Agencia Nacional de Vigilância Sanitária e a ISO 17.799[1]

Alexandre Vieira Silva, Alexey Monteiro, André Oliveira, Euler Pereira Pinto, Juliano Costa, Roseli Petry.[2]

Resumo

Este artigo tem como objetivo mostrar como o sistema corporativo da Agência Nacional de Vigilância Sanitária – ANVISA, está sendo tratado em relação aos padrões da norma ISO 17.799. Serão abordados os três pilares da segurança da informação: confidencialidade, Integridade e disponibilidade.

Palavras Chave

Sistema de Informação (S.I.); Tecnologia da Informação (T.I.); ISO; Gerenciamento; Segurança da Informação.

National Healthy and Surveillance Agency and ISO 17.799

Summary

This article have the main purpose to show how corporate systems of National Healthy and Surveillance Agency – ANVISA, has been treated following the standards of the ISO 17.799. The three bases of information security will be shown: confidentiality, integrity and availability.

Keywords

Information System (IS); Information Technology (TS); ISO; Management; Security Information.

[1] Artigo desenvolvido na pós graduação da Universidade Católica de Brasília.
[2] Alunos do 1º semestre do MBA em Gestão de Sistemas de Informação.

1. Introdução

Os altos índices de informatização, conectividade e negócios pela Internet e o compartilhamento de dados tornaram a informação um dos bens mais valiosos e mais vulneráveis das empresas. Com isso, incidentes nas redes de computadores passaram a afetar diretamente os resultados do negócio e a credibilidade das empresas.

Muitas vezes a preocupação com segurança não é o foco das organizações, desta forma a possibilidade da ocorrência de incidentes aumenta. As pesquisas indicam que os principais responsáveis por esses incidentes são os usuários internos, aqueles que são funcionários, ou que possuem algum tipo de conexão com a rede corporativa.

Os serviços WEB são, atualmente, fundamentais para a conectividade entre as empresas e seus clientes. Entretanto estes pontos são extremamente vulneráveis, pois não posuem fronteiras nem limites, e são os alvos preferidos pelos *hackers* e suas variações.

Com o passar do tempo, os ataques e tentativas de invasão vêm aumentando gradativamente. Cada dia, surgem novas tecnologias de softwares, e posteriormente novas vulnerabilidades são encontradas e exploradas a fim de denegrir a imagem da corporação.

A Agência Nacional de Vigilância Sanitária – ANVISA, também está sujeita aos ataques, pois além de sua característica de corporação, é uma autarquia federal, ligada ao Ministério da Saúde e ao Governo Federal. Desta forma, os ataques, se bem sucedidos, contra a agência promovem a não credibilidade desta.

Este artigo é composto da descrição da ANVISA, na seção 02, onde serão apresentadas sua missão, valores, visão, competências, atribuições e um exemplo de um dos sistemas corporativos. Na seção 03 as principais características da norma ISO 17.799 detalhando os princípios da: confidencialidade, Integridade e disponibilidade; e sua aplicação nos procedimentos da ANVISA.. E a conclusão deste artigo na seção 04.

2. ANVISA – Agência Nacional de Vigilância Sanitária

A Agência Nacional de Vigilância Sanitária foi criada pela Lei nº 9.782, de 26 de janeiro de 1999. É uma autarquia sob regime especial, ou seja, uma agência reguladora caracterizada pela independência administrativa, estabilidade de seus dirigentes durante o período de mandato e autonomia financeira. A gestão da Anvisa é responsabilidade de uma Diretoria Colegiada, composta por cinco membros. Na estrutura da Administração Pública Federal, a Agência está vinculada ao Ministério da Saúde, sendo que este relacionamento é regulado por Contrato de Gestão.

