# SEGURANÇA DA INFORMAÇÃO: CONVIVENDO COM A CRISE [1]

*Raphael Pereira*[2]

**Resumo**
Este artigo tem por objetivo apresentar boas práticas de segurança da informação que podem ser implementadas com baixo custo e alto valor agregado, reduzindo os riscos do ambiente de produção. Neste trabalho não serão apresentados novas tecnologias ou tendências, mas ações práticas operacionais que ao serem implementadas trazem benefícios imediatos ao ambiente de produção e reduzem os riscos operacionais
**Palavras-chave**: Segurança da informação; Sistemas industriais; Tecnologia da automação; Tecnologia da informação.

## INFORMATION SECURITY: SURVIVING THE NEW CRISIS

**Abstract**
The objective of this article is to present good practices of information security, with low cost, higher value, to be implemented to reduce risks in industrial environment. In this paper will not be present new technologies or tendencies, this is intend to present operational practices with rapid absorption and benefits to production environment.
**Key words**: Information security; Industrial systems; Information technology; Automation technology.

[1] *Contribuição técnica ao 13° Seminário de Automação de Processos, 7 a 9 de outubro de 2009, São Paulo, SP.*
[2] *MBA, CISSP, CISA, CISM, Information Security*

## 1 INTRODUÇÃO

O processo de gestão da automação é um processo complexo, onde o ambiente heterogêneo de ativos e sistemas interagem com o objetivo de controlar o processo de forma a gerar os produtos definidos dentro das especificações esperadas pelos clientes de forma produtiva, eficiente e conseqüentemente lucrativa.

Nos últimos dois anos, as indústrias do setor de óleo e gás e mineração viveram um momento impar onde a demanda voraz pela matéria prima gerada pelos seus processos era esgotada pelas organizações e países mundo afora, elevando os preços e a demanda por produção a números elevados.

Infelizmente, no final do ano de 2008 uma crise econômica atingiu o mundo, e os seus reflexos diretos para o setor foi a forte redução da demanda e a incerteza sobre o futuro no ano seguinte.

Como reflexo direto a este processo foi à necessidade de reestruturação das indústrias e a redução imediata de projetos planejados ao longo do ano de 2009, muitos deles para otimizar o processo, aumentar a produção, melhorar a qualidade do produto e é claro reduzir os riscos de segurança da informação.

O processo de segurança da informação na indústria de processo no Brasil estava se consolidando nos últimos dois anos. Com uma margem maior no lucro sobre o faturamento e com a crescente demanda, muitas empresas realizaram melhorias operacionais em suas plantas e a maioria destes projetos já nasceram e foram implementados olhando para os requisitos de segurança.

Muito embora o cenário positivo tenha reduzido os riscos de segurança dos ambientes implementados ou suportados, é fundamental que o processo de gestão seja mantido e novos controles sejam inseridos para reduzir os riscos residuais existentes no processo.

Este trabalho tem por objetivo demonstrar boas práticas de segurança da informação que podem ser implementadas no processo de gestão e operacional, de forma a manter o ambiente implementado e reduzir os riscos do ambiente de produção.

## 2 PROCESSO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

O processo de gestão de segurança da informação é o primeiro a ser atingido em uma crise no setor. Com a necessidade de redução dos quadros ou a redução dos investimentos na área acabam gerando no processo um desligamento natural das atividades.

Este fato se concretizado será o causador de um GAP na tecnologia implementada quando a área retomar o processo. Um exemplo simples é o sistema de antivírus, que se for esquecido de lado no momento da crise, pode estar obsoleto ou falho no momento de uma retomada da economia, necessitando de uma nova implementação ou remoção do ambiente por estar incapacitado de ajudar no processo.

Desta forma, para evitar que o processo de gestão de segurança da informação seja renegado pela empresa, uma técnica simples é estabelecer uma rotina de trabalho e indicadores básicos para a gestão da segurança da informação que deve ser cumprida na rotina da equipe de produção. A Tabela 1 apresenta um exemplo de rotina de trabalho e os indicadores para o processo.

