Universidade Católica de Brasília

MBA – Gestão de Sistemas de Informação

Segurança da Informação
Prof. Ly Freitas Filho

Política de Segurança da Informação
Banco Dinâmico S.A.

2º Semestre de 2002

Política de Segurança da Informação

Banco Dinâmico S.A.[1]

Equipe do MBA Gestão de Sistemas de Informação
Universidade Católica de Brasília – 02/2002
Disciplina: Segurança da Informação[2]

Resumo

A Política de Segurança da Informação tem como objetivo proteger as informações da Instituição, assegurar a continuidade dos negócios, garantir a integridade, confidencialidade e disponibilidade das informações, sistemas de informação e recursos, observando as normas e padrões internos.

Uma das principais metas da área comercial dos bancos é a intensificação do atendimento eletrônico a clientes. Alcançar este objetivo envolverá uma mudança de comportamento e hábitos. Cabe aos gestores de segurança a adequação nas regras e nos meios para atender a esta nova formulação.

Palavras-chave

Política de Segurança da Informação; confiabilidade; integridade; disponibilidade; gerenciamento de risco, auto-atendimento;

An Information Security Policy

Summary

The Information Security Policy has as objective to protect the information of the Institution, to assure the continuity of the businesses, to guarantee the integrity, confidence and availability of the information, systems of information and resources.

One of the main goals of the commercial area of the banks is the intensification of the electronic attendance the customers. To reach this objective will involve a change of behavior and habits. The adequacy in the rules and the half ones fits to the security managers to take care of to this new formularization.

Keywords

Information Security Policy; confidence; integrity; availability; risk management, auto-attendance.

[1] Trabalho desenvolvido no MBA – Gestão de Sistemas de Informação.
[2] Equipe formada por: Kátia Cristina da Costa M. da Silva; Marcelo Rodrigues Silva.

1 Introdução

A Política de Segurança da Informação (PSI) do BANCO DINÂMICO S.A. tem como objetivo proteger as informações da Instituição e assegurar a continuidade dos negócios, garantindo a integridade, confidencialidade e disponibilidade das informações, sistemas de informação e recursos.

A PSI foi definida e tem seu cumprimento controlado pelo Comitê de Segurança da Informação. As unidades são responsáveis pela segurança na sua área de atuação. Cada unidade deve conhecer, assimilar e administrar a PSI de forma a permitir proteção adequada às informações, pessoas e aos recursos envolvidos, podendo adaptá-lo às suas necessidades específicas, desde que observadas as normas .

2 Abrangência

Para atender as necessidades de segurança do BANCO DINÂMICO S.A., a PSI aborda os seguintes segmentos: segurança de processos, segurança de sistemas e segurança física; as pessoas e sua segurança permeiam todos estes segmentos. Esses segmentos não são necessariamente isolados. Existem regiões de sobreposição, que servem para reforçar a segurança.

