UFSM

TRABALHO DE GRADUAÇÃO Nº 152

DESENVOLVIMENTO DE UM MODELO DE SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO DO CRSPE

Orientador: KOITI OZAKI
Co-Orientadora: ROSECLEA MEDINA DUARTE

Aluno: EVALDO GALVÃO MENDONÇA

CCC

Santa Maria, RS, Brasil

2004

EVALDO GALVÃO MENDONÇA

DESENVOLVIMENTO DE UM MODELO DE SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO DO CRSPE

Trabalho de Graduação apresentado ao Curso de Ciência da Computação da Universidade Federal de Santa Maria - UFSM, como requisito parcial à obtenção do título de Bacharel em Ciência da Computação.

Banca Examinadora:

_____
Koiti Ozaki
Orientador

_____
Silvano Bofoni Dias

_____
Antonio Marcos Candia

Santa Maria, RS, Brasil

2004

Dedico primeiramente este trabalho ao meu bondoso pai Deus, o princípio de tudo, onde silenciosamente busco forças para superar os obstáculos. Forças estas que Ele nunca me deixou faltar.

Dedico também aos meus pais que, com seus exemplos de vida sempre me mostram o caminho certo e cujos conselhos até hoje são sábios e atuais.

AGRADECIMENTOS

Ao amigo e orientador Koiti Ozaki e a amiga, professora e co-orientadora Roseclea Duarte Medina, cuja paciência e conselhos sempre vieram na hora certa e que não pouparam esforços e preciosas horas de seu tempo em minha orientação.

A amiga e secretária Marinelma Aimi de Carvalho, que por vezes contribuiu com seus sábios conselhos, sem poupar esforços para ajudar os problemas administrativos.

Aos meus amigos de trabalho que sempre me ajudaram e sempre souberam suprir minha falta que se fizeram necessárias.

Aos meus amigos pele amizade e companheirismo que também entenderam a minha ausência e cansaço.

Aos professores e colegas que com suas presença e companheirismo me incentivaram e proporcionaram-me vários momentos de aprendizagem.

Aquelas pessoas que mesmo em anonimato contribuíram de alguma forma para a efetivação deste trabalho.

Ao Centro Regional Sul de Pesquisas Espaciais - CRSPE, que proporcionou a motivação para este trabalho em seu ambiente.

RESUMO

Encontra-se na literatura específica da área inúmeros diagnósticos e análises que ilustram o alto grau de complexidade e heterogeneidade encontrados nos atuais ambientes computacionais das organizações. Por outro lado é patente que as organizações necessitam manter seguras suas informações. No entanto, pelo nosso conhecimento, não se encontra na literatura uma metodologia básica, ou mesmo um conjunto de idéias consistentes e coerentes, que auxilie as organizações no planejamento e implantação de um sistema de segurança da informação nestes ambientes computacionais.

Visando a suprir esta deficiência, este trabalho procura apresentar um arcabouço teórico-conceitual, isto é, um esboço de *framework*, capaz de auxiliar na concepção, elaboração e implantação de sistemas de segurança da informação em ambientes computacionais complexos e distribuídos.

Para tanto, este trabalho fundamenta-se sobre a norma internacional para segurança da informação ISO/IEC 17799:2000, tem foco gerencial abordando Conceitos Gerais, Análise de Risco, Política de Segurança e Implementação de Segurança incluindo aí, Plano de Ação. Ao final existe um capítulo sobre um estudo de caso no Centro Regional Sul de Pesquisas Espaciais – CRSPE, organização que motivou o desenvolvimento deste trabalho.

Palavras-Chave: Segurança da informação, gerenciamento de segurança da informação, sistema de segurança da informação, Norma ISO/IEC 17799:2000.

SUMÁRIO

LISTA DA FIGURAS

1. INTRODUÇÃO

Ao longo da história, desde a mais remota Antigüidade, o ser humano vem buscando controlar as informações que julga importante. Conforme relaciona SCHNEIER (2001), na antiga China a própria linguagem escrita era usada como uma forma de criptografia na medida em que somente as classes superiores podiam aprender a ler e a escrever. Outros povos, como os egípcios e os romanos deixaram registrados na história suas preocupações com o trato de certas informações, especialmente as de valor estratégico e comercial. Com a Segunda Guerra Mundial, a questão da segurança ganhou uma nova dimensão, na medida em que sistemas automáticos, eletromecânicos foram criados tanto para criptografar como para efetuar a criptoanálise e quebrar a codificação.

NIMER (1998) diz que na sociedade de hoje, onde a informação é grande fonte de riqueza (e, portanto, um dos principais ativos a serem protegidos), subestimar a importância da segurança pode custar a sobrevivência das organizações que dedicam pouca atenção para os ativos de informação que possuem.

Em anos recentes, a informação assumiu importância vital para manutenção dos negócios, marcados pela dinamicidade da economia globalizada e permanentemente *on-line*, de tal forma que, atualmente, não há organização que não dependa da tecnologia de informações, em maior ou menor grau, de forma que o comprometimento do sistema de por problemas de segurança pode causar grandes prejuízos.

Visando minimizar esses riscos, a ISO (International Standardization Organization), publicou uma norma internacional para garantir a segurança das informações nas empresas a ISO/IEC 17799:2000. A ABNT (Associação Brasileira de Normas Técnicas) operando em sintonia com a ISO e atenta às necessidades nacionais quanto à segurança da informação, disponibilizou o projeto na versão brasileira da norma NBR ISO/IEC 17799:2001.

Segundo a NBR ISO/IEC 17799 (2001), os seguintes fatores são considerados críticos na implantação de sistemas de segurança da informação dentro de uma organização:

- Política de segurança, objetivos e atividades, que reflitam os objetivos do negócio;
- Um enfoque para a implementação da segurança da informação que vá ao encontro da cultura da organização;
- Comprometimento e apoio da administração;
- Bom entendimento dos requisitos de segurança, análise de riscos e gerenciamento de risco;
- Conhecimento das regras de segurança por todos os funcionários e terceiros;
- Treinamento adequado para uso das normas e políticas;
- Abrangente sistema de medição, usado para avaliar o desempenho do gerenciamento da segurança.

Neste contexto esse trabalho procura adequar as recomendações da norma ao Centro Regional Sul de Pesquisas Espaciais - CRSPE, que tem como missão desenvolver atividades de pesquisa e da formação de recursos humanos especializados, do desenvolvimento tecnológico e dos serviços relacionados às Ciências Espaciais, Ciências Atmosféricas, Clima e Metereologia e Sensoriamento Remoto, às tecnologias e suas engenharias associadas em convenio com a Universidade Federal de Santa Maria – UFSM.

O CRSPE está em fase de formação de suas instalações, tanto lógicas quando físicas com objetivo final de suportar um maior número de recursos de Tecnologia da Informação (TI)[1], cujo grau de importância é significativo no cenário da pesquisa espacial, necessitando assim em curto prazo da implementação de um modelo de segurança da

[1] *Entende-se por TI: Hardware, Software e Peopleware.*

informação com padrões internacionais que implantados juntamente com a fase de formação do Centro[2] tem maior facilidade de alcançar sucesso em seus objetivos.

1.1. ESTRUTURA DO TRABALHO

O capítulo 2 trata dos conceitos básicos relacionados à Segurança da Informação, identificando alguns novos termos, mostrando os princípios da segurança, ameaças, vulnerabilidades e ativos da informação segundo NBR ISO/IEC 17799 (2001).

O capítulo 3 trata da análise de riscos, mostrando sua importância no contexto da Segurança de uma Organização e como deve ser desenvolvida para facilitar o levantamento das vulnerabilidades que estão sujeitas as ameaças em potencial.

O capítulo 4 apresenta a Política de Segurança, com os elementos que fazem parte da sua definição, elaboração e implantação, bem como as etapas de sua produção e a importância da sua difusão dentro cultural dentro da Organização.

O capítulo 5 trata da implementação prática da Política na organização, com suas técnicas de planejamento e Planos de Ação com a finalidade de aumentar a eficiência sem causar um impacto de seu desenvolvimento.

O capítulo 6 faz um estudo de caso onde se aplica a metodologia proposta no ambiente em estudo, o CRSPE, sendo possível notar os passos descritos nos capítulos anteriores, quando começamos a estudar a norma a ser adotada, desenvolvendo a análise de riscos e gerando uma Política de Segurança que será proposta como ponto inicial da Segurança da Informação.

O capítulo 7 apresenta as conclusões em torno do modelo proposto e busca uma reflexão confrontando o direcionamento que o trabalho tomou e os objetivos inicialmente propostos. Além disso, discorre-se sobre o que se poderia realizar sobre a metodologia proposta visando reforçar os pontos fortes e minimizar os pontos fracos. Como a tecnologia mostra-se extremamente dinâmica fica uma ponderação sobre eventuais modificações que podem servir bem como sugestão para trabalhos futuros visando acompanhar e se ajustar a essas transformações fechando o ciclo da Segurança da Informação.

---

[2] *Centro: Entenda-se Centro Regional Sul de Pesquisas Espaciais – CRSPE.*

2. CONCEITOS BÁSICOS

Desde o surgimento da raça humana no planeta, a informação esteve presente sob diversas formas e técnicas. O homem buscava representar seus hábitos, costumes e intenções em diversos suportes que pudessem ser utilizados por ele e por outras pessoas, que pudessem também ser levados de um lugar para outro. As informações valiosas eram registradas em objetos preciosos e sofisticados, pinturas magníficas, que eram armazenados com muito cuidado, em locais de difícil acesso, cuja forma e conteúdo eram apenas acessados por quem fosse autorizado ou preparado para interpretá-la.

Hoje em dia as informações são o objeto de maior valor para as empresas. O progresso da informática e das redes de comunicação nos mostra um novo cenário, onde os objetos do mundo real estão representados por bits e bytes que ocupam lugar em uma outra dimensão e possuem formas diferentes das originais, não deixando de ter o mesmo valor que seus objetos reais, e, em muitos casos, vindo a ter um valor superior.

Por estes e outros motivos que a segurança das informações é um assunto tão importante para todos, pois afeta diretamente os negócios de uma empresa ou de um indivíduo. Ela tem como objetivo proteger as informações que se encontram registradas, onde quer que estejam: em papéis, nos discos rígidos de computadores ou até na memória das pessoas que as conhecem.

Os objetos reais são protegidos por técnicas que os encerram atrás de grades ou dentro de cofres, sob a mira de câmeras ou guardas de segurança. Mas e as informações que se encontram dentro de servidores de arquivos, que trafegam pelas redes de comunicação ou que são lidas em uma tela de computador? Como fazer para protegê-las, já que não é possível usar as mesmas técnicas da proteção de objetos reais?

Estas são as preocupações da segurança da informação: proteger os elementos que fazem parte da comunicação. Assim, para começar, é necessário identificar os elementos que a segurança da informação busca proteger.

Figura 2-1. Estes elementos são o que chamamos de ativos

2.1. ATIVOS

A figura 2-1 mostra os três elementos que juntos formam o que a NBR ISO/IEC 17799 (2001) chama de ativo: as informações, os objetos que as suportam e as pessoas que as utilizam. Um ativo é todo elemento que compõe o processo da comunicação, a contar da informação, seu emissor, o meio pelo qual ela trafega, até seu receptor.

Os ativos são elementos que a Segurança da Informação visa proteger. Eles possuem um valor para as empresas e em conseqüência precisam ter uma proteção adequada para que seus negócios não sejam prejudicados.

Os ativos podem ser divididos em grupos, que apresentamos abaixo, também com alguns exemplos.

2.1.1. EQUIPAMENTO

Estes ativos representam toda a infra-estrutura tecnológica que suporta a informação durante o seu uso, tráfego e armazenamento. Os ativos pertencentes a este grupo englobam os computadores, os servidores de arquivos, notebook, mainframe, as mídias, os equipamentos de conectividade, roteadores, switches, dentre outros, ou seja, elementos de uma rede de computadores por onde a informação trafega.

2.1.2. APLICAÇÕES

Este grupo de ativos contém todos os programas de computador utilizados para a automatização de processos, ou seja, acesso, leitura, tráfego e armazenamento da informação. Dentre eles citamos os softwares de mercado, programas institucionais, sistemas operacionais, etc. A segurança da informação busca avaliar a forma como as aplicações são criadas, como estão disponibilizadas e a forma como são utilizados pelos usuários e por outros sistemas, para detectar e corrigir problemas existentes na comunicação entre eles.

Os sistemas e suas aplicações devem estar seguros para que a comunicação entre os bancos de dados, outras aplicações e os usuários seja realizada de forma segura, atendendo aos princípios básicos da segurança da informação.

Exemplos: Sistema operacional (Unix, Windows, Linux, sistemas informatizados, aplicações específicas etc.), Programas de Correio Eletrônico, Sistemas de backup, Banco de Dados, Firewalls, etc.

2.1.3. INFORMAÇÃO

Este grupo de ativos engloba os elementos que contém informação registrada, em meio magnético ou físico, como documentos, relatórios, livros, manuais, correspondências, patentes, informações de mercado, códigos de programação, linhas de comando, arquivos de configuração, contracheques de funcionários, plano de negócio de uma empresa, etc.

2.1.4. USUÁRIOS

O grupo usuários refere-se aos indivíduos que fazem uso da estrutura de comunicação da empresa e que manipulam as informações. O foco da segurança nos usuários está voltado à conscientização de ou para formação de hábitos de segurança para a tomada de decisão e ação por parte de todos os funcionários de uma empresa, desde a sua alta direção até os usuários finais da informação, incluindo os grupos que mantêm a estrutura tecnológica em funcionamento, como os técnicos, operadores, administradores de ambientes tecnológicos.

2.1.5. ORGANIZAÇÃO

Neste grupo estão incluídos os itens que compõem a estrutura física e organizacional das empresas. Quanto ao ambiente físico, são considerados: salas e armários onde estão localizados os documentos, fitoteca, sala de servidores de arquivos, etc.

2.2. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Proteger os ativos significa mantê-los seguros contra ameaças que possam afetar sua funcionalidade: os mesmos podem ser corrompidos, podem se acessados indevidamente ou podem até ser eliminados ou furtados.

Logo, entendemos que a segurança da informação visa proteger esses ativos de uma empresa ou de um individuo, com base na preservação de três princípios básicos, segundo PUTTINI (2001): confidencialidade, disponibilidade e integridade das informações, veremos mais detalhes destes princípios a seguir.

2.2.1. CONFIDENCIALIDADE

As informações que são trocadas entre indivíduos e empresas nem sempre devem ser conhecidas por todo mundo. Muitas das informações geradas pelas pessoas são destinadas a um grupo restrito de indivíduos, e muitas vezes a uma única pessoa. Isso significa que as informações devem ser conhecidas apenas por um grupo controlado de pessoas, definido por quem é o responsável pelas informações. Logo, elas possuem um grau de confidencialidade que deve ser preservado para que pessoas sem autorização não as conheçam.

