

# E-BOOK INTELIGÊNCIA EMPRESARIAL



Flavio Souza

Rio de Janeiro, agosto de 2016

## Sobre o Autor



Meu nome é Flavio Souza, sou graduado em Administração de Organizações pela Universidade Veiga de Almeida, pós-graduado em Gestão de Segurança Corporativa pela Universidade Cândido Mendes, Especialista em Inteligência de Segurança pela Subsecretaria de Inteligência de Segurança Pública do Estado do Rio de Janeiro, Chief Executive Officer (CEO) na FDSouza Consultoria em Segurança Patrimonial e possuo mais de dezesseis anos de experiência no ramo de segurança patrimonial.

Meu objetivo aqui é te ajudar no seu desenvolvimento profissional, compartilhando conhecimento e informações preciosas que com certeza vai te ajudar muito no desempenho de suas atividades profissionais.

Um grande abraço e sucesso!

## Sumário

INTRODUÇÃO .....	3
INTELIGÊNCIA ORGANIZACIONAL E A VANTAGEM COMPETITIVA .....	3
INVESTIGAÇÃO EMPRESARIAL .....	5
SISTEMA DE INTELIGÊNCIA COMPETITIVA (SIC) .....	6
INTELIGÊNCIA E CONTRAINTELIGÊNCIA.....	8
Inteligência.....	9
Contra Inteligência .....	11
CONCLUSÃO .....	15

## INTRODUÇÃO

Para poder compreender a importância do significado de Inteligência e sua utilização no mundo empresarial, é preciso falar um pouco da história da Inteligência no Brasil e no Mundo.

O primeiro serviço de inteligência organizado que se teve notícia foi da Inglaterra quando Sir Francis Walsingham, Ministro do Exterior da Rainha Elizabeth I, o criou, ainda na Idade Média. Somente na Idade Contemporânea este adquiriu uma forma organizada e aperfeiçoada, podendo assim ser considerada, como instituição com estrutura própria.

A Atividade de inteligência no Brasil teve início em 1927 no governo de Washington Luís com a criação do Conselho de Defesa Nacional (CDN). No governo de Getúlio Vargas o CDN foi implementado, alterando sua denominação para Conselho Superior de Segurança Nacional (CSSN).

Durante o Estado Novo, foram criados o Departamento Federal de Segurança Pública (DFSP), origem da Polícia Federal (PF) de hoje; Delegacia da Ordem Política e Social (DOPS), que objetivava a correção de atitudes da sociedade, segundo parâmetros da época.

No governo de Eurico Gaspar Dutra, em 1946, foi criado o Serviço Federal de Informações e Contrainformações (SFICI).

Em junho de 1964, foi criado o Serviço Nacional de Informações (SNI). Com sua extinção em 1990 pelo então Presidente da República Fernando Collor, foi criado a Secretaria de Assuntos Estratégicos (SAE) e em 1995 nasce a Agência Brasileira de Inteligência (ABIN).

## INTELIGÊNCIA ORGANIZACIONAL E A VANTAGEM COMPETITIVA

Hoje, no Brasil, o serviço de inteligência ainda é muito pouco utilizado, talvez porque os empresários temam sua utilização pensando nos anos pós Revolução de 1964, onde o objetivo deste serviço era levantar pessoas ou grupo de pessoas envolvidas em ações contra os princípios democráticos e o Governo Federal.



É evidente que a finalidade é outra e o grande objetivo é a manutenção de uma vantagem competitiva garantindo sua sustentabilidade no mundo globalizado. Os empresários não podem mais se preocupar tão somente com os clientes é preciso estar atento a seus

concorrentes.

“Devido à competitividade dos mercados, já não basta compreender os clientes. As empresas precisam começar a prestar atenção a seus concorrentes. Empresas bem sucedidas projetam e operam sistemas para obter informações contínuas sobre seus concorrentes.” PHILIP KOTLER

A globalização tem forçado as organizações a se preocuparem com a competitividade e com a colocação no mercado de produtos com uma melhor qualidade a preços menores. Para isso há necessidade de constante vigilância quanto às mudanças de mercado acompanhando as tendências do seu ambiente externo e interno.

