SEGURANÇA DA INFORMAÇÃO EM AMBIENTES DE AUTOMAÇÃO[1]

Marco Tulio Duarte Rodriguez[2]
Raphael Gomes Pereira[3]

Resumo
Segurança da Informação é hoje uma *commoditie* na área de Tecnologia da Informação (TI), onde as soluções de mercado e os controles de proteção para a informação e seus ativos crescem de acordo com as novas ameaças aos ambientes corporativos. Na área de TA (Tecnologia da Automação), os sistemas de controle e automação estão convergindo para arquiteturas de software e hardware semelhantes às encontradas na área corporativa, com o uso de meio físico *ethernet* e protocolo TCP/IP em redes conectando sistemas supervisórios e controladores. Monitoramento e atuação remota à instrumentos através da internet utilizando protocolos seguros e VPN, também estão presentes em diversos sistemas já instalados. No nível de operação e supervisão, os principais Sistemas Digitais de Controle Distribuído (SDCDs) e supervisórios já migraram de ambientes proprietários para ambiente Windows. Entretanto, neste novo cenário, onde os sistemas geridos pelo grupo de TA se aproximam física e conceitualmente dos sistemas de TI, os mecanismos e ferramentas de proteção à segurança da informação ainda não estão tão difundidos entre os profissionais da TA quanto entre seus colegas da área de TI. Este trabalho irá abordar os principais componentes da área de Segurança da Informação, onde as políticas, processos e arquiteturas presentes em redes corporativas (TI) e de automação (TA) em indústrias de processo são analisadas sob a luz das principais normas e padrões de segurança da informação existentes (ISO 17799/27001/20000 e COBIT). Serão apontados ações e controles para minimizar os riscos de segurança das informações e, por conseqüência, no caso das redes de automação, o risco a própria segurança operacional das unidades. A aplicação dos conceitos aqui descritos é exemplificada na forma de um estudo de caso. Espera-se que, o conhecimento das boas práticas na área de segurança da informação, um tema ainda incipiente na indústria de processos, motive uma reflexão por parte dos responsáveis pelos grupos de TI e TA, no sentido de que suas políticas, processos e sistemas possam ser avaliados e integrados, permitindo a redução dos riscos inerentes ao processo produtivo e operacional da organização.
Palavras-chave: Segurança da informação; Tecnologia da automação; Redes de processo.

INFORMATION SECURITY AT AUTOMATION ENVIRONMENT

Abstract
Today, Information Security is a commodity in the area of Information Technology (IT), where the market of solutions and controls to information protection grows in accordance with the new threats to the corporative environments. In the AT (Automation Technology) area, the control and automation systems are converging to open software and hardware architectures, with the extensive use of Ethernet nets and protocol TCP/IP. In this new scenery, where the systems managed by the AT group near physics and conceptually of IT systems, the mechanisms and tools of information protection still not so well spread between the professionals of the AT as between his colleagues of the IT area. This work will be going to board the main components of the area of Information Security, where the policies, processes and architectures in corporative (IT) and automation (AT) networks in process industries are analyzed under the light of the existent standards of security of the information (ISO 17799/27001/20000 and COBIT). Actions and controls will be pointed to minimize the risks to information security and consequently, in case of the automation networks, the risk to operational security. The application of the concepts here described is exemplified in the form of a case study.
Key words: Information security; Automation technology; Process networks

[1] *Trabalho técnico apresentado ao X Seminário de Automação de Processos, 4 a 6 de outubro de 2006, Belo Horizonte – MG.*
[2] *Gerente Sênior, CHEMTECH ENGENHARIA.*
[3] *Security Officer, CHEMTECH ENGENHARIA.*