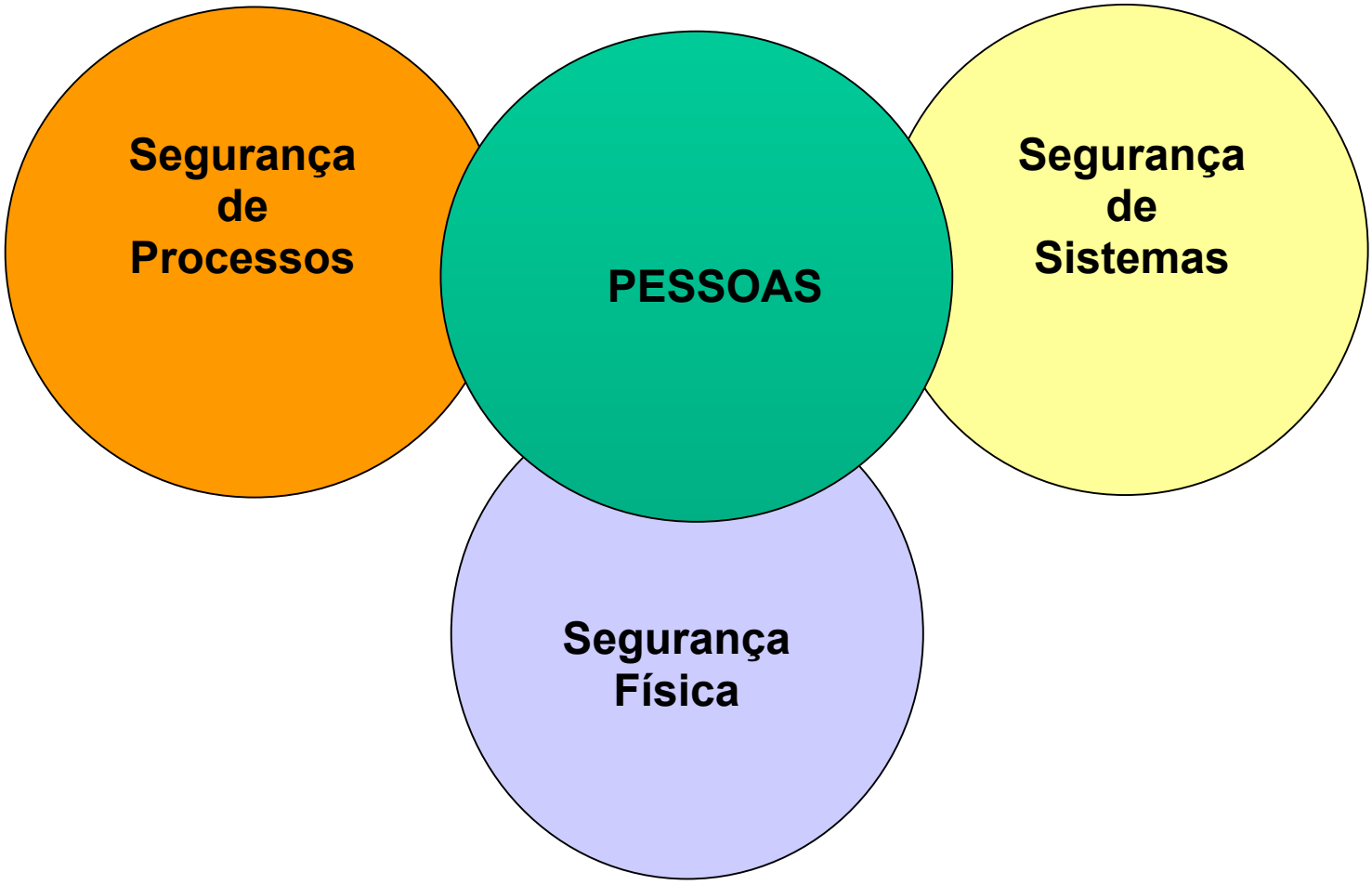

Figura 1 – Abrangência da Política de Segurança da Informação do BANCO DINÂMICO S.A.
A tabela a seguir define a abrangência da PSI:

SEGMENTO	DEFINIÇÃO	ABRANGÊNCIA
Físico	Conjunto de medidas destinado a prevenir riscos naturais, acidentais, intencionais e acessos não autorizados às instalações e recursos do BANCO DINÂMICO S.A..	Controle de acesso físico às dependências, documentação administrativa, contingência, combate a incêndio, inventário dos equipamentos e recursos, instalações, condições ambientais, controle de entrada e saída de bens e materiais e ações de prevenção de acidentes.
Pessoas	Conjunto de medidas destinado a prevenir acidentes, garantir a saúde e segurança dos empregados no trabalho, reduzir os erros, fraudes e mau uso de recursos e proteger o conhecimento obtido.	Ações de conscientização, atribuição de responsabilidades e procedimentos para minimizar as ameaças acidentais e intencionais, ações de prevenção relativas a saúde e integridade física dos empregados, CIPA [3], brigada de incêndio, mapa de riscos, PPRA [4], PCMSO [5] e ações de preservação do conhecimento.
Lógico	Conjunto de medidas destinado a garantir a integridade, confidencialidade e disponibilidade de sistemas, software, dados e informação.	Sistema operacional, controle de acesso, desenvolvimento de sistemas e aplicações, software básico e de apoio, documentação técnica e de sistemas, backup e recuperação de sistemas e arquivos, distribuição e catalogação de políticas, controle de versões, classificação da informação, log, verificação dos dados, separação de ambientes e banco de dados.
Comunicações	Conjunto de medidas destinado a garantir a integridade, confidencialidade e disponibilidade da informação, durante o tráfego na rede.	Componentes da rede, meios de comunicação, backup de recursos, conexão com outras redes, controle de acesso, transferência de arquivos, correio eletrônico e outros serviços disponíveis.
Computação Pessoal	Conjunto de medidas destinado a garantir a integridade, confidencialidade e disponibilidade das informações no ambiente de computação pessoal (estações de trabalho, microcomputadores *stand-alone* ou portáteis).	Sistema operacional, controle de acesso lógico e físico, combate a vírus e ao uso de software não-autorizado, proteção de informações armazenadas, backup e recuperação.

Tabela 1 - Segmentos da Política de Segurança do BANCO DINÂMICO S.A.

3 Benefícios da PSI

[3] Comissão Interna de Prevenção de Acidentes
[4] Política de Prevenção de Riscos Ambientais
[5] Política de Controle Médico de Saúde Ocupacional

- Minimizar riscos para o Negócio;
- Minimizar impactos devido a falhas;
- Atender requisitos dos contratos;
- Criar procedimentos para recuperação de falhas;
- Criar um ambiente de segurança compreensível;
- Atender as necessidades dos clientes;
- Manter a flexibilidade para atender necessidades e evolução tecnológica;
- Maximizar o uso de recursos disponíveis;
- Sistematizar as ações de segurança.