**Tabela 1 –** Exemplo de rotina de trabalho do processo de backup e seus indicadores

| **Ativo** | **Processo de Backup** | | | |
|---|---|---|---|---|
| **Rotina** | Objetivo | Procedimento | Periodicidade | KPI |
| **Validação da execução do Backup dos ativos de produção** | Validar a execução correta do backup e executar ações preventivas e corretivas | Acessar o software de backup e verificar o log do ultimo job de backup realizado | Diário | Número de processos de backup realizados com problema no mês. |
| **Rotação das mídias de backup** | Evitar a gravação dos dados em mídias incorretas ou a sobreposição dos Jobs de backup | Identificar a mídia utilizada no backup e registrar em planilha de controle de backup as informações sobre job executado, mídia utilizada e status do backup | Diário | Número de falhas identificadas no processo de rotação das fitas no mês. |
| **Validação de pacotes de atualização do software de backup** | Identificar a necessidade de atualização do software de backup e planejar a implementação | Entrar no site do fabricante e verificar a existência de novas atualizações ou versões para o sistema de backup | Mensal | Quantas atualizações precisam ser instaladas no ambiente por mês. |

O modelo acima de mapeamento de atividades chaves deve ser utilizado para todos os ativos críticos do processo. Entende-se por ativos críticos os processos, pessoas, tecnologia e ambiente. Estabelecendo o processo de gestão e os procedimentos de rotina e seus indicadores, o processo de manutenção do ambiente implementado será estabelecido e como conseqüência direta o ambiente será mantido estável e com o nível de riscos ao percentual estabelecido.

Este processo auxilia na gestão de segurança da informação, porém o motor que deve gerir o processo é o processo de gestão de risco. Muito embora este processo seja consumidor de recursos pessoais para a sua execução, um modelo básico pode ser criado para apoiar na identificação e classificação do risco, realizando a manutenção do processo mesmo em tempos de corte de custos. O modelo sugerido é a criação de um mecanismo de controle automático de vulnerabilidades técnicas através de ferramentas gratuitas e da utilização de um processo formal de conscientização das equipes sobre o assunto.

Estas ações permitirão a identificação de novos riscos através da tecnologia de análise de vulnerabilidades e através das pessoas, normalmente o elo mais fraco da segurança porém quando bem treinadas a melhor ferramenta de detecção e prevenção de riscos de segurança da informação.

O Backtrack CD[(1)] possui diversas ferramentas gratuitas para o processo de identificação de vulnerabilidades nos mais variados ativos (rede, wireless, sistemas Windows, Unix etc). Este CD é gratuito e pode ser utilizado em um equipamento conectado, onde os testes serão executados automaticamente ou manualmente, que é o mais recomendado, de forma a preventivamente identificar novos riscos.

O processo de conscientização deve seguir o modelo de comunicação da empresa, sendo estabelecidas através de emais, avisos na intranet, reuniões formais e informais, entre outras. Deve ser estabelecido um cronograma de assuntos relativos a segurança da informação, sempre utilizando como entrada para a escolha os maiores riscos ou ameaças ao ambiente.

## 3 MONITORAMENTO E INVENTÁRIO DE ATIVOS

O processo de inventário de ativos é o mais defasado quando o processo de gestão é deixado de lado ou possui recursos reduzidos. O processo de gestão normalmente é manual e é dificultado pela presença de diversas tecnologias com diferentes formas de controle e gestão.

Para reduzir os GAPS do inventário de ativo o primeiro passo é definir o que será parte do inventário e segregar em grupos de ativos por tecnologia ou forma de execução do processo de inventário.

Para a execução do inventário dos ativos de TI do ambiente industrial algumas ferramentas gratuitas podem auxiliar e inclusive monitorar o ambiente de forma simples e eficiente. São exemplos destas ferramentas o Nagios [2] e o LanSpy,[3] ferramentas gratuitas responsáveis por monitorar e inventariar o ambiente utilizando os protocolos SNMP e WMI.

O Nagios é uma ferramenta que possui diversas formas de probe, sendo configurado pelo administrador do sistema. O Nagios pode ser executado em ambiente Windows ou Linux, sendo instalado em uma maquina simples. O processo de configuração do Nagios consiste na configuração dos ativos para aceitar o protocolo SNMP para leitura e restringir o acesso somente ao endereço do servidor Nagios e posteriormente configurar quais os monitoramentos e inventários dos ativos devem ser executados. A Figura 1 - Interface Nagios, demonstra a interface de monitoramento dos ativos.

