SEGURANÇA CIBERNÉTICA INTEGRADA NA INDÚSTRIA 4.0*

José Maurício dos Santos Pinheiro[1]

Resumo
É cada vez maior o número de corporações que desenvolvem seus negócios baseados nas novas tecnologias de informação e na Internet. Neste contexto, a segurança cibernética configura-se paradoxalmente como um custo e uma necessidade para a sobrevivência de uma corporação. Obter um sistema mais seguro e protegido contra vírus, invasões pela Internet e atos de espionagem ou sabotagem hoje é visto como algo de valor significativo. A segurança cibernética deve ser tomada como opção estratégica e não apenas tecnológica ou gerencial, com impacto positivo e inegável sobre o negócio, estando relacionada ao conjunto das medidas que visam dotar as redes industriais com capacidade de inspeção, detecção, reação e reflexo aos potenciais ataques, permitindo reduzir e limitar as vulnerabilidades e o impacto quando estes se concretizam. Este artigo busca apresentar a importância das soluções integradas de segurança no ambiente das redes no conceito de Indústria 4.0.
Palavras-chave: Segurança cibernética; Ameaças; Ataques; Indústria 4.0

INTEGRATED CYBER SECURITY IN 4.0 INDUSTRY

Abstract
More corporations are developing their businesses based on new information technologies and the Internet. In this context, cyber security is paradoxically configured as a cost and a necessity for the survival of a corporation. Getting a system more secure and protected from viruses, Internet intrusions and acts of espionage or sabotage today is seen as something of significant value. Cyber security should be taken as a strategic option, not only technological or managerial, with a positive and undeniable impact on the business, being related to all the measures aimed at providing industrial networks with capacity for inspection, detection, reaction and reflection to potential attacks , allowing to reduce and limit vulnerabilities and their impact when they materialize. This article seeks to present the importance of integrated security solutions in the network environment in the concept of Industry 4.0.
Keywords: Cyber security; Threats; Attacks; Industry 4.0.

[1] *Pós-Graduação em Gerência e Segurança de Redes de Computadores pelo UniFOA, Professor do Centro Universitário de Barra Mansa - UBM, Barra Mansa, Rio de Janeiro, Brasil.*

1 INTRODUÇÃO

A revolução industrial caracterizou mudanças profundas nos paradigmas dos sistemas de produção que alteram toda a forma como os produtos eram fabricados, valorados e consumidos. A primeira revolução industrial, ocorrida entre os séculos XVIII e XIX, determinou o fim do trabalho artesanal e o início de uma manufatura impulsionada pelas máquinas e motores a vapor. A segunda revolução industrial introduziu novos tipos de produtos, com o setor automobilístico como seu maior exponencial. A informática e a microeletrônica são os atores que alavancam a terceira revolução industrial e com os sistemas computadorizados e seus microprocessadores, as indústrias incorporaram robôs capazes de executar as tarefas dos operários nas linhas de produção com mais velocidade e menor percentual de erros.
Dois séculos depois de o inglês Edmund Cartwright inventar o tear mecanizado, um dos maiores símbolos da primeira revolução industrial, vivemos um novo período revolucionário, com a conjunção de novas tecnologias digitais, Internet e sistemas de novas manufaturas. O tipo de manufatura que surge nessa quarta revolução é chamada de Indústria 4.0. O termo foi utilizado pela primeira vez em 2011, na Feira de Hannover, na Alemanha, e representa outra ruptura na forma como os produtos são fabricados. A Quarta Revolução Industrial é diferente de tudo o que a humanidade já experimentou. Como mencionado pela FIRJAN [1]:

> A indústria 4.0, também chamada de Quarta Revolução Industrial, é marcada pela era da informação digital. A tecnologia da informação se torna parte integral dos processos industriais, e decisões são tomadas de forma automática a partir do uso de um grande conjunto de dados armazenados, chamado de Big Data.

A Figura 1 ilustra as fases de evolução por que passou a indústria desde o final do século XVIII até a atualidade.