INTRODUÇÃO

Nos últimos anos houve uma consolidação da tendência dos modernos sistemas de controle e supervisão adotarem uma arquitetura cada vez mais aberta. SDCDs (Sistemas Digitais de Controle Distribuído) e supervisórios hospedados em ambiente Windows/Linux, CLPs (Controladores Lógicos Programáveis) com suporte integrado à redes *ethernet*/*wireless* e protocolo TCP/IP, estão se tornando um padrão de fato na indústria, inclusive com alguns fabricantes já disponibilizando modelos de CLPs com *firewall* integrado. Esta tendência aproximou a arquitetura e os protocolos dos sistemas de controle (também chamados de sistemas "chão-de-fábrica"), geridos pela Tecnologia da Automação (TA) à dos sistemas corporativos geridos pelos grupos de Tecnologia da Informação (TI). Adicionalmente, nas plantas industriais modernas, existe uma forte demanda para acesso instantâneo à informações geradas pelos sistemas de controle, que são utilizadas para tomada de decisão nos diversos níveis hierárquicos da empresa. Isto resultou em uma crescente integração entre os sistemas de controle e automação e os sistemas corporativos de informação.
Este novo cenário traz a perspectiva de melhorias de performance para o ambiente de TA e otimização dos processos de gestão da automação, porém riscos e ameaças, que antes estavam presentes somente nos ambientes de TI, passam agora a fazer parte também do ambiente de automação. Nas próximas seções serão apresentados os principais conceitos envolvidos na segurança da informação e sua aplicação a realidade dos grupos de automação.

ARQUITETURAS TÍPICAS NAS REDES DE TA

O uso generalizado de sistemas de informação de processo (PIMS – *Plant Information Management Systems*) praticamente estabeleceu um padrão de arquitetura na interligação entre redes/sistemas corporativos e industriais nas modernas indústrias de processo.
Esta arquitetura, em linhas gerais, consiste na criação de uma rede *ethernet* com protocolo TCP/IP, denominada de "processo", que interliga os diversos sistemas de controle à um ou mais servidores de comunicação ou *buffers* (intermediários) de dados pertencentes ao sistema PIMS. O servidor principal, normalmente está conectado à rede de processo através de uma placa de rede dedicada e a rede corporativa por outra placa de rede. Em alguns casos ambas as redes são conectadas por um roteador que define quais máquinas possuem acessos em ambas as redes, neste caso o servidor principal possui apenas uma placa na rede corporativa e, através do roteador, "enxerga" os servidores intermediários na rede de processo. Por motivos de segurança e estabilidade operacional, esta rede de processo deve ser utilizada apenas para a coleta de dados dos sistemas de controle, ou seja, nenhuma informação interna do sistema de controle trafega nesta rede, que é fisicamente independente das redes de controle.
A Figura 1 ilustra, de maneira macroscópica, esta arquitetura.