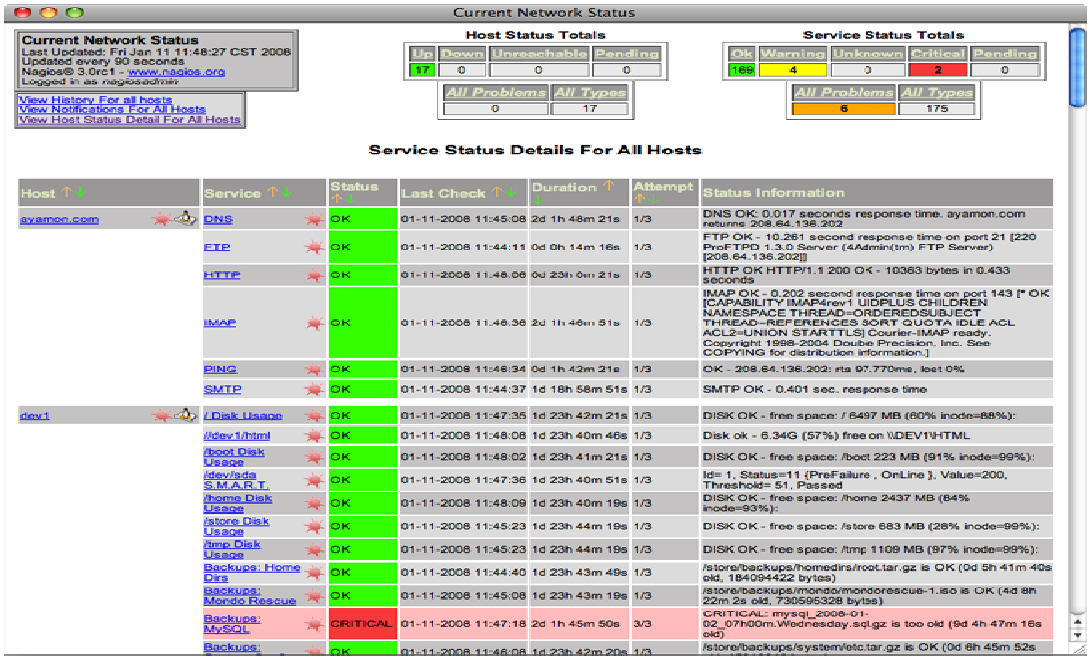


**Figura 1** - Interface Nagios.

O Nagios permite uma serie de alarmes no processo de monitoração que podem ser implementados para reduzir o tempo de parada do ambiente ou de seus ativos e conseqüentemente auxiliar na identificação das falhas.

O LanSpy é uma ferramenta gratuita que realiza uma analise em uma rede, ativo ou sub-rede, identificando a maioria das informações das maquinas Windows e as portas referentes aos serviços TCP/IP abertos. O LanSpy é uma ótima ferramenta para identificar usuários configurados nos sistemas Windows e seus grupos e permissões, assim como outras informações.

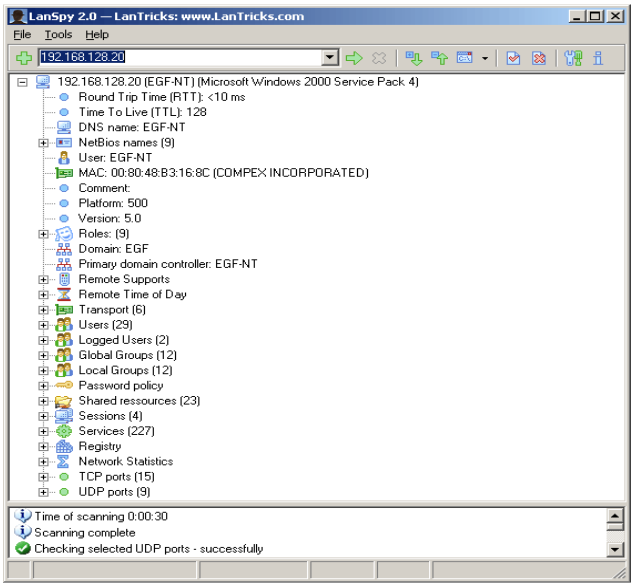


**Figura 2** - Interface LanSpy.

## 4 GESTÃO DO FIREWALL

O ambiente industrial possui conexões com diversos ambientes normalmente controlados por um Firewall. O processo de gestão de um Firewall consiste na criação e exclusão de regras de acesso e no monitoramento/verificação dos registros.

Dependendo da tecnologia utilizada diversas ferramentas de monitoramento e de análise de registros gratuitos e de baixo custo estão disponíveis na internet. Como um exemplo de ferramenta utilizada no processo de análise de registros é o produto da Manage Engine, capaz de analisar registros de diversas tecnologias e com baixo custo de implementação.

Outro fator importante na gestão dos ativos de Firewall é o processo de atualização do sistema, que deve ser definida através do modelo de gestão de segurança e definida os KPIs para monitoração.