4 Ciclo de Vida da PSI

A implantação da segurança tem um início bem definido, mas devido a constante evolução dos serviços, tecnologia e surgimento de novas vulnerabilidades, é uma atividade permanente. Dessa forma a PSI foi definida com um conjunto de etapas que devem ser realizadas periodicamente, constituindo o seu ciclo de vida, conforme apresentado na figura abaixo:

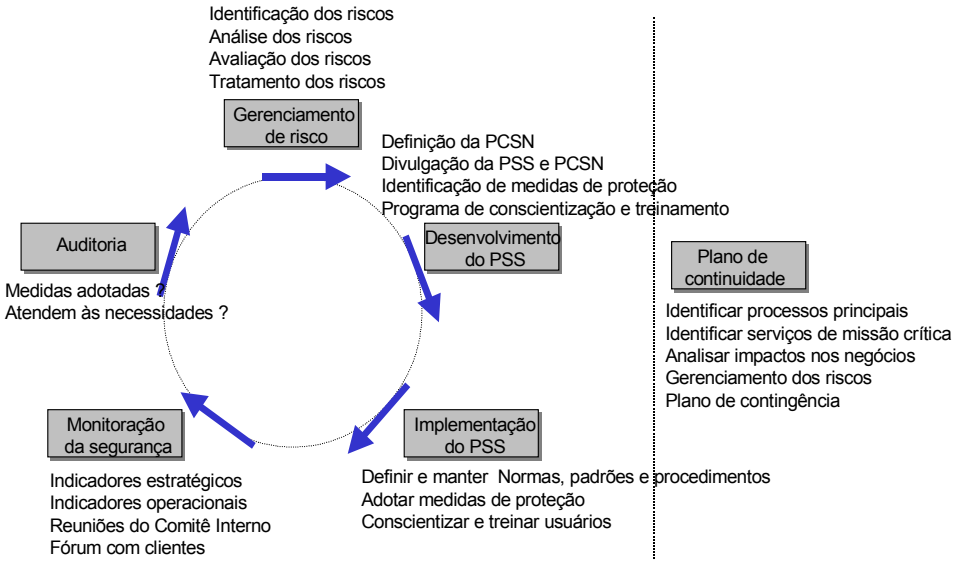

Figura 2- Ciclo de vida da Política de Segurança do BANCO DINÂMICO S.A.

• 1ª Etapa - Gerenciamento de Riscos

Etapa que visa a proteção dos recursos da empresa, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) mais viável. Os seguintes pontos devem ser identificados: o que deve ser protegido? Deve ser protegido contra quem ou contra o quê? Quanto pode ser gasto na proteção ? Necessidade de uma análise da relação custo x benefício para o negócio.

O gerenciamento de riscos consiste das seguintes fases principais:

- identificação dos recursos a serem protegidos (hardware, rede, software, dados, pessoas, documentação, suprimentos);
- identificação dos riscos (ameaças) - que podem ser naturais (tempestade, inundações), causadas por pessoas (ataques, furto, vandalismo, erro ou negligência) ou de outro tipo (incêndio);
- análise dos riscos (vulnerabilidades e impactos) - identificar as vulnerabilidades e os impactos associados;
- avaliação dos riscos (probabilidade de ocorrência) - levantamento da probabilidade da ameaça vir ou não a acontecer. Esta avaliação pode ser feita com base em informações históricas ou em tabelas internacionais.
- tratamento dos riscos (medidas a serem adotadas) - maneira como lidar com as ameaças. As principais alternativas são : eliminar o risco, prevenir, limitar ou transferir as perdas ou aceitar o risco;

Considerações importantes no gerenciamento dos riscos:

- os riscos que não puderem ser eliminados devem estar documentados e devem ser do conhecimento do cliente;
- um efetivo gerenciamento dos riscos permite decidir se o custo de prevenir um risco (medida de proteção) é mais alto que o custo das conseqüências do risco (impacto da perda);
- faz-se necessária a participação e o envolvimento do cliente.

• Valor da Informação

No gerenciamento de riscos uma variável fundamental é o valor da informação ou recurso a ser protegido. A informação ou recurso deve ser protegido conforme sua necessidade, evitando situações extremas de superproteção (elevando o custo) ou de falta de proteção (trazendo riscos para os negócios).

No processo de determinação do valor da informação três aspectos básicos devem ser considerados :

- toda informação requer algum tipo de recurso para ser produzida e mantida (dinheiro, tempo, equipamentos, pessoas, etc);
- nem toda informação causa danos se for divulgada;
- a informação deve ser protegida apenas pelo prazo necessário;

Na determinação do valor da informação algumas questões devem ser utilizadas :

- qual o custo para produzir a informação ?
- qual o custo para substituir a informação ?
- qual o impacto caso a informação esteja indisponível ?
- qual o impacto caso a informação seja divulgada de forma não autorizada?
- existe alguma exigência legal para a proteção da informação? Quais as penalidades caso a informação não seja protegida adequadamente?