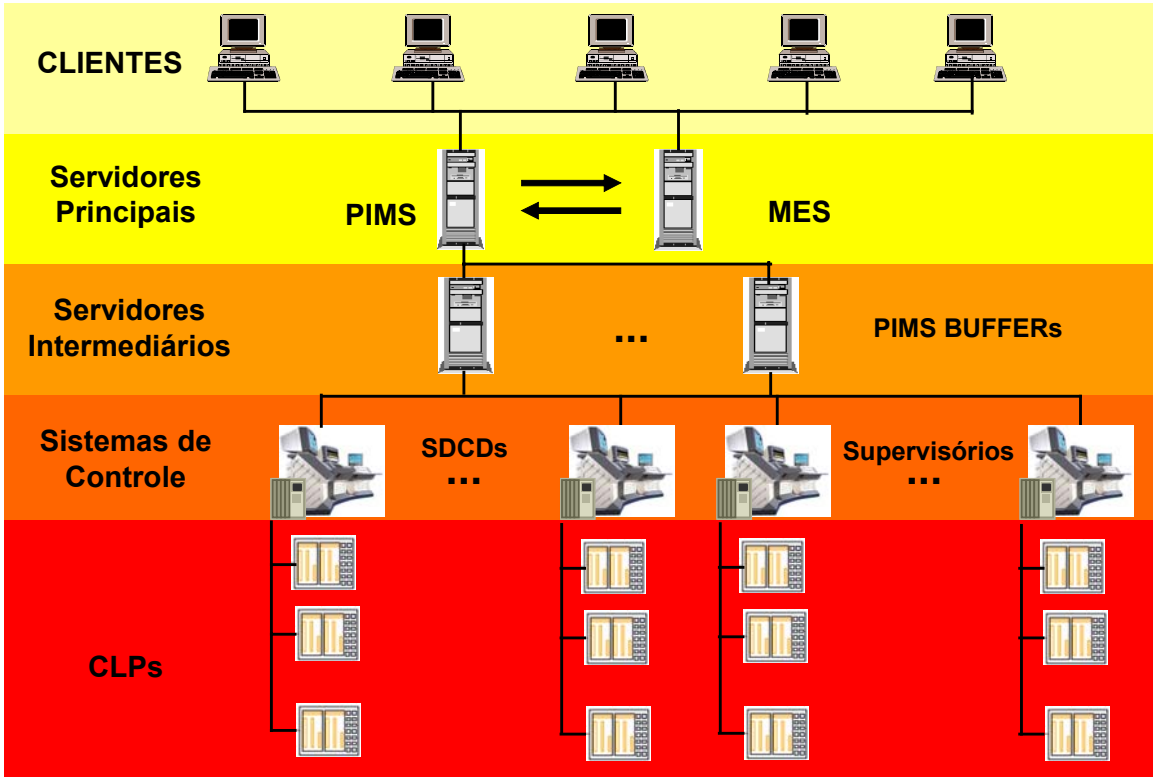

Figura 1. Arquitetura Típica de Interligação entre Redes Corporativas e de Controle

De qualquer forma, nas soluções hoje praticadas, pode-se perceber que existe um "caminho" físico e lógico que permite, em teoria, a qualquer estação cliente o acesso à rede de processo e daí até mesmo à atuação no processo. Se levarmos em conta que a rede corporativa também pode estar conectada a internet, os riscos potencias são ainda mais elevados.

Além das vulnerabilidades inerentes à arquitetura utilizada, as modernas redes de automação possuem ainda o agravante do uso intensivo do protocolo OPC (OLE *for Process Control*) para comunicação entre seus vários componentes, principalmente entre os sistemas de controle e os sistemas de informação de mais alto nível (PIMS). Entretanto, como os computadores envolvidos nesta comunicação geralmente pertencem a domínios completamente diferentes, para que a comunicação via OPC ocorra é necessária uma configuração de parâmetros DCOM na máquina que hospeda o OPC Server, que na maioria das vezes, é uma máquina pertencente à rede de controle. É muito comum, pela facilidade ou desconhecimento do responsável pela configuração do PIMS, uma configuração mais "aberta" que o necessário nos parâmetros DCOM, o que abre caminho para possíveis solicitações não controladas.

RISCOS E AMEAÇAS AO AMBIENTE DE TA

Para exemplificar a aplicação de alguns dos conceitos abordados nas normas à sistemas de controle e automação, vamos considerar a arquitetura SCADA com instrumentação *fieldbus*, representada na Figura 2.

