORMAÇÃO

ISSN 1678-2496N

Novembro - Dezembro 2008 | Edição 39ª

SUMÁRIO

A Revista Eletrônica Brasiliano &
Associados nº39 é uma publicação
bimestral.

Diretor Executivo: Antonio Celso Ribeiro Brasiliano
Diretora de Treinamento: Enza Cirelli
Projeto Gráfico e Editoração: Marina Brasiliano
e-mail: mabrasiliano@gmail.com

OS SEUS RISCOS ESTÃO SOB CONTROLE?

A desaceleração global da economia, que inevitavelmente provocará impactos no mercado e economia brasileira, está intensificando a adoção de sistemas mais rígidos de controles e de gestão de riscos nas operações das empresas. Isto significa que o gestor de riscos necessita de ferramentas de TI para poder realizar uma gestão com maior eficácia.

As empresas provedoras de software estão enxergando uma grande oportunidade com a crise, pois as empresas estão precisando de indicadores precisos para monitorarem e controlarem seus desempenhos. Instituições financeiras por exemplo não podem reduzir investimentos, podem e devem controlar custos operacionais, mas a dimensão dos investimentos deve manter a mesma velocidade em função da fragilidade da economia.

Por esta razão, nestes tempos de enorme turbulência, o gestor de riscos deve lemabrar de dois insights do economista Joseph Schumpeter:

1 A força motriz do progresso econômico é a inovação. Riqueza, prosperidade, desenvolvimento vêm da inovação e só dela. Para Schumpeter, inovação tem um significado preciso: é a substituição de formas antigas por formas novas de produzir e consumir. Produtos novos, processos novos, modelos de negócios novos. Essa substituição é permanente, e ele a chamou de “destruição criativa”. É esse processo que faz o sistema capitalista ser o melhor que existe para gerar riqueza e produzir crescimento econômico. O que Einstein chamou de “anarquia do sistema capitalista” é exatamente sua força, segundo Schumpeter. Sem “destruição criativa” não há riqueza.

2 Os agentes da inovação são os empreendedores. Empreendedores são indivíduos (são pessoas, não instituições, não governos, não partidos) movidos “pelo sonho e pela vontade de fundar um reino particular”. Por causa da “destruição criativa”, homens de negócios prósperos pisam num terreno que está permanentemente “se esfarelando embaixo de seus pés”. A instabilidade, o não equilíbrio, a desigualdade e a turbulência são inevitáveis - o preço a pagar pelo progresso.

Diante destes dois insights de Schumpeter só podemos, nós, que trabalhamos com riscos, ficarmos satisfeitos, pois a profissão nossa está alicerçada SEMPRE em terreno “minado”. Vai depender de nossas competências, tecnicidade e criatividade gerenciarmos muito bem os riscos corporativos.

Será que possuímos a capacidade de implantar o processo de “destruição criativa”?? Sugiro que reflitamos bem neste final de ano de 2008, pois 2009 a gestão de riscos será realmente a Fronteira do Sucesso!!!

Bom ano, muita sorte e sucesso a todos!!

b&a
BRASILIANO&ASSOCIADOS

Antonio Celso Ribeiro Brasiliano – Publisher
abrasiliano@brasiliano.com.br

CONHEÇA OS GRUPOS DE SISTEMAS DE CONTROLE DE ACESSO

Rodolfo Simon Halasz*

Os recursos podem ser adotados de vários modos, inclusive de forma integrada, e para isso é preciso saber quais as fórmulas mais indicadas

Controle de acesso é um sistema que permite determinar especificamente quais pessoas entram em quais locais e em quais horários isso acontece ou pode acontecer. O objetivo da instalação de um sistema de controle de acesso é o de aumentar o nível de segurança em um local, ao mesmo tempo em que se melhora o das informações obtidas e se aumenta a velocidade com que os usuários podem passar pelos controles.

Portas dotadas de chaves são o mais simples sistema de controle de acesso, porém as informações que ele proporciona são muito limitadas. Imagine-se um sistema com alguns milhares de usuários que devem acessar várias áreas em uma fábrica utilizando apenas chaves.

Para aumentar a qualidade das informações e, ao mesmo tempo, facilitar o acesso de muitas pessoas a vários locais diferentes, foram criados os sistemas de controle de acesso que são dispositivos que permitem o gerenciamento e monitoração inteligente de acessos.

É importante lembrar que a área de segurança está sempre em desenvolvimento, principalmente em tempos de conflitos e insegurança generalizada. Há uma contínua evolução tecnológica dos equipamentos e sistemas, com recursos sempre mais avançados e características técnicas cada vez melhores.

Para definir um sistema de controle de acesso, devemos verificar os principais equipamentos, sistemas e funções que devem ser instaladas e com que objetivos.

Pode-se dividir um sistema de controle de acesso em quatro grandes grupos: dispositivos de campo, interfaces de dispositivos de campo, controladoras ou concentradoras e servidor/estações de trabalho/software.

Dispositivos de campo

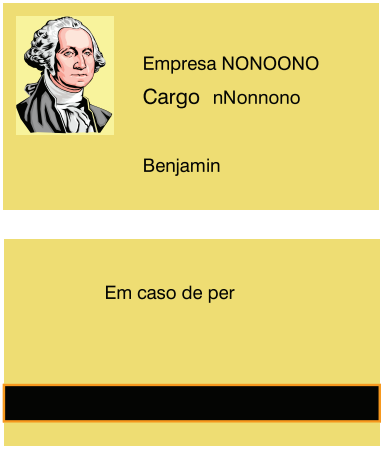
Os principais dispositivos de campo em um sistema de controle de acesso são os cartões.