Para que o sucesso nessa atividade seja conquistado, é necessário que as organizações tenham pelo menos um setor mínimo que seja de Inteligência, visando o acompanhamento dessas tendências por parte do Gestor, permitindo uma antecipação aos fatos e o auxiliando na sua tomada de decisão.

Desde a Segunda Grande Guerra sabemos que cerca de 70% das informações utilizadas para tomada de uma decisão estão disponíveis ostensivamente nos meios de comunicações. Hoje, esse conceito não mudou muito, pelo contrário, com a globalização e a tecnologia da informação, as informações estão disponíveis a qualquer pessoa que se disponha a pesquisar como, por exemplo, na Internet.

Para isso é conveniente que nesse setor haja uma equipe de coleta de dados, não esquecendo que em muitas das vezes as informações estão disponíveis dentro da própria organização. A necessidade da troca de informações interna é de suma importância e nem sempre é levada a sério no meio empresarial, o que torna a organização vulnerável, perdendo sua competitividade, com gastos desnecessários para obtenção das informações.

O restante das informações serão obtidas por meio da busca, pois os dados não estão disponíveis, fazendo com que a organização tenha que buscá-los no ambiente externo. Aqui precisamos de uma segunda equipe, que denominamos de equipe de busca, que visa coletar o dado negado, ou seja, a informação que não está disponível nos meios ostensivos.

## INVESTIGAÇÃO EMPRESARIAL



É importante lembrar que tanto na coleta, como na busca, o empresário não deve esquecer que a ética terá que nortear suas ações. A essas equipes atribui-se a responsabilidade da Investigação Empresarial que, normalmente não faz parte do seu escopo corporativo, fazendo com que as organizações terceirizem o serviço. É aqui o momento de maior atenção por parte de quem contrata o serviço de investigação, para não correr o risco de que as informações sejam conseguidas de forma antiética.

“É importante lembrar que a atividade de Inteligência é uma atividade especializada permanente executada com o objetivo de produzir conhecimento de interesse do usuário de qualquer nível, e proteger conhecimentos sensíveis, instalações e pessoal da organização contra ações patrocinadas pelos serviços de Inteligência dos concorrentes. ”



- Antecipar-se aos concorrentes e acompanhamento das mudanças do ambiente político Nacional e Internacional, dentre outras.

*“Inteligência Competitiva não é coletada de dados, e não é pesquisa de mercado. A Inteligência Competitiva diz respeito ao risco e não à informação. A lição: demarcar ou morrer!” BE GILAD*

Julgamos que, para atender a esse propósito, o SIC deva ser constituído da seguinte forma:

- **Área de Investigação:** composta por equipe de coleta e busca de informações. Para desencadear essa operação os investigadores necessitam de um planejamento, visando conduzir seus trabalhos com objetividade, pois caso contrário, o imprevisto tomará conta das ações o que sem dúvida nos levará a gastar tempo e dinheiro. Sabemos que improvisar faz parte dos atributos do investigador, mas se tomar isso como norma, fatalmente o resultado não será satisfatório e não atingirá os objetivos propostos;
- **Área de Análise:** composta por pessoas altamente treinadas para receber e analisar as informações atrelando esses dados ao negócio da organização. Aqui não só os dados coletados, mas principalmente as fontes, serão avaliadas para se ter a certeza quanto sua idoneidade. Essa equipe é a mais importante do sistema, pois é baseado nela que o Gestor terá suporte para tomar sua decisão;
- **Área de Disseminação:** é a responsável pela divulgação da informação analisada e processada. A informação só terá importância se sua divulgação for empregada dentro do princípio da oportunidade, ou seja, a informação tem prazo de validade, podemos comparar a um jornal, pois, jornal velho não se encontra nas bancas.

Os trabalhos aqui desenvolvidos produzirão uma gama de informações que serão armazenados em um Banco de Dados de Inteligência e que para sua segurança, deve ter pessoas selecionadas por características de acordo com a atividade desenvolvida dentro do SIC.



Cabe ressaltar que em todos os níveis organizacionais, há a necessidade de uma conscientização da importância do SIC e sua direção deverá ficar sob a responsabilidade de alguém que tenha carisma e respeito dentro da organização, para que suas informações sejam recebidas com credibilidade e aceitação. Seria aconselhável que o SIC fique ligado diretamente ao CEO ou a Presidência da organização, para que tenha ascensão sobre os demais departamentos. Essa aproximação não necessariamente é física, pois com o apoio da Tecnologia da Informação, as informações fluirão com segurança e numa velocidade compatível, princípio da oportunidade, com a necessidade de que o Gestor precise para auxiliar na sua tomada de decisão.