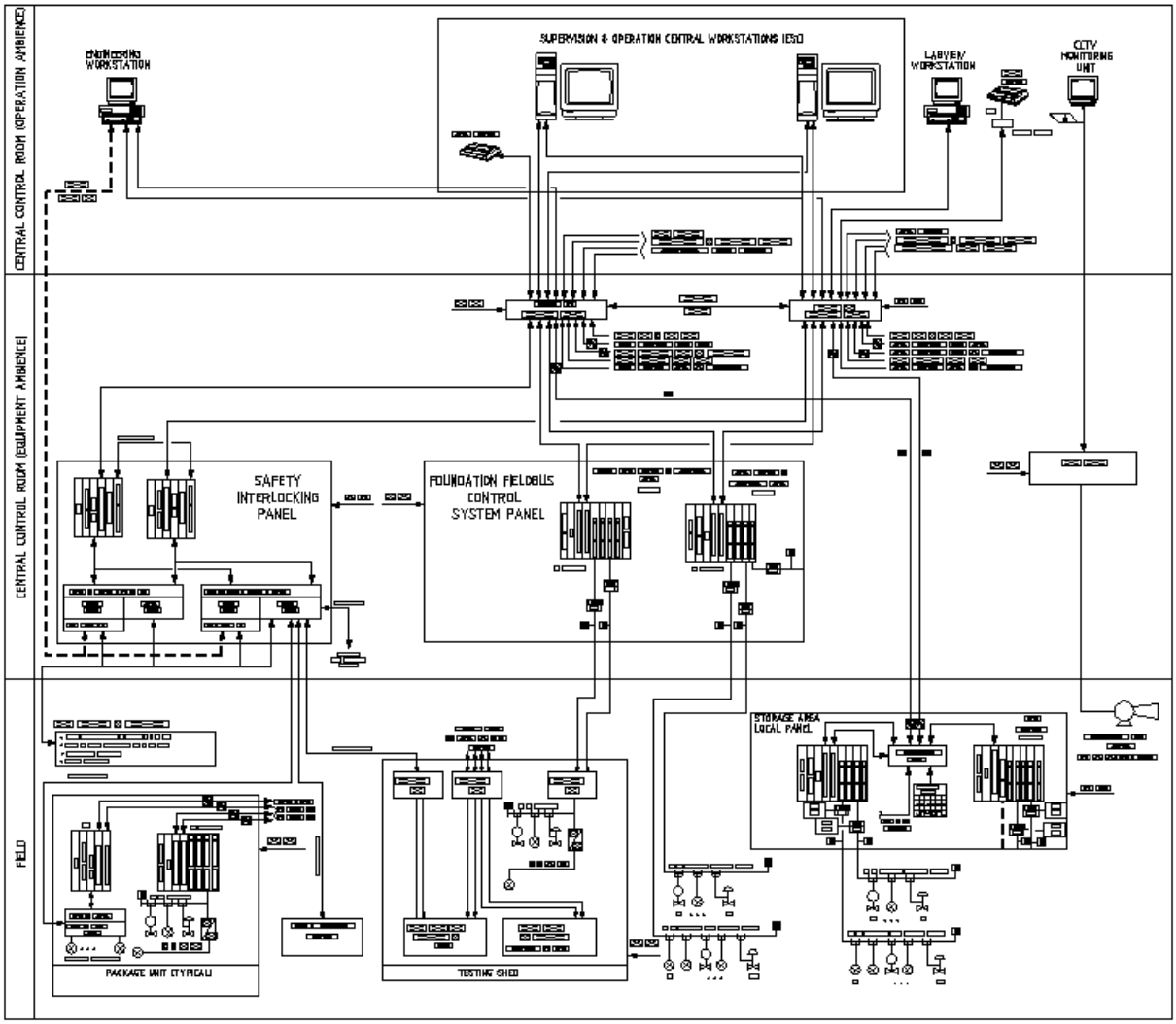

Figura 2. Arquitetura Típica de Automação com *Fieldbus*

As modernas instalações já adotam protocolo TCP/IP e meio físico *ethernet* nas redes de automação (redes envolvendo CLPs e as estações de supervisão e de engenharia). É nesta região, onde não existem grandes diferenças conceituais em relação a tecnologia empregada entre a rede de processo/automação e a rede corporativa, que iremos nos concentrar.

Partindo da premissa de que a ameaça para o ambiente seja algum indivíduo com acesso indevido à rede de controle, os principais ataques identificados neste caso seriam:

Spoofing – consiste em forjar um pacote de comunicação e introduzi-lo na rede com informações/instruções incorretas.

Replay – consiste em copiar um pacote válido e introduzi-lo na rede em um momento posterior.

Negação de Serviço – consiste em enviar um pacote contendo informações inconsistentes para explorar falhas de validação/tratamento de pacotes pelo CLP, podendo provocar a falha do mesmo.

ARP *spoofing* – consiste em burlar o sistema de identificação de cada máquina na rede com o objetivo de receber pacotes endereçados à outras máquinas.

Discovery – consiste em inserir pacotes para obter informações sobre os elementos da rede, como quantidade e identificação dos CLPs. Esta modalidade de ataque

geralmente precede os anteriores, pois as informações obtidas são úteis nas outras modalidades.
Não é difícil concluir quais os possíveis impactos que estes ataques poderiam provocar na produção e na própria segurança da planta. Pacotes inseridos com informações inválidas (*spoofing* ou *replay*) podem provocar alteração do *set-point* de um forno de pelotização, resultando na perda de especificação de um lote completo de produto. O desvio de um pacote (ARP *spoofing*) pode resultar no não recebimento de informações importantes enviadas pelo CLP ao supervisório (ou vice-versa), prejudicando a estratégia de controle ou a atuação do operador. Apesar de as boas práticas em instrumentação e controle recomendarem circuitos independentes e autônomos para intertravamentos de segurança, nem todas as plantas possuem este redundância, podendo transformar um problema operacional em um acidente de proporções imprevisíveis.
Existe ainda o perigo dos ataques à ambientes Windows vulneráveis, tais como vírus ou acesso indesejável às máquinas que hospedam os supervisórios e estações de engenharia.
Como possível tratamento para minimizar estes riscos, algumas normas prevêem uma série de medidas práticas que podem e devem ser tomadas para minimizar ou eliminar as chances de ataque ao ambiente de processo, dentre estas podemos mencionar algumas bastante simples e já bem conhecidas pelos administradores de sistemas corporativos:

1. Instalação/atualização de antivírus;
2. Aplicação de *patches* (atualizações dos softwares), principalmente do Windows, para evitar problemas já conhecidos do sistema operacional;
3. Implementar políticas de controle de identidade;
4. Manter o Windows corretamente configurado;
5. Substituição dos *switches* por *firewalls* (FW) ou IPS (*Intrusion Prevention System*) e
6. Implementar um controle de acesso físico.

PRINCIPAIS NORMAS

As Normas e Padrões internacionais são mecanismos facilitadores de implementação e normalização dos mais variados tipos de soluções para a sociedade. No âmbito da segurança da informação esta tendência começou a torna-se viável no ano 2000, quando a ISO (*International Organization for Standardization*) lançou a norma ISSO/IEC 17799:2000, baseada no padrão britânico da BS7799, disponível para os paises de língua portuguesa através da NBR-ISO17999:2000.
A evolução desta norma gerou a atual ISO/IEC 27001:2005 que compreende os requisitos de implementação e auditoria de um sistema de gestão de segurança da informação e é baseada na norma BS7799-2:2002. As normas ISO/IEC 27001:2005 e ISO/IEC 17799:2005 são complementares.
A norma ISO/IEC 17799 detalha os controles existentes no anexo A da norma ISO/IEC 27001:2005 onde encontramos 133 controles de segundo nível, divididos em 11 princípios básicos, sendo um conjunto de melhores práticas que podem ser seguidas para implementação de dispositivos de controle que suportam um sistema de gestão de segurança da informação. Esses princípios são:

- Política de Segurança da Informação;
- Gestão da Segurança da Informação;
- Gestão de Ativos;

- Segurança em Recursos Humanos;
- Segurança física e do ambiente;
- Gerenciamento das Operações e Comunicações;
- Controle de Acesso;
- Aquisição, desenvolvimento e manutenção de Sistemas de Informação;
- Gestão de Incidentes de Segurança da Informação;
- Gestão da Continuidade de Negócios e
- Conformidade (*Compliance*).

Outro padrão utilizado pelas organizações é o COBIT (*Control Objectives for Information and related Technology*). Criado pelo ITGI (*IT Governance Institute*)/ISACA (*Information Systems Audit and Control Association*), o COBIT define um conjunto de melhores práticas para governança de TI incluindo o assunto Segurança da Informação. Assim como a ISSO 27001, a adoção do COBIT ocorreu a partir de 2000, com o lançamento da versão 3.0. Neste ano, o ISACA lançou a nova versão do COBIT, 4.0 que compreende os níveis de maturidade da governança da IT.

O COBIT é fundamentado em 34 processos de TI. Cada processo é divido em 4 sessões que são:

- O Objetivo de controle de alto nível do processo;
- Os objetivos de controle detalhados para o processo;
- Guia de gestão: Entradas e Saídas dos processos, a tabela RACI (*Responsible, Accountable, Consulted and/or Informed*), gráficos, objetivos e métricas e
- O Modelo de maturidade para o processo.

O foco do modelo COBIT é a governança de TI, onde os fatores fundamentais citados são:

- Alinhamento estratégico com o plano de negócios da organização;
- Valor agregado na entrega de serviços de TI;
- Gestão de recursos;
- Gestão de risco e
- Avaliação de desempenho.

