AUTOMAÇÃO & TI
18º SEMINÁRIO DE
AUTOMAÇÃO & TI INDUSTRIAL

CONCEPÇÃO E DESENHO DE PROGRAMA INTEGRADO DE SEGURANÇA DA INFORMAÇÃO PARA AUTOMAÇÃO*

Vinicius Andres Strey[1]
Luiz Frederico de Freitas Kümmel[2]

Resumo
Segurança da informação é um tema crescente dentro do ambiente de Tecnologia de Automação. Da mesma forma que para outras rupturas que ocorreram, as grandes empresas desempenham um papel de vanguarda também quando se fala em segurança da informação. Grandes empresas, no geral, possuem diversas instalações. Neste caso, em se tratando de segurança da informação, é fundamental que os riscos sejam identificados e os controles sejam definidos e implantados de maneira integrada, de modo que vulnerabilidades quando exploradas não afetem o negócio como um todo. Desta forma, recomenda-se fortemente a adoção de um programa de segurança da informação com a participação das diversas instalações em vez de projetos isolados. Este trabalho apresenta a estratégia para o desenvolvimento deste programa através da adaptação de boas práticas e frameworks de referência, como ISA-62443 e NIST SP 800-82. As fases de concepção e desenho do programa estão contempladas, tomando como caso de referência o Programa de Cyber Security para Sistemas de Automação Industrial da Vale. Este programa foi concebido para ser abrangente nos aspectos de segurança da informação, considerando a situação individual de cada mina, usina ou porto envolvido, e estruturado de maneira a ser expandido facilmente para outras instalações.
Palavras-chave: Segurança da Informação; Programa de Segurança; Tecnologia de Automação.

CONCEPT AND DESIGN OF INTEGRATED PROGRAM OF INFORMATION SECURITY FOR AUTOMATION

Abstract
Information security is a growing subject within the Operational Technology environment. Just as for other breaches that occurred, large companies perform a leading role also when it comes to information security. Large companies, in general, have different facilities. In this case, when it comes to information security, it is essential that risks be identified and controls be defined and deployed in an integrated manner, so that vulnerabilities when exploited do not affect the business as a whole. Thus, it is strongly recommended the adoption of a program of information security with the participation of various facilities instead of isolated projects. This paper presents a strategy for the development of this program by adapting best practices and frameworks of reference, such as ISA-62443 and NIST SP 800-82. The phases of conception and design of the program are covered, taking as reference case the Program Cyber Security for Industrial Automation Systems of Vale. This program is designed to be comprehensive in the aspects of information security, considering the individual situation of each mine, plant or port involved, and structured so as to be easily expanded to other facilities.
Keywords: Information Security; Security Program; Operational Technology.

[1] *Engenheiro de Controle e Automação (UFSC), Engenheiro de Projetos, Chemtech Serviços de Engenharia e Software, Belo Horizonte, MG, Brasil.*
[2] *Engenheiro Eletricista (CEFET-MG), Engenheiro de Automação, Vale, Belo Horizonte, MG, Brasil.*

* *Contribuição técnica ao 18° Seminário de Automação e TI Industrial, 23 a 26 de setembro de 2014, São Paulo, SP, Brasil.*

1 INTRODUÇÃO

A Vale é a maior produtora mundial de minério de ferro e pelotas. Para atingir tais níveis de produção, conta no Brasil com um parque considerável de instalações, dentre as quais, minas, usinas de concentração, usinas de pelotização e portos. Todas estas instalações possuem, em algum nível, sistemas de controle e automação industrial.

A norma ISA-99.00.01 [1], no escopo de segurança da informação, define sistemas de controle e automação industrial (IACS), como o conjunto de pessoas, hardware e software que possa afetar ou influenciar a segurança e a confiabilidade da operação de um processo industrial. Isto inclui, mas não está limitado a:

- Sistemas de controle industriais, incluindo sistemas distribuídos de controle digital (DCS), controladores lógicos programáveis (PLC), unidades terminais remotas (RTU), sistemas de supervisão e aquisição de dados (SCADA), sensores eletrônicos em rede e sistemas de monitoramento e diagnóstico;
- Sistemas de informação associados, como controle multivariável ou avançado, otimizadores online, monitores de equipamentos, interfaces gráficas, historiadores de processo, sistemas de execução de manufatura (MES) e sistemas de gerenciamento de informações da planta (PIMS);
- Pessoal, redes, interfaces de máquinas associados que são usados para prover controle, segurança e funcionalidade para processos contínuos, em batelada e discretos.

A Figura 1 demonstra a evolução das tecnologias aplicadas dentro do ambiente de Tecnologia de Automação (TA). Por muito tempo, os IACS rodaram isolados do ambiente corporativo usando tecnologias proprietárias cujo domínio estava concentrado em alguns especialistas ligados ao fabricante do ativo.