Vemos com preocupação o desinteresse do setor de Segurança pela Inteligência Competitiva que, sem dúvida nenhuma, tem prejudicado ascensão dos profissionais deste setor a nível de Gestão de Segurança Corporativa Empresarial. Certamente que ainda há tempo para redirecionar os objetivos agregando o SIC ao escopo dos trabalhos dos gestores de segurança. Para isso, é necessário empenho de todos do setor, pois não existe Inteligência sem que o homem esteja à frente para coletar, buscar, analisar, processar e disseminar a informação. Como na sua própria definição a Inteligência nada mais é que produzir e proteger conhecimentos, instalações e pessoal da organização o que significa de uma forma muito precisa os elementos básicos da SEGURANÇA.

## INTELIGÊNCIA E CONTRAINTELIGÊNCIA



A inteligência empresarial é sem dúvida uma excelente ferramenta para que as organizações possam garantir sua sustentabilidade mercadológica, no Mundo Globalizado e para isso essa atividade conta com o Ramo da Inteligência e Contrainteligência.

## Inteligência

O Ramo da Inteligência abrange as ações especializadas, permanentemente executadas, com o objetivo de produzir conhecimento de interesse da Alta Gestão e de qualquer nível hierárquico sobre as mudanças do Negócio da Organização e dos Concorrentes, quando definido uma hipótese de mudança no cenário e/ou nas condições externas.

O objetivo dessa atividade é à busca do conhecimento que na realidade é o resultado do processamento de um dado (representação de um fato ocorrido, seja como um documento, fotografia, arquivo digital e outros, que ainda não tenham sido submetidos à metodologia para a produção do conhecimento), empregando para isso uma metodologia para a produção do conhecimento, e visando a avaliação ou conclusão sobre determinado fato ou situação. É na verdade o produto final do qual o usuário final do sistema poderá se basear para auxiliar em sua tomada de decisão.

A natureza das fontes de inteligência para a busca do conhecimento abrange as seguintes fontes:

- Pessoas;
- Documentos;
- Organizações ou equipamentos de onde se origina o dado de inteligência.

Quanto à sua natureza a fonte pode ser:

- Fonte Humana
- Fonte de Sinais
- Fonte de Imagem
- Fontes de inteligência Humanas – São as que obtêm dados a partir das atividades desenvolvidas por pessoas.
- Fontes de Inteligência de Sinais – São as que obtêm dados a partir da interceptação e monitoração das emissões, no espectro eletromagnético, dos sinais de comunicações e não comunicações.

- Fontes de Inteligência de Imagem – São as que obtêm dados a partir de imagem obtida por equipamento fotográfico, radares e sensores, montados em plataforma aéreas, espaciais ou terrestres.

Para realizar a integração das fontes existe a necessidade de se ter um departamento responsável por essa integração. O seu representante legal será o responsável pela manutenção do ciclo de inteligência, definindo sua atividade e coordenando suas ações.

Para darmos sequência na produção dos conhecimentos levantados pelos dois Ramos da Atividade de Inteligência, temos que observar e entender o Ciclo de Inteligência que consiste de três fases: Orientação, Produção e Utilização.

**Orientação** – A primeira fase deste ciclo, é de responsabilidade do Diretor ou Chefe do Departamento de Inteligência da Organização, devendo este, definir as ações a serem realizadas pelas equipes em suas atividades de inteligência (coleta e busca). É de suma importância que essas atividades estejam sincronizadas com a política da organização.

**Produção** – A segunda fase, os conhecimentos são produzidos de forma a atender as necessidades de Inteligência da Organização, definido pela Alta Gestão. Para essa fase usamos a seguinte metodologia (para produzir o conhecimento): Planejamento, Reuniões de coordenação, Análise, Interpretação e Disseminação.

Todas as fases são importantes, porém, é na análise que o Gestor se baseará para nortear a estratégia da organização, tomará suas decisões e em consequência, desenvolverá todas as suas atividades, sejam elas Operacionais, como principalmente as Estratégicas.