Ter confidencialidade na comunicação é ter certeza de que o que foi dito a alguém ou escrito em algum lugar será escutado ou lido apenas por quem tiver direito. Perder confidencialidade quer dizer perda de segredo. Se uma informação é confidencial, é secreta, deve ser guardada com segurança para não ser divulgada para pessoas não autorizadas.

Por exemplo, o numero de um cartão de credito só pode ser conhecido pelo seu dono e pelo vendedor da loja onde ele é usado. Se este número é descoberto por alguém mal intencionado, como nos casos denunciados nos jornais de crimes na internet, o prejuízo dessa perda de confidencialidade pode ser muito alto, pois este número poderá ser usado

por um criminoso para fazer compras via internet, trazendo prejuízos financeiros e muita dor de cabeça para o dono do cartão.

Também no caso de uso indevido de senhas de acesso a sistemas de bancos, por exemplo. Muito dinheiro é roubado diariamente por conta da ação de criminosos virtuais que se dedicam a invadir sistemas para quebrar a confidencialidade de pessoas e empresas.

Garantir a confidencialidade é um dos fatores determinantes para segurança e uma das tarefas mais difíceis de se implementar, pois envolve todos os elementos que fazem parte da comunicação da informação, desde seu emissor, o caminho que ela percorre, até seu receptor. E também, quanto mais valiosa for uma informação, maior deve ser o seu grau de confidencialidade. E quanto maior o grau de confidencialidade, maior será o nível de segurança necessário da estrutura tecnológica e humana que participa deste processo, do uso, acesso, tráfego e armazenamento das informações.

A confidencialidade deve ser considerada com base no valor que a informação tem para a empresa e os impactos que a sua divulgação indevida pode causar. Assim sendo, ela deve ser acessada, lida e alterada apenas por aqueles indivíduos que possuem permissões para tal. O acesso deve ser considerado com base no grau de sigilo das informações, pois nem todas as informações sensíveis da empresa são confidenciais.

Mas garantir apenas a confidencialidade das informações não é o suficiente, é importante que além de confidenciais, as informações devem estar integras também. Logo, vamos ver o que é manter a integridade de uma informação, segundo principio básico da segurança da informação.

2.2.2. INTEGRIDADE

Uma informação íntegra é uma informação original, que não tenha sido alterada de forma indevida, não autorizada. Para que as informações possam ser utilizadas elas devem estar íntegras. Quando há a alteração de informações em um documento, quer dizer que a sua integridade foi perdida.

A integridade das informações é fundamental para o sucesso da comunicação. O receptor de uma informação deve ter a certeza de que a informação acessada lida ou ouvida é exatamente a mesma que foi disponibilizada a ele para a devida finalidade.

A quebra de integridade ocorre quando as informações são corrompidas, falsificadas ou burladas. Logo, garantir a integridade é um dos principais objetivos para que haja segurança das informações de um indivíduo ou empresa.

Uma informação pode ser alterada de várias formas, tanto o seu conteúdo quanto o ambiente que a suporta. Logo, a quebra de integridade de uma informação pode ser considerada sob dois aspectos:

1. **Alterações do conteúdo de documentos** - inserções, substituições ou remoções de partes de seu conteúdo;
2. **Alterações nos elementos que suportam a informação** – alterações na estrutura física e lógica onde uma informação está armazenada, por exemplo, quando são alteradas as configurações de um sistema para se ter acesso a informações restritas, quando são ultrapassadas as barreiras de segurança de uma rede de computadores. Todos são exemplos de quebra de integridade que afetam a segurança. Logo, a prática da segurança da informação tem como objetivo impedir que eventos de quebra de integridade ocorram, vindo causar danos às pessoas e empresas.

Buscar a integridade é garantir que apenas as pessoas autorizadas possam fazer alterações na forma e conteúdo de uma informação, assim como no ambiente no qual ela é armazenada e pelo qual ela trafega, ou seja, em todos os ativos.

Logo, é necessário, para garantir a integridade, que todos os elementos que compõem a base para a gestão da informação sejam mantidos em suas condições originais definidas pelos seus responsáveis e proprietários.

2.2.3. DISPONIBILIDADE

Para que uma informação possa ser utilizada, ela deve estar disponível. Este é o terceiro princípio básico da segurança da informação: a disponibilidade da informação e de toda a estrutura física e tecnológica que permite a sua leitura, tráfego e armazenamento.

Garantir segurança na disponibilidade das informações é permitir que a mesma seja utilizada quando necessária e que esteja ao alcance de seus usuários e destinatários no momento em que precisam fazer uso delas.

Este princípio está associado à adequada estruturação de um ambiente tecnológico e humano que permita a continuidade dos negócios da empresa sem impactos negativos para a utilização das informações.

Não bastam estar disponíveis, as informações devem estar acessíveis de forma segura para que possam ser usadas no momento em que são solicitadas e que sua integridade e confidencialidade sejam garantidas.

Assim, o ambiente tecnológico e os suportes da informação devem estar funcionando corretamente e de forma segura para que a informação neles armazenada e que por eles trafega possa ser utilizada por seus usuários.

Para que a disponibilidade das informações possa ser garantida. É preciso conhecer quais são os seus parceiros de negócio, com base no principio da confidencialidade, para que possam ser organizadas e definidas as formas de disponibilizá-las, garantindo, conforme o caso, o seu acesso e uso quando necessárias.

1. A disponibilidade das informações deve ser considerada com base no valor que a informação tem e no impacto decorrente da sua indisponibilidade.
2. Para garantir a disponibilidade, muitas ações são tomadas. Dentre elas destaca a configuração segura de um ambiente, onde todos os elementos que fazem parte da cadeia da comunicação estão dispostos de forma adequada, garantindo o sucesso da leitura, tráfego e armazenamento da informação. Para também garantir a disponibilidade, são realizadas as cópias de segurança – backup. Fazer o backup de informações permite que elas estejam duplicadas em um outro local para serem utilizadas caso não seja possível recuperá-las de sua base original.

Para aumentar ainda mais a disponibilidade das informações, devem ser definidas estratégias para situações de contingência. Rotas alternativas para o trafego da informação também podem ser estabelecidas, a fim de garantir o seu acesso e a continuidade dos

negócios mesmo quando alguns dos recursos tecnológicos, ou humanos, não estejam em perfeitas condições de operação.

2.3. AMEAÇAS

As ameaças são agentes capazes de explorar falhas de segurança, que chamamos de vulnerabilidades e, conseqüentemente, causar perdas ou danos aos ativos de uma empresa, trazendo impactos aos seus negócios.

Os ativos estão constantemente submetidos a ameaças que podem colocar em risco a integridade, confidencialidade e disponibilidade das informações. Estas ameaças sempre existirão, pois estão relacionadas a causas naturais ou não, internas ou externas, que venham a representar riscos para a empresa. No entanto, a segurança da informação visa à implementação de controles e medidas que impeçam a concretização destas ameaças, para garantir que o negócio da empresa não seja prejudicado.

As ameaças são constantes e podem ocorrer a qualquer momento. Esta relação está baseada no conceito de risco. De acordo com SÊMOLA (2001) elas podem ser divididas em três grandes grupos:

1. **Naturais:** condições da natureza e suas intempéries que podem causar danos aos ativos, como fogo, terremoto, inundação.
2. **Intencionais:** são ameaças propositais, representadas por vírus eletrônicos, fraude, vandalismo, sabotagem, espionagem, invasões e ataques, roubos e furtos de informação, dentre outras.
3. **Involuntárias:** são ameaças decorrentes de ações inconscientes de usuários, muitas vezes causada pela falta de conhecimento dos ativos, como os erros, acidentes, falta de conhecimento etc.

Logo, entendemos que um dos objetivos da segurança da informação é impedir que ameaças explorem vulnerabilidades e afetam um dos princípios básicos da segurança da informação, causando danos ao negócio das empresas.

A análise de OLIVEIRA (1998) é corroborada pela 9ª Pesquisa Nacional sobre Segurança da Informação, MÓDULO (2004), que aponta que os vírus constituem, ainda

hoje, uma das maiores ameaças à segurança da informação nas organizações, conforme ilustra a Figura 2-2.

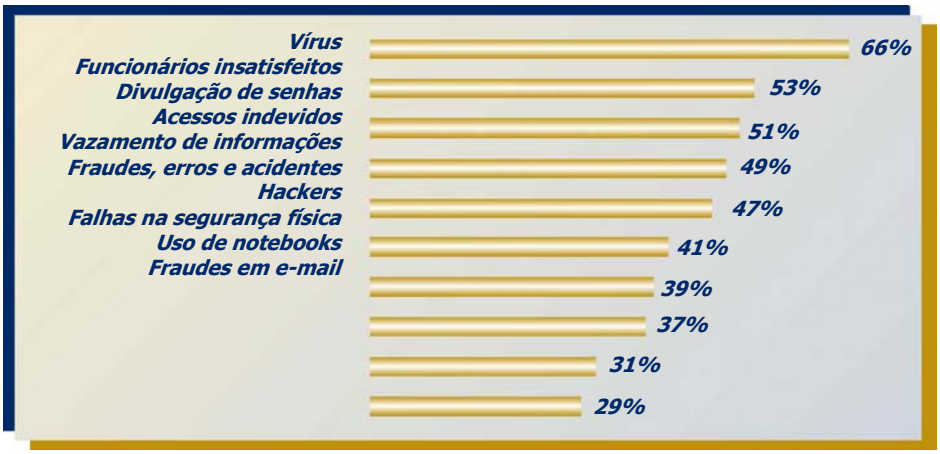

Figura 2-2. 9ª Pesquisa Nacional sobre Segurança da Informação.

Na 9ª Pesquisa Nacional sobre Segurança da Informação realizada pela Módulo Security Solutions S.A. este ano, são revelados os elementos que apresentam as principais ameaças às informações das empresas brasileiras. Dentre as principais ameaça, a ocorrência de vírus, divulgação de senhas, ação de hackers e funcionários insatisfeitos estão entre os mais freqüentes.

2.4. VULNERABILIDADES

SÊMOLA (200) diz que as vulnerabilidades são os elementos que, ao serem explorados por ameaças, afetam a confidencialidade, disponibilidade e integridade das informações de um indivíduo ou empresa. As vulnerabilidades são os elementos a serem rastreados e eliminados de um ambiente de tecnologia da informação, sendo este um dos primeiros passos para a implementação da segurança.

Ao se identificarem as vulnerabilidades, será possível dimensionar as ameaças às quais o ambiente está suscetível e definir as medidas de segurança apropriadas para a sua correção.

Vulnerabilidades são dependentes da forma com que foi organizado o ambiente em que a informação é manipulada. A existência de vulnerabilidades está relacionada à

presença de elementos que prejudiquem o uso adequado da informação e do meio em que ela está sendo utilizada.

Podemos compreender agora mais dos objetivos da segurança da informação: a correção de vulnerabilidades existentes no ambiente em que a informação é usada a fim de reduzir os riscos a que está submetida, evitando-se assim a concretização de uma ameaça.

A divisão das vulnerabilidades em categorias facilita o reconhecimento das mesmas. São elas:

2.4.1. FÍSICAS

As vulnerabilidades de ordem física são aquelas presentes nos ambientes em que a informação esta sendo armazenada ou manipulada. Exemplos disso são: instalações inadequadas do espaço de trabalho, ausência de recursos para combate a incêndio, disposição desorganizada de fios de energia e cabos de rede, ausência de identificação de pessoas e de locais, dentre outros.

Estas vulnerabilidades, ao serem exploradas por ameaças, afetam diretamente os princípios básicos da segurança da informação, principalmente a disponibilidade.

2.4.2. NATURAIS

As vulnerabilidades naturais são aquelas relacionadas às condições da natureza que possam colocar em risco as informações.

Muitas vezes a umidade, a poeira, a poluição, podem causar danos aos ativos. Portanto, os mesmos devem estar protegidos para que suas funcionalidades sejam garantidas.

O levantamento das ameaças naturais é determinante na escolha e montagem de um ambiente. Deve-se tomar cuidados especiais com o local, de acordo com o tipo de ameaça que possa ocorrer em uma dada região geográfica. Dentre as ameaças naturais mais comuns podemos citar ambientes sem proteção contra incêndio, locais próximos a rios suscetíveis a inundações, infra-estrutura despreparada para resistir às intempéries da natureza como terremotos, maremotos, furacões, etc.

2.4.3. HARDWARE

Muitos são os elementos que representam vulnerabilidades de hardware. Dentre eles podemos citar a ausência de atualizações conforme orientações dos fabricantes dos programas que são utilizados e conservação inadequada dos equipamentos.

Por isso, a segurança da informação busca avaliar se o hardware utilizado está dimensionado corretamente para as suas funcionalidades, se possui área de armazenamento suficiente, processamento e velocidades adequadas. Logo, entendemos que a segurança das informações também está associada ao desempenho dos equipamentos envolvidos na comunicação, pois se preocupa com a qualidade do ambiente que foi montado para o tráfego, armazenamento e leitura da informação.

2.4.4. SOFTWARE

Os softwares são os elementos que realizam a leitura da informação e que permite o acesso dos usuários às informações em meio eletrônico e, por esta razão, torna-se o alvo predileto de agentes causadores de ameaças.

Dentre eles, destacamos os sistemas operacionais como o Windows e o Unix, que oferecem a interface para configuração e organização de um ambiente tecnológico. Estes são alvo de ataques, pois por seu intermédio podem ser feitas quaisquer alterações da estrutura de um computador ou rede. Também são passíveis de vulnerabilidade de software os programas utilizados para edição de texto e imagem, para automatização de processos e os que permitem a leitura da informação de uma pessoa ou empresa, como os browsers de página da internet.

Estes softwares estão vulneráveis a várias ações que afetam a sua segurança, como por exemplo, a configuração e instalação inadequadas, ausência de atualização, programação insegura, etc.

As vulnerabilidades de software permitem que acessos indevidos a sistemas informatizados ocorram até mesmo sem o conhecimento de um usuário ou administrador de rede.

2.4.5. MÍDIAS

As mídias são os suportes físicos utilizados para armazenar as informações. Dentre elas estão os disquetes, cd-roms, fitas magnéticas, discos rígidos de servidores de banco de dados, assim como o arsenal documentário registrado em papel. Se estes suportes não forem utilizados de forma adequada, a informação neles contida pode estar vulnerável a uma série de fatores que podem afetar a integridade, disponibilidade e confidencialidade das informações.