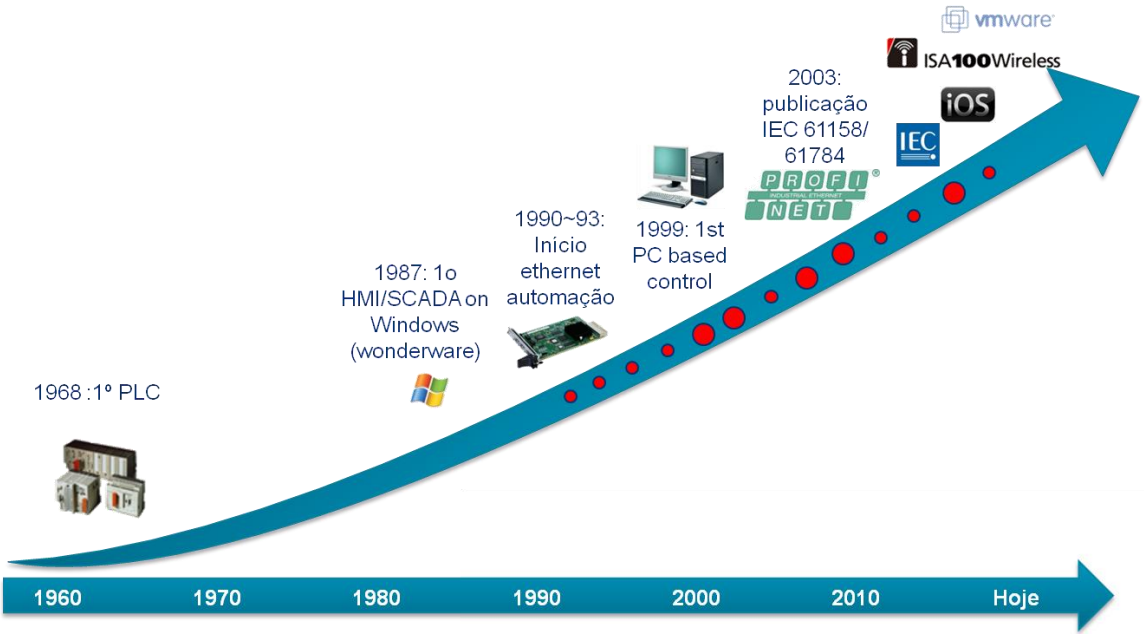

Figura 1. Evolução das tecnologias em ambiente industrial

No final da década de 80, começou a ocorrer o processo de convergência entre a Tecnologia de Automação (TA) e a Tecnologia de Informação (TI). Tecnologias antes exclusivas de TI, como sistemas operacionais, ethernet, TCP/IP,

---

** Contribuição técnica ao 18° Seminário de Automação e TI Industrial, 23 a 26 de setembro de 2014, São Paulo, SP, Brasil.*

computadores pessoais e, mais recentemente, até mesmo virtualização de servidores e aplicações, passaram a fazer parte da rotina de automação.
Com esta convergência, não apenas as tecnologias, mas também as vulnerabilidades de segurança de TI passaram a ser exploradas em ambiente de TA. Não raros são os incidentes de segurança que afetam plantas inteiras, que pecam por não terem controles de segurança compatíveis com os riscos a que estão expostas. Alguns exemplos são o incidente de Maroochy Water Services [2], a contaminação do ambiente industrial da usina nuclear de Davis-Besse pelo *worm* Slammer [3], o *superwom* Stuxnet [4] e suspeitas de correlação entre intrusões de *hackers* e os blackouts em escala nacional na década de 2000 no Brasil [5].
A ISA-62443, antiga ISA-99, surge como uma das normas de referência para o desenvolvimento de um Sistema de Gerenciamento da Segurança da Informação (SGSI) para sistemas de controle e automação industrial, visando o tratamento destas vulnerabilidades.
A ISA-62433 define na parte ISA-99.02.01 [6] um fluxo de atividades visando à implantação de um Sistema de Gerenciamento da Segurança da Informação (SGSI). Este fluxo está representado na Figura 2.

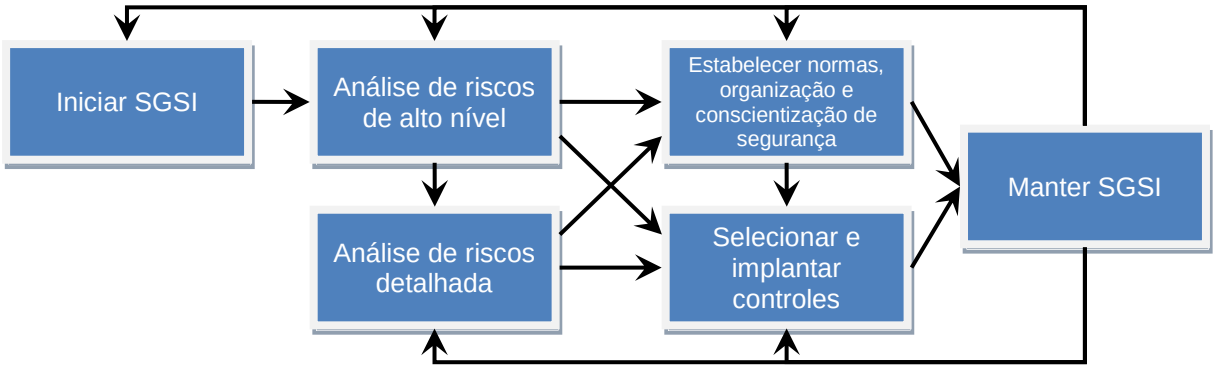

Figura 2. Atividades para um SGSI segundo ISA-99.02.01

A Vale enxergou a oportunidade de aplicar estas boas práticas dentro do ambiente de automação de algumas de suas áreas operacionais. Para tanto, a Chemtech foi a empresa selecionada para executar inicialmente a etapa de Business Case (ver seção 2) e depois a etapa de Desenho (ver seção 3) do Programa de Cyber Security para Sistemas de Automação Industrial da Vale. A estruturação destas etapas foi realizada aproveitando-se o fluxo representado na Figura 2.
Por questões de confidencialidade relacionadas ao tema de segurança da informação, detalhes do Programa de Cyber Security para Sistemas de Automação Industrial da Vale foram omitidos ou tratados de maneira menos específica.