**Utilização** – A terceira e última fase, é a fase onde o conhecimento produzido será difundido ao usuário que a solicitou ou que necessite dele para sua tomada de decisão. Nesta fase temos que atender os seguintes quesitos:

- Atender as necessidades específicas dos usuários (de quem solicitou a coleta ou a busca da informação);

- Relatar os assuntos em relatórios de fácil compreensão pelo usuário final;
- Lembrar que o **princípio da oportunidade** é de fundamental importância, para o Gestor tomar a sua decisão e se antecipar ao concorrente, bem como às mudanças do mercado;
- Manter o ciclo em constante funcionamento fazendo sua retroalimentação.

Vimos até aqui a importância de produzir o conhecimento e a partir deste momento, a organização precisa proteger tudo que se conseguiu com o Ramo da Inteligência Empresarial.

### Contra Inteligência

O setor responsável por esta manutenção dentro do departamento de Inteligência da Organização é o Ramo da Contraineligência. Este é o responsável pela segurança do Sistema de Informações da Organização e desenvolve sua atividade com ações especializadas, permanentemente executadas, com o objetivo de proteger conhecimentos sensíveis, instalações e pessoal da Organização, contra ações desenvolvidas por serviços de Inteligência da Concorrência.

Para cumprir sua finalidade que é proteger conhecimentos produzidos pelo serviço de inteligência da organização, pessoal e instalações da organização, precisamos conhecer alguns conceitos básicos. Pela importância que devemos dar na proteção dos conhecimentos produzidos pelo órgão de inteligência da organização, cito como exemplo, a ser seguido por qualquer organização, o conceito de **Segredo de Estado**:

- São dados ou conhecimentos que, por disposição legal por seu valor estratégico para a garantia das instituições fundamentais do Estado, devidamente reconhecidos por autoridades competentes, devam ficar vedados a toda pessoa que deles não seja legítima depositária. Acredito que se usarmos esse conceito dentro da organização, respeitando é claro,

a política adotada pela organização, nossos conhecimentos estarão protegidos.

Segue abaixo alguns conceitos para entendermos todo significado da definição do Ramo Inteligência Empresarial.

- **Acesso:** ato de uma pessoa ter condição de obter conhecimento e/ou dados e fazer uso desses.
- **Credencial de Segurança:** é o certificado (crachá, senha, código de segurança ou cartão de acesso) concedido por pessoa competente, que habilita uma pessoa a ter acesso, até determinado grau de sigilo, a conhecimentos e/ou dados que devam ser protegidos pela organização.
- **Necessidade de Conhecer:** é a condição indispensável, inerente ao exercício funcional, para que uma pessoa, com credencial de segurança adequada, tenha acesso a conhecimentos e/ou dados classificados com grau de sigilo igual ou inferior ao da sua credencial (crachá).
- **Compartimentação:** é o resultado eficaz de todas as medidas de salvaguarda que visam a restringir o acesso à necessidade de conhecer. Nem todos do departamento, mesmo o de Inteligência, deverá tomar conhecimento de todos os assuntos. Isso é uma prerrogativa apenas do chefe do Departamento, se não for a melhor, é uma das melhores medidas de segurança das informações estratégicas ou conhecimento que mereça sigilo.
- **Comprometimento:** é a perda de segurança resultante de acesso, por pessoa não autorizada.
- **Vazamento:** é a divulgação, não autorizada, de conhecimento ou dado sensível. Neste caso a informação saiu de dentro da organização sem o seu consentimento, talvez por falta de controle (segurança) ou até mesmo por uma seleção mal realizada.

Esses conceitos são simples e se adotados corretamente a organização estará salvaguardando o seu bem maior que é sua estratégia empresarial, garantindo sua competitividade e sustentabilidade.

O Ramo da Contrainteligência ainda poderá ajudar nessas ações com a utilização da segurança ativa e orgânica.

No Ramo da Contrainteligência contamos com os seguintes segmentos:

- Segurança Ativa;
- Segurança Orgânica.

A Segurança Ativa é o conjunto de medidas destinadas a detectar, identificar, avaliar e neutralizar as ações dos serviços de inteligência da concorrência.

Para a atividade empresarial a Segurança Ativa é composta por:

- Contrapropaganda;
- Desinformação.