A Figura 3 ilustra como os modelos citados na gestão das organizações estão relacionados:

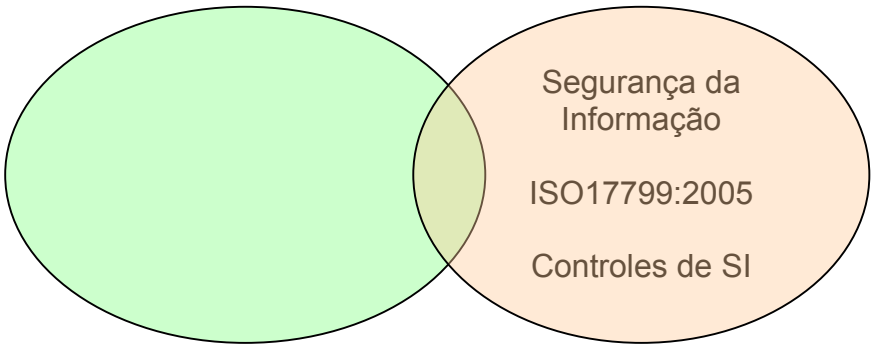

Figura 3. Relacionamento entre Modelos Propostos nas Normas

Estes padrões sugerem a gestão de TI e a proteção da informação que sabemos que é de grande importância para o ambiente de TI. No ambiente de TA a grande preocupação é o risco operacional, porém estes padrões podem ser seguidos para

implementação da segurança das redes de automação, permitindo a proteção da informação e a operação das corporações.
No nosso artigo vamos adotar a ISO/IEC 27001:2005 como base para a implementação de segurança em uma rede de automação. A norma especifica um conjunto de requisitos para a implantação de um sistema de gestão, que segue as mesmas características do Sistema de Gestão da Qualidade, para a segurança da informação.
Como todo sistema de gestão o ciclo PDCA deve ser seguido para garantir a melhoria continua do sistema através da retro alimentação. No nosso caso, os incidentes de segurança, as novas ameaças, novos ambientes, resultados de auditorias e analise de risco são algumas das fontes de alimentação do sistema.
A implantação de segurança utilizando como base a ISO/IEC 27001 passa normalmente pelas seguintes etapas:

1. Definição do escopo

Nesta etapa temos que definir a abrangência da implantação do SGSI, seu detalhamento e exclusões. A boa definição do escopo facilita a administração dos investimentos a serem feitos, protegendo melhor a organização.
A norma especifica que o escopo deve seguir entre outras coisas as características do negócio.

2. Definição da Política de Segurança

A Política de Segurança deve expressar os direcionamentos de alto nível da organização, devendo ser aplicada a todo o escopo de implementação. Uma boa política deve seguir a cultura da organização e estar alinhada com o escopo do negócio.

3. Elaboração da metodologia da Análise de Riscos

Nesta etapa, a organização deve elaborar uma metodologia de análise de risco definindo a estratégia de avaliação do risco, desenvolvendo critérios para aceitação do risco e identificação dos riscos aceitáveis, levando em conta que os resultados da análise de risco sejam reproduzíveis e comparáveis. A execução da análise de risco deve ser apropriada e metódica, identificando ameaças aos ativos, vulnerabilidades e possíveis impactos no negócio. O risco deve ser gerenciado baseado na política da organização e nível de segurança exigido;
Alguns padrões de metodologias estão disponíveis para uso, são eles:

- Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM}): Metodologia de análise de risco desenvolvida pelo CERT, centro de expertise de segurança da Internet da universidade de Carnegie Mellon. Possui dois tipos de modelos, o OCTAVE-S, recomendado para pequenas e médias empresas, e o OCTAVE, recomendado para grandes organizações e
- AS/NZS 4360 (Australian Standard 4360 Risk management): Metodologia que prove um padrão genérico para execução da análise de risco. Geraldo Ferreira, citou em seu artigo publicado no site Modulo.com, que a "*a AS/NZS 4360 (Australian Standard for Risk Management) publicada em 1995 e revisada em 1999, é uma norma Australiana / Neozelandesa para gerenciamento de riscos que foi elaborada pela Standards Austrália e Standards New Zealand através do Comitê de gestão de riscos (OB-007). É uma norma genérica que fornece orientações para gerenciamento de riscos de qualquer natureza.*

Ao contrário dos padrões de segurança existentes no mercado, que consideram risco como perigo ou impacto negativo para as organizações, a AS/NZS 4360 parte do princípio que a gestão de riscos tem como finalidade o equilíbrio entre as oportunidades de ganhos e a redução de perdas. Esta norma considera risco como "a exposição às conseqüências da incerteza ou como potenciais desvios do que foi planejado ou do que é esperado" e sua principal característica é avaliar considerando tanto os riscos com resultados positivos (ganhos potencias) quanto os riscos com resultados negativos (perdas potenciais), fornecendo uma visão única no gerenciamento de riscos.
As empresas também podem criar a sua metodologia de análise de risco, utilizando os padrões acima e a ISO13335, desde que atendam os requisitos mínimos da ISO27001.
Após a execução e o mapeamento do risco, todo o processo deve ser documentado e aprovado pelas partes envolvidas. Esta formalização serve para direcionamento para a próxima etapa de tratamento de risco.