## 5 GESTÃO DA AUTOMAÇÃO

O processo de gestão da automação possui uma serie de controles necessários para a manutenção do ambiente e que são diretamente ligados a segurança da informação do ambiente.

O processo de gestão de mudança é fundamental para manutenção da integridade dos sistemas e muitas vezes as empresas não possuem um processo formal para controlar os diversos itens deste processo.

Por exemplo, para a gestão de controle de versionamento de documentos e de arquivos de lógicas dos PLCs é recomendado o uso da ferramenta freeware Subversion[4], mais conhecida como SVN.(4) Esta ferramenta cria uma base de dados no servidor para repositório dos arquivos e gerencia o versionamento.

Atualmente, existe uma tendência a utilizar os sistemas de controle existentes ou servidores de dados históricos para monitorar e controlar o ambiente de TI da automação. O suporte aos protocolos SNMP e WMI permitem que sejam criados tags de controle para os ativos de TI e a monitoração através das interfaces do Supervisório.

O processo de manutenção do ambiente de TA faz parte do processo de gestão de segurança, onde o controle da manutenção dos meios de comunicação, a gestão dos dispositivos de suporte a geração e manutenção de energia para os ambientes como, por exemplo, no-breaks devem ser monitorados e testados periodicamente.

## 6 GESTÃO DE DIREITOS DE ACESSO

O direito de acesso do ambiente de automação é um fator de risco para o ambiente industrial e deve ser revisado periodicamente. O processo de revisão deve avaliar os usuários cadastrados em cada ambiente assim como os perfis de acesso dos usuários.

Para identificação dos perfis de acesso e usuários cadastrados no ambiente Windows é recomendado a utilização da ferramenta freeware LanSpy.(3) O processo de avaliação de usuários em sistemas Unix deve ser estabelecido através de scripts que podem ser criados para analisar os arquivos de usuários, normalmente identificados por /etc/passwd, /etc/shadow, entre outros. O Backtrack CD possui ferramentas para avaliação destes usuários.

Nos sistemas industriais, supervisórios, PIMS, LIMS, entre outros, o modelo de revisão deve ser realizado de acordo com o sistema. Muitas vezes o sistema utiliza usuários do sistema operacional, porem existem ambientes que utilizam uma base de dados separada.

## 7 CONCLUSÃO

Conforme demonstrado no artigo, diversas ferramentas e processos podem ser implementados com baixo custo no ambiente industrial, permitindo a manutenção do controle dos riscos operacionais e a otimização das atividades manuais.

Muito embora as ferramentas e processos sejam de baixo custo, demandam de um processo estruturado que deve ser mantido pela gestão da automação, através da alocação de recursos humanos para a execução das atividades. Muitas vezes, este processo deve ser iniciado com um recurso de maior senioridade, porém ao ser estabelecido pode ser feito uma passagem para recursos mais jovens.

A comunidade da Internet divulga uma serie de ferramentas de TI e de TA que podem ser utilizada com controle no ambiente de automação. A pesquisa de ferramentas ou metodologias para a resolução de problemas simples deve ser uma premissa da área de automação, permitindo a redução de tarefas individuais e o maior índice de controle.

O trabalho de identificação das tarefas de rotina por ativo contribui para a gestão do processo de gestão de segurança da informação. No processo de criação devem ser utilizadas rotinas que permitam o controle através de KPIs claros.

Muito embora este artigo não cite nenhum framework de gestão de segurança da informação como, por exemplo, a ISA S99,[5] é muito importante utilizar estes modelos para apoiar a decisão de qual caminho seguir. Outro fator importante, é que o processo de gestão de segurança da informação deve ser estabelecido através de um processo de gestão de risco.

O modelo de gestão de risco é bastante conhecido no ambiente industrial e já utilizado em diversas empresas do setor, porem caso o mesmo não esteja implementado no ambiente recomenda-se iniciar o processo pela definição da metodologia de avaliação de risco e posterior execução.

Fica claro que a utilização dos conceitos estabelecidos neste artigo pelas industrias de processo é recomendado permitindo a manutenção e sustentabilidade do ambiente.

## REFERÊNCIAS


1 Backtrack CD, disponível em www.remote-exploit.org, acessado em 17/06/2009.
2 Nagios, disponível em www.remote-exploit.org, acessado em 17/06/2009.
3 LANSPY, disponível em http://lantricks.com/lanspy/, acessado em 17/06/2009.
4 SVN, disponível em http://subversion.tigris.org/, acessado em 17/06/2009.
5 ISA, ISA-SP99, Manufacturing and Control Systems Security, disponível em <http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821>, acessado em 17/06/2009.