A Contrapropaganda é a atividade que se pré-dispõe a anular os efeitos da propaganda do concorrente sobre o público interno e externo, bem como nos segmentos sociais de seu interesse.

Já a Desinformação é a atividade que visa de forma intencional, ocultar, ludibriar ou induzir a erro de apreciação o serviço de inteligência da concorrência.

A Segurança Orgânica é o conjunto de medidas passivas destinadas a prevenir e a barrar as ações do serviço de inteligência do concorrente.

A composição da segurança orgânica abrange as seguintes atividades:

- Segurança Pessoal;
- Segurança da Documentação e do Material;
- Segurança das Comunicações;
- Segurança das Áreas e das Instalações e;
- Segurança da Informática.

Veremos a seguir seus principais objetivos:

A Segurança Pessoal visa – diminuir a possibilidade de admissão de pessoas comprometidas com interesses contrários à organização, e realizar uma campanha de endomarketing para estabelecer padrões educativos. Esses trabalhos deverão ser em conjunto com o RH.

Seus objetivos são:

- Prevenir e impedir ações de infiltração pela concorrência;
- Orientar o recrutamento feito pelo RH;
- Prevenir comportamentos inadequados e;
- Estabelecer padrões para campanha de endomarketing realizada pelo RH.

É importante ressaltar que, para se evitar qualquer tipo de fuga de informações pelo público interno, sejam observados os seguintes princípios:

- 1) A Necessidade de conhecer está ligada à função desempenhada;
- 2) O acesso a documentos sensíveis só é permitido a pessoas credenciadas e;
- 3) O conhecimento de assuntos sensíveis depende da função, não, do grau hierárquico.

A Segurança da documentação e do material visa evitar o comprometimento de seu uso pela concorrência, tendo como objetivos:

- Proteger conhecimento e/ou dados sensíveis da organização durante a produção, expedição, recepção, manuseio, arquivamento e destruição.

Um exemplo dessas medidas é a prática da “mesa limpa” ao término do expediente, o que em muitas vezes, é feito sem saber que se está adotando uma medida de Contra- Inteligência.

A Segurança das Comunicações têm por objetivos a proteção dos conhecimentos durante a sua transmissão e recepção. É importante que nesta operação haja uma integração muito forte com a área de Tecnologia da Informação (TI), pois só assim poderemos impedir ou dificultar a interceptação

por parte da concorrência, na análise e tráfego dos nossos conhecimentos e ações estratégicas. Uma das medidas adotadas nessa operação é a criptografia dos assuntos de interesse da organização.

É importante lembrar que assuntos relevantes à organização não sejam tratados por telefone ou rádio, pois apesar de não parecer, a interceptação e monitoração das comunicações é uma atividade de fácil execução.

*“... celular eu só uso para marcar encontros que eu não vou comparecer”. Itamar Franco, então Presidente da República.*

Segurança das Áreas e Instalações têm por objetivos proteger os locais onde são elaborados, tratados, manuseados ou guardados os conhecimentos sensíveis ou estratégicos da organização, visando a sua não utilização por parte da concorrência, ou impedindo o seu acesso por pessoas não autorizadas.

A Segurança da Informática visa prevenir a perda, mesmo que acidental, de conhecimentos e assuntos estratégicos da organização por falha humana ou do equipamento.

É aqui o local onde temos que investir em tecnologia para permitir o sigilo das atividades de processamento de dados e a integridade dos sistemas e programas de informática.

## CONCLUSÃO

Podemos concluir que se os assuntos abordados acima forem cuidadosamente observados pelos tomadores de decisão das empresas, suas organizações estarão protegidas contra eventuais investidas da concorrência, lembrando sempre que a vigilância deverá ser continua e sistemática, pois como disse Alexandre “O Grande”:

*“É perdoável ser derrotado, mas nunca, ser surpreendido”. Frederico II, o “Grande” Rei da Prússia.*



O serviço de Inteligência é de suma importância para as organizações sendo determinante para o sucesso de suas atividades e resultados, bem como para o setor de Segurança Empresarial.

**Conheça as ferramentas  
para Gestão de Segurança  
Empresarial que eu utilizo e  
recomendo.**



**Quero Conhecer Agora!**

**Compartilhe esse e-book com  
outras pessoas e ajude-as no  
desenvolvimento de suas  
carreiras profissionais.**