As mídias podem ser afetadas por vulnerabilidades que venham a danificá-las e até mesmo indisponibilizá-las. Dentre estas vulnerabilidades, destacamos as seguintes:

1. Prazo de validade vencido;
2. Defeito de fabricação;
3. Uso incorreto;
4. Local de armazenamento em locais insalubres, com alta umidade, mofo, etc.

2.4.6. COMUNICAÇÃO

Este tipo de vulnerabilidade abrange todo o trafego da informação.

Onde quer que a informação trafegue, seja via cabo, satélite, fibra ótica, ondas de radio ou outro meio, de haver segurança. O sucesso no tráfego dos dados é um aspecto crucial na implementação da segurança da informação.

Uma grande quantidade de informação é trocada através de meios de comunicação que rompem barreiras físicas tais como telefone, internet, Wap, fax, telex, etc. Sendo assim, estes meios devem receber tratamento de segurança adequado.

Qualquer falha na comunicação pode tornar uma informação indisponível para seus usuários, ou o contrário: estar disponível para quem não possui direitos de acesso. Também podem levar à alteração da informação em seu estado original, afetando sua integridade.

2.4.7. HUMANAS

Esta categoria de vulnerabilidade está relacionada aos danos que as pessoas podem causar às informações e ao ambiente tecnológico que as suporta.

As vulnerabilidades humanas podem também ser intencionais ou não. Muitas vezes erros e acidentes que ameaçam a segurança da informação ocorrem em ambientes institucionais. O maior deles é o descobrimento das medidas de segurança adequadas a serem adotadas por cada elemento constituinte, principalmente os membros internos à empresa.

Destacamos como vulnerabilidades humanas internas a falta de capacitação específica para a execução de atividades inerentes às funcionalidades de cada um, falta de consciência de segurança para atividades rotineiras, erros, omissões, insatisfações, etc.

Quanto às vulnerabilidades humanas de origem externa podemos considerar todas aquelas que possam ser exploradas por ameaças como vandalismo, fraudes, invasões, etc. São elas: senhas fracas, não uso de criptografia na comunicação, compartilhamento de identificadores como nome de usuário ou crachá de acesso, etc.

2.5. RISCOS

O risco é a probabilidade das ameaças explorarem vulnerabilidades, causando perdas ou danos aos ativos e impactos ao negócio, ou seja, afetando a confidencialidade, integridade e disponibilidade das informações de acordo com a NBR ISO/IEC 17799 (2001). A figura 2-3 mostra a relação que ocorre quando o risco aumenta, causando um maior impacto na empresa, ou seja, a possibilidade de ocorrer um incidente é proporcional às ameaças e às vulnerabilidades a que a organização está esposta.

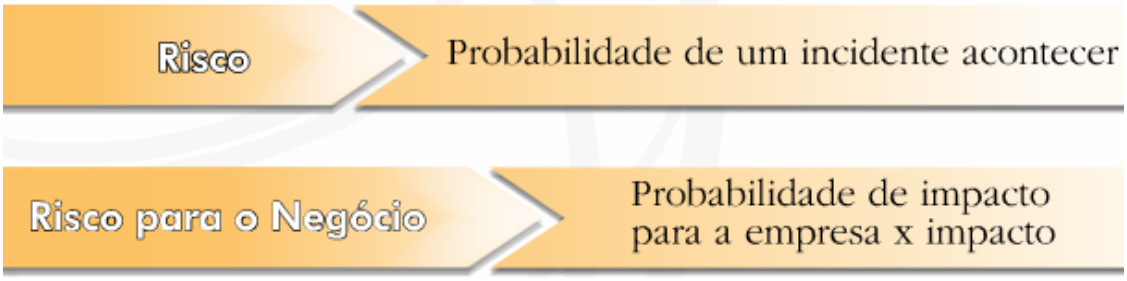

Figura 2-3. Risco X Impacto

Logo, concluímos que a segurança é uma pratica voltada à eliminação de vulnerabilidades para reduzir os riscos de uma ameaça se concretizar no ambiente que se quer proteger. Garantir o sucesso da comunicação segura é o principal objetivo, por meio de medidas de segurança que possam viabilizar o negócio de um indivíduo ou empresa com o menor risco possível.

2.6. MEDIDAS DE SEGURANÇA

As medidas de segurança são ações voltadas à eliminação de vulnerabilidades com vistas a evitar a concretização de uma ameaça. Estas medidas fazem parte do passo inicial para o aumento da segurança da informação em um ambiente de tecnologia e deve considerar o todo.

Uma vez que há uma variedade de tipos de vulnerabilidades que afetam a disponibilidade, confidencialidade e integridade da informação, deve haver medidas de segurança específicas para o tratamento de cada caso. Antes de se definirem as medidas de segurança a serem adotadas, deve-se conhecer o ambiente em seus mínimos detalhes, à busca das vulnerabilidades existentes.

A partir deste conhecimento, tomam-se as ações de segurança que podem ser de cunho **preventivo** (buscando evitar o surgimento de novas vulnerabilidades e ameaças), **detectivo** (voltado à revelação de atos que ponham em risco a informação) ou **corretivo** (voltado à correção dos problemas de segurança conforme sua ocorrência).

As medidas de segurança são as práticas da segurança da informação, representando vários elementos que ao serem integrados, constituem uma solução de segurança global e eficiente. Dentre as principais medidas de segurança, destacamos:

1. **Analise de riscos** – medida que busca rastrear um ambiente à procura de vulnerabilidades que possam ser exploradas por ameaças. A análise de riscos tem como resultado um grupo de recomendações para a correção dos ativos que os mesmos possam ser protegidos.
2. **Política de Segurança** – é uma medida que busca estabelecer os padrões de segurança a serem seguidos por todos os envolvidos com o uso e manutenção dos ativos. É uma forma de prover um conjunto de normas

para guiar as pessoas na realização de seus trabalhos. É o primeiro passo para aumentar a consciência de segurança das pessoas, pois está voltada à formatação de hábitos, por meio de manuais de instrução e procedimentos operacionais.

3. **Especificação de segurança** – medidas que visam a correta implementação de um novo ambiente tecnológico, por meio do detalhamento de seus elementos constituintes e a forma com que eles devem estar dispostos para atender aos princípios da segurança da informação.
4. **Administração de segurança** – medidas integradas para que haja uma gerência dos riscos de um ambiente. A administração de segurança envolve todas as medidas citadas acima, de forma preventiva, detectiva e corretiva, com base no ciclo da segurança que apresentamos a seguir.

2.7. CICLO DA SEGURANÇA DA INFORMAÇÃO

No ciclo de segurança mostrado na figura 2-4 podemos visualizar os fatores que contribuem para a existência e diminuição dos riscos, que surgem em decorrência da presença de vulnerabilidades exploradas por ameaças devido às falhas de configuração ou inexistência de medidas de proteção adequadas.

Conforme MOREIRA (2001) o ciclo se inicia com a identificação das ameaças às quais as empresas estão submetidas. A identificação das ameaças permitirá a visualização das vulnerabilidades que podem ser exploradas, expondo os ativos a riscos de segurança.

Esta exposição leva à perda de um ou mais princípios básicos da segurança da informação, causando impactos no negócio da empresa, vindo a aumentar ainda mais os riscos que as informações estão expostas.

Para que os impactos dessas ameaças ao negócio possam ser diminuídos, medidas de segurança são tomadas para impedir a ocorrência de vulnerabilidades.

Figura 2-4. Ciclo da Segurança da Informação

A segurança é uma atividade dedicada à proteção de ativos contra acessos não autorizados, alterações indevidas ou indisponibilidade das informações pertencentes a um indivíduo ou empresa, viabilizada por meio de políticas e procedimentos de segurança que permitiam a identificação e controle de ameaças e vulnerabilidades, preservando a confidencialidade, integridade e disponibilidade das informações.

A figura 2-5 mostra que os ativos são os elementos que sustentam a operação do seu negócio e estes sempre trarão consigo vulnerabilidades. As ameaças por sua vez, mesmo mudando sua forma de ação, sempre existirão. Assim, a segurança entra como uma camada isolante que irá minimizar os riscos e evitar que as ameaças se aproveitem das vulnerabilidades e alcancem os ativos, atingindo então o seu negócio.

Figura 2-5. Impacto no Negócio

3. ANÁLISE DE RISCOS

Este capítulo apresenta os conceitos referentes à atividade de análise de riscos, também conhecida como análise de segurança.

Antes de se implementar a segurança, é fundamental que o ambiente seja conhecido nos seus mínimos detalhes. O ambiente que suporta um processo de negócio da organização deve ser compreendido quanto à sua composição e criticidade, para que sejam priorizadas as ações de segurança junto aos processos mais críticos, de acordo com a relevância que os mesmos têm para o alcance dos objetivos da organização.

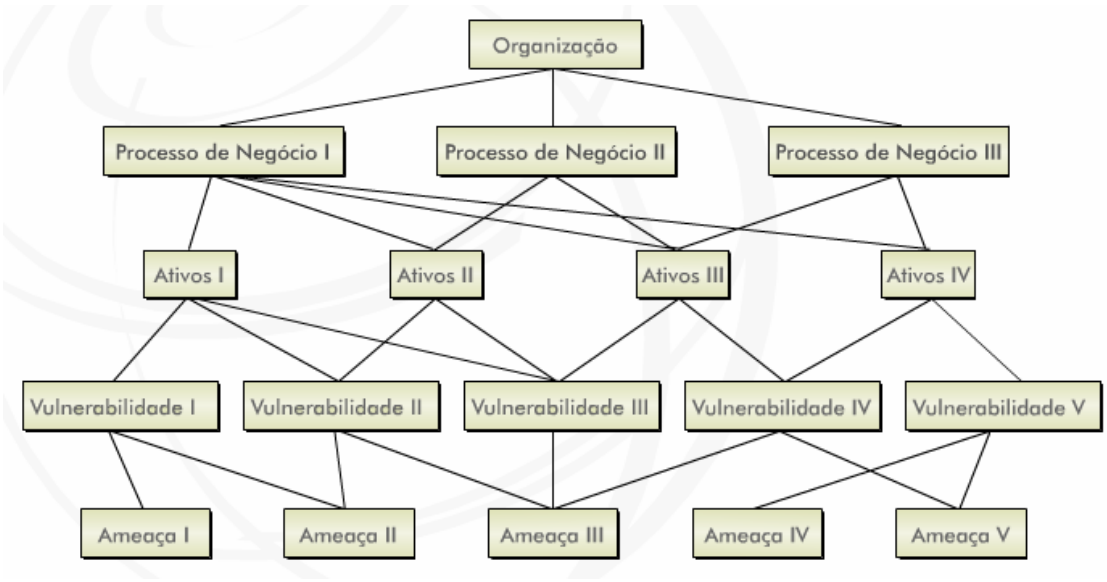

Figura 3-1. Ambiente Organizacional

Na figura 3-1 podemos notar que os passos da análise de riscos levam ao conhecimento sistêmico e específico de um processo de negócio, permitindo a identificação de seus elementos constituintes. Isto é, identificar:

1. Os processos de negócio da organização;
2. Os ativos que os compõem, considerando-se toda a infra-estrutura tecnológica, organizacional e humana;

3. As ameaças potenciais que podem causar incidentes de segurança;
4. As vulnerabilidades presentes nos ativos definidos para devida correção.

3.1. O QUE É ANÁLISE DE RISCOS

De acordo com a NBR ISO/IEC 17799 (2001), a análise de riscos é um passo importante para se implementar a segurança da informação. Como o próprio nome já diz, ela é realizada para que sejam analisados os riscos aos quais os ativos de uma organização estão submetidos, ou seja, qual é a probabilidade de ameaças se concretizarem.

As ameaças se concretizam por meio de falhas de segurança, que conhecemos como vulnerabilidades e que devem ser eliminadas ao máximo para que o ambiente que se deseja proteger esteja livre de riscos de incidentes de segurança.

Logo, compreendemos que a análise de riscos é uma atividade voltada à identificação de falhas de segurança que evidenciem vulnerabilidades que possam ser exploradas por ameaças, causando impactos aos negócios da organização. Esta análise visa, por meio deste rastreamento, identificar os riscos aos quais os ativos estão expostos. O resultado da análise de riscos é a consolidação das vulnerabilidades encontradas, as ameaças que podem explorá-las, os potenciais impactos e as recomendações para que as mesmas sejam corrigidas ou reduzidas.

Um outro importante elemento a ser considerado quando da realização da análise de riscos é a relação custo-benefício. Este cálculo permite que sejam avaliadas as medidas de segurança quanto à sua aplicabilidade e o benefício que ela irá agregar ao negócio. Logo, esta visão irá orientar a implementação das medidas de segurança apenas nas situações em que a relação custo-benefício é justificada.

Todavia, é fundamental que esteja claro na organização esta relação, ou seja, os envolvidos na implementação da segurança (a equipe de execução do projeto, a alta administração e todos seus usuários) devem estar conscientes dos benefícios que as medidas de segurança a serem sugeridas irão trazer para os indivíduos e para a organização como um todo.

3.2. MOMENTO DA ANÁLISE DE RISCOS

A análise de riscos pode acontecer antes ou depois da definição de uma política de segurança. De acordo com NBR ISO/IEC 17799 (2001), esta atividade pode ser feita após a definição da política para que a mesma possa balizar a realização da análise, verificando-se nos ativos os pontos vulneráveis que contradizem o que nela foi estabelecido, com base nas ameaças potenciais que foram definidas de antemão.

No entanto, a realização da análise de riscos como primeiro elemento da ação de segurança é fato determinante para processos críticos em que todas as ameaças são consideradas. Desta forma, todos os ativos da organização (analisados em sua totalidade ou por amostragem) podem ser considerados e analisados para estarem isentos de vulnerabilidades, visando a redução dos riscos.

No próximo capítulo iremos entender o que é uma política de segurança. Enquanto isso, serão abordados neste capítulo todos os elementos necessários para a realização de uma análise de riscos como etapa de rastreamento de vulnerabilidades de todo o ambiente de um processo de negócios.

3.3. FOCOS DA ANÁLISE DE RISCOS

A análise de riscos como mostra a figura 3-2 pode ser realizada em diversos âmbitos. Geralmente todos eles são considerados, uma vez que a implementação de segurança visa a correção de todo o ambiente no qual está inserida a informação e suas atividades de geração, tráfego, processamento e armazenamento.