Os cartões de acesso são os que possuem uma numeração apropriada ou códigos que permitem a identificação

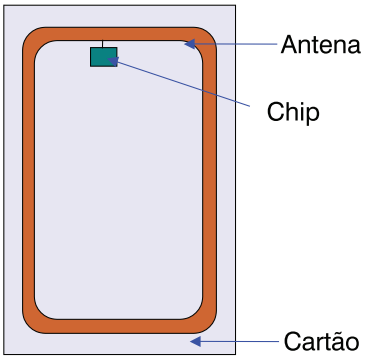
única de cada cartão, e sua associação (também única) com cada um dos usuários do sistema. As principais tecnologias de cartões utilizados e suas aplicações, benefícios e deficiências são:

Exemplos de códigos de barras sem e com proteção

Cartões de códigos de barras: são os mais antigos e formados por um conjunto de barras. Obedecem a uma certa padronização, são impressos ou colados sobre cartões de PVC, papel cartão ou outro material para ter resistência mecânica.O código de cada cartão é definido pela composição de barras e espaços em branco, representando "zeros" e "uns", em uma codificação binária. Como o código era visível, a duplicação destes cartões era extremamente fácil, bastando fazer uma cópia reprográfica do mesmo. Para se evitar esta cópia e aumentar o nível de segurança, criaram-se os cartões de "código de barras protegido". Esta proteção baseia-se na impressão de uma tarja de cor vermelha entre os espaços das barras. Esta cor não é lida por alguns leitores de códigos de barras que utilizam luz infravermelha para a leitura, porém tornam a cópia por máquinas comuns impossível. Os cartões de código de barras tem sido cada vez menos utilizados, pois já existem outros com tecnologias mais avançadas.

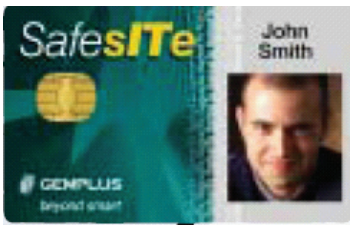


Cartões magnéticos: ou de tarja magnética foram desenvolvidos para uso bancário, tendo sido padronizados por uma instituição de bancos norte-americanos, a American Bank Association (ABA), que definiu os padrões dos cartões, modelo de uso e dados a serem gravados. A definição foi que o sistema utilizaria uma tarja de material ferromagnético com três trilhas de dados gravados. A trilha mais utilizada é a trilha do meio, a número 2. Esta utilização se tornou tão comum que muitos fabricantes se referem a este sistema como sendo ABA trilha (ou track) 2. Os dois tipos de tarjas magnéticas mais utilizados são as de baixa e as de alta coercividades. Os cartões de baixa coercividade (capacidade que o cartão tem de armazenar e manter os dados mesmo diante de campos magnéticos, tal como os produzidos por televisores, monitores e outros equipamentos eletrônicos) não são muito utilizados pois os dados se perdem com grande facilidade. Tal como para os cartões código de barras, a cópia de cartões magnéticos é simples e não oferecem segurança.

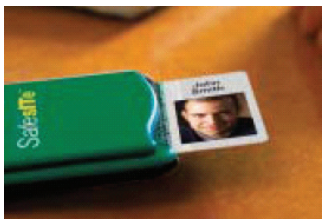


Cartões de proximidade: O cartão de proximidade tem este nome porque não é necessário o contato físico entre o cartão e o leitor para que os dados sejam lidos. Os cartões de proximidade são cartões muito mais seguros, possuem um microchip em seu interior e uma antena para captar as ondas eletromagnéticas produzidas pelo leitor de proximidade. Cada microchip possui um código único, que pode ser gravado de acordo com a necessidade de cada cliente. Tipicamente cada fabricante utiliza freqüências de operação diferenciadas, logo cartões de um fabricante não funcionarão com cartões ou leitores de outro.Os cartões de proximidade são geralmente produzidos para gerar uma saída com um certo número de bits (“zeros” e “uns”). O número de 26 bits de saída é considerado um padrão “aberto” e podem ser comprados de fornecedores diferentes, o que,obviamente reduz a segurança do sistema. Para aumentar o nível de segurança criou-se um código chamado “facility code”. Este código é uma referência ao projeto: cada instalação tem um facility code próprio. Assim, pode-se ter um cliente que utiliza cartões numerados de 0001 a 9999 com facility code 05 e outro cliente com a mesma numeração mas com facility code 43. Os cartões de um cliente não poderão ser utilizados pelo outro. O sistema de controle de acesso deve permitir o reconhecimento do facility code, pois é uma das características mais importantes para o aumento do nível de segurança do sistema.

Cartões SmartCard: ou cartões inteligentes são os que possuem microchips embutidos, mas com uma diferença em relação aos de proximidade, os microchips podem conter dados, que podem ou não ser gravados pelo próprio sistema de segurança.Existem basicamente dois tipos de cartões smartcard: com e sem contato.



Cartão SmartCard com contato


Cartão SmartCard com contato inserido em um leitor

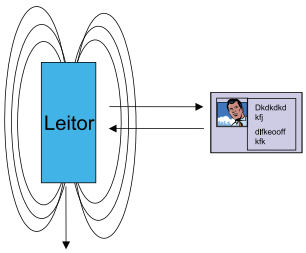
Os cartões com contato são a primeira geração de cartões smartcard e apresentam uma área de contatos visíveis (ver figura). Para se acionado é necessário o contato físico do cartão com o leitor.

Todos os cartões que dependem de inserção acarretam erros de leitura e devem, se possível, ser evitados.

A nova geração de cartões smartcard é sem contato e o maior fabricante mundial utiliza um produto denominado de Mifare, uma marca registrada. Esta tecnologia tem operação muito semelhante à do cartão de proximidade, exceto pelo fato de que o microchip pode armazenar dados e não apenas transmitir os previamente gravados. Em um cartão Mifare existe uma área livre de acesso, onde é armazenado o número serial do cartão, ou ID number, e existem 16 setores restritos para os quais o acesso deve ser feito com o uso de senhas. É nestes setores que é possível armazenar dados. Os cartões Mifare permitem o armazenamento de 512 bytes a 4kb, sendo que os mais utilizados são os de 1kb. A nova geração de cartões smartcard é chamada Desfire e poderá armazenar até 256kb, em 256 setores. Os cartões sem contato (contactless) são largamente utilizados em aplicações de transporte público.

Leitores: são os dispositivos que lêem os dados armazenados nos cartões de acesso e os enviam ao restante do sistema. Para cada tecnologia de cartão utilizado é necessário o uso de um leitor de tecnologia correspondente.

Leitores de código de barras e magnético: Os mais simples e são de preço baixo e fácil aquisição. O único ponto ao qual se deve prestar atenção é que foram desenvolvidos basicamente para uso interno e não são em sua maioria adequados para uso externo, pois deve haver um contato físico entre o cartão e o leitor, o que acaba sendo prejudicado por sujeira, poeira etc. Deve ainda haver compatibilidade entre a comunicação do leitor com o restante do sistema, geralmente padrão ABA trilha 2.



