# ALINHANDO A SEGURANÇA ELETRÔNICA COM O NEGÓCIO[1]

## A importância de uma abordagem processual para a obtenção de altos níveis de segurança eletrônica nos sistemas industriais

*Sérgio Cordeiro*[2]
*Sylvio Leal Barbosa*[3]

**Resumo**
Alcançar um nível adequado de segurança eletrônica para os sistemas industriais é ao mesmo tempo uma tarefa indispensável e um objetivo que só pode ser alcançado no longo prazo. Sem a abordagem gerencial correta, é grande a probabilidade de o programa de segurança encontrar dificuldades de financiamento e de justificar os resultados obtidos perante a alta direção da empresa. Propomos uma abordagem alinhada com os objetivos e as práticas de negócio da empresa como solução para esse problema. Será apresentado um resumo dos principais obstáculos encontrados pelas empresas ao implantar a segurança eletrônica em seus sistemas industriais, baseado na bibliografia especializada e na experiência dos autores. Em seguida, serão expostas as diversas abordagens possíveis e avaliados os méritos de cada uma. Finalmente, conclui-se a favor da superioridade da metodologia proposta frente às demais. Uma relação das vantagens e desvantagens relativas das diversas abordagens, que facilita a justificativa, perante a alta direção, do porquê da sua adoção, é outro resultado prático do levantamento realizado.
**Palavras-chave**: Segurança eletrônica; Programa de segurança; Análise de riscos

## ALIGNING CYBERSECURITY AND BUSINESS

**Abstract**
Achieving sound cybersecurity levels in industrial systems is at the same time an inescapable task and a goal that can only be reached in the long term. Without the right managerial approach, there is a great likelihood that the Security Program faces difficulties in justifying financial support and in exposing its results to the company's high level management. As a solution to this problem we propose an approach that is aligned with the company business objectives and practices. It will be presented a summary of the main problems found by organizations in the implementation of Cybersecurity Programs for their industrial systems, based on the specialized literature and on the authors' experience. Some possible approaches will be exposed and the merits of each one will be evaluated. Finally, we conclude in favor of the aforementioned methodology. Another practical outcome of the work is a list of the relative strengths and weaknesses of the various approaches, in order to make it easier to justify its adoption before the company's managers.
**Key words**: Cybersecurity; Security program; Risk assesment.

[1] *Contribuição técnica ao 12° Seminário de Automação de Processos, 1 a 3 de outubro de 2008, Vitória, ES*
[2] *Engenheiro e Analista de Sistemas – IHM Engenharia e Sistemas de Automação*
[3] *Engenheiro*

## 1 INTRODUÇÃO

O interesse em aumentar os níveis de segurança da informação nos sistemas industriais é bastante recente, podendo seu surgimento ser datado por volta de 2002, como uma conseqüência de a integração dos sistemas de chão-de-fábrica com os sistemas corporativos ter passado a ser uma realidade. A visão inicial resumia-se à defesa das redes de automação e controle contra ameaças provenientes das redes corporativas (segurança do perímetro). Além dessa visão limitada do problema, faltava conhecimento teórico e prático a respeito dos vários aspectos técnicos e organizacionais que tornam os sistemas industriais diferentes dos demais sistemas de informação. Essas dificuldades frustraram algumas tentativas pioneiras de implementação de programas de segurança.

Ao longo dos anos, estudos específicos e experiências com casos reais contribuíram para ampliar-se a visão do problema, hoje entendido de forma abrangente como garantia da disponibilidade, da integridade e da confidencialidade dos dados. Além disso, consolidou-se o conhecimento e emergiram conjuntos de recomendações e boas práticas, conjuntos esses em vias de tornar-se normas internacionais. Com isso, atualmente, várias empresas no Brasil e no exterior já estão dedicando recursos à organização e à execução de seus programas de segurança.

Em artigo escrito há dois anos,[(1)] citei as diferenças entre os sistemas industriais e os de informação, do ponto de vista da segurança, e enumerei as principais dificuldades enfrentadas para se conseguir levar os sistemas do primeiro tipo a um nível adequado de segurança: a complexidade das tecnologias e dos aspectos humanos envolvidos, a carência de normas e de fornecedores de serviços específicos. Ressaltei ainda que os dois primeiros fatores seriam estruturais, não existindo possibilidade de desaparecerem ao longo do tempo, e que os dois últimos seriam fatores conjunturais, cuja importância teria duração apenas momentânea.

Como se previa, as dificuldades apontadas como conjunturais têm perdido força com o tempo. As do tipo estrutural mantém-se obviamente ainda presentes, mas não constituem empecilho sério para o êxito dos programas de segurança, embora esteja fora de dúvida que para algumas atividades as ferramentas ainda precisem sofrer muitos aperfeiçoamentos. Pode-se então perguntar o que é que atrapalha o sucesso dos programas de segurança que começam a ser implantados nas organizações? Para tentar responder a essa pergunta, introduz-se em seguida a temática das abordagens possíveis para implantação da segurança.