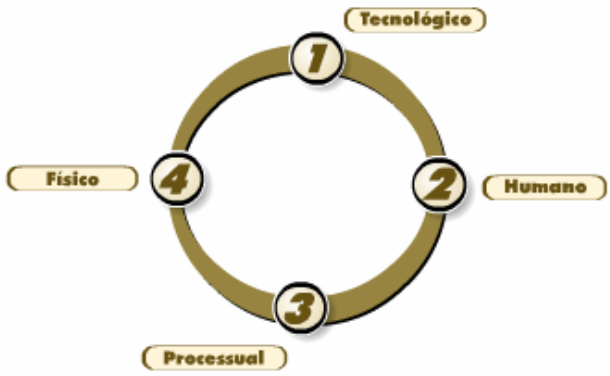

Figura 3-2. Focos da Análise de Riscos

3.3.1. TECNOLÓGICO

A análise de riscos realizada no ambiente tecnológico visa o conhecimento das configurações e da disposição topológica dos ativos de tecnologia que compõem toda a infra-estrutura de suporte da informação para comunicação, processamento, tráfego e armazenamento das mesmas. Neste caso são considerados em primeira instância os ativos do tipo aplicação e equipamento, não se deixando de considerar também a sensibilidade das informações que são por eles manipuladas, os usuários que os utilizam e também a infra-estrutura que os suporta.

3.3.2. HUMANO

A análise de riscos também está voltada à compreensão da forma com que as pessoas se relacionam com os ativos. Diversos são os aspectos analisados, como por exemplo: o nível de acesso que as pessoas possuem na rede ou nas aplicações, quais as restrições e permissões elas precisam ter para a realização de suas tarefas junto aos ativos, qual o nível de capacitação e formação educacional que as mesmas precisam ter para manipulá-los, etc. Assim sendo, é possível detectar a que vulnerabilidades, oriundas de ações humanas, os ativos estão submetidos, podendo-se direcionar recomendações para a melhoria da segurança no trabalho humano e garantia da continuidade dos negócios da organização. Esta análise visa em primeira mão identificar vulnerabilidades nos ativos do tipo usuário e organização.

3.3.3. PROCESSUAL

Análise dos fluxos de informação da organização e a forma com que as informações trafegam de uma área para outra, como são geridos os recursos em termos de organização e manutenção. Desta forma, será possível identificar os elos entre as atividades e os insumos necessários para sua realização a fim de identificar as vulnerabilidades que possam afetar a confidencialidade, disponibilidade e integridade das informações e, conseqüentemente, do negócio da organização. Ao identificarem-se as pessoas envolvidas no fluxo de informações, é possível avaliar a real necessidade de acesso que as mesmas têm

aos ativos, avaliando-se os impactos decorrentes do uso indevido da informação por pessoas não autorizadas. Neste âmbito, o ativo foco principal é do tipo usuário e informação.

3.3.4. FÍSICO

A análise física de segurança visa identificar, na infra-estrutura física do ambiente em que os ativos estão contidos, vulnerabilidades que possam trazer algum prejuízo à informação e a todos os demais ativos. Os focos principais deste âmbito de análise são os ativos do tipo organização, pois são aqueles que dão o suporte físico ao ambiente em que está sendo manipulada a informação.

3.4. ATIVIDADES DA ANÁLISE DE RISCOS

Uma análise de riscos é realizada por meio de um conjunto de atividades pré - estabelecidas que visem identificar o processo a ser considerado, quais os seus elementos constituintes, quais as equipes necessárias na condução do trabalho, dentre outras coisas.

3.4.1. DEFINIÇÃO DE ESCOPO

A primeira tarefa na análise de riscos é identificar os processos de negócios da organização em que se deseja implementar ou analisar o nível de segurança das informações. Logo, identificamos esta etapa como a definição do escopo do projeto de análise de riscos. A definição do escopo permitirá a realização de análises onde elas forem realmente necessárias, com base na relevância do processo de negócio e seus ativos para o alcance dos objetivos da organização.

Prioritariamente a definição do escopo surge por conta da necessidade de se delimitar o universo de ativos que serão alvo de análise e provimento de recomendação. Ao se definir o escopo é importante considerar:

OS PROCESSOS DE NEGÓCIO E SEUS ATIVOS

Os processos de negócio podem ter uma atuação da organização frente o mercado, uma funcionalidade interna ou externa, uma atividade exercida, um produto elaborado,

considerando-se toda a organização necessária para a sua viabilização. Vamos tomar como exemplo um produto que oferece serviços bancários via Internet como sendo um processo de negócio de uma organização do ramo financeiro.

Nesta organização, consideram-se sob os quatro âmbitos da análise de riscos, os seus componentes:

HUMANOS

As pessoas que fazem uso do Internet Banking, as pessoas que dão suporte aos usuários, as pessoas que administram os ativos na organização, as pessoas responsáveis pelo planejamento e coordenação do trabalho, as equipes que atuam na definição das políticas e procedimentos para a realização processo de negócio.

TECNOLÓGICOS

Os servidores de arquivos, em que estão contidas as informações sobre o produto, um servidor de banco de dados que armazena os dados das contas dos clientes do Internet Banking, um roteador, um servidor de e-mail (para envio de extratos por correio eletrônico), um servidor Web, que permite que sejam feitas consulta ao produto via WWW (nas suas diversas plataformas: Windows, Unix, Solaris, etc.), além dos elementos de uma rede de comunicação para envio e recebimento das informações (por exemplo: firewall, roteador, switch, link, bridge, etc.).

PROCESSUAL

A estrutura organizacional humana que foi estabelecida para a realização do processo de negócio em questão. Podemos considerar, tomando-se o exemplo do Internet Banking citado, como sendo a definição das equipes para a manutenção e garantia de continuidade dos ativos de tecnologia do processo; as pessoas e o fluxo de atividades relacionadas ao atendimento a clientes; o fluxo de informações necessário para a realização de uma transação pelo banco virtual, etc.

FÍSICO

O ambiente operacional que comporta as atividades do produto Internet Banking, como por exemplo, os locais de trabalho das equipes envolvidas, os locais de armazenamento de informações críticas, as agências ou postos de atendimento ao cliente, as centrais de processamento de informações como por exemplo os CPDs, as salas de servidores, as centrais de teleprocessamento, a sala-cofre, a fitoteca, etc.

3.5. RELEVÂNCIA DOS PROCESSOS DE NEGÓCIO E SEUS ATIVOS

Ao se fazer a análise de risco, é importante identificar também a relevância dos processos de negócio para a organização, a fim de se priorizar as ações de segurança, ou seja, iniciar o trabalho de implementação de segurança nas atuações mais estratégicas que possam trazer o maior impacto ao negócio da organização quando ocorrerem incidentes.

A identificação da relevância do processo de negócio para a organização é determinante para que as ações de segurança sejam direcionadas às áreas mais críticas, mais prioritárias. Este trabalho também irá permitir que sejam priorizadas as ações onde são mais emergenciais, direcionando-se também os custos e otimizando-se os gastos onde eles são realmente necessários.

Um segundo passo, também fundamental, é identificar a relevância dos ativos identificados para o processo de negócio. Isto quer dizer também que cada ativo que compõe o processo de negócio deve ser considerado em uma escala de criticidade para que, como acontece nos processos, as priorizações de ações de correção e proteção sejam tomadas de imediato onde forem mais necessárias. Evita-se, desta forma, o investimento de segurança onde não é realmente necessário, ou pelo menos prioritário.

A análise de riscos busca prover dados quantitativos e qualitativos sobre o nível de segurança existente na organização para que as ações possam ser tomadas e a segurança da informação atinja seus objetivos, que é garantir a confidencialidade, integridade e disponibilidade.

A análise de segurança é na verdade o reconhecimento do ambiente que se pretende implementar segurança para que possam ser realizadas as seguintes atividades:

1. Identificar os pontos fracos para serem corrigidos, isto é, as vulnerabilidades presentes nos ativos dos processos de negócio;
2. Conhecer os elementos constituintes da infra-estrutura de comunicação, processamento e armazenamento da informação, a fim de dimensionar onde serão feitas as análises e quais elementos serão considerados.
3. Conhecer o teor das informações manipuladas pelos ativos, com base nos princípios da confidencialidade, integridade e disponibilidade;
4. Direcionar ações para incremento tecnológico e humano em áreas críticas e desprotegidas.
5. Permitir um gerenciamento periódico de segurança, visando a identificação de novas ameaças e vulnerabilidades, assim como a verificação da eficácia das recomendações providas.

3.6. DEFINIÇÃO DA EQUIPE ENVOLVIDA

A definição da equipe é importante tanto para se dimensionar a força de trabalho necessária à realização da análise de riscos (análise de segurança) como ao levantamento das pessoas que atuam nos processos de negócio que precisam prover informações para o projeto da análise de riscos, as quais também serão as responsáveis pelo acesso aos ativos para coleta de informações.

As equipes precisam ser definidas de antemão, mas também podem ser incluídos novos elementos em virtude de novas descobertas tecnológicas ou processuais que venham a acontecer durante a análise.

É importante considerar a confidencialidade da análise de riscos, uma vez que a mesma consta de um processo de identificação dos pontos fracos da organização, seus resultados devem ser resguardados e serem acessados e utilizados apenas por pessoas previamente identificadas e autorizadas. Por isso a necessidade de delimitar-se de forma segura e controlada as pessoas que estarão envolvidas na análise de riscos.

3.7. ENTREVISTA A USUÁRIOS

A entrevista a usuários dos processos de negócio permite que sejam obtidos detalhes sobre como os mesmos são gerenciados, implementados e utilizados. Assim, pode-se fazer um mapeamento da criticidade destes processos diante das circunstâncias organizacionais a que ele está submetido, isto é, nível de capacitação necessária da equipe envolvida na sua sustentação, forma com que se dá o fluxo de informação dentro do processo, forma de uso e tratamento de seus produtos decorrentes, dentre outras coisas.

É fundamental obter dos usuários dos processos de negócios (tanto aqueles que os gerenciam quanto aqueles que os suportam e utilizam) o grau de consciência que os mesmos têm quanto a criticidade das informações por eles manipuladas. Desta forma será possível avaliar até que ponto a equipe envolvida está ciente dos procedimentos de segurança necessários para a continuidade do processo.

As entrevistas poderão guiar as análises técnicas, uma vez que elas mapeiam os envolvidos com a administração dos ativos que serão analisados e considerados quanto às suas vulnerabilidades que possam desencadear ameaças ao processo de negócio. Também na análise podem der destacados novos elementos humanos ou tecnológicos que fazem parte do processo de negócio e que precisam ser analisados.

3.8. ANALISE TÉCNICA DE SEGURANÇA

A análise técnica de segurança como explica NORTHCUTT (2002), aborda todos os recursos de hardware de uma rede, como é mostrado na figura 3-3, é uma das etapas mais importantes da análise de riscos, uma vez que é por meio dela que são feitas as coletas sobre a forma com que os ativos foram configurados, estruturados na rede de comunicação, como eles são administrados por seus responsáveis e a maneira como eles são geridos em geral. Assim, é possível identificar nas entrelinhas das configurações a forma com que estes ativos são utilizados e manipulados, buscando identificar vulnerabilidades de segurança. No processo de análise técnica de segurança, vários tipos são considerados, dependendo do escopo definido no inicio do projeto, para fins de rastreamento de vulnerabilidades presentes por meio de erros de configuração ou desconhecimento das possibilidades de investida de ameaças potenciais.

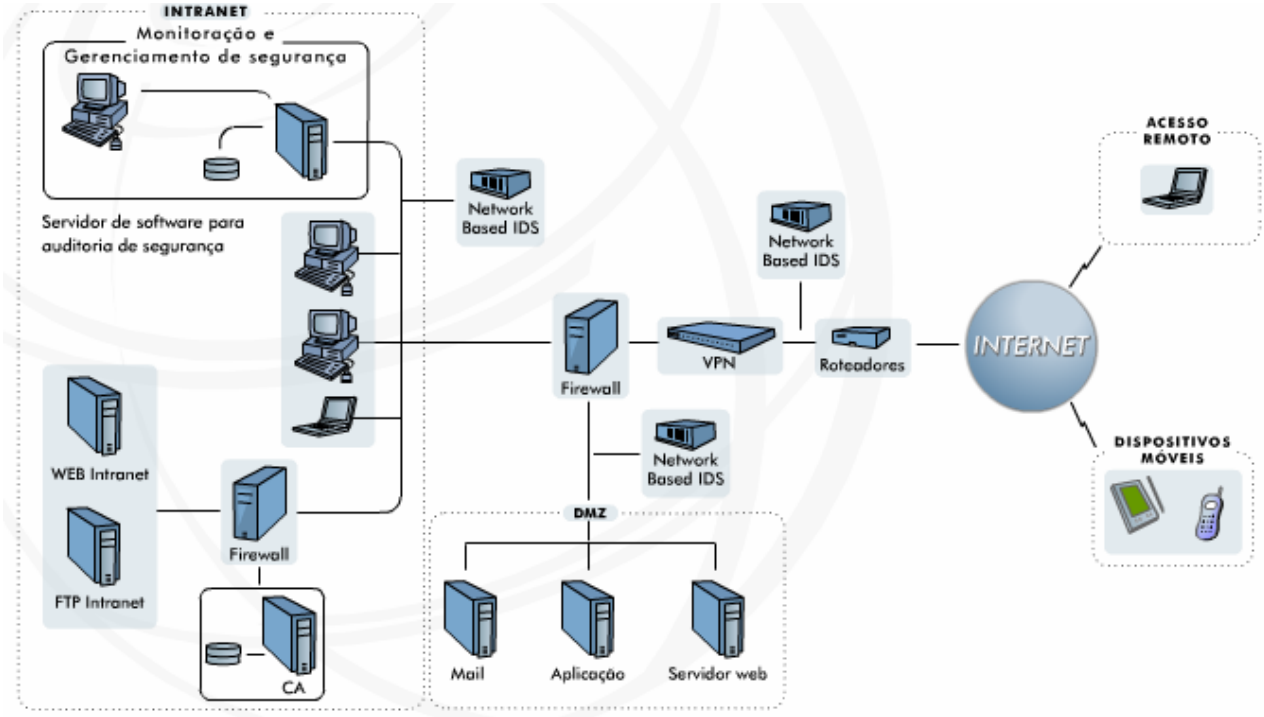

Figura 3-3. Análise Técnica de Segurança

Dentre os mais conhecidos dos níveis tecnológicos analisados tecnicamente, listamos os seguintes:

3.8.1. Análise de Estações de Trabalho

A forma com que as mesmas estão configuradas para evitar que usuários (muitas vezes inconscientemente) permitam a ação de ameaças. Exemplos de vulnerabilidades comuns neste tipo de ativo são: ausência de proteção pela tela bloqueada por senha, a qual permite que máquinas deixadas sozinhas não sejam utilizadas por quem não tiver autorização; ausência de configurações de segurança que permitam a instalação ou execução de arquivos maliciosos; periodicidade de atualização de programas de antivírus, forma de organização de diretórios, presença ou ausência de documentos confidenciais, forma de utilização da estrutura de servidores de arquivos, que garantam de uma forma mais eficiente a cópia de segurança dos dados, ou seja, a disponibilidade dos mesmos.