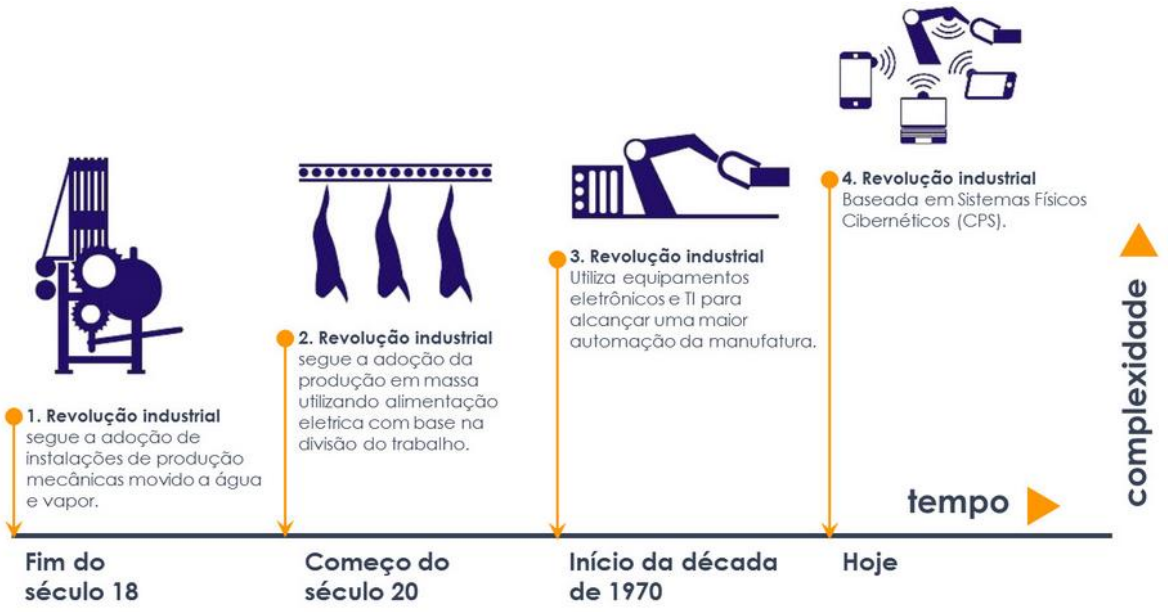

Figura 1 - As Revoluções Industriais

2 CIBERESPAÇO E SEGURANÇA CIBERNÉTICA

Há algumas décadas, o ambiente industrial era isolado do ambiente corporativo. Entretanto, com a evolução tecnológica, hoje é uma realidade a interligação desses dois ambientes e o compartilhamento de informações entre um e outro levanta uma série de questões de segurança que antes eram exclusivos do ambiente corporativo, tais como a exploração de falhas de programação, ataques a serviços, acessos não autorizados, introdução de vírus e outros tipos de vulnerabilidades e ameaças tanto na rede local quanto na rede industrial.

O ciberespaço está intrinsecamente associado com a Internet, mas não exclusivamente. Ele também se refere a qualquer forma de comunicação de computador para computador numa rede local (LAN). A segurança cibernética ou cyber segurança entra nesse contexto tratando de ameaças e ataques nas redes locais e Internet e incluindo os controles defensivos que são necessários para lidar com as ameaças e os riscos provenientes de cyber espaço. A grande maioria desses controles são de natureza técnica, mas isso não quer dizer que eles são exclusivamente técnicos. Treinamento e educação, pessoal habilitado e gestão de incidentes podem ser abordados pela segurança cibernética, que também considera as medidas defensivas para dissuadir e impedir as intenções dos atacantes, mas enfoca nas ações técnicas de desenvolvimento, servidores, banco de dados, redes, firewalls não atingindo a esfera estratégica.

A existência de problemas de configuração de equipamentos ou de serviços são aspectos que podem facilitar acessos indevidos a recursos da rede industrial e por esse motivo também podem ser abordados pela segurança cibernética. Como exemplo, citam-se a habilitação de serviços que não são utilizados na operação da planta industrial, a colocação de regra de firewall que não funciona de acordo com o que foi planejado ou um roteador ou gateway mal configurado fazendo a divulgação indesejada de uma determinada rota da rede.

Outra forma de expor a rede industrial aos riscos de segurança é permitir a utilização abusiva de seus recursos. Isso se dá, por exemplo, através da utilização não autorizada de espaço em disco para armazenar e disponibilizar arquivos ou software de procedência duvidosa ou ainda, permitir acessos físicos para a colocação em rede de equipamentos não autorizados. Pode-se citar também a utilização de serviços da rede para o envio de mensagens eletrônicas automáticas não solicitadas (spam), o uso de jogos eletrônicos através da rede e a utilização de programas P2P (Peer-to-Peer).