## 2 ABORDAGENS POSSÍVEIS

Identificamos basicamente quatro tipos de abordagens possíveis com relação à segurança da informação nos ambientes industriais.

*1)* Abordagem *ad-hoc*
2) Abordagem pontual
3) Abordagem tecnicista
4) Abordagem processual

A abordagem *ad-hoc* é fundamentalmente reativa. A segurança não é encarada de forma sistêmica. O departamento responsável pelos sistemas, normalmente o de manutenção, é notificado dos problemas pelos usuários finais e a partir daí se mobiliza para saná-los. A atuação pode ser mais ou menos profunda, envolvendo da instalação de *patches* até a reprogramação dos aplicativos, mas resume-se a resolver o problema específico apontado naquele momento. Com isso, é impossível

abandonar a postura reativa e passar a uma preventiva. O nível de segurança global alcançado nunca será razoável. Além disso, dificilmente as soluções adotadas estarão de acordo com padrões da indústria.

A abordagem pontual consiste em atacar os problemas relacionados à segurança sem um estudo preliminar abrangente da literatura especializada e das peculiaridades e necessidades específicas da organização. Uma abordagem pontual tenta ser preventiva, em lugar de meramente reativa, e deixa espaço para o aprofundamento técnico da equipe responsável pela segurança, mas geralmente enfatiza demasiadamente determinados pontos e negligencia outros. Por exemplo, investe-se na segurança de um sistema vital para a continuidade do processo produtivo e descura-se da segurança de um sistema de apoio a ele interligado, esquecendo-se o fato de que o comprometimento deste último pode levar ao comprometimento do primeiro. Outro exemplo são os programas que se preocupam exclusivamente com a tecnologia e descuidam dos fatores ligados ao pessoal (treinamento, imputabilidade etc.), sendo que as pesquisas mostram que a maior parte dos incidentes registrados na realidade têm causas humanas. Assim, é raro que esse tipo de abordagem leve a um nível de segurança adequado.

A abordagem tecnicista é superior às duas anteriores. Consiste em pesquisar as melhores práticas na literatura especializada e aplicá-las nos sistemas industriais. Como hoje estão disponíveis listas de práticas bastante abrangentes e detalhadas, esta abordagem normalmente resulta em um nível de segurança elevado. No entanto, esse tipo também apresenta problemas. Uma abordagem tecnicista conduz à adoção das recomendações mais atualizadas quanto à segurança das redes insutriais, sem estabelecer na empresa um processo para garantir a manutenção e a melhoria contínua. Não existe o cuidado de definir métricas, já que não se enxerga a segurança como um processo. Sem métricas, não é fácil explicar de onde se veio e para onde se vai, o que dificulta justificar investimentos; assim, deve-se lutar sempre contra a crônica escassez de recursos. Pode-se afirmar que esse tipo de abordagem traz belos resultados nos primeiros anos, mas torna difícil o avanço a partir daí, devido principalmente aos altos custos envolvidos e a falta de informação a respeito dos benefícios obtidos.

A Tabela 1 traz um sumário das características das abordagens acima.

**Tabela 1:** Sumário das características das abordagens citadas

| | *Ad hoc* | Pontual | Tecnicista |
|---|---|---|---|
| Nível de segurança local | Baixo | Alto | Alto |
| Nível de segurança global | Baixo | Baixo | Alto |
| Custo | Alto | Médio | Alto |
| Padronização | Baixa | Média | Alta |

## 3 A ABORDAGEM PROCESSUAL

As primeiras metodologias voltadas para a criação de programas de segurança em sistemas industriais eram bastante simples e diretas. Um bom exemplo é a referência (2), que reflete a preocupação do governo britânico em proteger os sistemas que cuidam da infraestrutura vital do país. Essas metodologias desempenharam um papel importante devido ao seu pioneirismo, mas a abordagem padece dos problemas citados acima. Trabalhos mais recentes, como a norma ISA-99,[3-5] adotam o que chamamos aqui de abordagem processual.

Nessa abordagem, a segurança é vista como um processo cíclico, composto pelas quatro fases clássicas PDCA: planejamento, execução, medição e melhoria do processo. A fase de execução é, evidentemente, a mais importante e a que consome maiores recursos, mas o roteiro oferecido pela metodologia contempla um estágio preliminar, de planejamento, em que as necessidades e dificuldades específicas de cada planta devem ser levantadas e analisadas; exige que todo o trabalho seja documentado de maneira padronizada e que o resultado das intervenções feitas seja devidamente avaliado, não em termos estritamente técnicos, mas de forma significativa para o negócio da empresa, até chegando-se a valores monetários, quando possível; e, finalmente, contempla os procedimentos a seguir para aperfeiçoar-se o próprio programa de segurança, de maneira a obter-se melhores resultados no próximo ciclo.