O risco pode ser definido da seguinte forma:

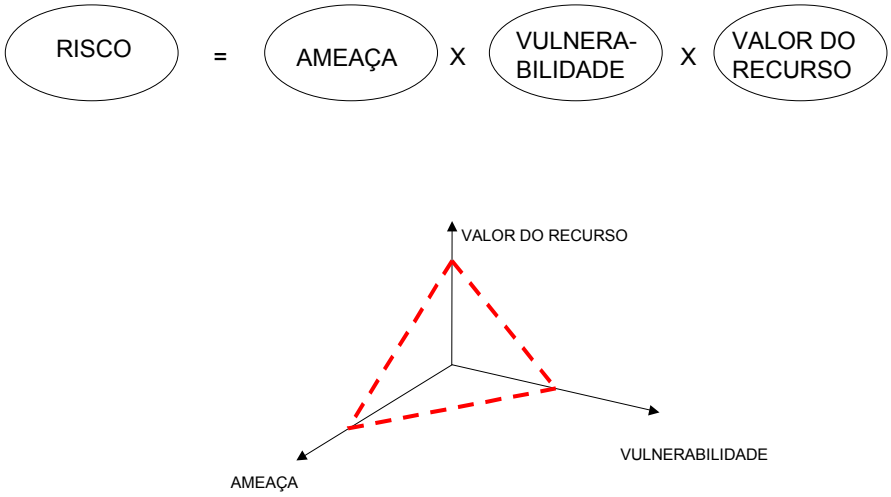

Figura 3 – Componentes do Risco

• 2ª Etapa - Desenvolvimento da PSI

A Política Corporativa de Segurança do Negócio (PCSN) é o referencial para a PSI e deve orientar na definição e adoção de normas, padrões e procedimentos em cada Unidade de Gestão, para reduzir riscos e garantir a integridade, confidencialidade e disponibilidade das informações, sistemas de informação e recursos.

A PCSN tem os seguintes objetivos específicos:

- Orientar a PSI;
- Definir o escopo da segurança no BANCO DINÂMICO S.A.;
- Contribuir para o direcionamento e a efetividade das soluções de segurança, mantendo uma identidade empresarial ;
- Auxiliar na identificação do real valor dos recursos e informação;
- Permitir a adoção de soluções integradas e homogêneas;
- Servir de referência para auditoria, apuração e avaliação de responsabilidades;

A PCSN se aplica a todos os empregados e contratados do BANCO DINÂMICO S.A. e deve ser adotada por todas as suas unidades organizacionais. Sua aplicação pode atingir a relação com Clientes, parceiros e fornecedores.

• Política Corporativa de Segurança do Negócio

O BANCO DINÂMICO S.A. deve permanentemente :

- Garantir a utilidade, disponibilidade, integridade e privacidade das informações;
- Tratar a informação como um patrimônio, protegendo-a de acordo com sua classificação;
- Tratar a inviolabilidade das informações sob a sua guarda;
- Orientar seus clientes e empregados sobre as medidas de segurança a serem adotadas para as informações e recursos;
- Assegurar a capacidade de recuperação dos sistemas e recursos que suportam as funções críticas para o negócio.

• Comitê de Segurança Interno

A PSI prevê a existência de um Comitê de Segurança Interno constituído por representantes de cada UG, com os seguintes objetivos principais:

- Oportunidade para identificar as necessidades e propor prioridades de ações de segurança, de acordo com a PSI;
- Discutir e homologar as normas relativas à segurança do negócio;
- Evitar a adoção de soluções de segurança conflitantes ou que tornem o ambiente vulnerável;
- Reduzir a duplicidade de esforços na adoção de soluções de segurança;
- Facilitar a implantação de medidas de segurança corporativas;
- Dar visibilidade às medidas de segurança disponíveis.

As normas, padrões e procedimentos desenvolvidos para atender à PCSN devem ser elaborados pela UG responsável. A discussão e a aprovação das normas devem ser feitas por meio do Comitê de Segurança Interno. As ações de segurança que extrapolem os limites de uma UG devem ser propostas ao Comitê para avaliação.