Outros fatores, menos técnicos, mas também relevantes, podem levar a comprometimentos de segurança da rede industrial. Um deles, de origem interna, consiste no abuso de privilégios. Esse fator pode possibilitar a um usuário ter acesso a informações com nível de privilégio maior do que aquele lhe é facultado. Deve-se levar em consideração também a possibilidade da existência de profissionais insatisfeitos, mal-intencionados ou que estejam a serviço de outra corporação praticando espionagem industrial. Não se pode deixar de considerar o roubo, puro e simples, de equipamentos com informações sensíveis e a utilização de técnicas de engenharia social como forma de obter informações que podem comprometer a segurança. Mitnick e Simon [2] enfatizam:

> A medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano.

2.1 SEGURANÇA CIBERNÉTICA NA INDÚSTRIA

No início da automação não havia preocupação com ameaças e ataques, uma vez que não havia uma rede formalizada e os dados estavam disponíveis apenas localmente nos dispositivos. No entanto, com a natural evolução tecnológica e convergência dos processos, passamos a ter redes industriais conectadas ao ambiente corporativo e ao mundo externo através Internet e serviços em nuvem, abrindo brechas de segurança que antes não existiam nas plantas industriais.
As redes industriais apresentam características próprias que trazem consigo vulnerabilidades de segurança, como protocolos de baixo nível de segurança, redes de controle sem segmentação, sistemas operacionais sem atualização, ausência de criptografia ao nível de rede, dificuldade de se obter Log's dos sistemas de automação, entre outros.
É notório o crescimento das invasões a plantas industriais e no que se refere a segurança de dados, podemos ter inúmeros cenários de ataque que desafiam os profissionais de segurança. Os ataques podem ocorrer por meio de um programa que pode ser instalado dentro do sistema (hospedeiro), de forma intencionada ou não, a partir de uma unidade portátil como um pendrive, por exemplo, ou um e-mail com anexo. Uma vez instalado (e executado), o programa atua no interior da rede de comunicação, permitindo ao atacante monitorar externamente os processos, copiar dados, trocar parâmetros da planta, entre outros.
Uma solução eficiente em segurança corporativa envolve conhecimento do negócio do cliente, tecnologia e, principalmente, conscientização e capacitação dos profissionais. De acordo com Dawel [3]:

> Na prática, é impossível prever todas as possibilidades de fraudes e ataques contra a corporação. É comum encontrar empresas que estabelecem controles indiscriminados, esperando com isso obter maior produtividade.

É importante reconhecer a importância do elemento humano nos ambientes computacionais e torná-lo peça da solução de segurança, uma vez que o ser humano é invariavelmente o elo mais fraco da cadeia de segurança e sobre ele devem recair os principais cuidados durante as fases de especificação, implantação e gestão de sistemas de segurança. Tal cuidado poderá possibilitar o desenvolvimento de uma cultura de prevenção sistemática dos problemas, valorização dos princípios éticos e de responsabilidade no trabalho, além da própria disseminação do conhecimento sobre o tema.

2.2 IMPACTOS DOS ATAQUES

Os impactos dos ataques variam entre consequências mais simples de mensurar, como operações comerciais interrompidas, até a perdas que são mais difíceis de calcular, como prejuízos ao nome da corporação. Falhas na rede de comunicação, perda de informações por motivos diversos, disseminação de vírus e roubo de informações pela Internet, sabotagem, espionagem industrial, entre outros, são alguns dos fatores que os profissionais da área de segurança cibernética precisam observar, definindo estratégias de atuação e implantando medidas de recuperação eficazes. Segundo Ferreira e Araújo [4]:

A classificação da informação é o processo de estabelecer o grau de importância das informações mediante seu impacto no negócio. Ou seja, quanto mais importante, estratégica e decisiva para a manutenção ou sucesso da organização, maior será sua importância. Sua aplicação deve ser realizada a todo instante, em qualquer meio de armazenamento.