2 *BUSINESS CASE* DE SEGURANÇA DA INFORMAÇÃO

A Figura 3 é um desdobramento da Figura 2 para a etapa de Business Case de Segurança da Informação.
As atividades com cor de fundo vermelha foram realizadas dentro desta etapa de acordo com as necessidades do Programa de Cyber Security para Sistemas de Automação Industrial da Vale. As atividades com fundo alaranjado foram realizadas parcialmente dentro desta etapa. Neste último caso, o escopo restante deve ser realizado em etapa posterior. Esta distribuição de cores aplica-se para outras figuras adiante no documento em formato de diagrama de blocos.

---

* *Contribuição técnica ao 18° Seminário de Automação e TI Industrial, 23 a 26 de setembro de 2014, São Paulo, SP, Brasil.*

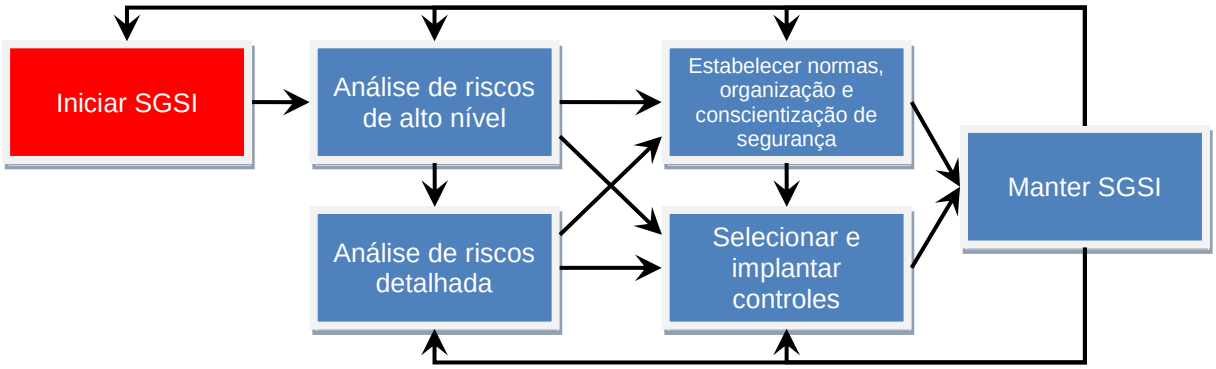

Figura 3. Atividades para um SGSI segundo ISA-99.02.01: *Business case*

2.1 Motivação

Em resumo, um SGSI visa reduzir os níveis dos riscos intoleráveis de segurança da informação. Para que este objetivo seja atendido, é necessário antes de tudo identificar estes riscos, definir papeis e responsabilidades sobre a segurança da informação e criar mecanismos para monitorar o desempenho de todo este processo.
A criação desta infraestrutura depende de investimentos financeiros e em outros recursos. Grandes empresas, como a Vale, possuem ciclos orçamentários que seguem padrões corporativos para a priorização dos investimentos mais atrativos.
Para mostrar que um investimento é atrativo, a abordagem sugerida pela ISA-99 é o *business case* (ou *business rationale*). O objetivo do *business case* é buscar o patrocínio e comprometimento da organização através do reforço com as pessoas que possuem autonomia política e financeira, tipicamente a direção ou a gerência, de que vale a pena investir em segurança da informação.

2.2 Estruturação

No *business case* do Programa de Cyber Security para Sistemas de Automação Industrial da Vale foram utilizadas as seguintes estratégias para obtenção do patrocínio e comprometimento:

- Utilização dos mesmos critérios para avaliação de riscos da norma corporativa de análise de riscos operacionais: alguns investimentos são justificados pela redução de algum risco de e, por isto, é comum que a organização já tenha seu padrão para avaliação de riscos. A ISA-99.02.01 recomenda esta integração entre as análises de riscos de segurança da informação e de HSE (*Health, Safety and Environment*). Neste projeto, foram feitas poucas adaptações nos critérios já existentes em uma norma interna da Vale para gerenciamento de riscos operacionais visando à realização da análise de riscos de segurança da informação em ambiente industrial;
- Envolvimento de uma amostragem representativa das áreas operacionais com apoio de área corporativa (ponto focal): em um projeto envolvendo várias áreas operacionais, é de grande valia que haja uma autoridade central que fomente e dissemine as boas práticas em segurança da informação e que faça a integração entre as áreas operacionais;
- Estimativa de perda financeira anual: embora segurança da informação justifique-se em grande parte pela redução de riscos de segurança da

informação, é fundamental durante o *business case* que sejam calculados os retornos financeiros dos investimentos em segurança da informação. As bases de cálculo podem variar desde danos à imagem da organização até lucros cessantes. O *business case* trabalha tradicionalmente com incertezas razoáveis na precisão dos valores financeiros, entretanto, mesmo assim, as bases de cálculo devem ser coerentes;

- Avaliação de conformidade aos controles de uma norma de referência: neste business case, avaliou-se a conformidade geral média dos sistemas de automação das áreas operacionais da Vale à norma NIST SP800-82 [7]. Os desvios de conformidade a esta norma servem como mecanismo de sensibilização para o investimento em segurança da informação. Esta avaliação de conformidade será explorada melhor na seção 3.2.1;
- Transparência nos riscos e fatores críticos de sucesso: descrever os principais obstáculos e oportunidades do programa de segurança agrega em confiança com as principais partes interessadas e faz com que compartilhem.