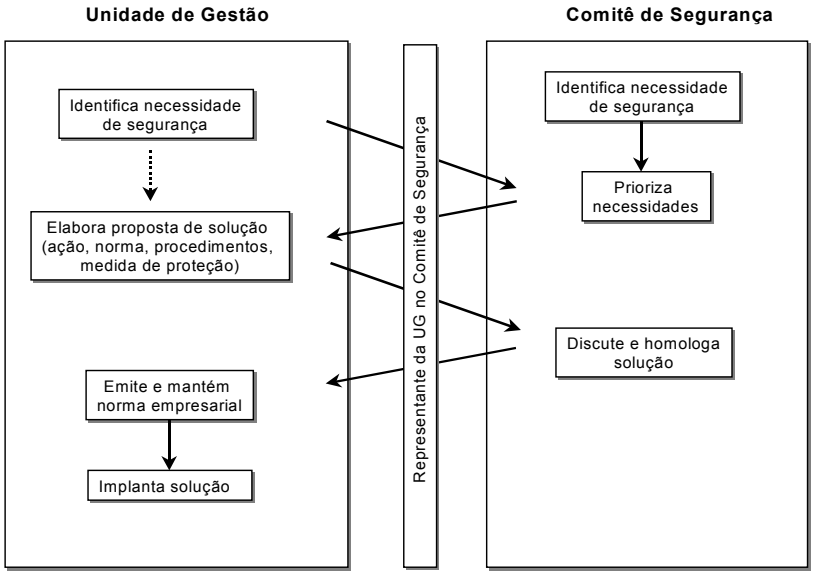

Figura 4 – Relacionamento UG – Comitê de Segurança

• Fórum de Segurança com os Clientes

Objetivos do Fórum de segurança com os clientes:

- Servir de fórum para identificar novas necessidades de segurança ou ajustes nos procedimentos e medidas já implantadas;
- Facilitar o processo de conscientização de segurança;
- Facilitar a implantação de medidas de segurança corporativas;
- Dar visibilidade às medidas de segurança disponíveis;
- Obter respaldo nas ações que exijam atuação do cliente;

• Medidas de Segurança

As medidas de segurança consistem de mecanismos e procedimentos a serem adotados de forma a atender à PCSN e normas de segurança. O grau de implementação dessas medidas está associado com o resultado da etapa de gerenciamento de riscos, necessidades do Cliente, classificação da informação e criticidade do recurso a ser protegido.

• Política de Conscientização e Treinamento

Muitos dos problemas de segurança estão associados a erros e ações cometidas por pessoas autorizadas. Parte significativa desses problemas refere-se à falta de conhecimento das ameaças e vulnerabilidades existentes, dos mecanismos disponíveis para proteção e falta de treinamento. Para ser efetiva a política de treinamento e conscientização tem de atingir todos os empregados.

A conscientização em aspectos básicos como proteção de senhas, combate à vírus e uso de software não-autorizado, procedimentos de backup e recuperação adequados são fundamentais para a segurança da informação.

• Documentação de segurança

A documentação de segurança consiste das normas, padrões e procedimentos que devem estar atualizados e disponíveis para as pessoas envolvidas.

• 3ª Etapa - Implementação

Uma vez identificados os recursos a serem protegidos e riscos associados, as medidas de segurança necessárias devem ser implantadas de acordo com as normas e procedimentos estabelecidos na etapa anterior – Desenvolvimento da PSI.

A implementação e a manutenção da PSI dependem de ações específicas da Unidade Corporativa, Unidades de Gestão e área responsável pela auditoria.

A Unidade Corporativa deve:

- Formular políticas e controlar seu respectivo cumprimento;
- Rever periodicamente a PCSN para adaptá-la às novas necessidades identificadas junto aos clientes, diretrizes da empresa, legislação vigente ou surgimento de novas ameaças e vulnerabilidades;
- Realizar monitoração estratégica da segurança;
- Participar do comitê de segurança interno.

As Unidades de Gestão devem:

- Identificar recursos que requerem proteção;
- Desenvolver e manter, baseado na PCSN, as normas e procedimentos referentes a sua área de atuação;
- Propor normas ao comitê de segurança interno;
- Adotar medidas de segurança;
- Analisar e definir ajustes necessários em sistemas ou processos essenciais;
- Elaborar, distribuir e manter atualizada a documentação de segurança;
- Executar política de conscientização e treinamento;
- Assegurar a efetividade das medidas adotadas em função das evoluções;
- Participar do comitê de segurança interno.

A auditoria interna deve:

- Realizar verificação sistematizada das ações e medidas de segurança definidas;
- Verificar se as medidas definidas foram adotadas e se atendem às necessidades de segurança;
- Definir as informações necessárias para a realização do processo de auditoria, relativas aos aspectos de segurança.