101110111– 26 bits

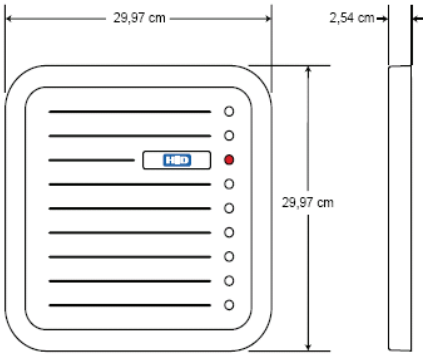
Leitores de proximidade: O princípio de funcionamento de um leitor de proximidade é o da indução eletromagnética. O leitor está continuamente emitindo um campo eletromagnético ao seu redor. Com a aproximação do cartão, correntes são induzidas, o que energiza o chip do mesmo, que emite o código gravado. Este código é captado pelo leitor, que o envia ao restante do sistema para análise.

Os leitores de proximidade são fabricados em uma grande variedade de formatos e com diferentes distâncias de leitura. Os de menor tamanho podem ler cartões de proximidade a distâncias de até 7cm, mas leitores de longo alcance podem ler cartões de proximidade a até 70cm. Alguns leitores de proximidade também podem vir com teclados, para que o usuário digite uma senha de confirmação. O uso de cada leitor depende de características particulares de cada projeto e seu uso deve ser baseado nos locais, tráfego, nível de segurança etc.Tipicamente se utilizam leitores de curto alcance para controle de acesso a portas e catracas, leitores com teclado para portas de salas onde é necessário um nível de acesso maior (CPD, Tesourarias, RH) e leitores de longo alcance para acesso de veículos.


Figura 2 – Leitor de proximidade de curto alcance

Como os leitores de proximidade podem ser selados, são indicados para uso interno ou externo.


Leitor de proximidade com teclado



Leitor de longo alcance com dimensões

Exemplo de leitores smartcard

Leitores de Smartcard: Esta aplicação surgiu como uma aplicação de curto alcance, para transações comerciais.A distância de leitura de um leitor smartcard é de 3cm, podendo chegar a 7cm em alguns modelos. Tal como nos leitores de proximidade, existem modelos com e sem teclado.

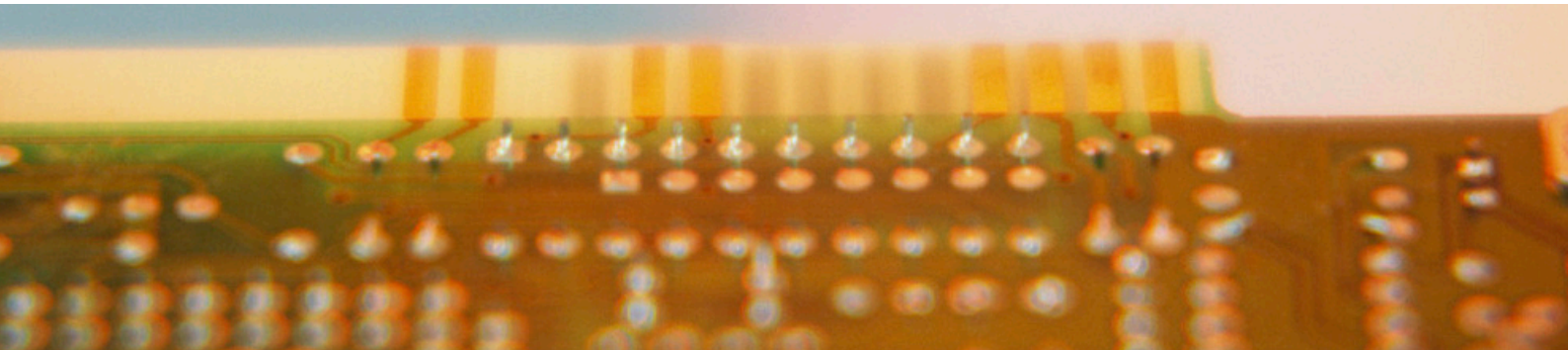
Leitores de biometria: Os leitores de biometria surgiram recentemente e tem se destacado na preferência dos usuários, apesar do custo ainda ser elevado. A grande vantagem dos leitores de biometria é que não é necessário que estejam associados com cartões, bastando para o usuário o uso de uma parte do seu corpo (item biométrico). Portanto, o usuário não necessita mais levar nenhum cartão. Esta tecnologia ainda tem preço elevado e seu uso é restrito a áreas de alta segurança, porém vem aumentando consideravelmente nos últimos anos, principalmente em aplicações como marcação de ponto eletrônico, onde se pode afirmar com certeza se o funcionário está presente ou não.

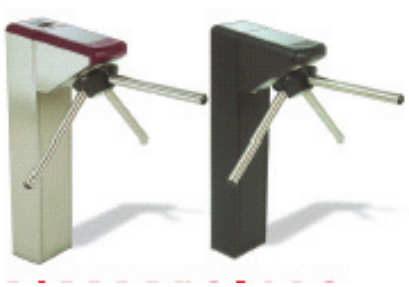
Controladores de fluxo: Os controladores de fluxo são os dispositivos que são utilizados para o controle efetivo da passagem dos usuários pelos locais. Os dispositivos controladores mais comuns são as fechaduras, catracas, torniquetes e cancelas.

Fechaduras: São os dispositivos controladores mais utilizados. Existem basicamente dois tipos de fechaduras: as eletromecânicas e as eletromagnéticas. As eletromecânicas também são chamadas de elétricas e operam com um solenóide, que uma vez energizada, destrava o fecho. Estas fechaduras emitem um alto nível de ruído durante seu destravamento, o que não indica o uso para áreas internas, onde as mais indicadas são as eletromagnéticas.

Fechadura eletromecânica

As eletromagnéticas são eletroímãs que realizam o destravamento pela interrupção da energia. Sua operação é muito mais silenciosa com uso indicado para escritórios, recepções e outras áreas internas. As fechaduras eletromagnéticas são formadas por um ímã e por uma armadura, que é uma placa metálica e são produzidas em função da sua força de fechamento, geralmente medida em kgf ou lbf (quilogramaforça ou libraforça). A instalação de fechaduras eletromagnéticas também é recomendada em portas de vidro, que não permitem a passagem de cabos por seu interior. As fechaduras eletroímãs ou eletromagnéticas são também chamadas de failsafe, pois sem energia ficam liberadas, permitindo a fuga. Isto é muito importante em caso de sinistros, como incêndio. O maior problema com a instalação de controles de acesso em portas é o fato de que, uma vez aberta, é impossível controlar o número de pessoas que passam por ela e por isso as portas controladas não são dispositivos muito seguros pois não asseguram o controle do “carona”.)