Apenas com o sucesso do *business case*, através da abordagem acima, foi possível obter o patrocínio para a realização da etapa de desenho, descrita na seção 3.

3 DESENHO DO PROGRAMA DE CYBER SECURITY

A Figura 4 é um desdobramento da Figura 2 para a etapa de Desenho do Programa de Cyber Security para Sistemas de Automação Industrial da Vale.

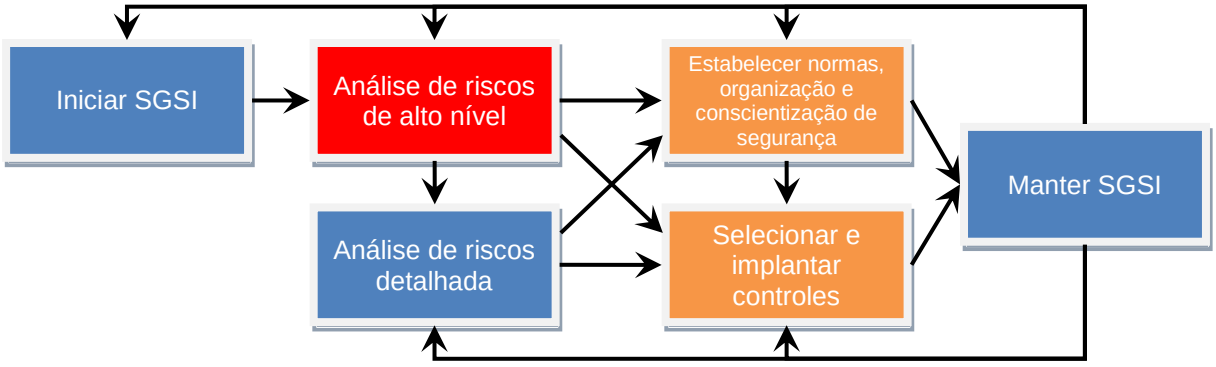

Figura 4. Atividades para um SGSI segundo ISA-99.02.01: Desenho

3.1 Análise de Riscos de Alto Nível

A análise de riscos de alto nível está estruturada através da combinação entre ameaças potenciais de segurança da informação para a Tecnologia de Automação (TA) e as principais classes de ativos dentro do escopo da TA. O principal objetivo da análise de riscos de alto nível foi embasar a priorização inicial dos investimentos em segurança (ver seção 3.2.2). Esta análise de risco de alto nível foi conduzida para cada uma das áreas operacionais envolvidas.
Como mostra a Figura 5, para cada par ameaça/classe de ativos gera-se um risco potencial, o qual deve foi priorizado conforme probabilidade e severidade.

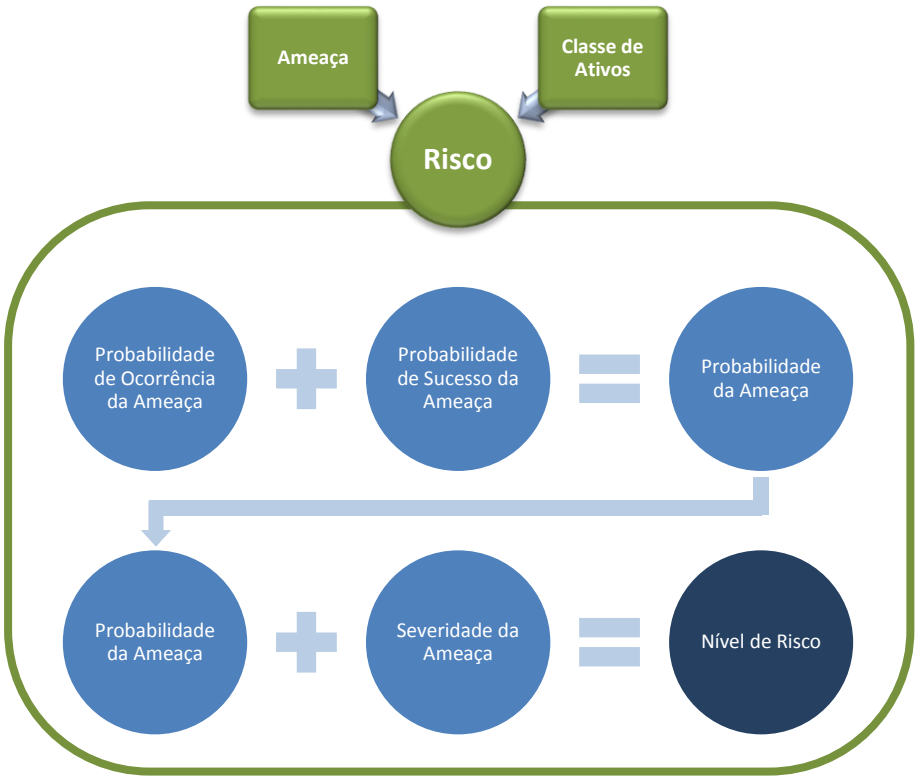

Figura 5. Análise de riscos de alto nível

3.1.1 Composição do risco

As classes de ativos foram orientadas aos tipos de ativos de automação com relevância para a segurança da informação em ambiente industrial. Dentre estas classes de ativos poderiam ser citados PLC, Servidores SCADA, Controladores de Domínio, Switches e Roteadores, Estações de Operação, entre outros.