A figura a seguir apresenta a arquitetura de implementação da PSI :

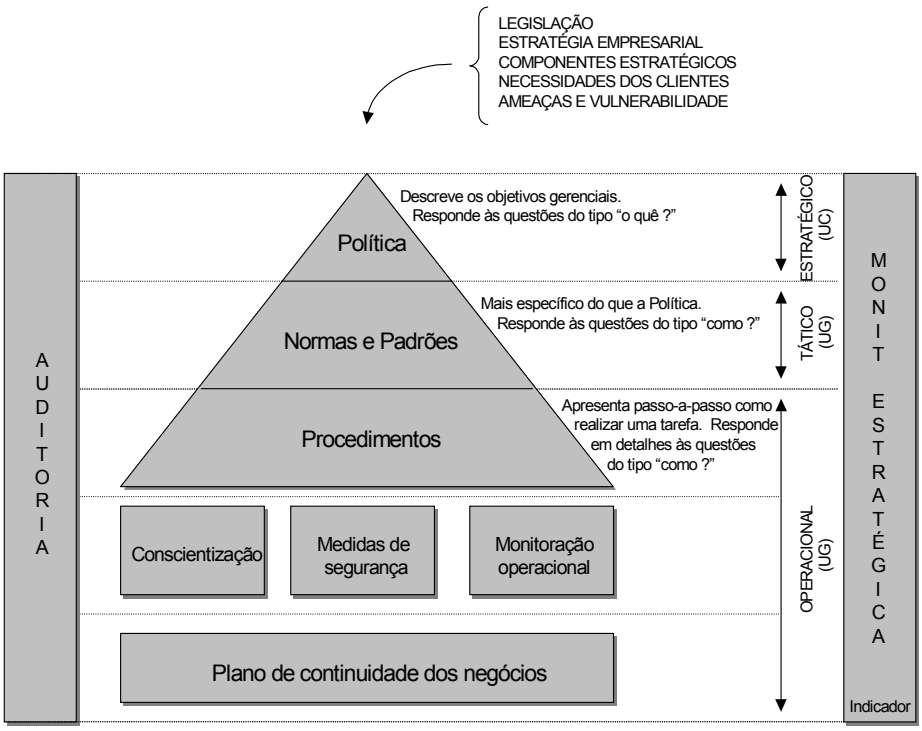

Figura 5 - Arquitetura de implementação da Política de Segurança do Banco Dinâmico S.A.

A figura a seguir apresenta uma visão simplificada da arquitetura de implementação da PSI, onde é destacada a necessidade de realimentação para mantê-la adequada às necessidades do negócio e cultura do BANCO DINÂMICO S.A..

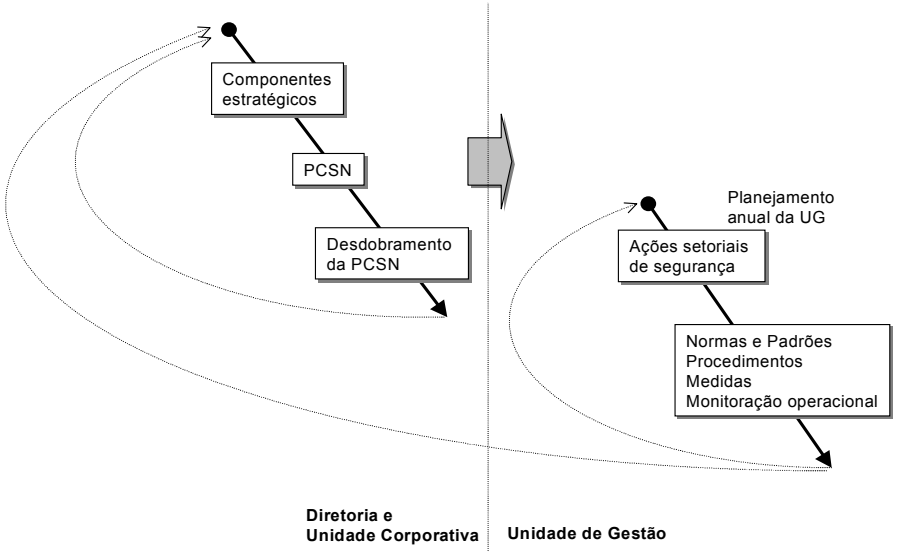

Figura 6 - Encadeamento das ações

As unidades gestoras, para implementação e manutenção da PSI, devem observar:
- O fluxo Implementação da PSI;
- A relação entre determinações definidas e Unidades de Gestão responsáveis pelas implementações.

As determinações são estabelecidas tendo como foco as necessidades e características do ambiente do BANCO DINÂMICO S.A. e não tomando como base as atividades específicas de cada UG. Dessa forma algumas determinações, apesar de estarem sob a responsabilidade de uma UG, ficam compartilhadas entre mais de uma UG.

• 4ª Etapa - Monitoração da Segurança

A PSI e sua efetividade devem ser monitoradas e revisadas permanentemente de forma estratégica pela UG, visando manter soluções de segurança integradas e homogêneas, considerando as mudanças tecnológicas, direcionamentos estratégicos de negócio e necessidades dos Clientes.