A finalidade institucional da Agência é promover a proteção da saúde da população por intermédio do controle sanitário da produção e da comercialização de produtos e serviços submetidos à vigilância sanitária, inclusive dos ambientes, dos processos, dos insumos e das tecnologias a eles relacionados. Além disso, a Agência exerce o controle de portos, aeroportos e fronteiras e a interlocução junto ao Ministério das Relações Exteriores e instituições estrangeiras para tratar de assuntos internacionais na área de vigilância sanitária.

Sua missão é: proteger e promover a saúde da população garantindo a segurança sanitária de produtos e serviços e participando da construção de seu acesso. Tendo como valores: conhecimento como fonte da ação, transparência, cooperação e responsabilização. Visando ser agente da transformação do sistema descentralizado de vigilância sanitária em uma rede, ocupando um espaço diferenciado e legitimado pela população, como reguladora e promotora do bem-estar social.

A ANVISA tem como sua competência:

- Coordenar o Sistema Nacional de Vigilância Sanitária;
- Fomentar e realizar estudos e pesquisas no âmbito de suas atribuições;
- Estabelecer normas, propor, acompanhar e executar as políticas, as diretrizes e as ações de vigilância sanitária;
- Estabelecer normas e padrões sobre limites de contaminantes, resíduos tóxicos, desinfetantes, metais pesados e outros que envolvam risco à saúde;
- Intervir, temporariamente, na administração de entidades produtoras que sejam financiadas, subsidiadas ou mantidas com recursos públicos, assim como nos prestadores de serviços e ou produtores exclusivos ou estratégicos para o abastecimento do mercado nacional.
- Administrar e arrecadar a Taxa de Fiscalização de Vigilância Sanitária;
- Autorizar o funcionamento de empresas de fabricação, distribuição e importação dos produtos regulados pela agência;
- Anuir com a importação e exportação dos produtos regulados pela agência;
- Conceder registros de produtos, segundo as normas de sua área de atuação;
- Conceder e cancelar o certificado de cumprimento de boas práticas de fabricação;
- Exigir, mediante regulamentação específica, o credenciamento ou a certificação de conformidade no âmbito do Sistema Nacional de Metrologia, Normalização e Qualidade Industrial - SINMETRO, de instituições, produtos e serviços sob regime de vigilância sanitária, segundo sua classe de risco;
- Interditar, como medida de vigilância sanitária, os locais de fabricação, controle, importação, armazenamento, distribuição e venda de produtos e de prestação de serviços relativos à saúde, em caso de violação da legislação pertinente ou de risco iminente à saúde;
- Proibir a fabricação, a importação, o armazenamento, a distribuição e a comercialização de produtos e insumos, em caso de violação da legislação pertinente ou de risco iminente à saúde;
- Cancelar a autorização, inclusive a especial, de funcionamento de empresas, em caso de violação da legislação pertinente ou de risco iminente à saúde;
- Coordenar as ações de vigilância sanitária realizadas por todos os laboratórios que compõem a rede oficial de laboratórios de controle de qualidade em saúde;
- Estabelecer, coordenar e monitorar os sistemas de vigilância toxicológica e farmacológica;
- Promover a revisão e atualização periódica da farmacopéia;
- Manter sistema de informação contínuo e permanente para integrar suas atividades com as demais ações de saúde, com prioridade para as ações de vigilância epidemiológica e assistência ambulatorial e hospitalar;
- Monitorar e auditar os órgãos e entidades estaduais, distritais e municipais que integram o Sistema Nacional de Vigilância Sanitária, incluindo-se os laboratórios oficiais de controle de qualidade em saúde;
- Coordenar e executar o controle da qualidade de bens e de produtos regulados pela agência;