Exemplo de catracas

Catracas tipo pedestal: Também chamadas de roletas ou mini-bloqueios são os mais utilizados para o controle de grandes quantidades de pessoas a áreas comuns, como os acessos de prédios, saguões, recepções. Têm pequenas dimensões, necessitando apenas uma área de aproximadamente 80x80cm. Em um bom sistema de controle de acesso, ao se passar um cartão por um dos leitores, a catraca destrava permitindo o giro apenas no sentido em que foi solicitado o acesso. Ao se instalar catracas é necessário que se tenha o cuidado de se manter uma área livre de pelo menos 2 metros para saída em caso de emergências, como incêndio, por exemplo (rota de fuga).Também é necessário que se tenha o cuidado de permitir o acesso de deficientes físicos, por meio de catracas especiais ou de portões de deficientes.

Catraca de deficientes físicos

As catracas, quando utilizadas com cartões de proximidade ou smartcard sem contato (Mifare) permitem o uso de urnas coletoras, dispositivo instalado no interior da catraca com uma abertura na tampa superior e é voltada para a coleta dos cartões dos visitantes.

Exemplo de catracas tipo balcão ou bloqueios

Catracas tipo balcão: São versões mais reforçadas das catracas citadas no item anterior. As catracas tipo balcão ou bloqueios possuem dois pedestais, apresentando resistência mecânica muito superior. Seu uso é indicado para locais em que o número de usuários for muito grande ou onde possa haver tumultos como metrôs e estádios. Assim como para as catracas, é possível instalar coletores de cartão (urnas) nos bloqueios.Nada impede, porém, que o usuário mal intencionado pule por sobre uma catraca, uma vez que os braços não estão localizados a grande altura.

Torniquetes: São dispositivos de alta segurança, geralmente indicados para uso industrial, devido à sua aparência. Evitam o carona pois não é possível a entrada de mais de uma pessoa em seu interior. A fim de amenizar o seu desenho, alguns modelos são fabricados com braços em vidro, se tornando uma opção bem interessante do ponto de vista de aumento da segurança, apesar de ser um investimento relativamente alto.

Figura 3 - Torniquete

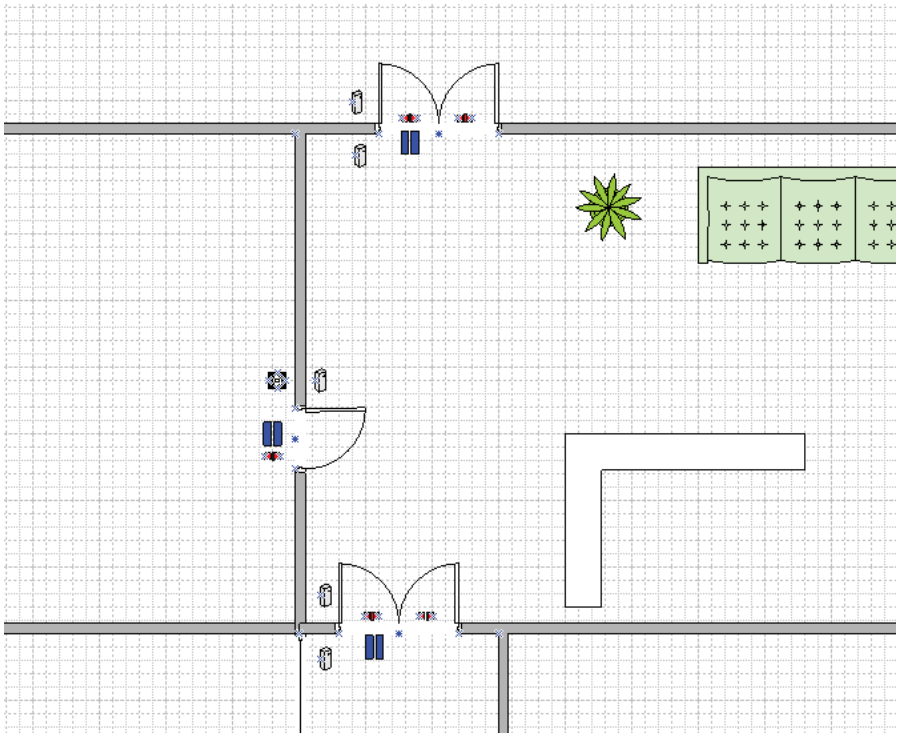
Cancelas: São controladores destinados ao acesso de veículos. As principais características de uma cancela são a velocidade de abertura e fechamento, capacidade de fluxo de veículos controlados por dia e o comprimento de sua haste. As cancelas podem ser utilizadas em solução de entrada/saída (bidirecional) ou serem utilizadas uma cancela para a entrada e uma cancela para a saída (unidirecionais). Uma cancela bidirecional deverá possuir dois leitores, um para a entrada e um para a saída. Valores típicos de capacidade de fluxo de aberturas/fechamentos são 1000, 2000, 3000 e 5000 por dia. Os valores mais comuns para os comprimentos das hastes são de 3 a 6 metros.

Exemplo de cancela

Sensores de porta: Todas as portas controladas devem indicar se estão abertas ou fechadas, caso contrário a instalação de um sistema de controle de acesso perde o sentido. O mais utilizado dispositivo de campo para a indicação do estado de portas é o sensor magnético que é composto por um par de dispositivos, sendo um deles um ímã e o outro uma ampola de material magnetizável. Ao se afastar o ímã da ampola a uma distância superior a um certo limite, esta abre um contato indicando que a porta está aberta. No caso do controle de acesso ser realizado em portas com duas folhas, as duas deverão ter sensores.