O planejamento, o acompanhamento e a avaliação do atendimento de metas definidas devem ser executados por meio do Indicador de Segurança. Paralelamente, outros pontos de verificação podem ser considerados, visando a evolução dos trabalhos de segurança:

- Resultado de análise de risco;

- Normas e procedimentos existentes;
- Atividades de conscientização;
- Mecanismos de proteção;
- Reuniões com os responsáveis pela segurança nas Unidades de Gestão;
- Reporte de incidentes;
- Ações de ajustes e melhorias.

É responsabilidade da UG adotar ações de monitoração operacional que permitam identificar falhas, uso não autorizado, ataques e outras situações que possam ameaçar os negócios. As ações de monitoração devem ser conduzidas considerando as questões éticas e legais.

- **Indicadores**

O uso de indicadores tem os seguintes objetivos principais:
- Identificar os riscos e minimizá-los de uma forma consistente;
- Acompanhar a implantação das medidas de segurança;
- Realizar ajustes medidas de segurança adotadas;
- Identificar evolução no processo segurança;
- Justificar os investimentos na segurança.

5ª Etapa - Auditoria

O processo de auditoria deve ser conduzido pela auditoria interna e sua operacionalização pode ser realizada internamente ou por empresa externa. As Unidades de Gestão devem ter disponíveis informações que permitam atender às suas necessidades de auditoria e necessidades dos Clientes.

O BANCO DINÂMICO S.A. deve oferecer também aos Clientes, a possibilidade de realizar auditoria nos seus respectivos sistemas e ambientes, por meio de consultoria externa.

5 Responsabilidades

Visando estabelecer uma evolução para as questões associadas com a segurança, cada área ou pessoa atua em um ou mais papéis, conforme definição e descrição nas tabelas a seguir:

PAPEL	***DEFINIÇÃO***
Proprietário	Pessoa ou órgão que cria a informação ou é seu usuário principal.
Depositário	Pessoa ou órgão responsável pelo tratamento e armazenamento da informação.
Usuário	Pessoa ou processo autorizado ao uso de determinada informação ou conjunto de dados.
Alta direção	Diretoria Colegiada.
Gerentes	Superintendentes, Coordenadores, Chefes de departamento, divisão ou setor, Supervisores.
Gestão do Processo - Segurança do Negócio	Um dos processos que compõem a UC, que tem por finalidade apoiar a ação da Diretoria Colegiada, nos aspectos de segurança.

Tabela 3 - Definição de papéis

PAPÉIS	***RESPONSABILIDADES***

Proprietário	• Adotar as orientações de segurança; • Classificar o recurso de acordo com a sua sensibilidade, criticidade ou importância para o negócio; • Autorizar o uso e acesso aos recursos; • Delegar funções de classificação e autorização, se necessário; • Identificar em conjunto com o depositário (ou gerente responsável pela guarda do recurso) as medidas de segurança necessárias; • Avaliar periodicamente as medidas de segurança adotadas.
Depositário	• Adotar as orientações de segurança; • Administrar a segurança das informações, sistemas de informação e recursos conforme especificação do proprietário; • Administrar o acesso autorizado à informação; • Prover e administrar proteções físicas e procedimentos para a proteção da informação; • Comunicar efetivamente a proprietários e usuários as regras, restrições e recursos de controle da instalação; • Detectar e agir, em tempo hábil, às tentativas não autorizadas de acesso a dados ou áreas restritas; • Assegurar o uso autorizado de terminal em localização autorizada; • Levar ao conhecimento das gerências, situações de quebra de segurança, uso indevido ou descumprimento de normas ou procedimentos; • Definir medidas de controle de acesso à instalação; • Disponibilizar ferramentas de auditoria e controle para os Clientes e proprietários.
Usuário	• Adotar orientações de segurança; • Proteger dados, informações e recursos sob sua responsabilidade; • Identificar recursos sensíveis ou críticos; • Utilizar recursos à sua disposição apenas para atividades do BANCO DINÂMICO S.A.; • Não utilizar recursos da empresa para atividades ilegais; • As falhas, ou vulnerabilidades, identificadas devem ser comunicadas à gerência; • Não explorar falhas existentes; • Não divulgar ou permitir acesso a informações às quais tenha sido autorizado.
Alta Direção	• Aprovar a PSI; • Dar conseqüência a PSI.