3.8.2. ANÁLISE DE SERVIDORES

Os servidores são analisados prioritariamente quanto à suas regras de acesso definidas. Vê-se quais são os tipos de usuários que possuem direitos a que tipos de informações, com base na classificação quanto a confidencialidade dos mesmos, a fim de se identificar excesso ou carência de privilégios para a realização de tarefas. O foco principal é nos arquivos de configuração e de definição de usuários que possuem direitos de administração do ambiente, uma vez que são os super-poderes que mais ameaçam os ambientes de tecnologia e também são os mais almejados pelos invasores.

A interação que estes servidores têm com as estações de trabalho dos usuários, com os bancos de dados, com as aplicações que ele suportam são os objetos da análise técnica de servidores, independentes de suas funcionalidades: de arquivos, de correio eletrônico, de ftp, web, dentre outras.

3.8.3. ANÁLISE DE EQUIPAMENTOS E CONECTIVIDADE

A análise de equipamentos de conectividade também está voltada à detecção de configurações que coloquem em risco as conexões realizadas pela rede de comunicação que suporta um processo de negócio. Deve-se identificar nesta análise, a forma com que estes ativos foram configurados: roteadores, switchs, modems, hubs, bridges, dentre outros.

Estes equipamentos devem possuir um nível de segurança muito alto, pois são normalmente situados na entrada de uma rede de comunicação. Ao ser atribuído um alto nível de configuração a estes ativos, o acesso externo à rede do processo de negócio estará naturalmente mais protegido.

3.8.4. ANÁLISE DE LINKS

Os links de comunicação entre as redes devem estar seguros: fibra ótica, satélite, rádio, antenas... Para tanto, é importante realizar atividades de análise sobre a forma como que os links estão configurados e dispostos na representação topológica da rede. Isto garantirá que a comunicação está sendo realizada via meio seguro, se necessário criptografado, isento de possibilidades de rastreamento de pacotes ou mensagens, assim como o desvio de tráfego para outros destinos não desejados.

3.8.5. ANÁLISE DE BANCO DE DADOS

Os bancos de dados representam um elemento de extrema importância na cadeia comunicativa, pois são os armazenadores de informações relativas aos processos de negócio e, muitas vezes, sobre os usuários dos processos de negócio. A forma com que o banco de dados conversa com as demais aplicações de leitura de suas informações é um dos primeiros elementos a ser considerado. Também são avaliados os níveis de confidencialidade, integridade e disponibilidade das informações alí contidas, para que se possam identificar as necessidades de proteção e configuração de segurança para que a informação alí disponibilizada possa estar de acordo com os princípios da segurança da informação.

Nos bancos de dados são avaliados os privilégios dos usuários quanto às permissões de uso, principalmente no tocante ao acesso de aplicações que fazem a leitura destas informações.

3.8.6. ANÁLISE DE APLICAÇÕES

As aplicações são os elementos que fazem a leitura das informações de um processo de negócio ou organização, desta forma, elas são um elemento de grande criticidade, visto que estão fazendo a interface entre diversos usuários e diversos tipos de informação quanto a confidencialidade, integridade e disponibilidade. Assim sendo, considera-se que as aplicações devem garantir um acesso restrito, com base nos privilégios de cada usuário, às informações que elas manipulam, garantindo que suas configurações estejam de acordo com os princípios de segurança estabelecidos (muitos dos quais reconhecidos por organismos internacionais – como a COMMON CRITERIA[3]) quanto à disponibilidade das informações, forma com que a aplicação as lê, as guarda e as transmite; a forma com que a aplicação foi desenvolvida, como são atualizados e armazenados os seus fontes, dentre outras.

[3] *Iniciativa usada para validação de produtos e sistemas e para iniciar a padronização dos critérios de segurança dentro da ISO.*

3.9. A ANÁLISE DE SEGURANÇA FÍSICA

A análise de riscos também busca identificar no ambiente físico quais são as vulnerabilidades que possam colocar em risco os ativos neles envolvidos. Para tanto, uma série de aspectos são observados e considerados dentro de um ambiente organizacional onde são realizados os trabalhos.

Este ambiente deve estar organizado de forma a garantir a continuidade e o bom desenvolvimento das atividades individuais e da manutenção devida dos ativos.

Preocupações como o excesso de umidade ou calor, disposição do cabeamento lógico e elétrico, a existência de falhas na organização do ambiente, todas podem levar à necessidade de reestruturação do espaço físico a fim de permitir que haja uma administração segura desta infra-estrutura e, conseqüentemente, das informações da organização.

Isto quer dizer que aspectos como controle de acesso, disposição topográfica de áreas e ativos, salubridade dos ambientes de trabalho (atentando-se para salinidade, umidade, luz, vento, chuva, alagamentos) são considerados sob a ótica da análise de segurança física.

A análise de segurança física se inicia com a visita técnica pelos ambientes nos quais são desempenhadas atividades relacionadas direta ou indiretamente aos processos de negócio que estão sendo analisados, aos quais devem ser atribuídas soluções de segurança. Estes ambientes devem ser observados quanto aos seguintes aspectos:

3.9.1. CONTROLE DE ACESSO

Disposição de sistemas de detecção e autorização de pessoas para acesso: câmeras de vídeo; homens-segurança; catraca de acesso, e demais mecanismos de reconhecimento individual, etc.

3.9.2. TOPOGRAFIA

Localização do CPD ou da Fitoteca, áreas críticas quaisquer, como relação à topografia do terreno: se localizadas em subsolos, à mercê de inundações, próximas a áreas

de risco como proximidade ao mar, rios ou córregos ou áreas de retenção de água ou sujeitas a vazamentos das tubulações hidráulicas.

3.9.3. EXPOSIÇÃO

Disposição das janelas e portas do ambiente crítico: se localizadas próximas a ativos críticos, se os mesmos estão sujeitos a receber luz solar ou possibilidade de ameaças causadas por intempéries da natureza, como vento ou chuva fortes.

3.9.4. DISPOSIÇÃO ORGANIZACIONAL

Preocupação com a organização do espaço em relação à disposição do mobiliário e dos ativos de informação. As áreas de circulação de pessoas em locais de alta criticidade estão livres de ativos sensíveis. Os ativos de alta criticidade estão localizados em áreas livres de circulação de pessoas não autorizadas a operá-los. As consoles de equipamentos críticos estão livres do acesso ou da disponibilidade de acesso físico não identificado? Os ativos críticos estão localizados longe das portas de acesso a áreas de circulação de pessoas não autorizadas?

3.9.5. SISTEMAS DE COMBATE A INCÊNDIO

Disposição dos equipamentos de combate a incêndio. Se há, se estão nos locais adequados: posicionamento dos sprinklers de água, disponibilidade de extintores de incêndio, etc.

3.10. SEVERIDADE DO PROCESSO DE NEGÓCIO PARA A CONDUÇÃO DA ANÁLISE DE RISCOS

Para que uma análise de riscos possa ser realizada, é importante que os processos de negócio da organização, alvo de proteção, sejam considerados quanto a sua importância para a realização dos negócios. Para tanto, na análise de riscos é sugerida a pontuação da relevância do processo de negócio. Esta pontuação permite que se tenha idéia do impacto que um incidente de segurança poderá causar ao processo do negócio, levando-se em conta o valor estratégico que ele possui para a organização como um todo. Quanto maior a sua relevância, maior é a criticidade dos ativos que dele fazem parte e, conseqüentemente,

maior é o risco a que a organização está sujeita, caso ocorra um incidente de segurança. A consideração da relevância também permite que sejam direcionadas ações de correção de problemas nos ativos que são mais prioritários no momento da análise, pois fazem parte de processos de negócio de alta relevância.

3.11. OS RESULTADOS DA ANÁLISE DE RISCOS

Uma vez realizada a análise de riscos, a organização possui em mãos uma poderosa ferramenta para tratamento de suas vulnerabilidades e um diagnóstico geral sobre o status da segurança de seu ambiente como um todo.

A partir deste momento, será possível estabelecer políticas para a correção dos problemas já detectados e o gerenciamento de segurança dos mesmos ao longo do tempo, para que se garanta que as vulnerabilidades encontradas anteriormente não sejam mais sustentadas ou mantidas, analisando a ocorrência de novas vulnerabilidades que possam surgir ao longo do tempo.

É sabido que as inovações tecnológicas estão cada vez mais freqüentes, o que traz consigo uma série de novas oportunidades para que indivíduos maliciosos se aproveitem delas e venham realizar ações indevidas aos ambientes humanos, tecnológicos, físicos e processuais.

Uma vez de posse das recomendações, iniciam-se as ações de distribuição das mesmas para fins de correção do ambiente e redução de riscos a que está submetida à infra-estrutura humana, tecnológica, processual e física que suporta um ou mais processos de negócio de uma organização.

Assim, será possível implementar nos ativos analisados, e também nos ativos de mesmas características que os analisados, as medidas de correção e tratamento das vulnerabilidades.

A análise de riscos tem como resultado os relatórios de recomendações de segurança, para que a organização possa avaliar os riscos a que está submetida e quais são os ativos dos processos e negócio que estão mais suscetíveis à ação de ameaças a confidencialidade, integridade e disponibilidade das informações utilizadas para alcance dos objetos intermediários ou finais da organização.

Uma vez que os resultados são mapeados e pontuados quanto a sua criticidade e relevância, um dos produtos finais da análise de riscos, a matriz de criticidade, indica por meio de dados qualitativos e quantitativos a situação de segurança na qual se encontram os ativos analisados, listando as vulnerabilidades, ameaças potenciais e respectivas recomendações de segurança para a correção das vulnerabilidades.

Ao realizar-se a análise de riscos, aumenta-se o nível de segurança da organização, uma vez que já há uma preocupação com este elemento para a continuidade dos negócios, pois já houve conhecimento por parte dos envolvidos na análise da real situação de segurança em que se encontra a organização. Isto nos leva a compreender a real importância da análise de riscos como primeiro passo na implementação de segurança, pois permite que se conheça todo o ambiente em que se realiza um processo de negócio, do ponto de vista processual, físico, humano e tecnológico. A partir deste diagnóstico, tanto das vulnerabilidades quanto do impacto que as mesmas podem trazer ao negócio (obtido junto à pontuação da relevância dos processos de negócio e seus ativos) é possível implementar medidas corretivas, preventivas e detectivas que se fizerem necessárias para o alcance dos objetivos da organização.

Depois de uma análise, vem a política de segurança. Esta tarefa, que será abordada no próximo capitulo, visa a orientação dos padrões de segurança a serem adotados por toda a organização. Geralmente baseada no resultado da análise de riscos, a política de segurança constitui o estabelecimento das normas de segurança que norteiam a prática diária das pessoas que manipulam os ativos, assim como a forma com que os ativos se comunicam entre si.

4. POLÍTICA DE SEGURANÇA

Este capítulo mostra o que é uma política de segurança da informação, conforme foi introduzido no capítulo 2. A análise de riscos permite que sejam identificados os pontos críticos em uma gestão processual, para fins de implementação de recomendações de segurança em um ambiente tecnológico e humano. O passo seguinte é estabelecer os valores e regras a serem seguidos por todos os envolvidos no uso das informações aos seus diversos ativos. A política é colaborada levando-se em conta o ambiente em questão, assim como o estado da arte e da segurança da informação, para que os controles estabelecidos estejam de acordo com as melhores práticas internas da organização e com as práticas de segurança corretamente adotadas.

4.1. DEFINIÇÃO

De acordo com NBR ISO/IEC 17799 (2001), uma política é um conjunto de diretrizes, normas, procedimentos e instruções de trabalho que estabelecem os críticos de segurança para serem adotados em nível local ou intencional, visando o estabelecimento, padronização e normalização da segurança junto tanto ao âmbito humano quanto tecnológico. A partir de seus princípios, é possível tornar a segurança da informação um esforço comum, visto que todos poderão contar com um arsenal informativo documentado e normalizado, voltado à padronização do modus operandi de cada um dos indivíduos envolvidos na gestão da segurança da informação.

4.2. ELABORAÇÃO DA POLÍTICA DE SEGURANÇA

Para elaborar uma política de segurança da informação, é importante considerar os requisitos básicos e as etapas necessárias para a sua produção.

4.2.1. REQUISITOS DA POLÍTICA

A política é elaborada tendo-se por base a cultura da organização e o know-how de segurança dos profissionais envolvidos com a sua aplicação e comprometimento

É importante considerar que para a elaboração de uma política de segurança institucional seja formada uma equipe multidisciplinar que represente grande parte dos aspectos culturais e técnicos da organização e que se reúna periodicamente, dentro de um cronograma estabelecido pelo Comitê de Segurança. Esse comitê é formado por um grupo definido de pessoas responsáveis por atividades referentes à criação e aprovação de novas regras de segurança na organização. Nas reuniões são definidos os críticos da segurança adotados em cada área e o esforço comum necessário para que a segurança atinja um nível mais alto. Deve-se ter em mente que as equipes envolvidas precisam de tempo livre para analisar e escrever todas as regras discutidas durante as reuniões. A oficialização de uma política tem como passo inicial a aprovação pela administração da organização. Ela deve ser publicada e comunicada de forma adequada para todos os empregados, parceiros, terceiros e clientes, se necessário.

Neste documento devem estar expressas as preocupações da administração, onde são estabelecidas regras para gestão da segurança da informação contendo a definição da própria política, uma declaração da administração apoiando os princípios estabelecidos e uma explicação dos requisitos de conformidade quanto a:

1. Legislação e cláusulas contratuais;
2. Educação e treinamento em segurança da informação;
3. Prevenção contra ameaças (vírus, trojans, hackers, incêndio, intempéries, etc.)
4. Princípios, objetivos e requisitos necessários para a operação da empresa e para o processamento da informação.

Deve conter também a atribuição das responsabilidades das pessoas envolvidas, onde estejam claros os papéis de cada um na gestão dos processos e da segurança.

Não se pode esquecer que toda documentação já existente sobre a condução das tarefas deve ser analisada quanto aos princípios da segurança da informação, aproveitando-se ao máximo as práticas correntes, avaliando e agregando segurança a essas tarefas.

4.2.2. ETAPAS DA PRODUÇÃO

Elaborar uma política é um processo que demanda tempo e informação. É necessário conhecer como a organização está estruturada e como seus processos são conduzidos corretamente. A partir deste reconhecimento é avaliado o nível de segurança existente e pode-se então detectar os pontos que devem ser considerados para que estejam em conformidade com os padrões de segurança.

O trabalho de produção é composto de diversas etapas, dentre as quais destacam-se:

OBJETIVO E ESCOPO DA POLÍTICA

Neste item deve constar a apresentação do assunto da norma quanto a seus propósitos e conteúdo, visando identificar de forma sucinta que padrões a política visa estabelecer, assim como a abrangência que a mesma terá em termos de ambientes, indivíduos, áreas de departamentos da organização envolvidos.