Dispositivos em conjunto

Porta controlada: Uma porta pode ser controlada com a instalação de um leitor para a entrada na área segura e um leitor ou botão de destrava para a saída. Além disso, devem ser instalados os sensores magnéticos e a fechadura. Ao se solicitar o acesso, o sistema deverá verificar se o usuário pode entrar naquele leitor naquele horário e então liberar ou não a porta. O evento deve sempre ser armazenado. A grande diferença entre a porta com leitor/botão de destrava e a porta com leitor/leitor é que a primeira não permite saber quem saiu. Tipicamente se utilizam portas com leitor/botão em salas fechadas, sem conexão a outras salas. Para portas localizadas em corredores e passagens, geralmente se utiliza o controle com dois leitores. Caso se utilize leitores de proximidade, os leitores geralmente são de curto alcance (da ordem de 7cm). A instalação de controle de acesso em portas deve sempre ser feita com critério, pois se coloca um impedimento natural às rotas de fuga. A boa prática recomenda que se instalem fechaduras tipo fail safe em todas as portas, dotadas de botões de pânico tipo “quebre o vidro” para cortar mecanicamente a alimentação das fechaduras, liberando assim o acesso. Como a porta será aberta sem o cartão, deverá ser gerado um alarme de porta forçada na central de controle.



Exemplo de planta com leitores alocados

Catraca controlada: A catraca pode ser controlada por um leitor, caso seja somente de entrada ou de saída (muito comum em restaurantes). O mais comum é a catraca ser controlada por dois leitores, um para a entrada e um para a saída. O sistema deve liberar o giro dos braços da catraca somente no sentido solicitado. Existem casos em que são instalados três leitores: para a entrada, para a saída e para a urna coletora dos cartões dos visitantes. A maioria dos sistemas de segurança permite definir que o visitante somente possa sair depositando o cartão na urna. A urna coletora apenas se aplica a sistemas com cartões sem contato: proximidade ou Mifare, já que não é possível fazer uma urna coletora para cartões que necessitem de contato. O mesmo princípio vale para o bloqueio e para o torniquete. Caso se utilizem leitores de proximidade, os leitores geralmente são de curto alcance, da ordem de 7cm.

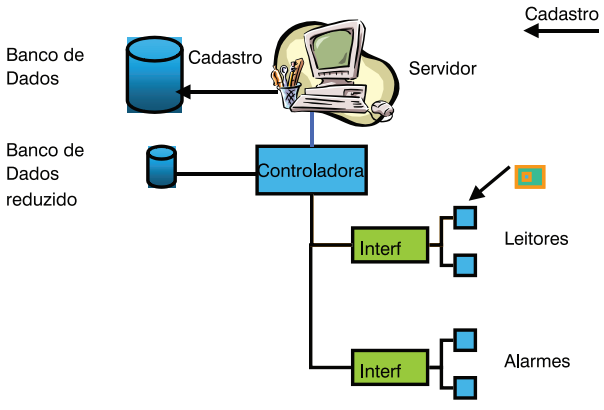
Cancela controlada: A cancela pode ser controlada por um único leitor, no caso ser utilizada uma para a entrada e outra para a saída. No caso de ser utilizada uma única cancela para a entrada e para a saída, serão instalados dois leitores, um em cada lado. Devem ser instalados dispositivos que impeçam que a cancela desça sobre o veículo. Geralmente se utilizam laços sensores ou sensores ópticos. Caso se utilizem leitores de proximidade, os leitores geralmente são de longo alcance, da ordem de 70 cm.

Rotas de fuga: Elas são determinadas de acordo com cada caso. Se forem instalados controles em portas, se deve instalar botões quebre o vidro ou outro dispositivo mecânico para a liberação das portas em caso de pânico; se forem instaladas catracas, se deve manter uma área de pelo menos dois metros de fechamento que possa ser removido ou derrubado em caso de pânico; se for instalado um torniquete, é importante manter uma área ao lado que possa ser aberta em caso de pânico. Embora seja possível instalar controle de acesso em portas corta-fogo, alguns cuidados devem ser tomados. Os melhores dispositivos para portas corta-fogo são as barras anti-pânico eletromecânicas. Do lado seguro elas possuem uma barra antipático, que basta ser pressionada. Do lado não seguro podem ser instalados leitores de acesso. Uma vez liberado o acesso, o sistema pode acionar a interface eletromecânica desta barra liberando o acesso.

Interfaces de dispositivos de campo

Os dispositivos vistos até agora precisam ser controlados por algum equipamento responsável pela interface entre o sistema e os dispositivos de campo. Este equipamento é genericamente chamado de interface de dispositivos. Cada fabricante tem sua própria arquitetura e aponta vantagens em relação às dos concorrentes. Aqui, daremos apenas o conceito que deverá ser aplicado a cada caso.

As interfaces de dispositivos podem ser equipamentos com capacidade de decisão sobre a liberação do acesso ou não. O mais importante é que estes equipamentos fazem a interface direta com os dispositivos de campo, monitorando o correto funcionamento, condição (aberto/fechado) e realizando a interface de sua operação, por comandos para abrir/fechar.



Exemplo de arquitetura de sistema de controle de acesso

Para a maioria dos fabricantes as interfaces de dispositivos se comunicam com controladoras inteligentes via rede Internet ou um canal serial.

A quantidade de dispositivos que cada interface pode controlar/monitorar depende de cada fabricante, mas tipicamente varia de um a oito. Quantidades muito maiores que oito podem ser oferecidas, mas devem ser aceitas com cautela, pois uma única interface que apresente problemas pode deixar uma área inteira não operacional.

Controladoras inteligentes

São as que caracterizam o chamado sistema de inteligência distribuída. Neste sistema, os dispositivos possuem uma autonomia que, mesmo em caso de falha do servidor, o sistema permanece operando. É o que tem se mostrado mais eficiente e tolerante às falhas. O conceito que deve ser entendido é o de que o sistema de controle de acesso não deve residir unicamente no servidor, pois caso este apresente problemas o sistema não pode ficar inoperante. As controladoras não devem controlar um número excessivo de dispositivos de campo, pois caso apresente falha, uma grande parte do sistema poderá ficar inoperante. As controladoras são dispositivos sem discos rígidos, baseadas em memória flash ou outro tipo de memória estável. O papel da controladora é o de gerenciar o sistema que está a ela conectado, poupando o servidor para funções mais nobres. Caso o sistema de controle de acesso necessite consultar o servidor, a consulta deve ser a mais breve possível e apenas em casos muito especiais, já que a controladora deve ter autonomia de decisão sobre todos os acessos. Ao se solicitar um acesso em um leitor qualquer, a consulta deverá ser feita à controladora e não ao servidor.