Por exemplo, a integração entre as aplicações SCADA, essencialmente voltadas para a supervisão e o controle de processos, e as redes corporativas, com foco no processamento, armazenamento e recuperação de informações, incorpora alguns problemas relacionados com segurança que podem alterar ou interromper a operação de processos críticos que são supervisionados e controlados pelos sistemas SCADA. Assim, os eventuais problemas de segurança, antes restritos a cada um dos ambientes de rede, passam a ser compartilhados. Outras consequências dos ataques podem incluir:

- **Interrupção das operações** - resultam em perda da produtividade e da receita, e os custos associados à restauração da rede podem aumentar o impacto financeiro geral. Não somente a produção é interrompida até que uma correção seja implementada; como a equipe técnica é retirada de suas tarefas de rotina, existe uma perda de produtividade;
- **Responsabilidade legal e litígio** - corporações que necessitam cumprir com regulamentos de privacidade ou segurança devem demonstrar sua devida diligência minimizando sua exposição a ataques de rede. Esse processo é uma drenagem na produtividade e no fluxo de caixa da corporação;
- **Capacidade reduzida de competição** – a informação é considerada um dos bens mais valiosos de uma corporação e uma boa parte do seu valor reside nos seus bens de propriedade intelectual; a perda ou roubo da informação podem causar sérias consequências, até a retribuição indefensável da posição de mercado;
- **Dano à qualidade da marca** – os danos podem assumir várias formas, cada uma delas capaz de degradar a posição da corporação no mercado. A corporação poderá ter uma grande dificuldade em restaurar a confiança dos clientes na sua marca.

3 SEGURANÇA INTEGRADA NA INDÚSTRIA 4.0

As soluções de segurança atuais são normalmente compostas por vários produtos, resultando muitas vezes em falta de interoperabilidade entre eles, dificuldade de gerenciamento e alto custo de propriedade. A segurança integrada combina as várias tecnologias de segurança com compatibilidade de política, gerenciamento de cliente, serviço e suporte, e pesquisa avançada para a proteção completa.
Adotar uma estratégia que lida com a segurança em cada nível da rede permite as organizações reduzir custos, melhorar o gerenciamento dos ativos, melhorar o desempenho dos sistemas, aumentar a segurança e reduzir o risco de exposição da rede como um todo.
São três os aspectos básicos que um sistema de segurança integrada deve atender para uma abordagem mais efetiva no raio máximo de custo-benefício, comparado às implementações de segurança de vários produtos em separado e evitar a concretização de ameaças e ataques às redes industriais: Prevenção, Detecção e Recuperação.

3.1 Prevenção

- **Proteção de hardware**: normalmente chamada de segurança física, impede acessos físicos não autorizados à infraestrutura da rede, prevenindo roubos de dados, desligamento de equipamentos e demais danos quando se está fisicamente no local;
- **Proteção de arquivos e dados:** proporcionada pela autenticação, controle de acesso e sistemas antivírus. No processo de autenticação, é verificada a identidade do usuário; o controle de acesso disponibiliza apenas as transações pertinentes ao usuário e os programas antivírus garantem a proteção do sistema contra programas maliciosos;
- **Proteção de perímetro:** ferramentas de firewall e roteadores cuidam desse aspecto, mantendo a rede protegida contra tentativas de intrusão (interna e externa à rede).

3.2 Detecção

- **Alertas:** sistemas de detecção de intrusões alertam os responsáveis pela segurança sobre qualquer sinal de invasão ou mudança suspeita no comportamento da rede que possa significar um padrão de ataque. Os avisos podem ser via e-mail, mensagem no console de gerência, celular etc.;
- **Auditoria:** periodicamente deve-se analisar os componentes críticos do sistema a procura de mudanças suspeitas. Esse processo pode ser realizado por ferramentas que procuram, por exemplo, modificações no tamanho dos arquivos de senhas, usuários inativos etc.

3.3 Recuperação

- **Cópia de segurança dos dados (Backup)**: manter sempre atualizados e testados os arquivos de segurança em mídia confiável e separados física e logicamente dos servidores;
- **Aplicativos de Backup**: ferramentas que proporcionam a recuperação rápida e confiável dos dados atualizados em caso da perda das informações originais do sistema;
- **Backup do Hardware**: a existência de hardware reserva, fornecimento autônomo de energia, linhas de dados redundantes etc., podem ser justificados levando-se em conta o custo da indisponibilidade dos sistemas.