Além das classes de ativos, foram identificadas as ameaças potenciais para o ambiente industrial. Sabe-se que um ambiente, dependendo do seu tamanho, está exposto a milhares de ameaças. Entretanto, na análise de riscos de alto nível Programa de Cyber Security para Sistemas de Automação Industrial da Vale foram selecionadas apenas as mais prováveis, abrangentes e que possam realmente representar um nível de risco considerável. Dentre estas, poderiam ser citadas:

- Acesso lógico ou físico não autorizado de dentro da organização: acesso não autorizado aos ativos por funcionários, visitantes ou terceiros que estão fisicamente dentro das fronteiras da unidade;
- Acesso lógico não autorizado de fora da organização;
- Contaminação por código malicioso: contaminação dos ativos da TA por vírus, *worms*, *spyware* e outras formas de código malicioso;
- Instalação de aplicativo não homologado ou não licenciado;
- Perda de disponibilidade ou integridade devido à mudança mal sucedida;
- Indisponibilidade devido a dano no ambiente (incêndio, alagamento, outros);
- Distúrbio na rede elétrica (sobretensão, subtensão, interrupção no fornecimento).

* *Contribuição técnica ao 18° Seminário de Automação e TI Industrial, 23 a 26 de setembro de 2014, São Paulo, SP, Brasil.*

3.1.2 Determinação do nível de risco

A análise de risco de cada par ameaça/classe de ativos requer a identificação, pelo entrevistado, da probabilidade da ameaça que é desdobrada em:

- Probabilidade de ocorrência da ameaça: é realizada através do histórico de incidentes associados a cada risco. Em ambiente industrial, é muito comum que não se tenha o histórico de incidentes de segurança da informação, seja pela ausência de mecanismos de registro, bem como pela ausência de mecanismos de monitoramento do ambiente (incidentes ocorrem ou estão acontecendo sem a percepção da ocorrência). Desta forma, a avaliação de probabilidade de ocorrência do risco foi adaptada para utilizar supletivamente (quando sem a perspectiva do histórico) aspectos relacionados à motivação e à capacidade necessárias para o agente realizar a ameaça. Um risco cuja ameaça exige um agente muito capaz e motivado possui probabilidade mais baixa que um risco cuja ameaça pode ser realizada não intencionalmente ou por agente pouco capaz ou sem motivação específica de dano;
- Probabilidade de sucesso da ameaça: além da probabilidade de ocorrência, para riscos de segurança, deve ser considerada a identificação da probabilidade de sucesso considerando os controles existentes para cada tipo de ativo. A probabilidade de sucesso das ameaças é elevada nos casos em que os controles adotados sejam inexistentes ou pouco confiáveis. Por outro lado, a probabilidade é reduzida caso os controles sejam existentes e eficazes.

Por sua vez, a escala de severidade foi utilizada na sua forma original presente na norma corporativa da Vale e considera tanto impactos financeiros na materialização do risco como impactos em imagem e em HSE.

A composição das probabilidades de ocorrência e de sucesso e da severidade gera o nível de risco para cada risco (par ameaça/classe de ativos). O nível de risco poderia assumir cinco níveis: muito alto, alto, médio, baixo e muito baixo.

3.2 Selecionar e Implantar Controles

A Figura 6 representa as tarefas da atividade “Selecionar e Implantar Controles” da Figura 4.

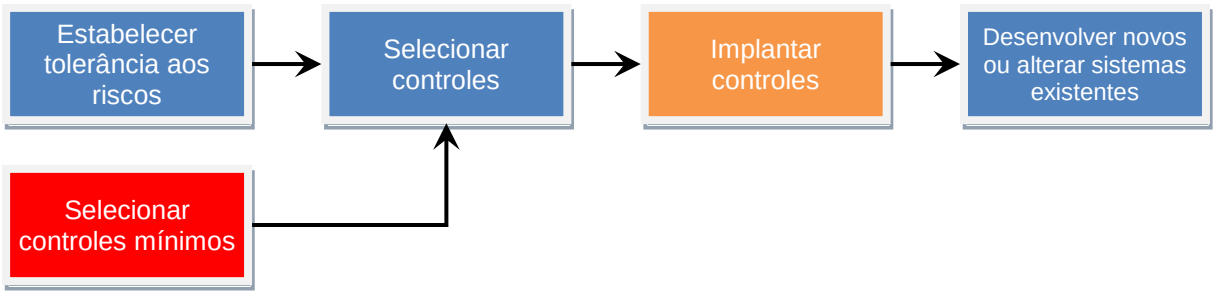

Figura 6. Tarefas para seleção e implantação de controles

Este projeto possui dificuldades para a seleção e implantação de controles, pois envolve mais de uma área operacional, sendo que as equipes de automação de cada área possuem grande autonomia sobre os serviços que prestam. Desta forma, há diferentes níveis de maturidade em segurança da informação entre as áreas operacionais, que se reflete no nível de controles aplicados atualmente.