Servidor/ estação de trabalho/ software

As estações de trabalho serão a interface principal entre os usuários do sistema (operadores) e os dispositivos de campo. Devem ter uma interface gráfica amigável e fáceis de operar, com comandos simples, sem caminhos tortuosos para conseguir chegar no comando correto. As principais estações de trabalho são a de cadastro e a de operação. A de cadastro é a estação utilizada para o cadastro dos funcionários, emissão de novos cartões e cadastro dos visitantes. No Brasil se utiliza muito a captura das fotos dos visitantes, que devem ficar armazenadas no banco de dados do sistema com outros dados para que quando o visitante retornar os dados já estarão cadastrados. A estação de operação é a voltada para a operação diária do sistema, configuração de dispositivos de campo, geração de relatórios e outras funções administrativas. O servidor do sistema deve ser o responsável pelo aplicativo e pelo gerenciamento do acesso ao banco de dados, não devendo ser utilizado para operação a menos que não

seja possível outra solução. O sistema de controle de acesso não é só um sistema que permite a configuração de leitores, alarmes e usuários. É também um poderoso banco de dados e deve ser um sistema seguro. O uso de senhas para seu acesso e configuração é imprescindível.

Banco de dados: É o depósito de todas as informações e eventos do sistema e deve permitir um desempenho aceitável mesmo em condições de máximo uso. Os mais utilizados para sistemas de controle de acesso são o MS-SQL, o MSDE (antigo Access) e o Oracle. Outros bancos de dados podem ser utilizados, mas deve-se sempre ter em mente que o sistema deve permitir a manutenção periódica e o uso de dados proprietários deve ser evitado. Bancos de dados como o Access/MSDE não oferecem performance suficiente para aplicações de grande porte e devem ser evitados. Em aplicações de médio e grande porte deve ser dada preferência ao SQL e ao Oracle. Álbuns sistemas de controle de acesso permitem a escolha do banco de dados que vai ser utilizado.

Níveis de usuários: A maioria dos sistemas no mercado possui vários níveis de usuários. Um recepcionista somente pode fazer o cadastramento de visitantes, enquanto um usuário do tipo administrador pode fazer configurações e apagar registros.Isto evita que ocorram problemas de erros de configuração. O sistema deve permitir a definição do usuário e a associação deste usuário com um cartão. No momento da associação, o sistema deve indicar se o cartão escolhido já se encontra associado, pois esta é uma falha grave de segurança.O sistema deve permitir ainda definir claramente onde o usuário pode entrar e em quais horários isso pode acontecer.

Zonas de tempo:O sistema de controle de acesso deve permitir a criação de zonas de tempo lógicas. Cada uma pode estar associada a um dia da semana, a vários dias, a uma hora de início e a uma hora de término. Isso define completamente uma zona de tempo. Exemplos de zonas de tempo são: segunda a sexta-feira, das 8 às 18 h, domingo das 14 às 19h. O sistema também deve permitir o registro de feriados e o correto tratamento pelo sistema. O objetivo é ser possível determinar que durante um feriado todo acesso à área administrativa fica restrito, por exemplo. Para a maioria dos sistemas, algumas dezenas de zonas de tempo são mais que suficientes.

Níveis de acesso: É um termo muito comum no mercado de segurança e indica onde e quando um usuário pode fazer um acesso autorizado. Para a maioria dos sistemas de controle de acesso, o nível de acesso é realizado pela combinação das zonas de tempo com os leitores. Este tipo de arquitetura é extremamente flexível e permite um número gigantesco de combinações, mesmo com poucas zonas de tempo.

Criação de cartões: Embora não seja fundamental, é muito desejável que um único sistema possa criar a arte gráfica do cartão e também imprimi-lo, o que evita que sejam criados mais do que um único banco de dados.

Dispositivos de campo: O sistema deve permitir a configuração de todos os dispositivos de campo, tais como leitores, cancelas, catracas, portas, sensores etc. A definição permite que se ajustem parâmetros exclusivos de cada dispositivo e se determine qual o tempo de fechamento de uma porta antes de ser gerado um alarme de porta aberta. Também deve ser possível dar nomes significativos aos dispositivos, pois torna o sistema muito mais fácil de ser operado e monitorado. Um leitor que tem como nome “entrada sala diretoria” é muito mais indicativo do que apenas leitor31.

Relatórios: São provavelmente a mais importante função do sistema de controle de acesso. De nada adianta ter leitores instalados em portas e catracas se não for possível saber quem entrou, onde e quando. Os sistemas possuem vários relatórios prontos como acesso por leitor, por dia e hora, por usuário. Também é possível personalizar os relatórios de acordo com relações específicas de cada cliente.

Funções avançadas do sistema/ antidupla entrada: Algumas funções avançadas permitem que se configure o sistema de modo permitir a inibição ou a redução dos problemas causados por deficiências inerentes aos dispositivos controladores. Um bom exemplo é a chamada “antidupla entrada”. Por este recurso é possível programar o sistema de controle de acesso para negar o ingresso a uma determinada área caso não tenha havido uma saída válida antes. Deste modo, não é possível passar por um banco de catracas e dar o cartão para que outra pessoa entre, pois o sistema negará o ingresso uma vez que não houve uma saída da área. Isto também evita o “carona”.

Coação: A senha de coação pode ser utilizada em leitores com teclado. Ao se digitar a senha pode-se alterar um único dígito que indicará á central de monitoramento que há um evento de coação. A porta se abrirá, mas será gerado um alarme.

Controle de lotação: Alguns sistemas de controle de acesso permitem o controle de um número de vagas pré-estipulado, negando acesso caso o número tente ser ultrapassado. A aplicação típica é para estacionamentos, porém o mesmo princípio pode ser utilizado para refeitórios.

Elevadores: Alguns sistemas permitem o controle do acesso aos elevadores. Geralmente existem duas soluções possíveis. A primeira é a de substituir os botões de chamada de elevador por leitores que somente chamarão o elevador caso o usuário tenha permissão de acesso. Outra solução é instalar um leitor em cada elevador. O usuário passa o cartão pelo leitor que libera o acesso a todos os pavimentos a que o usuário tem direito de descer.

Integração

Os sistemas de controle de acesso tem muitos recursos, permitindo a integração com vários outros. Os principais sistemas integrados aos de controle de acesso são:

Ponto eletrônico: O sistema de controle de acesso possui as informações que o sistema de ponto eletrônico necessita, logo é natural supor que estes acabem se tornando integrados.

CFTV: O sistema de CFTV, dada sua característica de permitir que um evento seja visualizado remotamente, é uma ferramenta de suporte de grande valia para o sistema de controle de acesso. Dependendo do nível de integração, é possível definir que um determinado acesso movimente automaticamente uma câmera móvel e inicie uma gravação.