ENTREVISTA

As entrevistas buscam identificar junto aos usuários e gestores da organização as preocupações que os mesmos têm com os ativos, processos de negócio, área ou tarefa que executam ou da qual participam. As entrevistas buscam identificar as necessidades de segurança existentes na organização.

PESQUISA E ANÁLISE DE DOCUMENTOS

Nesta etapa são identificados e analisados os documentos existentes na organização e que tem alguma relação com o processo de segurança no tocante à redução de riscos, diminuição de re-trabalho e falta de orientação. Dentre a documentação existente

podem-se considerar as seguintes: livros de rotinas, metodologias, políticas de qualidade, dentre outras.

REUNIÃO DA POLÍTICA

Nas reuniões, realizadas com as equipes envolvidas na elaboração, são levantados e discutidos os assuntos e redigidos os parágrafos para a composição das normas, com base no levantamento do objetivo e do escopo da política especifica.

GLOSSÁRIO DA POLÍTICA

É importante esclarecer quaisquer dúvidas conceituais que possam surgir quando da leitura da política. Por isso todos os leitores devem ter o mesmo referencial conceitual de termos. Logo, é recomendável que a política tenha um glossário específico onde são apresentados termos e conceitos presentes em toda a política de segurança.

RESPONSABILIDADES E PENALIDADES

É fundamental identificar os responsáveis pela gestão de segurança dos ativos normalizados, visando estabelecerem-se relações de responsabilidade para cumprimento de tarefas, assim como as regras de aplicação de sanções decorrentes de casos de inconformidade com a política elaborada. Assim, busca-se o nível de consciência necessário para os envolvidos quanto às penalidades que lhe serão aplicadas em caso de infração da política e da segurança.

4.3. DOCUMENTOS DA POLÍTICA

Ao iniciar o processo de elaboração da política de segurança é necessário levantar alguns dados junto aos usuários dos ativos e efetuar estudos nos documentos existentes.

O objetivo dessa tarefa é definir qual adaptação deve ser feita no modelo de padronização existente para atender as características da empresa (em termos de layout, identificação, numeração e linguagem utilizada). Se já existem esses padrões definidos, os documentos da política de segurança deve se adaptar a eles, a fim de garantir uma proximidade entre a política e a prática gerencial existente.

A figura 4-1 mostra que a política está estruturada três grandes camadas segundo SÊMOLA (2001); as Diretrizes, as Normais e os Procedimentos e Instrução de trabalho, sustentadas por três grandes aspectos; ferramentas, cultura e monitoração.

.

Figura 4-1. Modelo Estrutural de Política

4.3.1. DIRETRIZ

Conjunto de regras gerais de nível estratégico onde são expressos os valores de segurança da organização. É endossada pelo líder empresarial da organização e tem como base a sua visão e missão, a fim de abranger toda a filosofia de segurança da informação.

As diretrizes correspondem às preocupações da empresa sobre a segurança da informação, estabelecendo seus objetivos, meios e responsabilidades.

As diretrizes estratégicas, no contexto de segurança, correspondem a todos os valores que devem ser seguidos, para que o principal patrimônio de empresa – a informação – tenha o nível de segurança exigido.

Como a informação não está presente em somente um único ambiente (microinformática, por exemplo) ou meio convencional (fax, papel, comunicação de voz

etc), deve permitir ser aplicada a qualquer ambiente existente, não devendo conter termos técnicos de informática.

Compõe-se de um texto, não técnico, com as regras gerais que nortearão a elaboração das normas de segurança.

4.3.2. NORMAS

Norma – conjunto de regras gerais e específicas da segurança da informação a serem usadas por todos os segmentos atuantes nos processos de negócios da instituição, podendo ser elaborado por ativo, área, tecnologia, processo de negócio, público alvo, etc.

As normas, por estarem em um nível tático podem ser específicas para o público a que se destina, por exemplo, para técnicos e para usuários.

4.3.3. PROCEDIMENTOS E INSTRUÇÕES DE TRABALHO

Procedimento – conjunto de orientações para condução das atividades operacionais de segurança, representando as relações interpessoais e interdepartamentais e suas respectivas etapas de trabalho para a implantação ou manutenção da segurança da informação.

Instrução de Trabalho – conjunto de comandos operacionais a serem executados quando da realização de um procedimento de segurança estabelecido por uma norma, estabelecidos em modelo de passo a passo para os usuários do ativo em questão.

4.3.4. ACOMPANHAMENTO DA POLÍTICA

Uma política de segurança, para ser efetiva, precisa ter os seguintes elementos com base de sustentação:

1. **Cultura** – o treinamento das pessoas deve ser constante de tal forma a atualizar toda a empresa quanto aos conceitos e normas de segurança, bem como sedimentar a consciência da segurança, visando torná-la um esforço comum entre todos os envolvidos.

2. **Ferramentas** – Os recursos humanos, financeiros e as ferramentas de automação devem estar de acordo com as necessidades de segurança. Parte de segurança pode ser automatizada, ou melhor, controlada com ferramentas específicas, tais como backup obrigatório programado, controle de acesso com log de execução, etc.

3. **Monitoração** – a implementação da política de segurança de ser constantemente monitorada. É necessário efetuar um ciclo de manutenção para acertos na padronização decorrente de problemas encontrados, reclamações de funcionários ou resultados de auditoria. Deve-se também adaptar a seguranças as novas tecnologias, as mudanças administrativas e ao surgimento de novas ameaças.

4.4. IMPLANTAÇÃO DA POLÍTICA

Uma política é bem implantada quando reflete os objetivos do negócio da organização, ou seja, está sempre de acordo com a operacionalização necessária para o alcance das metas estabelecidas, agregando segurança a estes processos, garantindo uma gestão inteligente dos riscos.

Deve estar de acordo com a cultura organizacional e estar apoiada no comprometimento e adesão. Deve também permitir um bom entendimento dos quesitos de segurança e permitir uma avaliação e gerenciamento dos riscos a que a organização está submetida.

Sua implantação depende de uma boa estratégia de divulgação entre os usuários e uma disponibilização de seu conteúdo a todos os envolvidos, a fim de aumentar o nível de segurança e comprometimento de cada um. Campanhas, treinamentos, palestras de divulgação, sistemas de aprendizado, dentre outros, são mecanismos adotados para se tornar a segurança um elemento comum a todos.

Como todo processo de avaliação é possível mudança das práticas atuais, uma política deve ter como base uma estratégia de mensuração de eficácia, onde podem ser avaliados o desempenho da gestão de segurança e os pontos fracos que devem ser melhorados.

A política deve basear-se na análise de risco e visar a padronização de ambientes e processos de modo a evitar as vulnerabilidades existentes. Sua criação está diretamente ligada a concretização dessa análise, pois por meio do levantamento das vulnerabilidades é que se pode elaborar a documentação de segurança, cujo objetivo é minimizar os riscos das ameaças se concretizarem.

4.5. ASSUNTOS DA POLÍTICA

Para se elaborar uma política, é necessário delimitar os assuntos que serão normatizados. Isso é feito a partir do conhecimento do ambiente organizacional, humano ou tecnológico, assim como a partir do levantamento das preocupações com segurança que os usuários, gestores e executivos da empresa possuem. A divisão dos assuntos da política depende das necessidades da organização.

Exemplos de alguns assuntos:

1. **Segurança Física -** Acesso físico, Infra-estrutura predial, Data Center.
2. **Segurança da Rede Corporativa -** Configuração dos sistemas operacionais, acesso lógico e remoto, autenticação, Internet, disciplina operacional, gerenciamento de mudanças, desenvolvimento de aplicativos.
3. **Segurança de Usuários -** Composição de senhas, segurança em estações de trabalho, treinamento e conscientização.
4. **Segurança de Dados -** Criptografia, classificação, privilégios, backup e recuperação, anti-vírus, plano de contingência.
5. **Auditorias de Segurança -** Análise de risco, revisões periódicas, visitas técnicas, monitoração e auditoria.
6. **Aspectos Legais -** Práticas pessoais, contratos e acordos comerciais, leis e regulamentação governamental.

4.6. USO DA POLÍTICA

Uma vez elaborada, a política de segurança é importante para que se garanta a implantação de controles de segurança apropriados. Ela deve ser usada para auxiliar na

seleção de produtos e no desenvolvimento das preocupações da direção sobre segurança a fim de que o negócio da organização seja garantido.

Ao ser usada, a política torna-se o primeiro passo para transformar a segurança em um esforço comum, por meio da definição de controles em sistemas informatizados, estabelecimentos dos direitos de acesso com base nas atribuições de cada pessoa, assim como orientação dos usuários quando à disciplina necessária para se evitarem violação de segurança. Este quesito visa também evitar que a organização seja prejudicada em casos de quebra de segurança, permitindo a condução de investigações de crimes por computador.

Uma vez que causa impacto no dia-a-dia das pessoas, a política deve ser clara (escrita em boa forma e linguagem), concisa (evitando-se informações desnecessárias ou redundantes), estar de acordo com a realidade prática da empresa (para que possa ser reconhecida como um elemento institucional) e, principalmente, deve ser revisada periodicamente.

5. IMPLEMENTAÇÃO DA SEGURANÇA

Já foram apresentadas nos capítulos anteriores as questões relativas à análise de riscos e a política; agora vamos ver como poderemos implementar a segurança da informação. Uma vez que se conheceu a situação do ambiente na análise de riscos e definiu a estratégia de segurança na política, deve-se agora concentrar os esforços no próximo passo que é a implementação.

5.1. A IMPORTÂNCIA DA IMPLEMENTAÇÃO

Após o conhecimento das ameaças e vulnerabilidades do ambiente adquirido na análise de riscos, ou após a definição formal das intenções e atitudes da organização definidas na política de segurança das informações, algumas ações devem ser tomadas para a implementação das medidas de segurança recomendadas ou estabelecidas.

Não basta conhecer as fragilidades do ambiente ou ter uma política de segurança escrita. Ferramentas devem ser instaladas, regras divulgadas, usuários conscientizados do valor da informação, ambientes configurados etc. Cada medida de proteção deve ser escolhida e implementada, para contribuir com a diminuição do risco.

Os objetivos de cada medida de proteção têm de estar claros e cada medida deverá ser escolhida de forma que, uma vez em funcionamento, atinja os objetivos definidos.

5.2. CONSIDERAÇÕES PARA A IMPLEMENTAÇÃO

Varias são as medidas de proteção que podem ser recomendadas para a diminuição do risco às informações. Como por exemplo:

1. Proteção contra vírus;
2. Implementação de firewall;
3. Controles de acesso aos recursos da rede;

4. Controles de acesso físico.
5. Sistemas de vigilância;
6. Detecção e controle de Invasões;
7. Políticas gerais ou específicas;
8. Equipamentos;
9. Configuração de ambientes;
10. Treinamento;
11. Campanhas de divulgação;
12. Planos de conformidade;
13. Classificação de informações
14. Acesso Remoto Seguro;
15. Monitoramento e gerenciamento de segurança;

Deve-se notar que o escopo de implementação das medidas de segurança extrapola a informática, devendo abranger os ambientes que tratam da informação não só em meios eletrônicos, mas também convencionais.

De nada adianta, por exemplo, definir regras para a criação e uso de senhas difíceis de serem adivinhadas, se os usuários compartilham essas senhas ou escrevem em papéis e os colam ao lado dos monitores.

5.3. PLANO DE SEGURANÇA

A partir da Política de Segurança, define-se que ações devem ser implementadas (ferramentas de software ou hardware, campanhas de conscientização, treinamento, etc), para se atingir um maior nível de segurança.

Estas ações devem estar definidas em um Plano de Segurança em que se priorizam as ações principais em termos de seu impacto nos riscos em que se quer atuar e do tempo e custo da implementação, definindo assim ações de curto, médio e longo prazo.

O plano de Segurança apóia-se em cronograma retalhado e contempla, para cada ação a ser tomada, os seguintes itens:

1. **O risco que se quer atenuar -** Uma ação é determinada pelo risco que se quer atenuar e pelos objetivos de segurança. Os objetivos de segurança, por sua vez, se baseiam nas melhores práticas de mercado, em padrões e normas de segurança e na própria política de segurança definida.
2. **Os ativos envolvidos -** Uma ação é tomada visando um ou alguns ativos. Por exemplo, pode-se implementar uma ferramenta de software (como firewall) para proteger um servidor de banco de dados que contenha informações críticas ao negócio. Neste caso, o ativo a ser protegido é o banco de dados. Um outro exemplo é quando se pretende aumentar a conscientização dos funcionários com relação à segurança das informações. Pode-se, neste caso, se implementar um treinamento de segurança em que o ativo envolvido são os funcionários da empresa.
3. **Justificativa, em função dos objetivos de segurança;**
4. **Tempo de implementação;**
5. **Recursos (humanos e matériais) necessários;**
6. **Análise custo X benefício –** A relação custo X beneficio é derivada do tempo de implementação e dos recursos que serão necessários, tanto humanos como materiais;
7. **Pontos críticos previstos para a implementação e como superá-los –** É importante se preparar para enfrentar situações adversas. Por exemplo, no caso da implementação de um Firewall, pode-se necessitar tirar um servidor importante do ar por alguns instantes. Caso isso aconteça, deve-se estar preparado.
8. **O responsável pelo sucesso da implementação e por manter o nível de segurança da medida implementada;**
9. **O risco residual;**

10. **Indicadores para o acompanhamento (monitoração) da medida implementada –** Deve-se pensar também na continuidade da medida implementada. Qual é o risco residual que se espera, que indicadores serão usados para medir a efetividade da medida e controlar o risco e quem ficará responsável por sua operação e controle.

5.4. PLANO DE AÇÃO

Uma vez definido e aprovado o Plano de Segurança, parte-se para a definição do Plano de Ação para as medidas que deverão ser implementadas.

Um plano de ação tem vários formatos, mas deve possuir as seguintes características:

1. **Objetivos bem definidos –** Um plano de ação deve ter objetivos bem definidos de forma que ao ser cumprido, sejam alcançados. Também deve ser claro, preciso, escrito corretamente não permitindo dúvidas, dupla interpretação;
2. **Coerência –** As atividades devem estar relacionadas e deve existir harmonia entre situações, acontecimentos e idéia de tal maneira que nada se disperse do foco. Da unidade e correlação das proposições dependerá o alcance dos objetivos;
3. **Seqüência –** Deve existir um caminho previamente definido que propicie a integração das atividades racionalizando os esforços e otimizando o tempo;
4. **Flexibilidade –** Um plano de ação deve prever contingências durante a execução das tarefas e do processo como um todo. Assim, é necessário estruturá-lo de tal maneira que seja possível inserir ou atualizar itens e/ou atividades que enriqueçam ou facilitem a implementação como novas tecnologias que surjam, por exemplo. Muitas vezes, em função de orçamentos, é necessário suprimir algo, mas isso não deve significar o fim do plano. Ajustes são feitos sem, entretanto, que o plano perca seu eixo.