A motivação para a adoção desse tipo de abordagem é a consciência de que a segurança da informação em ambientes industriais é um tema muito complexo e que os resultados devem ser esperados e avaliados no longo prazo. Não basta aplicarem-se as melhores práticas registradas na literatura especializada. É preciso adaptar as soluções para ajustarem-se às características, às prioridades e às possibilidades orçamentárias de cada planta. Os resultados obtidos devem ser mensurados e divulgados adequadamente, de modo a fortalecer politicamente a equipe e eliminar as dificuldades de financiamento que normalmente afligem os programas de segurança.

A tendência atual é inclusive considerar a existência não de apenas um, mas de vários processos relacionados à segurança, funcionando de maneira relativamente independente.[6] Por exemplo: gerenciamento de riscos, resposta a incidentes, gerenciamento de mudanças, garantia de desempenho, etc. Com isso, evita-se usar uma métrica única para avaliar o nível de segurança dos sistemas. Essa tendência já é uma realidade nas metodologias voltadas para a segurança da informação em ambientes de TI e deve aparecer em breve nas próximas edições das metodologias voltadas para os ambientes industrais.

**Quadro 1:** Sumário das características da abordagem processual

| | *Processual* |
|---|---|
| Nível de segurança local | Alto |
| Nível de segurança global | Alto |
| Custo | Médio |
| Padronização | Alta |

## 4 MÉTRICAS SIGNIFICATIVAS

Definir métricas é uma tarefa bastante difícil. As organizações estão apenas começando a adquirir prática na definição de indicadores de desempenho relacionados com processos mais conhecidos, como o processo produtivo, a manutenção dos equipamentos e a gestão do pessoal. Escolher indicadores para medir o sucesso de um programa de segurança é muito mais complicado, em vista da limitada experiência dos gerentes nesse assunto. No entanto, sem métricas definidas, todo o processo perde o sentido e a abordagem deixa de produzir os frutos desejados.

Infelizmente, nenhuma das normas existentes sugere indicadores para avaliação de programas de segurança em sistemas industriais. Quem desejar elaborar

procedimentos de medição precisará consultar bibliografia voltada para a segurança de sistemas de informação tradicionais e a partir daí montar uma lista de indicadores inicial, que poderá ir sendo refinada com o tempo.
Em primeiro lugar, os indicadores escolhidos não podem ser muito numerosos; em segundo lugar, devem ser significativos; além disso, o processo para seu cálculo deve ser simples. Os indicadores devem ser adequados à realidade de cada planta, mas ao mesmo tempo alguma padronização é necessária, para que a situação de cada sistema possa ser confrontada com a de outros similares na mesma ou em outras organizações. Não se deve descurar da necessidade de se exprimir as métricas, sempre que possível, em unidades monetárias, de maneira a facilitar a interpretação dos resultados por parte de outros setores da organização.

## 5 CONCLUSÕES E RECOMENDAÇÕES

A adoção de uma abordagem processual para o tratamento do problema da segurança da informação nos sistemas industriais traz grandes vantagens com relação a outras abordagens mais ingênuas. As principais são a possibilidade de se obter altos níveis de segurança, tanto local quanto globalmente, através da implementação de soluções padronizadas e com um custo justificável no longo prazo.
Atualmente, estão disponíveis normas específicas voltadas para a segurança de sistemas industriais e que empregam uma abordagem processual. Essas normas encontram-se em estágio relativamente maduro no que concerne às fases de planejamento e execução, mas a importante fase de avaliação do programa, que envolve a definição de métricas adequadas, ainda precisa evoluir muito. Como não é possível esperar pela publicação de revisões dessas normas que tragam uma solução para esse problema, é preciso consultar a literatura especializada voltada para a segurança de sistemas de informação tradicionais e usar de discernimento e do conhecimento das necessidades da organização para obter-se um conjunto de indicadores de desempenho que seja útil para os primeiros anos do programa de segurança.

## REFERÊNCIAS


1 CORDEIRO, S. Melhores Práticas para o Gerenciamento de Redes de Automação. Controle & Instrumentação, São Paulo, SP, n° 127, maio 2007.
2 PA CONSULTING GROUP. NISCC Good Practice Guide. Process Control and SCADA Security. 2006. Disponível em: http://www.cpni.gov.uk/docs/re-20061107-00752.pdf. Acesso em: 02/04/2007.
3 ANSI/ISA. ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems. Part 1: Terminology, Concepts, and Models. Research Triangle Park, NC, 2007.
4 ISA. DRAFT dISA-99.00.02 Manufacturing and Control Systems Security. Part 2: Establishing a Manufacturing and Control System Security Program. Draft 1, Edit 5. Research Triangle Park, NC, 2005.
5 ISA. ANSI/ISA—TR99.00.02—2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment.Research Triangle Park, NC, 2004.
6 MICROSOFT. The Security Risk Management Guide. 2006. Disponível em: http://www.microsoft.com/downloads/details.aspx?FamilyID=C782B6D3-28C5-4DDA-A168-3E4422645459. Acesso em: 30/01/2008.