- Fomentar o desenvolvimento de recursos humanos para o sistema e a cooperação técnico-científica nacional e internacional;
- Autuar e aplicar as penalidades previstas em lei;
- Monitorar a evolução dos preços de medicamentos, equipamentos, componentes, insumos e serviços de saúde;
- A Agência poderá delegar, por decisão da Diretoria Colegiada, aos Estados, ao Distrito Federal e aos Municípios a execução de algumas das atribuições de sua competência;
- A Agência poderá assessorar, complementar ou suplementar ações estaduais, do Distrito Federal e municipais para exercício do controle sanitário;
- As atividades de vigilância epidemiológica e de controle de vetores relativas a portos, aeroportos e fronteiras serão executadas pela Agência sob orientação técnica e normativa da área de vigilância epidemiológica e ambiental do Ministério da Saúde;
- A Agência poderá delegar a órgão do Ministério da Saúde a execução de algumas atribuições;
- A Agência poderá dispensar de registro os imunobiológicos, inseticidas, medicamentos e outros insumos estratégicos, quando adquirida por intermédio de organismos multilaterais internacionais, para uso em programas de saúde pública pelo Ministério da Saúde e suas entidades vinculadas;
- O Ministro de Estado da Saúde poderá determinar a realização de ações previstas nas competências da Agência, em casos específicos e que impliquem risco à saúde da população;

Os bens e produtos controlados pela ANVISA são:

- Medicamentos de uso humano, suas substâncias ativas e demais insumos, processos e tecnologias;
- Alimentos, inclusive bebidas, águas envasadas, seus insumos, suas embalagens, aditivos alimentares, limites de contaminantes orgânicos, resíduos de agrotóxicos e de medicamentos veterinários;
- Cosméticos, produtos de higiene pessoal e perfumes;
- Saneantes destinados à higienização, desinfecção ou desinfestação em ambientes domiciliares, hospitalares e coletivos;
- Conjuntos, reagentes e insumos destinados a diagnóstico;
- Equipamentos e materiais médico-hospitalares, odontológicos, Hemoterápicos e de diagnóstico laboratorial e por imagem;
- Imunobiológicos e suas substâncias ativas, sangue e hemoderivados;
- Órgãos, tecidos humanos e veterinários para uso em transplantes ou reconstituições;
- Radioisótopos para uso diagnóstico in vivo, radiofármacos e produtos radioativos utilizados em diagnóstico e terapia;
- Cigarros, cigarrilhas, charutos e qualquer outro produto fumígero, derivado ou não do tabaco;
- Quaisquer produtos que envolvam a possibilidade de risco à saúde, obtidos por engenharia genética, por outro procedimento ou ainda submetidos a fontes de radiação;

Os serviços controlados pela ANVISA são:

- Aqueles voltados para a atenção ambulatorial, seja de rotina ou de emergência, os realizados em regime de internação, os serviços de apoio diagnóstico e

terapêutico, bem como aqueles que impliquem a incorporação de novas tecnologias;

- As instalações físicas, equipamentos, tecnologias, ambientes e procedimentos envolvidos em todas as fases de seus processos de produção dos bens e produtos submetidos ao controle e fiscalização sanitária, incluindo a destinação dos respectivos resíduos;

A ANVISA está organizada conforme o organograma apresentado na figura 01:

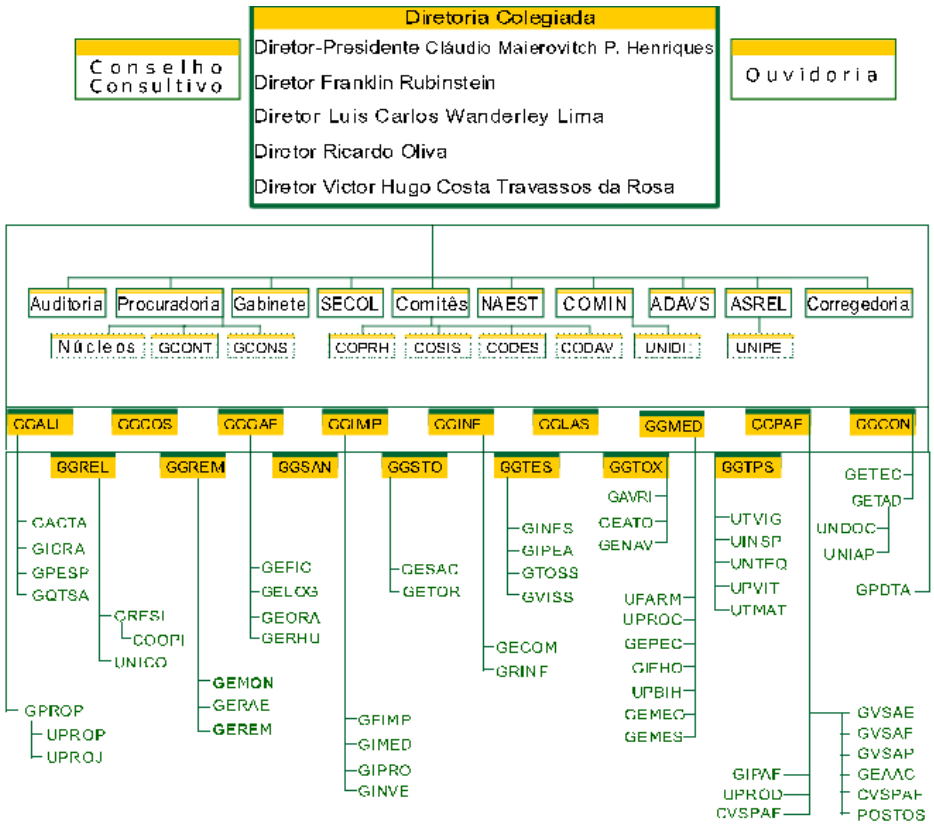

Fig. 01 - Organograma da ANVISA

Para solicitar os serviços fornecidos pela ANVISA o agente regulado deve efetuar o peticionamento junto a UNIAPE. Como meio de facilitar o processo de solicitação foi desenvolvido o caminho eletrônico onde as requisições são realizadas pela internet.

O fluxo do peticionamento ocorre da seguinte forma:

1. Login no Sistema de Segurança Externo;
2. É criado o documento de solicitação que é armazenado no IDC;
3. Os dados são transferidos para o Sistema corporativo – DATAVISA;
4. Os usuários Internos acompanham o processo;
5. Os encaminhamentos necessários são adotados;
6. O processo recebe um desfecho.

A estrutura do sistema é apresentada na figura 02:

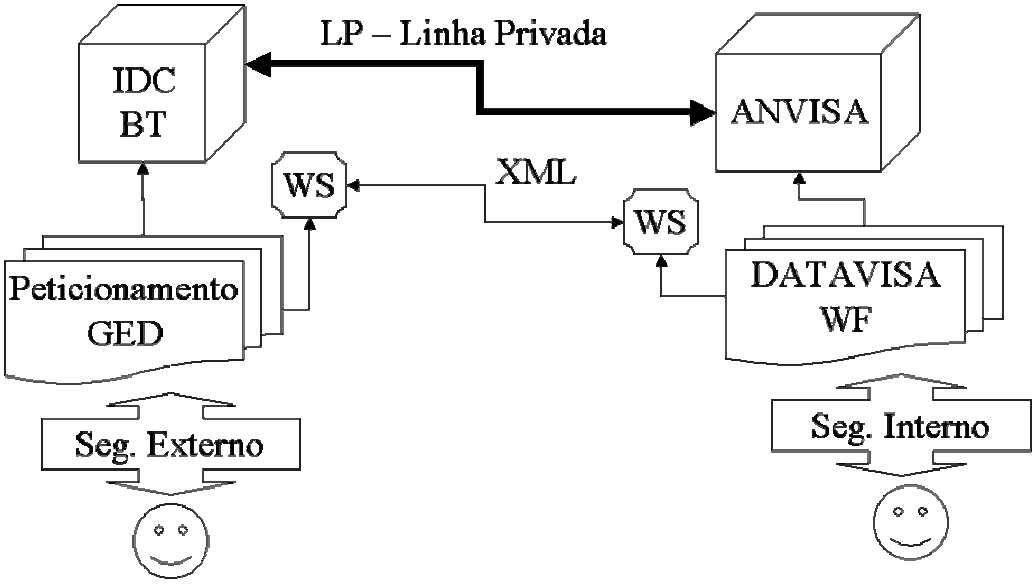

Fig. 02 – Esquema do peticionamento e DATAVISA.