** Contribuição técnica ao 18° Seminário de Automação e TI Industrial, 23 a 26 de setembro de 2014, São Paulo, SP, Brasil.*

Para a criação de um SGSI que tenha um caráter corporativo é fundamental que se consiga atingir um nível fundamental de segurança mínimo global. Para tanto, no Programa de Cyber Security para Sistemas de Automação Industrial da Vale lançou-se mão do uso dos controles mínimos. Trata-se de controles de segurança indiscutíveis para a organização que independem dos resultados da análise de riscos. Os controles mínimos assemelham-se a prática de linha de base de segurança, já conhecida no mundo da segurança da informação [8].
Alguns controles tratados comumente como indiscutíveis na atual conjuntura dos sistemas de automação são, por exemplo, a implantação de uma Rede DMZ entre o ambiente de automação (TA) e o ambiente corporativo (TI) e a exigência de, pelo menos, um mecanismo de autenticação para acesso aos sistemas de automação.

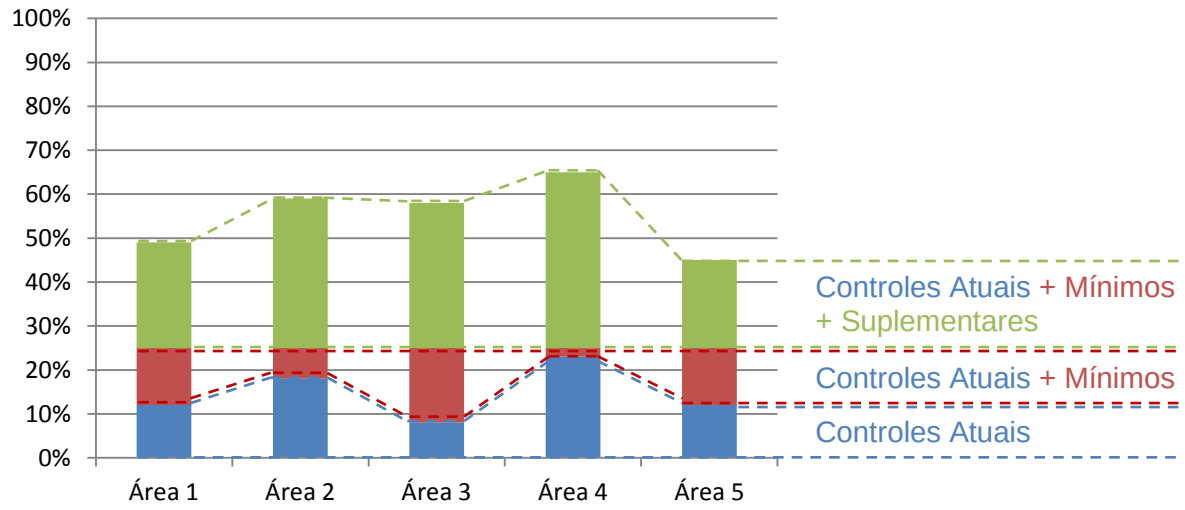

Figura 7. Representação gráfica do uso dos controles mínimos

A Figura 7 ilustra a importância da definição dos controles mínimos como mecanismo para homogeneização da segurança da informação no ambiente de automação de todas as áreas envolvidas.
Antes da implantação de um SGSI (barra azul), as áreas possuem distintos níveis de controles atuais (preexistentes). Com os controles mínimos (barra vermelha), as áreas desenvolvem-se a fim de que todas atendam a linha de base de segurança. Percebe-se na figura um nível (fictício) de controles ao redor de 25%. Além disso, é necessária que sejam conduzidas análises de riscos detalhadas periódicas (ver atividades da seção 4) para identificar controles suplementares.
Cada área possui algumas particularidades em termos de segurança que irão ser refletidas na análise de riscos detalhada e, por conseguinte, nos controles suplementares a serem planejados e implantados.

3.2.1 Selecionar controles mínimos

A seleção dos controles mínimos envolveu todas as áreas operacionais participantes do projeto. É fundamental que todos opinem e cheguem a um consenso do que é aceitável em termos de segurança e, principalmente, do que é viável de ser atendido. Os controles mínimos podem ser agrupados em diversas áreas do conhecimento, que guardam similaridade com os elementos do SGSI da ISA 99, dentre os quais, por exemplo, Segurança Física, Segurança de Redes, Administração de Contas, Continuidade de Negócios.

3.2.2 Implantar controles

Os únicos controles que podem ser planejados e implantados neste momento são os controles mínimos. Entretanto, por ser um projeto de desenho, os controles não foram implantados neste momento. A implantação fica por conta de cada uma das áreas operacionais envolvidas no projeto. Entretanto, é fundamental que seja feita alguma priorização dentro dos controles mínimos definidos. Antes da priorização, os controles foram definidos em dois tipos:

- Controles continuados: possuem uma pré-condição (gatilho) temporal ou não temporal que define quando devem ser executados;
- Controles que demandam ação específica: dependem da realização de melhorias no ambiente de Automação, que são agrupadas em projetos de implantação.

Os controles que demandam ação específica devem ser agrupados em projetos. Para determinar o escopo, extensão, custo e prazo de cada um dos projetos, deve-se antes identificar quais dos controles mínimos já estão preexistentes em cada área operacional (nível azul da Figura 7).