IDENTIFICAÇÃO DA REALIDADE

É necessário conhecer o ambiente para o qual se vai planejar, fazendo as seguintes perguntas:

1. Qual o negócio da organização?
2. Há um plano de negócio, o que ele diz?
3. Já foi feita a análise de segurança?
4. E a política?
5. Qual a cultura da empresa?
6. De um modo geral já existe uma percepção da necessidade de segurança?
7. Existem ações efetivas realizadas?
8. Existem normas regulamentadoras da atividade da organização?
9. Existem recursos?
10. Existe orçamento para segurança?

Observando isso no CRSPE, concluímos:

1. Partir do universo conhecido, associando a informação nova aos padrões anteriormente convencionados;
2. Considerar a diversidade cultural e a multiplicidade de tipos humanos que atuam na organização;
3. Estimular o inter-relacionamento entre os membros da(s) equipe(s) que executarão as tarefas;
4. Durante a orientação da(s) equipe(s) utilizar casos e termos próprios da organização para ilustrar a informação e facilitar a compreensão;

5.4.1. ESBOÇO DO PLANO DE AÇÃO

Enfim, desenvolvemos uma metodologia abaixo descrita para que fique mais claro o cenário e seja mais fácil elaborar o plano e implementar a segurança.

OBJETIVOS

Os objetivos devem estar claros. Está sendo elaborado um planejamento para alcançar o propósito de implementar a segurança da informação, e não simplesmente cumprindo a tarefa de elaborar um plano. Assim, os objetivos devem ser:

1. Expressos em termos do resultado esperado, observável e mensurável;
2. Explícitos quanto a tarefa ao qual o desempenho se relacione;
3. Realistas e alcançáveis nos limites de um período de tempo determinado;
4. Coerentes entre si, contribuindo para o alcance do objetivo geral do plano de ação;
5. Claros, sem alternativas, sem palavras inúteis, mencionando o desempenho relativo a cada tarefa inteligíveis;
6. Inspirados nas atividades diárias;
7. Importantes e significativos no contexto

Os objetivos do plano de ação visam dentre outras coisas:

1. Racionalizar as atividades;
2. Assegurar a implantação efetiva e econômica do programa de segurança;
3. Conduzir ao alcance das metas;
4. Verificar o andamento do processo.

TAREFAS

Ao selecionar as tarefas considere sua relevância, sua atualidade e aplicabilidade, se correspondem aos objetivos já definidos e se estão adequados ao perfil da organização. Selecionando as tarefas lembre-se de adotar critérios como:

1. **Validade –** significa que as tarefas sejam representativas para o alcance dos objetivos;

2. **Significação –** é importante que as tarefas estejam vinculadas à realidade da organização dando-lhes credibilidade e valor. As tarefas necessitam ter algum significado para o plano;
3. **Utilidade –** cada tarefa deve resultar em algo útil para o processo como um todo. Não devem existir sem um propósito definido claramente. Tipicamente, cada tarefa gera um produto.

As tarefas estão ordenadas de modo que permita uma integração (vertical, seqüencial ou matricial) de maneira que o resultado e o progresso de cada uma possa auxiliar na otimização de tarefas das que estão em andamento.

Com certeza, algumas atividades ocorrem ao mesmo tempo e ao se preocupar com a integração, certamente otimizamos tempo e recursos e diminuimos custos.

METODOLOGIA

Em nosso plano usamos uma abordagem dedutiva (partindo do geral para o particular) ao invés da abordagem indutiva, (do particular ao geral). A estratégia de implementação está definida considerando:

1. Estabelecer uma implantação piloto;
2. Iniciar por ambientes que suportem impactos em sua operações;
3. Solucionar um problema de cada vez.

RECURSOS

É crítico para o sucesso do plano a disponibilização dos recursos. Sendo ssim, o apoio da alta administração é fundamental para que o plano atinja seus objetivos. Considerando-se 3 tipos de recursos:

1. **Humanos –** O trabalho de planejar e implementar a segurança pressupõe equipes interdisciplinares de especialistas. Essas pessoas deverão ser orientadas quanto aos objetivos e ao escopo do trabalho, às tarefas, ao método, aos prazos, etc.

2. **Materiais –** Selecionar e utilizar recursos que estejam de acordo com a natureza da tarefa, utilizar o recurso escolhido e programar o seu uso de acordo com o tempo disponível, etc.
3. **Financeiros –** Fazer a previsão orçamentária e a financeira, estabelecer um sistema de controle das despesas, etc.

5.4.2. RECOMENDAÇÕES DE FABRICANTES

É de extrema importância que as recomendações dos fabricantes dos produtos sejam conhecidas antes da implementação.

5.4.3. SUPORTE

Você pode precisar de ajuda de profissionais com a experiência necessária à execução de determinadas atividades.

5.4.4. PLANEJAMENTO DE IMPLANTAÇÃO

Algumas implantações (por exemplo, softwares, equipamentos, campanhas de divulgação e conscientização, etc.) poderão durar vários dias e afetar vários ambientes, processos e pessoas da organização. Nesses casos, pode ser útil um planejamento em separado.

5.4.5. PLATAFORMA DE TESTES

Em alguns casos, uma plataforma de testes pode ser necessária para avaliar a solução e diminuir possíveis riscos sobre o ambiente de produção.

5.4.6. IMPLEMENTAÇÃO

Na hora da implementação, propriamente dita, é muito importante seguir uma metodologia. A metodologia define como dar os passos necessários para se executar um plano de ação. Um dos objetivos da metodologia é manter um mesmo padrão de qualidade na implementação, independente de que estiver executando.

Portanto, é importante ter definido como se acompanhará o progresso da implementação e, em caso de dificuldades, que ações devem ser tomadas e quem deverá ser notificado.

5.4.7. REGISTRO DE SEGURANÇA

Após a implementação de uma nova medida de segurança, é importante que se mantenha o registro do que foi implementado. Deve-se registrar informações como: o que foi implementado (ferramenta, treinamentos, etc.); quais os ativos envolvidos; que dificuldades foram encontradas e como foram superadas; até que ponto se atingiu o objetivo esperado, etc. Este registro tem dois objetivos principais: manter o controle de todas as medidas implementadas e aproveitar a experiência acumulada.

5.4.8. MONITORAÇÃO E ADMINISTRAÇÃO DO AMBIENTE

A administração de um ambiente seguro envolve todo um ciclo de macro-atividades. No terceiro capítulo falamos da primeira fase desse ciclo que é a análise de riscos, onde se conhece o ambiente e o que precisa ser implementado. No capítulo anterior falamos da política de segurança e neste capítulo abordamos a implementação de medidas de segurança na prática. Mas o ciclo não termina aqui. É preciso monitorar os ativos, a partir da medição constante de indicadores que mostrem o quão eficaz são as medidas adotadas e o que precisa ser mudado. A partir então da leitura desses indicadores, faz-se outra análise de riscos e começa-se o ciclo outra vez. O sucesso de uma implementação de segurança só pode ser alcançado quando se busca a administração efetiva de todo o ciclo.

6. ESTUDO DE CASO: CRSPE

O Modelo de Gerência do CRSPE está definido em equipes de trabalho do Grupo de Suporte, dividida em função de suas atribuições e hierarquia, como o descrito abaixo:

- Gerência
- Gerência de Rede
- Gerência de Desempenho
- Gerência de Segurança
- Gerência de Projetos

A Gerencia de Desempenho, Configuração, Qualidade, Risco, Requisitos aparecem como uma espécie de "casca" em toda estrutura organizacional, pois isso permite a geração de informações gerenciais, graças à implementação de atividades adicionais (simples) de apontamento (por exemplo), que darão condições de Gerência ao ambiente como um todo, como registros em formulários da: atividade executada, duração, data, usuário, solução, verificações efetuadas, ações tomadas...

A criação de uma estrutura organizacional no Grupo do Suporte do CRSPE leva em conta a recomendação de colocar a Gerência de Segurança dentro da Gerência de Rede, pois desta formam se torna mais eficiente suas ações, uma vez que incidentes de segurança podem ser detectados pelo Grupo de Gerência da Rede e repassados imediatamente ao Grupo de Gerência de Segurança.

A Gerência de Segurança é responsável pela elaboração, implementação e administração de mecanismos e regras que permitirão aos usuários de todo o CRSPE manipularem de maneira segura os documentos e dados. O Grupo de Segurança no CRSPE tem a estrutura hierarquicamente subordinada ao Grupo de Redes ou no mesmo nível:

- Grupo de Administração de Serviços e Sistemas: implementa as regras de segurança baseadas no Plano de Segurança do CRSPE;
- Grupo de Administração de Qualidade: verifica se os objetivos do Plano de Segurança estão sendo atingidos;
- Grupo de Operação: ativa os procedimentos definidos no Plano de Segurança e Política de Segurança.
- Grupo de Gerência de Segurança: especifica procedimentos de segurança a serem operacionalizados, obedecendo ao Plano e Política de Segurança;
- Grupo de Administração de Segurança: valida o Plano de Segurança, valida a Política de Segurança;
- Grupo de Administração de Planejamento: elabora o Plano de Segurança do CRSPE baseado na Política de Segurança em vigor.

O intuito deste trabalho como passo inicial do modelo de segurança, é o de fornecer uma Política de Segurança inicial para que esses grupos comecem seus trabalhos, buscando o ciclo de segurança como vimos em capítulos anteriores, fazendo isso, de maneira gradual, avaliando riscos, a qualidade, re-avaliando requisitos, desempenho e principalmente, permitindo o registro das atividades realizadas tanto pelos usuários (ao fazer o pedido de suporte), assim como as atividades realizadas pelo pessoal do Suporte.

6.1. ANÁLISE DE RISCO EM CONFORMIDADE COM A NORMA ISO 17799

Este teste é desenvolvido como passo inicial ao desenvolvimento de um modelo de segurança para fazer com que a direção do CRSPE perceba o grau de aderência às recomendações de Segurança da Informação da norma internacional ISO/IEC 17799:2000, ou de sua versão brasileira NBR ISO/IEC 17799:2001.

Este questionário foi desenvolvido para o CRSPE, mas pode ser aplicado a qualquer outra organização, pois ele aborda os domínios da norma, e não peculiaridades do ambiente, comparando os cuidados de diferentes departamentos dentro da organização com relação à informação, bem como a importância da informação para as atividades de tais departamentos. Verificar pontos de vulnerabilidade do CRSPE com relação ao tratamento

da Informação e o grau de risco destes pontos. Receber conselhos específicos referentes à segurança da Informação de acordo com o perfil definido nas questões.

O profissional responsável pelo departamento e/ou organização responde o questionário. Uma análise é feita a cada questão, conforme seu grau de importância. De acordo com as respostas coletadas, chega-se a um nível de conformidade que determina o resultado apresentado nas legendas condicionais. Os conselhos complementares são definidos de acordo com as questões individuais ou grupo de questões relacionadas.

Deste modo, para termos dados referenciais do CRSPE, é necessário contar com a colaboração do responsável pela organização, respondendo às questões abaixo.

6.1.1. QUESTIONÁRIO DE CONFORMIDADE COM A ISO 17799

Este capítulo mostra o questionário desenvolvido e as respostas dadas pelo responsável pelo CRSPE identificadas em negrito.

Dados de Identificação

Empresa: Instituto Nacional de Pesquisas Espaciais/Centro Regional Sul de Pesquisas Espaciais

Política de Segurança

Sua Organização possui uma Política de Segurança da Informação (SI)?

Sim Sim, porém desatualizada **Não**

Existe em sua organização alguém responsável pela gestão da política de SI?

Sim Sim, porém não possui especialização adequada **Não**

Existe algum documento que formaliza a política de SI aprovada pela direção, publicado e comunicado de forma adequada, para todos os integrantes da organização?

Sim Sim, porém desatualizada **Não**

Segurança Organizacional

A organização possui uma infra-estrutura de SI para gerenciar ações corporativas?

Sim Sim, porém desatualizada **Não**

A organização possui um fórum de segurança formado pelo corpo diretor, a fim de gerir mudanças estratégicas?

Sim Sim, mas não está sendo utilizado atualmente **Não**

Existe na organização uma definição clara das atribuições de responsabilidades associadas a SI?

Sim Sim, porém desatualizada **Não**

Existe uma norma de identificação dos riscos no acesso dos prestadores de serviço?

Sim Sim, porém desatualizada **Não**

Existe um controle de acesso especifico para prestadores de serviço?

Sim Sim, porém desatualizada **Não**

Existem requisitos de segurança nos contratos com prestadores de serviços?

Sim Sim, porém desatualizada **Não**

Existem requisitos de segurança nos contratos de terceirização?

Sim Sim, porém desatualizada **Não**

Classificação e Controle dos Ativos de Informação

Existem na organização inventários dos ativos físicos, tecnológicos e humanos?

Sim Sim, porém desatualizada Não

Existem critérios de sigilo para classificar a informação?

Sim Sim, porém desatualizada **Não**

Segurança em Pessoas

Existem na organização critérios de seleção e política de pessoal?

Sim Sim, porém desatualizada Não

Na contratação é previsto um acordo de confidencialidade, termos e condições de trabalho?

Sim Sim, porém desatualizada Não

Existem processos de capacitação e treinamento de usuários?

Sim Sim, porém desatualizada **Não**

Existe uma estrutura para notificar e responder aos incidentes e falhas de segurança?

Sim Sim, porém desatualizada **Não**

Segurança Física e de Ambiente

Existe na organização uma definição de perímetros e controles de acesso físico aos diversos ambientes?

Sim Sim, porém sem uma definição adequada **Não**

Existem recursos de segurança e manutenção dos equipamentos?

Sim Sim, porém desatualizados **Não**

Existe uma estrutura para o fornecimento adequado de energia?

Sim Sim, porém desatualizada Não

Existe uma segurança no cabeamento da organização?

Sim Sim, porém desatualizada **Não**

Gerenciamento das Operações e das Comunicações

São previstos na organização procedimentos e responsabilidades operacionais?

Sim **Sim, porém desatualizados** Não

Existe um controle de mudanças operacionais?

Sim Sim, porém desatualizado **Não**

Existe segregação de funções e ambientes?

Sim Sim, porém desatualizada Não

Existe um planejamento e aceitação dos sistemas?

Sim Sim, porém desatualizados **Não**

Existem procedimentos para copias de segurança?

Sim Sim, porém desatualizados **Não**

Existem controles de Gerenciamento de Rede?

Sim Sim, porém desatualizados **Não**

Existem mecanismos de Segurança e tratamento de mídias?