3. ANVISA e ISO 17.799

A norma ISSO 17.799 estabelece os padrões da segurança da informação no Brasil. Os principais pontos desta norma são confidencialidade, integridade e disponibilidade. Estes três pilares norteiam as ações que as organizações devem adotar para procurar o caminho da segurança da informação.

Associado a estes princípios existe o custo, que está diretamente relacionado aos critérios de segurança. Ou seja, quanto maior o nível de segurança desejado, maior será o custo. Assim o gestor deve estar sempre analisando e avaliando a relação custo benefício para adotar a melhor medida, conforme suas necessidades.

Para o critério de confidencialidade a ANVISA tem adotado entre outros aspectos os seguintes pontos principais: Sistema de Segurança para Usuários Internos; Sistema de Segurança para Usuários Externos; e, LP – Linha Privada de Comunicação.

A integridade foi tratada pela agência através de *Web Services* para troca de informações entre os dois ambientes. Estes serviços garantem que os dados enviados pelo IDC chegarão íntegros, corretos, na ANVISA, e vice-versa.

Para a disponibilidade foi implementado uma solução possuindo dois ambientes distintos, permitindo a garantia de comunicação, e o alívio do tráfego da rede em apenas um dos pontos.

A ISO 17.799 trata de alguns pontos referentes a segurança organizacional, de pessoas, e física do ambiente. Foram elencadas algumas destas características com as soluções adotadas pela ANVISA.

- Atribuição de responsabilidades pela proteção dos ativos;
  - GGCON – Gerência Geral de Conhecimento e Documentação;
- Processo de autorização para instalações de processamento da informação;

    - GGINF – Gerencia Geral de Informação
- Tipos e razões para acessos;
    - Gerências Gerais através da GGCON e GGINF
- Contratados para serviços externos;
    - Serviço de Limpeza e Segurança terceirizado controlado pela Gerência Geral de Gestão Administrativa e Financeira;
    - Serviço de Informática terceirizado controlado pela Gerencia Geral de Informação;
- Requisitos de Segurança nos contratos e acessos de prestadores de serviços;
    - Termos do edital de Licitação e;
    - Contrato de Prestação de Serviço.
- Responsabilidades do trabalho;
    - Estabelecido do contrato de Trabalho;
- Acordos de confidencialidade;
    - Estabelecida do contrato de Trabalho;
- Termos e condições de trabalho;
    - Estabelecida do contrato de Trabalho;
- Notificação de falhas na segurança;
    - E-mail corporativo
- Mau funcionamento de software;
    - Cada sistema possui sua rotina
- Perímetro de segurança;
    - Entradas controladas por Equipe de Segurança contratada;
- Controles de entrada física;
    - Crachá
- Segurança dos equipamentos;
    - Sala cofre e controle de patrimônio
- Instalação e proteção dos equipamentos
    - Rede Estabilizada e *No-break* para servidores
- Cabeamento;
    - Estruturado e IDS – *Intrusion Detection System*

4. Conclusão

Não existe sistema seguro. Cada organização possui seus problemas e de acordo com sua avaliação de risco, tenta investir seus recursos da melhor maneira possível. Desta forma, a ANVISA não seria diferente.