Para identificação dos controles atuais (preexistentes) utilizou-se uma ferramenta de apoio, que é o Cyber Security Evaluation Tool (CSET®), versão 5.0. O CSET é um produto da Divisão Nacional de Segurança Cibernética do Departamento de Segurança Nacional (DHS/NCSD) dos Estados Unidos. A avaliação que a ferramenta provê é realizada através de questionamentos baseados em requisitos das normas de referência. O CSET fornece um banco de normas de referência que podem ser empregadas nesta atividade.

Neste projeto, a avaliação foi realizada considerando a norma de referência “NIST SP800-82: Guia para Segurança de Sistemas de Controle Industriais”, que é uma das principais normas de referência acerca de segurança da informação para infraestrutura crítica. Esta norma identifica atividades e controles típicos. Da mesma forma que a análise de riscos de alto nível, a avaliação do CSET foi realizada para todas as áreas operacionais.

Vale reforçar que como a própria norma NIST SP800-82 menciona, ela não deve ser interpretada como um *checklist* para a implantação de controles de segurança. Não é desejável que todos os controles desta norma sejam implantados. O resultado deste trabalho deve ser avaliado em conjunto com uma análise de riscos que irá direcionar os controles necessários de acordo com os requisitos do negócio.

Após a classificação das ações, é necessária a priorização das ações, de forma que a ordenação da implantação ao longo do tempo reflita as percepções globais de custo e benefício.

Para tanto, as ações foram priorizadas considerando os seguintes critérios:

- Nível dos riscos mitigados: foram avaliados quais riscos são mitigados para cada controle. As ações cujos controles mitigam mais riscos e com maior efetividade tendem a ser priorizadas;
- Estimativa de CAPEX: as ações com menor custo inicial de implantação tendem a ser priorizadas. A dimensão financeira poderia ser avaliada com outros mecanismos de engenharia econômica, como a Taxa Interna de Retorno (TIR) que envolvem, além do custo inicial, o retorno esperado com cada ação;
- Duração estimada do projeto: as ações com menor duração tendem a ser priorizadas;

- Dependências de outras áreas: as ações que dependem menos do envolvimento de outras áreas internas da organização (ex: manutenção, operação, segurança patrimonial e TI) tendem a ser priorizadas.

O coeficiente de priorização de cada ação é a soma da pontuação para cada um dos critérios acima. Ações prioritárias (com alta pontuação) são alocadas para serem implantadas no curto prazo, por exemplo, no próximo ciclo orçamentário. Ações não prioritárias (com baixa pontuação) são alocadas para o médio ou longo prazo.

3.3 Estabelecer Normas, Organização e Conscientização

A Figura 8 representa as tarefas da atividade “Estabelecer normas, organização e conscientização” da Figura 4.

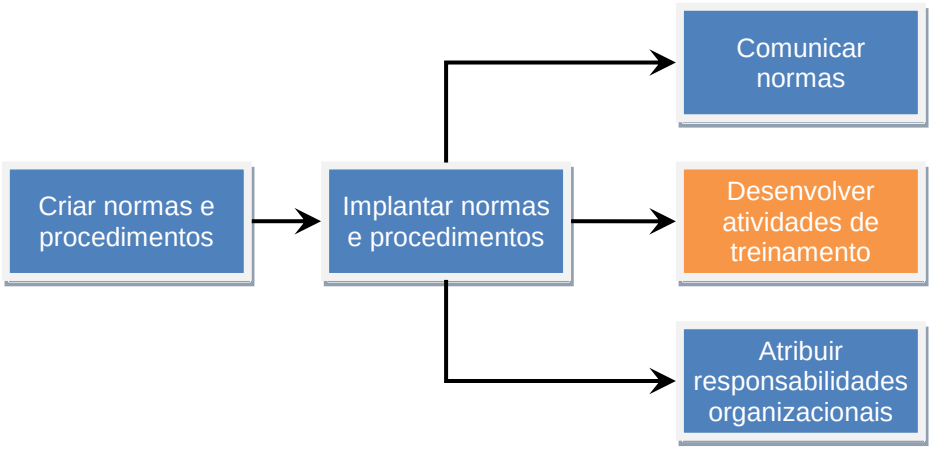

Figura 8. Tarefas para estabelecimento de normas, organização e conscientização

No ambiente de TA, tradicionalmente costuma-se dar muito foco em controles tecnológicos de segurança quando possíveis métodos de mitigação encontram-se voltados para pessoas e processos (ver Figura 9). A ISA-99 entende isto e criou uma atividade única para o desenvolvimento destas ações.
Para tanto, dentro do projeto de desenho do Programa de Cyber Security para Sistemas de Automação Industrial da Vale foram executados treinamentos visando essencialmente à capacitação e conscientização, com enfoque neste último. Há pessoas no ambiente de automação que ainda possuem visões clássicas acerca de segurança da informação e mantém certos mitos sobre o assunto:

- Segurança da informação trata-se apenas de se proteger contra *hackers*;
- *Hardware* dos IACS é imune a incidente de segurança, tais como código malicioso e intrusão;
- O ambiente de automação da minha empresa não está interligado ao ambiente corporativo ou a Internet e, por este motivo, não está exposto a nenhuma ameaça de segurança.

O foco destes treinamentos é mostrar a real pertinência do tema de segurança em automação a fim de que o Programa de Cyber Security seja encarado como algo de valor para a Vale. Além disso, é fundamental que se deixe claro que implantar este programa em várias áreas operacionais concomitantemente é um desafio demanda o engajamento de todas as áreas no mesmo nível.