PAPÉIS	*RESPONSABILIDADES*
Gerentes	• Adotar as orientações de segurança; • Avaliar as conseqüências de uma falha na segurança de sua responsabilidade: impedimento de realizar tarefas necessárias; perda, uso inadequado ou roubo de recursos; perda de credibilidade (interna / externa); • Definir o equilíbrio entre o risco aceitável e os recursos gastos com segurança; • Verificar continuidade; • Definir o tempo que o sistema pode ficar indisponível; • Atuar para a garantia da precisão das informações;
Gestão do processo - Segurança do Negócio	• Definir, divulgar e manter a PSI; • Definir e manter a PCSN; • Definir estratégias para assegurar a continuidade dos serviços em situações de contingência; • Monitorar o nível de segurança; • Identificar soluções de segurança que possam ser agregadas às soluções do BANCO DINÂMICO S.A.; • Assessorar as Unidades de Gestão na identificação e definição das necessidades específicas com relação à segurança; • Ser o ponto central para a difusão, apoio e assessoria em temas de segurança e controle associados; • Identificar e avaliar novos mecanismos, tecnologias e controles necessários e recomendar estratégias para proteger os recursos de acordo com sua criticidade e valor; • Definir as estratégias de conscientização dos empregados com relação à segurança do negócio;

Tabela 4 - Papéis x Responsabilidades

6 Objetivo da PSI do Auto-atendimento

- Preservar as informações de nossos clientes
- Eliminar / reduzir fraudes
- Garantir o atendimento rápido e seguro aos clientes
- Reduzir custos (diretos / indiretos)

7 PSI Auto-atendimento

- Monitoração de todo o ambiente de auto-atendimento (disponibilidade, suprimento, violação de equipamento) 7x24 - via linha de dados e linha discada; linhas distintas para alarme e dados;
- Robôs monitoram os equipamentos a cada 15 minutos - Caso o equipamento apresente qualquer alarme, sinal de violação ou falha, uma ronda dirige-se ao local;
- Acompanhamento dos defeitos / falhas dos equipamentos, com manutenção preventiva,

caso sejam observados problemas freqüentes em um mesmo dispositivo;

- Controle das visitas e serviços executados pela equipe de manutenção;
- Acionamentos para manutenções / suprimentos centralizados;
- Pessoal especializado em monitoração de auto-atendimento;
- Suprimento programado, resultando em: menor indisponibilidade por falta de numerário, melhor gerenciamento do caixa da instituição
    - os cassetes vêm lacrados da transportadora
    - processos de preparação do numerário racionalizado nas empresas de transporte de valores; menor retorno de numerário;
- Aplicativos para gerenciamento da rede pelo banco;
- Equipamentos com criptografia de teclado; leitora smart card; leitora de código de barras;
- Segurança dos equipamentos (porta reforçada – fechadura, pinos e esferas; proteção lateral antimaçarico; alarme monitorado)
- Fixação dos equipamentos – são realizados testes periódicos para análise de resistência;
- Serviço de manutenção e limpeza dos ambientes de auto-atendimento prestado por pessoal treinado;
- Auditoria dos equipamentos a cada 60 dias (conferência de numerário) – além de auditoria automática;
- No transporte dos equipamentos são adotados cuidados para evitar danos – estrado com material para absorção de impactos;
- Requisitos a serem observados no armazenamento dos equipamentos, pela prestadora de serviços;
    - organização, proteção contra poeira, local limpo e com acesso restrito a pessoas autorizadas;
- Software e hardware disponibilizados pela prestadora de serviços;
- Adequação do aplicativo de acordo com as necessidades do banco;
- Ambientes segregados para desenvolvimento; testes pelos bancos (clientes) em laboratório;

8 Conclusão

Escrever uma política de segurança é uma tarefa fácil, se compararmos os recursos necessários para implementá-la efetivamente. Técnicas de segurança mal empregadas são piores que a sua inexistência, portanto profissionais especializados em segurança são indispensáveis em determinadas empresas, notadamente naquelas que lidam com informações críticas, como um banco, por exemplo.

Apesar de não existirem ambientes cem por cento seguros e de serem as pessoas o elo mais fraco da corrente de segurança, as empresas têm que persistir em seus investimentos na área, pois os *hackers* certamente estão investindo.

Identificamos como ações eficazes quando se trata de Segurança da Informação:

- "Aculturação" corporativa;
- Security Office;
- Outsourcing especializado;
- Plano Diretor de Segurança;
- Desmembramento do Plano de Ação;
- Conformidade com as Normas (BS7799 / ISO17799);
- Questionamento e pesquisa constantes.

É indiscutível, atualmente, a necessidade de obtenção de conhecimento organizado e preferencialmente voltado à aplicação imediata que gere resultados no menor prazo possível. Desta forma, não poderia ser diferente para os aspectos tecnológicos e os ligados à proteção da informação que sustentam os negócios.

Referências

BS 7799 e NBR ISO/IEC 17799 – ABNT – Associação Brasileira de Normas Técnicas, Agosto 2001.

[Dias, Cláudia , 2000] – Dias, Cláudia **. "**Segurança e Auditoria da Tecnologia da Informação" . Axcel Books do Brasil, 2000.

Dalton Matsuo Tavares - USP - Seminário "Segurança em Sistemas Computacionais"

Developers´ - CIO Magazine N°70 – www.developers.com.br

Executivos Financeiros N°134 – www.executivosfinanceiros.com.br

Módulo – www.modulo.com.br