4. Tratamento de Risco

O processo de tratamento de risco deve ser realizado de acordo com o nível de aceitação de cada empresa, podendo ser definido por grau de risco ou por risco identificado. As ações possíveis para cada ponto encontrado são: Aceitar, Mitigar, Negar, Transferir.
Estas ações basicamente contemplam três medidas para tratamento do risco:

- Correção: Resolução do risco de forma pontual;
- Prevenção: Implementação de controles para que o risco não retorne após a correção e
- Detecção: Implementação de controles para identificação do risco.

5. Auditoria e revisão dos controles

O processo de auditoria deve ser formalizado pela organização em um plano de auditoria e revisões. É recomendado que as auditorias planejadas não ocorram logo após a implementação dos controles, devendo aguardar a maturidade da implementação e a geração de evidências para a auditoria.
Para execução da auditoria as empresas podem montar equipes internas, desde que realizado por pessoas que não tenham relacionamento com o processo ou controle, ou externa. É importante que os auditores conheçam os processos e as tecnologias envolvidas, para garantir a efetividade da auditoria.
As auditorias realizadas devem ter o seu resultado avaliado pelo time de gestão permitindo a melhoria continua do sistema de gestão. As seguintes informações devem ser utilizadas como entrada para o processo de melhoria continua:

- Resultados de auditorias e revisões do sistema;
- *Feedback* de *stakeholders;*
- Técnicas, produtos ou procedimentos que poderão ser usados na organização para melhorar o desempenho e a efetividade do sistema;
- Status das ações corretivas e preventivas;
- Vulnerabilidades ou ameaças não endereçadas corretamente no plano de tratamento de risco anterior;
- Resultado dos indicadores de efetividade;
- Avaliação das ações de revisões anteriores;
- Mudanças que podem afetar o sistema e
- Recomendações para melhorias.

O resultado da revisão do sistema deve incluir quaisquer decisões ou ações relacionadas com:

- Melhorias na efetividade do sistema;
- Alterações na Análise de Risco e no Plano de Tratamento de Risco;
- Modificações de procedimentos e controles que afetam a Segurança da Informação para responder a ocorrências internas ou externas que podem impactar o sistema, incluindo mudanças:
    - Requisitos de Negócio;
    - Requisitos de Segurança;
    - Processos de negócios que afetam os requisitos de negócios existentes;
    - Requisitos legais e regulamentares;
    - Obrigações contratuais e
    - Nível de risco e/ou critério de aceitação de risco.
- Necessidade de Recursos e
- Melhorias na efetividade dos índices referentes aos controles implantados.

Todas as normas são unânimes em afirmar que a Alta Direção deve ter a responsabilidade pela tomada de decisões e de disponibilizar recursos para implantação das melhorias para eficácia do sistema.

CONCLUSÕES

Com a crescente convergência entre os sistemas de informação industrial/corporativa e de automação, o tema segurança da informação deixou de ser exclusivo dos grupos de TI para se tornar uma preocupação também dos responsáveis pela TA.

Para facilitar a implementação dos mecanismos de segurança da informação na área de TA, os responsáveis devem utilizar os padrões e normas citados neste artigo que foram amadurecidos ao longo dos últimos anos pela área de TI. O acompanhamento das ameaças e riscos aos quais os modernos sistemas de controle estão sujeitos, será um grande desafio para os responsáveis pelas redes de automação nos próximos anos.

A proteção deste ambiente também está diretamente relacionada à ameaças que no Brasil são ainda incipientes, tais como ataques terroristas ou criminosos (sabotagem, espionagem industrial, etc...), porém como a globalização é um processo ainda não consolidado, estas ameaças podem se tornar significativas em um futuro não muito distante.

Agradecimentos

Colaboraram para este trabalho:

Cintia Rodrigues Filho, Gerente de Projetos, CHEMTECH Engenharia.

Rosângela Caubit de Carvalho, Consultora de TI & Gestão da Qualidade, 5S TECNOLOGIA.