Figura 9. Fatores organizacionais para segurança da informação

4 CONCLUSÃO

As seções anteriores descreveram as boas práticas para a concepção e desenho do Programa de Cyber Security para Sistemas de Automação Industrial da Vale, considerando as especificidades deste desafio para uma grande companhia. Este trabalho deve continuar ainda a ser executado a posteriori nas etapas de implantação e monitoramento, de acordo com as atividades destacadas na Figura 10.

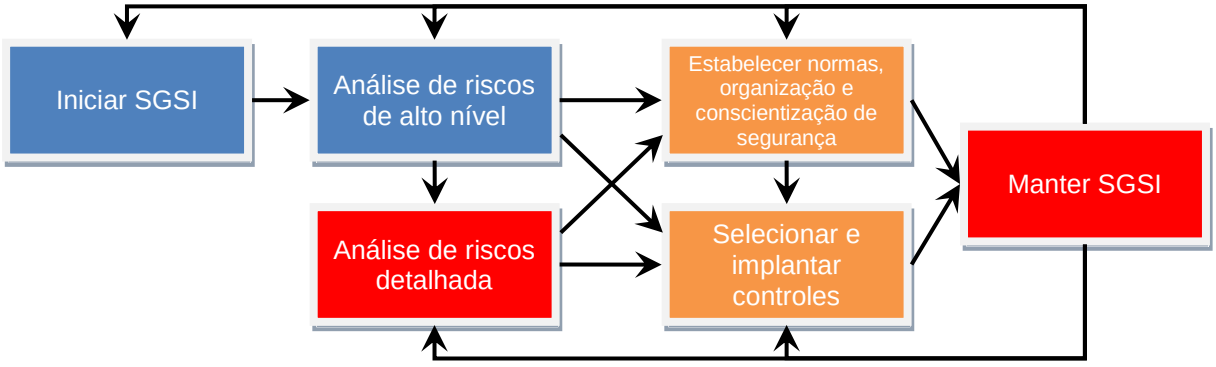

Figura 10. Atividades para um SGSI segundo ISA-99.02.01: Perspectivas futuras

A etapa de implantação é de responsabilidade de cada uma das áreas operacionais. É dever de cada uma destas:

- Análise de Riscos Detalhada: diferentemente da análise de riscos de alto nível que considera riscos criados a partir de ameaças e grupos de ativos, a análise de riscos detalhada engloba a identificação de vulnerabilidades e ameaças diretamente para cada um dos ativos do parque instalado de automação;
- Estabelecer Normas, Organização e Conscientização: complementarmente aos treinamentos realizados na etapa de desenho, devem ser definidas os papeis e responsabilidades sobre a segurança da informação em cada área.

Recomenda-se fortemente um projeto de Governança e Gestão de Serviços para suportar a evolução da organização interna;

- Selecionar e Implantar Controles: a partir da análise de riscos detalhada e das normas definidas, devem ser selecionados os controles complementares aos controles mínimos definidos na etapa de desenho. Além disso, os controles suplementares devem ter sua implantação também planejada e realizada;

A última etapa, após a implantação, envolve a criação de mecanismos de monitoramento, através da atividade “Manter SGSI” da Figura 10. Recomenda-se fortemente a adoção de uma estratégia uniforme entre as áreas operacionais no monitoramento de maneira a assegurar a evolução homogênea do Programa de Cyber Security entre as áreas. Para executar o monitoramento, podem ser utilizadas as seguintes estratégias:

- Auditorias de segurança: visa verificar se o gerenciamento da segurança está sendo realizado conforme previsto nos controles mínimos e processos de gestão definidos. Além disto, checa se os controles implantados ainda cumprem seus objetivos ou já estão degradados. Recomenda-se o uso da estrutura corporativa de auditoria, quando capacitada;
- Indicadores e relatórios: podem ser criados indicadores que avaliam a aderência a normas de referência (benchmark) e relatórios para monitoramento da evolução dos principais riscos;
- Infraestrutura para resposta a incidentes: uma infraestrutura centralizada e corporativa, envolvendo tecnologias, pessoas e processos para prestar suporte às áreas operacionais no ambiente de TA quando da ocorrência de incidentes de segurança da informação.

REFERÊNCIAS

1 The International Society of Automation. ANSI/ISA-99.00.01: Security for Industrial Automation and Control Systems – Part 1: Terminology, Concepts and Models. 2007.
2 Abrams M, Weiss J. Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia. 2008. Disponível em: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf.
3 Poulsen, K. Slammer Worm Crashed Ohio Nuke Plant Network. SecurityFocus. 2003. Disponível em: http://www.securityfocus.com/news/6767.
4 Falliere, N, Murchu, L, Chien E. W32.Stuxnet Dossier. Symantec. 2011. Disponível em: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
5 Soares, M. Brazilian Blackout Traced to Sooty Insulators, Not Hackers. Wired. 2009. Disponível em: http://www.wired.com/2009/11/brazil_blackout/.
6 The International Society of Automation. ANSI/ISA-99.02.01: Security for Industrial Automation and Control Systems – Establishing an Industrial Automation and Control Systems Security Program. 2007.
7 National Institute of Standards and Technology. NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security. 2011.
8 National Institute of Standards and Technology. NIST Special Publication 800-27. Engineering Principles for Information Technology Security (A Baseline for Achieving Security. 2004.

* *Contribuição técnica ao 18° Seminário de Automação e TI Industrial, 23 a 26 de setembro de 2014, São Paulo, SP, Brasil.*