Alarmes: Os alarmes são tão importantes para os sistemas de controle de acessos que geralmente estão totalmente integrados em uma mesma plataforma. Na verdade, às vezes é difícil diferenciar o que é acesso e o que é alarme, como no caso do sensor em portas controladas.

Rodolfo Simon Halasz é graduado em engenharia elétrica pela Escola Politécnica Universidade de São Paulo e tem cursos no exterior e no Brasil; professor do curso avançado em Segurança Eletrônica da Brasiliano & Associados e FESP.

SUBTRAÇÃO DE INFORMAÇÕES EMPRESARIAIS SENSÍVEIS INDICADORES DE RISCO

Hélio Santiago Vaitsman*

Indicadores de risco empresarial

No mundo empresarial globalizado e competitivo a demanda por informações cresce a cada momento. Nessa fascinante atividade, não há lugar para curiosos e amadores. Quaisquer que sejam os meios empregados para o acesso aos conhecimentos sensíveis em empresas, em especial as concorrentes, por si só se justificam, especialmente, se alguma economia de recursos (vantagem empresarial competitiva) puder ser conseguida.

A luta pelo domínio de tecnologias situadas na fronteira do conhecimento humano é tratada como questão empresarial fundamental, principalmente a busca de informações privilegiadas (inside information), visando o conhecimento de fatos passíveis de colocar em risco as empresas concorrentes.

No mercado mundial surgem anualmente cerca de 500.000 novos produtos. Não é por outra razão que atividades voltadas para a transferência ilegal de conhecimentos, empreendidas por pessoas acobertadas pelo anonimato, pelo desconhecimento e/ou desinformação dos empresários ganham cada vez mais espaço no mundo empresarial.

Informações valiosas sobre produtos, técnicas, processos etc., por não terem sido protegidas por medidas preventivas nem terem sido objeto de avaliações de risco para a própria sobrevivência da organização, vêm sendo irremediavelmente perdidas. No Brasil, tais perdas somam R$6,5 bilhões anualmente (Fonte Jornal O Globo de 28 JAN 95).

Proteger-se deste jogo, levado a efeito pelos profissionais de informações mais atuantes, é imperativo empresarial de sobrevivência. O nível de proteção será tanto mais efetivo, quanto melhor for a avaliação dos fatores externos capazes de subjugar as barreiras de proteção (física e lógica) da empresa-alvo. Tais fatores são denominados de INDICADORES DE RISCO, os quais, a título de ilustração passamos a alinhar a seguir:

a) trocas “inocentes” de emprego por parte de altos executivos que possam favorecer o vazamento ou comprometimento (perda de segredos, em função das ações ilegais de terceiros) de informações – avaliação das possibilidades de pessoas levarem consigo importantes segredos de suas antigas empresas;

b&a
BRASILIANO&ASSOCIADOS

b) contratação intencional de empregados por parte dos concorrentes – oferecimento de vantagens profissionais, pecuniárias etc.;

c) "extravios" sem causa plausível de documentos, estudos, projetos etc., considerados sensíveis;

d) constatação da divulgação, via INTERNET, de relatórios referentes a pesquisas científicas, políticas, estratégias comerciais e outros conhecimentos empresariais sensíveis;

e) detecção de ações e artifícios, nem sempre éticos, por parte de concorrentes, visando melhorar sua competitividade no mercado.

f) ações declaradas ou veladas de empresas concorrentes desejosas de saltar etapas visando alcançar posição de destaque no mercado;

g) conhecimento, de resoluções estratégicas tomadas em ambiente fechado e em nível de diretoria, por terceiros não vinculados à empresa

h) publicações na imprensa de "furos" de reportagens sobre ações políticas e estratégias empresariais, às quais poucas pessoas tenham tido acesso;

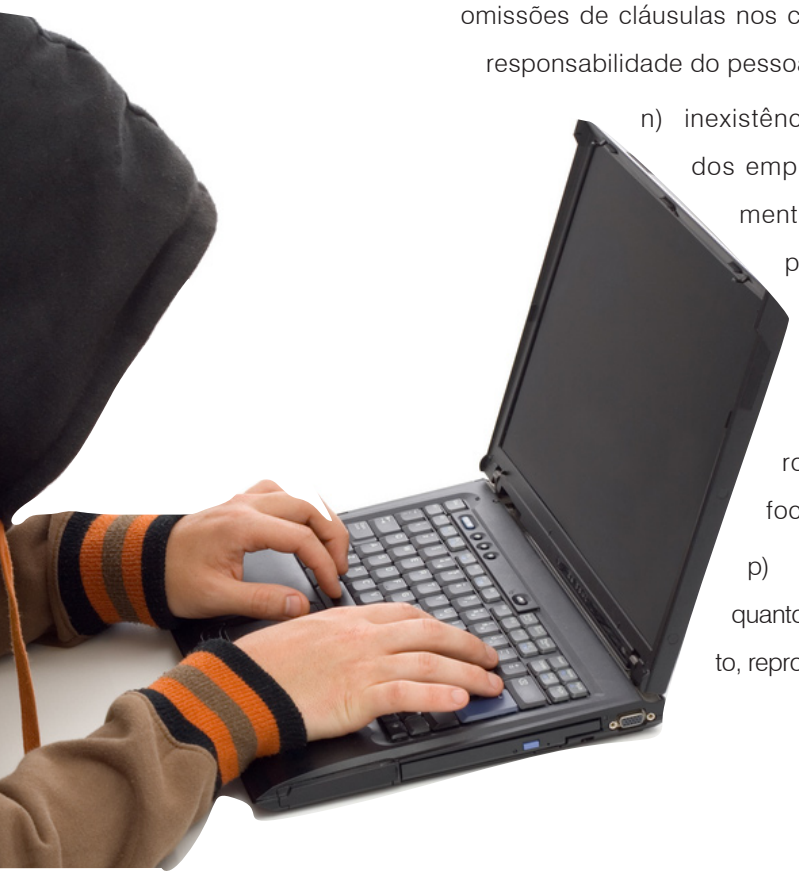
i) reincidências de ações gerenciais caracterizadas como abuso de confiança por parte de Gerentes, assessores e colaboradores próximos à alta direção da empresa

j) realização freqüente de almoços de negócios onde são comentados, sem os devidos cuidados, assuntos sensíveis, não considerando a existência de ouvidos inconfidentes capazes de captá-los impondo alto grau de risco às políticas e estratégias empresariais;