As camadas do gateway, servidores e estações de trabalho estão interconectadas para atender às necessidades da corporação, o que significa que as informações críticas do negócio podem ser encontradas em vários níveis na rede interna, onde cada nível requer um grau de proteção específico. Enquanto o enfoque tradicional está em uma segurança centralizada da base de dados, agora é preciso lidar com as definições sempre em expansão do alcance de rede e com os requisitos de segurança correspondentes. Ao mesmo tempo, as ameaças à rede industrial têm se tornando cada vez mais sofisticadas. Os ataques empregam vários meios de propagação, assim como descobrem e exploram as vulnerabilidades.
Do ponto de vista da segurança corporativa, os objetivos executivos de um sistema de segurança integrada incluem o seguinte:

- Implementação de soluções que garantam infraestruturas de rede seguras e robustas para proteger os bens e informações e garantir a continuidade do negócio;
- Manutenção dos requisitos de operação, como alta disponibilidade de rede, integridade dos dados e privacidade, e as ameaças de segurança correspondentes;
- Obtenção dos requisitos de registro, relatório, auditoria e compatibilidade;
- Mediação desses desafios com recursos limitados a um custo mais baixo;
- Seleção das soluções que maximizem a produtividade, administração e gerenciamento das soluções de segurança.

Soluções integradas de segurança devem permitir a criação de um fluxo de informações entre os diversos níveis funcionais através da integração dos recursos computacionais de forma eficiente e segura, o que virá possibilitar aumento na produtividade, melhorias da qualidade dos serviços internos, agilidade nas transações e aumento da competitividade. Neste contexto, devem ser escolhidas ferramentas eficazes e sintonizadas com o negócio, buscando sempre a maximização dos investimentos na área de rede. Tais ferramentas devem prover condições que permitam uma abordagem ampla dos problemas e oferecer soluções que vão desde o planejamento estratégico até a implantação e gestão dos sistemas computacionais. Segundo Peixoto [5]:

> Programar diversos mecanismos de identificação, autorização, armazenamento de dados, sistemas de auditoria, inspeção e checagem ajudam. E devem ser levados em conta, para que haja maior segurança quanto à exposição involuntária ou não de informações pessoais e técnicas, enfim, confidenciais.

A segurança integrada deve fornecer uma estrutura de segurança holística e completa que combina várias tecnologias de segurança com compatibilidade de política, gerenciamento, serviço e suporte, e pesquisa avançada para a proteção completa. Ele usa funções de segurança complementares em vários níveis dentro da infraestrutura da rede.
Através da combinação de várias funções, a segurança integrada pode proteger com mais eficiência contra uma variedade de ameaças em cada nível para minimizar os efeitos dos ataques de rede. As tecnologias de segurança principais que podem ser integradas incluem:

- **Firewalls** - controlam o tráfego de rede através da verificação das informações que entram e saem da rede visando garantir que nenhum acesso não autorizado a computadores e/ou a rede ocorra;
- **Detecção de Intrusão** - detecta o acesso não autorizado e fornece alertas e relatórios que podem ser analisados para políticas e planejamento;
- **Filtragem de conteúdo** - identifica e corrige o tráfego não desejado de informações;
- **Rede Privada Virtual (VPN)** - assegura as conexões além do perímetro, permitindo que organizações se comuniquem com segurança com outras pela Internet;
- **Gerenciamento de vulnerabilidades** - permite a avaliação da posição de segurança da rede descobrindo falhas de segurança e sugerindo melhorias;

- **Antivírus** – proteção contra vírus, worms, cavalos de tróia e outros tipos de malwares.

Individualmente, essas tecnologias de segurança podem ser complexas para instalar e geralmente são difíceis e caras para gerenciar e atualizar. Entretanto, quando integradas em uma solução única, elas oferecem uma proteção completa enquanto a complexidade e o custo são reduzidos.
Na maioria das corporações, uma variedade de produtos de segurança, de diferentes fornecedores, é implementada à medida que a necessidade de segurança da rede cresce. Migrar gradualmente para uma solução de segurança integrada permite garantir a interoperabilidade e a integração desses diferentes produtos de segurança em cada nível da rede. Essa abordagem envolve inicialmente a integração de um subconjunto de funções de segurança:

- Criar times específicos de segurança para identificar e avaliar os possíveis cenários de ataque. Esses times devem identificar situações de ataque e avaliar as vulnerabilidades potenciais dos sistemas. O time deve ser multidisciplinar, o que possibilita fornecer pareceres sobre os pontos fracos da rede local, sistemas supervisórios e de aquisição de dados, sistemas físicos e controles de segurança.
- Documentar a arquitetura de rede e identificar os sistemas que servem as funções críticas ou que contenham informações confidenciais que exigem níveis adicionais de proteção. Desenvolver e documentar uma arquitetura de segurança robusta como parte do processo para estabelecer a efetiva estratégia de proteção das informações. Sem essa compreensão, os riscos não podem ser devidamente avaliados e as estratégias de proteção podem não ser suficientes. Documentar a arquitetura de segurança da informação e dos componentes é fundamental para a compreensão da estratégia de proteção global e identificação dos pontos de falha;
- Estabelecer uma estratégia de proteção de rede com base no princípio da defesa em profundidade. Essa filosofia deve ser considerada no início da fase de concepção do processo de desenvolvimento e deve ser parte integrante nas tomadas de decisão técnicas associadas à rede. Utilizar os controles técnicos e administrativos para reduzir as ameaças e riscos identificados e os pontos de falha devem ser evitados;
- Estabelecer processos eficazes de gerenciamento de configuração e manter um processo de gestão da configuração de ativos. O gerenciamento de configuração deve abranger as configurações de hardware e software, uma vez que alterações poderão introduzir vulnerabilidades que comprometam a segurança da rede. Os processos são necessários para avaliar e controlar qualquer mudança para assegurar que a rede continue segura;
- Realizar autoavaliações de rotina e processos de avaliação de desempenho, que são necessárias para fornecer às organizações feedback sobre a eficácia da política de segurança cibernética e sua execução técnica. Processos de autoavaliação são parte de um programa eficaz de segurança cibernética e incluem a digitalização da rotina em busca de vulnerabilidades, de auditoria automatizada da rede, e autoavaliações do desempenho organizacional e desempenho individual;
- Estabelecer backups dos sistemas e planos de recuperação de desastres que permitem a recuperação rápida de qualquer emergência (incluindo um ataque

cibernético). Backups do sistema são uma parte essencial de qualquer plano para permitir a reconstrução rápida da rede. Rotineiramente exercer recuperação de desastres e testar os planos para assegurar que eles trabalham e que o pessoal estará familiarizado com eles;

- Estabelecer um programa de segurança, a fim de criar a cultura de segurança e treinar e capacitar os colaboradores a não divulgarem de forma inadvertida informações confidenciais a respeito dos sistemas, seja de design, operações ou dos controles de segurança, conforme mostra a Figura 2.

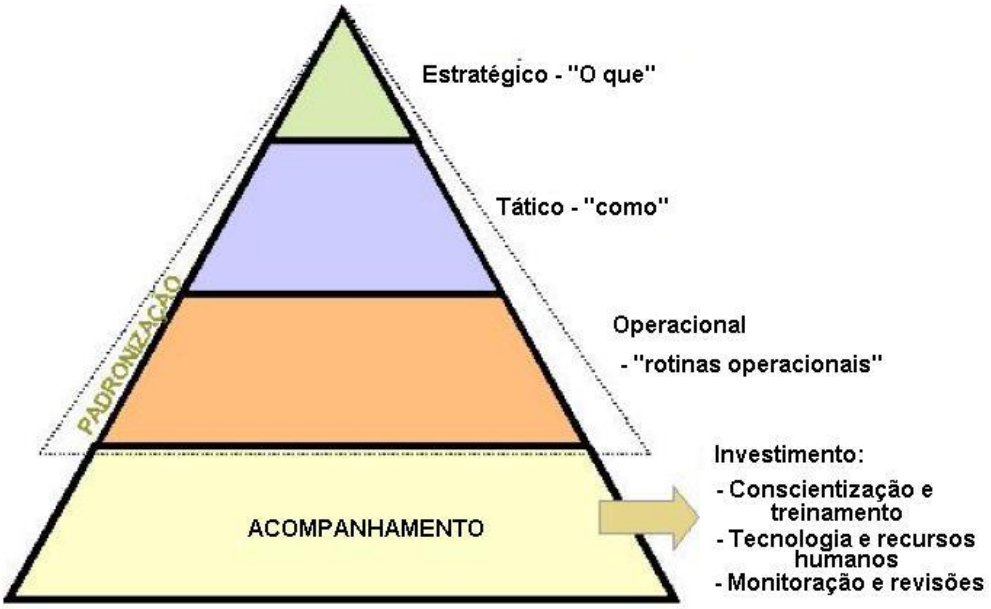

Figura 2 – Estrutura de um programa de segurança e procedimentos estruturados

Conforme a NBR ISO/IEC 17799 [6]:

> Muitos sistemas de informação não foram projetados para serem seguros. A segurança que pode ser alcançada por meios técnicos é limitada e convém que seja apoiada por gestão e procedimentos apropriados. A identificação de quais controles convém que sejam implantados requer planejamento cuidadoso e atenção aos detalhes.

4 BENEFÍCIOS DA SEGURANÇA INTEGRADA

A segurança integrada reduz a necessidade de compra, instalação, atualização e gerenciamento de vários produtos de segurança de diferentes fornecedores, ou gerenciamento de questões de interoperabilidade entre produtos de vários fornecedores em cada nível de rede. Com a redução e otimização dos recursos, permite a realocação do pessoal técnico para projetos estratégicos, maximizando a produtividade do departamento do time de tecnologia, melhorando o gerenciamento de segurança no geral.

Considerando que uma solução de segurança integrada pode ser implementada em todos os níveis da rede, ela oferece maior proteção dos bens de propriedade. Ao aplicar uma abordagem uniforme aos sistemas e dispositivos que contêm bens de informações sensíveis e de negócios críticos, as organizações podem garantir a atualização integrada de arquivos de padrão de vírus, assinaturas de detecção de intrusão, configurações de firewall e outros aspectos críticos de um sistema de segurança.

É importante salientar que a segurança cibernética, mais que um problema de utilização de tecnologias, deve ser encarada como a gestão inteligente da informação, priorizando recursos e focando os investimentos no ambiente em que está inserida.

4 CONCLUSÃO

A tecnologia em si não lida com as questões de segurança. A segurança, mais que simples produto ou tecnologia que se pode adquirir, aplicar e esquecer, mais do que um supressor de sintomas é um processo contínuo e abrangente, com implicações em todas as áreas, desde a alta direção até os usuários que executam operações cotidianas elementares, devendo ser encarada como um facilitador dos processos e como forma de aumentar os níveis de confiança internos e externos. Assim, uma solução de segurança integrada funciona melhor quando criada com base em políticas e procedimentos rígidos, e suplementada pelo pessoal e medidas de segurança físicas apropriados.

Uma estratégia de segurança integrada melhora a postura de segurança geral da rede de uma forma não possível através da implementação de produtos individuais de vários fornecedores diferentes. Através de integração de segurança em todos os níveis da rede, os recursos do administrador serão otimizados, já que a instalação, relatório e atualizações serão possíveis a partir de um único console. Esse recurso de gerenciamento mais adiante melhorará a proteção, enquanto reduzirá os custos administrativos, de suporte e de propriedade normalmente associados à segurança da corporação.

Independente da segurança ser gerenciada no local ou ser terceirizada, a garantia de que todos esses recursos estejam implementados é vital para a manutenção de uma infraestrutura crítica de segurança.

REFERÊNCIAS

1. FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DO RIO DE JANEIRO - FIRJAN. **Indústria 4.0: Internet das Coisas**. FIRJAN Publicações, 2016.
2. MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar** - **ataques de hackers: controlando o fator humano na segurança da informação**. São Paulo: Pearson Education do Brasil Ltda, 2003.
3. DAWEL, George. **A Segurança da Informação nas Empresas**. Rio de Janeiro: Editora Ciência Moderna Ltda, 2005.
4. FERREIRA, Fernando Nicolau Freitas, ARAÚJO, Marcio Tadeu. **Política de Segurança da Informação: Guia Prático para Embalagem e Implementação**. Rio de Janeiro: Editora Ciência Moderna Ltda, 2006.
5. PEIXOTO, Mário César Pintaudi. **Engenharia Social & Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006
6. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799: Tecnologia da Informação - Código de Prática para a Gestão da Segurança da Informação**. Rio de Janeiro, 2001.