No estudo realizado pela *Ernst & Young*, mais de 700 empresas questionadas – representando 26 indústrias em 66 países – afirmaram que a falta de orçamento era o principal obstáculo para garantirem uma proteção da sua informação de forma eficaz. Embora a escassez de fundos seja o principal problema, parece ser reforçada pelo fato de quase metade dos CIO's, os CIS's e outros executivos, na área da tecnologia da informação, acreditam que estão conciliando da melhor forma os seus gastos com os principais objetivos de negócio. Surge, como fundamental, uma mudança de mentalidade nas organizações. **[ERNST, YOUNG 2003]**

A falta de recursos é facilmente perceptível nas empresas e também nos organismos federais. A ANVISA possui recursos limitados e por isso o investimento em segurança é feito de maneira a se adaptar ao orçamento previsto. O processo de melhoria da segurança da informação é realizado pela ANVISA de acordo com seus

recursos. Desta forma a gerencia da área de informática aplica da melhor maneira possível.

A auditoria *Ernst & Young* aponta três iniciativas que devem ser adotadas pelas empresas, de modo a melhorar a performance do seu programa de segurança da informação. Comunicar os temas relacionados com a segurança da informação, de forma a que os *stakeholders* percebam sua importância; alinhar os objetivos de negócio com os objetivos de segurança em toda a empresa; e, por fim, passar efetivamente do planejamento para a ação quando se fala desta matéria. **[ERNST, YOUNG 2003]**

Os pontos abordados pela auditoria, nem sempre são observado pela agência, entretanto a atual gerência de informação vem estudando novas medidas para solucionar os problemas. A comunicação das diretrizes de segurança de forma clara, ainda não é divulgada por toda a organização, mas foi iniciado este processo. A diretoria possui o conhecimento da necessidade da segurança da informação e vem adotando as medidas necessárias, haja vista a criação da nova sala cofre, entre outras medidas. Logo, a ação vem sendo executada.

A *Ernst & Young* concluiu que mais de um terço das empresas considera que não conseguem determinar se os seus sistemas informáticos estão propensos a ataques, um terço das empresas considera que a sua capacidade de resposta a incidentes de segurança é inadequada, e apenas 34% das empresas afirmam agir de acordo com os padrões e regulamentações de segurança. Muitos executivos seniores continuam a dar mais atenção a quebras de segurança que chamam mais a atenção da mídia tais como os ataques de *hackers* ou os vírus de computador. *Mark Doll* entende que se deve prestar ainda mais atenção às ameaças que não são tão óbvias e públicas, como por exemplo, funcionários descontentes, ex-colaboradores, *links* com redes de parceiros que não têm sistemas seguros, roubos de computadores portáteis ou ainda, colaboradores que acessem à rede através de locais que não oferecem a segurança necessária como pontos de acesso *wireless* inseguros e acesso remoto. **[ERNST, YOUNG 2003]**

Os temas abordados neste trabalho e pela consultoria *Ernst & Young* são de extrema importância e devem ser observados pelas organizações, incluindo a Agência Nacional de Vigilância Sanitária. A agência deve procurar se enquadra, ainda mais, ao lado daquelas empresas que tem a capacidade de saber se sua capacidade de resposta a incidentes está aceitável, de acordo com as normas, principalmente a ISO 17.799. Lembrando sempre que os incidentes não são apenas aqueles que se tornam públicos, mas principalmente aqueles que acontecem sem o conhecimento dos responsáveis. Não se esquecendo dos perigos internos, que são a maior fonte de incidentes.

Referências

[ANVISA, 2004] AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA. *"Site da ANVISA", http://www.anvisa.gov.br, consulta em junho de 2004.*

[ISO, 2001] ABNT "*Tecnologia da informação - Código de prática para a gestão da segurança da informação*", NBR ISO/IEC17799:2001.

[ERNST, YOUNG 2003] Ernst & Young. "*Protecção da informação é decisiva na estratégia de negócio das empresas*", http://www.ey.com/global/content.nsf/International/Home, consultado em junho de 2004.