k) inexistência de instrumentos normativos internos à empresa, visando coibir ações e tentativas de obtenção de conhecimentos empresariais sensíveis sem a competente autorização de seus proprietários;

l) inexistência de políticas de proteção de conhecimentos sensíveis residentes em sistemas informatizados;

m) inexistência de cláusulas de manutenção de sigilo em contratos celebrados com parceiros omissões de cláusulas nos contratos com prestadores de serviços (terceiros), quanto à responsabilidade do pessoal envolvido em processos sensíveis;



n) inexistência de cultura interna de proteção quanto conscientização dos empregados no sentido de se absterem do trato de conhecimentos empresariais sensíveis com pessoas estranhas à Empresa, especialmente ex-empregados, que, não raro, prestam serviços a concorrentes;

o) livre acesso de terceiros a assuntos relacionados a planos, projetos e propostas comerciais, trato com parceiros, fornecedores e clientes, a menos que esses sejam o foco explícito do relacionamento;

p) intencionalidade no descumprimento de regras formais quanto ao recebimento, protocolo, classificação, manuseio, arquivamento, reprodução e destruição de documentação sensível em geral;

m) omissões nas publicações internas da Empresa, de notas relativas às suas classificações sigilosas, bem como ao acesso e à sua reprodução;

n) não inclusão de cláusulas de manutenção sigilo nos processos licitatórios;

n) acesso livre e indiscriminado aos cadastros de clientes e de fornecedores, bem como inexistência de restrições à sua divulgação para o ambiente externo à Empresa.

o) falhas constantes nos procedimentos relativos às barreiras, controles de guardas de vigilância, pessoas, pacotes, objetos, circulação de veículos, claviculários, dispositivos de prevenção de combate a incêndios (Brigadas de Incêndio), a investigação de sinistros e ocorrências irregulares.

p) falta de orientação aos empregados no sentido de restringir, ao mínimo necessário, o acesso de visitantes em áreas e instalações sensíveis da Empresa, evitando-se, tanto quanto possível sua circulação.

q) inexistência de normas relativas às comunicações objetivando impedir que assuntos sensíveis cheguem ao conhecimento de pessoas ou organizações não autorizadas, por ocasião de sua circulação em qualquer meio.

r) inexistência de normas e rotinas internas determinando ao órgão de pessoal informar ao órgão de segurança de dados, as demissões, os desligamentos, as transferências, as licenças, etc., para fins de cancelamento das respectivas senhas.

s) inexistência de procedimentos de proteção das informações sensíveis residentes nos equipamentos de informática destinados à manutenção.

t) inexistência de regras específicas de proteção estabelecidas por gerentes e proprietários dos sistemas, como por exemplo a proibição de acesso remoto (de fora da empresa) às suas bases de dados;.

u) inexistência de medidas sistêmicas com o objetivo de impedir a violação das informações sensíveis em meios magnéticos, estabelecendo procedimentos coerentes com as políticas da empresa voltadas para essa atividade.

Muitos outros indicadores de risco empresarial poderiam ser alinhavados. Cada empresa, em função da natureza de sua atividade tem seus indicadores específicos. Porém, sejam elas privadas ou públicas, estarão expostas a riscos comuns. A falta de políticas de salvaguarda dos conhecimentos sensíveis, complementadas pela inexistência de programas voltados para a criação de cultura empresarial de proteção, agravam os riscos. Deve estar bem claro que a responsabilidade pelo sucesso das políticas e pela execução dos planos é de todos, uma vez que o risco de vazamento de segredos industriais não está restrito a apenas um setor específico dentro da organização.

A determinação de indicadores de riscos em ambiente competitivo e globalizado é vital para a sobrevivência das organizações; uma vez identificados, os indicadores contribuirão para a neutralização das intenções maldosas de potenciais autores de delitos e outras apropriações indébitas. Adicionalmente, deve-se prever o emprego de recursos de auditoria, ferramenta para aferição das contra-medidas de inteligência objetivando a validação e a substituição, quando for o caso, dos indicadores de riscos previamente eleitos que se revelem inoportunos.

A determinação dos indicadores de risco precedem a adoção das medidas sistêmicas de proteção dos conhecimentos empresariais sensíveis, englobando as áreas de pessoal, documentação, comunicações, instalações, processamento eletrônico de dados, prestação de serviços e desenvolvimento de novas tecnologias, dentre outras. A área de informática, assume papel de destaque nesse contexto, tendo em vista a possibilidade futura de vir a encampar as funções das demais áreas. Nas áreas de desenvolvimento tecnológico e de prestação de serviços, ressaltamos que ambas reúnem um pouco de cada uma das áreas anteriormente descritas. Os significativos recursos e esforços aplicados devem merecer especial atenção, em face da necessidade da oferta de inovações em prol da sobrevivência da própria organização.

As medidas sistêmicas acima referidas, devem guardar coerência e compatibilidade com os indicadores de riscos determinados.

Empresas que travam contato permanente com tecnologias de ponta, que licitam, que contratam, que possuem estratégias que lhes permitam sobreviver e conquistar novos espaços, devem promover uma precisa delimitação de indicadores de riscos visando a salvaguarda dos seus conhecimentos estratégicos.

Conclusão

É inquestionável que a obtenção não autorizada de conhecimentos relativos às opções administrativas, tecnológicas, políticas e estratégias será sempre alvo do interesse de grupos e de profissionais que vivem à espreita de uma oportunidade.

Caso sua empresa não possua planejamento prevendo respostas capazes de se contrapor efetivamente aos indicadores acima alinhavados, será bom que se cuide: é provável que o seu fim esteja mais próximo do que se imagina....

HÉLIO SANTIAGO VAITSMAN

Bacharel e licenciado em Física, Analista de Sistemas, Especializado Inteligência e Informações Estratégicas, nível A e B, pela CEFARH/Presidência da República do Brasil. Exerceu as funções de assessor de Segurança e Informações na Embratel, tendo chefiado e implantado o Departamento de Sistematização das Informações Estratégicas, autor de diversos artigos em jornais e revistas relacionados com Inteligência Empresarial. Autor do Livro Inteligência Empresarial: Atacando e Defendendo. Professor Universitário em Cursos de Especialização em Gestão da inteligência Estratégica. Atualmente é Consultor de Segurança e Informação da Unidade de Segurança Empresarial da Petrobrás.