Sim Sim, porém desatualizados **Não**

Existem procedimentos de segurança na documentação do sistema?

Sim Sim, porém desatualizados **Não**

São previstos mecanismos de segurança para o correio eletrônico?

Sim Sim, porém desatualizados **Não**

Controle de Acesso

Existem na organização normas para o controle de acesso?

Sim Sim, porém desatualizadas Não

Existe um gerenciamento de acesso dos usuários?

Sim Sim, porém desatualizado Não

Existe um controle de acesso à rede remota da organização?

Sim Sim, porém desatualizado **Não**

Existe um controle de acesso ao sistema operacional?

Sim Sim, porém desatualizado **Não**

Existe um controle de acesso às aplicações?

Sim Sim, porém desatualizado **Não**

Existe uma monitoração do uso e acesso ao sistema?

Sim **Sim, porém desatualizada** Não

São definidos critérios para a computação móvel e trabalho remoto?

Sim Sim, porém desatualizados **Não**

Desenvolvimento e Manutenção de Sistemas

Existem requisitos de segurança para os sistemas?

Sim Sim, porém desatualizados **Não**

Existem na organização controles de criptografia?

Sim Sim, porém desatualizados **Não**

São previstos mecanismos de segurança no processo de desenvolvimento e suporte?

Sim Sim, porém desatualizados **Não**

Gestão da Continuidade do Negocio

Existe na organização um processo de Gestão da Continuidade do negocio?

Sim Sim, porém desatualizado **Não**

A organização realiza testes, manutenção e reavaliação do plano de continuidade do negocio?

Sim Sim, porém sem uma regularidade adequada **Não**

Conformidade

Existe uma Gestão de Conformidades técnicas e legais?

Sim Sim, porém desatualizada **Não**

A organização faz, a intervalos regulares, uma analise critica da política de segurança e da conformidade técnica?

Sim Sim, sem ser de forma regular **Não**

Existem na organização recursos e critérios para auditoria de sistemas?

Sim Sim, porém desatualizados **Não**

6.1.2. RESULTADOS DO CRSPE

A partir da análise das respostas obtidas pelo questionário, foi possível ter uma idéia da situação geral da segurança da informação no CRSPE, a qual não é confiável. A Segurança da Informação não está sendo tratada com prioridade e o resultado dessa pesquisa indica a ausência ou ineficácia de muitos dos controles recomendados pela NBR ISO/IEC 17799.

Dentre as diversas causas podemos destacar, talvez o desconhecimento dos riscos e a falta de sensibilização dos executivos e da alta administração, ou também que a Segurança da Informação não seja vista por seus integrantes como um fator critico de sucesso por conta da natureza de sua atividade. Apesar de tudo, não é hora de desanimar. Sempre há tempo de reverter a situação. Propomos, por exemplo, começar por uma análise acurada de riscos.

6.2. RELATÓRIO DE PONTOS A MELHORAR PARA O CRSPE:

Nesta seção apresentamos uma série de recomendações de segurança gerada a partir do resultado do questionário e das peculiaridades da organização, em relação à norma em estudo.

POLÍTICA DE SEGURANÇA

- Implantar uma política de Segurança da Informação;
- Designar um responsável pela gestão da política de Segurança da Informação;
- Providenciar a confecção de um documento que formaliza a política de Segurança da informação;

SEGURANÇA ORGANIZACIONAL

- Criar uma infra-estrutura de Segurança da informação para gerenciar ações corporativas;
- Criar um fórum de segurança;

- Definir de forma clara atribuições e responsabilidades associadas a Segurança da Informação;
- Criar uma norma de identificação dos riscos no acesso de prestadores de serviços;
- Implantar um controle de acesso específico para prestadores de serviço;
- Estabelecer os requisitos de segurança nos contratos de prestadores de serviços;
- Estabelecer requisitos de segurança nos contratos de terceirização;

CLASSIFICAÇÃO E CONTROLE DOS ATIVOS DA INFORMAÇÃO

- Estabelecer critérios de sigilo para classificar a informação;

SEGURANÇA EM PESSOAS

- Criar processos de capacitação e treinamento de usuários;
- Criar uma estrutura para notificar e responder aos incidentes e falhas de segurança;

SEGURANÇA FÍSICA E DE MEIO AMBIENTE

- Estabelecer adequadamente controles de acesso físico aos diversos ambientes;
- Estabelecer recursos para segurança e manutenção dos equipamentos;
- Criar um projeto de segurança no cabeamento;

GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

- Atualizar os procedimentos e responsabilidades operacionais;
- Criar um controle de mudanças operacionais;
- Elaborar o planejamento e aceitação de sistemas;

- Estabelecer procedimentos para copias de segurança;
- Criar controles e gerenciamento de rede;
- Criar mecanismos de segurança e tratamento de mídias;
- Criar procedimentos de segurança para documentação de sistemas;
- Criar mecanismos de segurança para a utilização de correio eletrônico;

CONTROLE DE ACESSO

- Estabelecer o controle de acesso à rede remota;
- Estabelecer o controle de acesso ao sistema operacional;
- Estabelecer o controle de acesso às aplicações;
- Atualizar a monitoração do uso e acesso aos sistemas;
- Estabelecer critérios para a computação móvel e trabalho remoto;

DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

- Estabelecer os requisitos de segurança para os sistemas;
- Criar controles de criptografia;
- Criar mecanismos de segurança nos processos de desenvolvimento e suporte;

GESTÃO DA CONTINUIDADE DO NEGOCIO

- Criar o processo de gestão da continuidade do negocio;
- Realizar, regularmente, testes, manutenção e reavaliação do plano de continuidade do negocio;

CONFORMIDADE

- Criar a gestão de conformidades técnicas e legais;

- Realizar, a intervalos regulares, uma analise critica da política de segurança e da conformidade técnica;
- Criar recursos e critérios para auditoria de sistemas

6.3. PROPOSTA DE POLÍTICA DE SEGURANÇA PARA O CRSPE

Esta seção propõe uma política inicial a ser adotada para nortear os próximos passos do CRSPE, ela foi desenvolvida a partir da análise que fizemos da seção anterior juntamente com os estudos feitos na norma, proposta especificamente para o CRSPE.

6.3.1. INTRODUÇÃO

Este documento tem por finalidade estabelecer as diretrizes de segurança que deverão ser adotadas pelos integrantes do CRSPE. Tais diretrizes fundamentarão as normas e procedimentos de segurança a serem elaborados e implementados por parte do grupo de suporte, considerando as suas particularidades; Para o cumprimento da finalidade supramencionada são estabelecidos os objetivos a seguir.

6.3.2. OBJETIVOS

A Política de Segurança Geral do CRSPE tem os seguintes objetivos específicos:

1. Definir o escopo da segurança do grupo de suporte;
2. Orientar, por meio de suas diretrizes, todas as ações de segurança do grupo, para reduzir riscos e garantir a integridade, sigilo e disponibilidade das informações dos sistemas de informação e recursos;
3. Permitir a adoção de soluções de segurança integradas;
4. Servir de referência para auditoria, apuração e avaliação de responsabilidades.

6.3.3. ABRANGÊNCIA

A Política de Segurança abrange os seguintes aspectos:

1. Requisitos de Segurança Humana;

2. Requisitos de Segurança Física;
3. Requisitos de Segurança Lógica;
4. Requisitos de Segurança dos Recursos Criptográficos.

6.3.4. TERMINOLOGIA

As regras e diretrizes de segurança devem ser interpretadas de forma que todas as suas determinações sejam obrigatórias e cogentes.

6.3.5. CONCEITOS E DEFINIÇÕES

Aplicam-se os conceitos abaixo no que se refere à Política de Segurança do Grupo de Suporte:

1. **Ativo de Informação** – é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos do grupo;
2. **Ativo de Processamento** – é o patrimônio composto por todos os elementos de *hardware* e *software* necessários para a execução dos sistemas e processos dos grupos, tanto os produzidos internamente quanto os adquiridos;
3. **Controle de Acesso** – são restrições ao acesso às informações de um sistema exercido pela gerência de Segurança da Informação do Grupo de Suporte;
4. **Custódia** – consiste na responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros;
5. **Direito de Acesso** – é o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

6. **Ferramentas** – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação do CRSPE;
7. **Incidente de Segurança** – é qualquer evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo do CRSPE e integrantes do Grupo de Suporte;
8. **Política de Segurança** – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação do CRSPE;
9. **Proteção dos Ativos** – é o processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;
10. **Responsabilidade** – é definida como as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informações;
11. **Senha Fraca ou Óbvia** – é aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequenas, tais como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, seqüências numéricas simples, palavras com significado, dentre outras.

6.3.6. REGRAS GERAIS

GESTÃO DE SEGURANÇA

1. A Política de Segurança Geral do CRSPE se aplica a todos os recursos humanos, administrativos e tecnológicos pertencentes ao Sistema de Informação. A abrangência dos recursos citados refere-se tanto àqueles ligados ao CRSPE em caráter permanente quanto temporário;

2. Esta política deve ser comunicada para todo o pessoal envolvido e largamente divulgada através dos departamentos, garantindo que todos tenham consciência da mesma e a pratiquem na organização;
3. Todo o pessoal deve receber as informações necessárias para cumprir adequadamente o que está determinado na política de segurança;
4. Um programa de conscientização sobre segurança da informação deverá ser implementado para assegurar que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações do laboratório. Especificamente, o pessoal envolvido, Grupo de Suporte, ou que se relaciona com os usuários deve estar informado sobre ataques típicos de engenharia social e como se proteger deles;
5. Os procedimentos deverão ser documentados e implementados para garantir que quando o pessoal contratado ou prestadores de serviços sejam transferidos, remanejados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam devidamente revistos, modificados ou revogados;
6. Previsão de mecanismo e repositório centralizado para ativação e manutenção de trilhas, logs e demais notificações de incidentes. Este mecanismo deverá ser incluído nas medidas a serem tomadas por um Grupo encarregado de responder a este tipo de ataque, para prover uma defesa ativa e corretiva contra os mesmos;
7. Os processos de aquisição de bens e serviços, especialmente de Tecnologia da Informação – TI, devem estar em conformidade com esta Política de Segurança;
8. Esta Política de Segurança deve ser revisada e atualizada periodicamente no máximo a cada 2 (dois) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata;

9. No que se refere a segurança da informação, deve-se considerar proibido, tudo aquilo que não esteja previamente autorizado pelo responsável da área de segurança do CRSPE;

GERENCIAMENTO DE RISCOS

O processo de gerenciamento de riscos deve ser revisto, no máximo a cada 18 (dezoito) meses, pelo CRSPE, para prevenção contra riscos, inclusive aqueles advindos de novas tecnologias, visando à elaboração de planos de ação apropriados para proteção aos componentes ameaçados;

INVENTÁRIO DE ATIVOS

Todos os ativos dos laboratórios integrantes do CRSPE devem ser inventariados, classificados, permanentemente atualizados, e possuírem gestor responsável formalmente designado;

PLANO DE CONTINUIDADE DO NEGÓCIO

1. Um plano de continuidade do negócio deve ser implementado e testado, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio;
2. Todas as Áreas de Gerenciamento deverão apresentar planos de gerenciamento de incidentes e de ação de resposta a incidentes a serem aprovados pelo Gerente superior do CRSPE;
3. A conta ou processo do usuário deverá ser imediatamente revogado se um evento provocar a perda ou comprometimento dos serviços disponíveis ou do seu meio de armazenamento. Nesta situação, o usuário deverá seguir os procedimentos detalhados na sua Política de Utilização da Rede;
4. Todos os incidentes deverão ser reportados ao Grupo de Suporte imediatamente, a partir do momento em que for verificada a ocorrência. Estes incidentes devem ser reportados de modo sigiloso a pessoas especialmente designadas para isso.

6.3.7. REQUISITOS DE SEGURANÇA DE PESSOAL

DEFINIÇÃO

Conjunto de medidas e procedimentos de segurança, a serem observados pelos prestadores de serviço e todos os empregados, necessário à proteção dos ativos dos laboratórios integrantes do CRSPE;

OBJETIVOS

1. Reduzir os riscos de erros humanos, furto, roubo, apropriação indébita, fraude ou uso não apropriado dos ativos dos laboratórios integrantes do CRSPE;
2. Prevenir e neutralizar as ações sobre as pessoas que possam comprometer a segurança dos laboratórios integrantes do CRSPE;
3. Orientar e capacitar todo o pessoal envolvido na realização de trabalhos diretamente aos recursos de TI integrantes do CRSPE, assim como o pessoal em desempenho de funções de apoio, tais como a manutenção das instalações físicas e a adoção de medidas de proteção compatíveis com a natureza da função que desempenham;
4. Orientar o processo de avaliação de todo o pessoal que trabalhe nos vários laboratórios do CRSPE, mesmo em caso de funções desempenhadas por prestadores de serviço;

DIRETRIZES

O PROCESSO DE ADMISSÃO

1. Devem ser adotados critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros dos Grupos integrantes do CRSPE, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade do CRSPE;

2. Nenhum Grupo integrante da Segurança do CRSPE admitirá estagiários no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de controles sensíveis à segurança;
3. O empregado, funcionário ou servidor assinará termo de compromisso assumindo o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos do CRSPE;

AS ATRIBUIÇÕES DA FUNÇÃO

Relacionar claramente as atribuições de cada função, de acordo com a característica das atividades desenvolvidas, a fim de determinar-se o perfil necessário do empregado ou servidor, considerando-se os seguintes itens:

1. A descrição sumária das tarefas inerentes à função;
2. As necessidades de acesso a informações sensíveis;
3. O grau de sensibilidade do setor onde a função é exercida;
4. As necessidades de contato de serviço interno e/ou externo;
5. As características de responsabilidade, decisão e iniciativa inerentes à função;
6. A qualificação técnica necessária ao desempenho da função;

O LEVANTAMENTO DE DADOS PESSOAIS

Deve ser elaborada pesquisa do histórico da vida pública do candidato, com o propósito de levantamento de seu perfil;

A ENTREVISTA DE ADMISSÃO

1. Deve ser realizada por profissional qualificado, com o propósito de confirmar e/ou identificar dados não detectados ou não confirmados, durante a pesquisa para a sua admissão;

2. Avaliar, na entrevista inicial, as características de interesse e motivação do candidato, sendo que as informações veiculadas na entrevista do candidato só deverão ser aquelas de caráter público;

AVALIAÇÃO PSICOLÓGICA

Deve ser realizada por profissional legalmente qualificado, com o propósito de avaliar o candidato e a existência de atributos pessoais exigidos para o cargo e/ou função a ser desempenhada;

O DESEMPENHO DA FUNÇÃO

1. Acompanhar o desempenho e avaliar periodicamente os empregados ou servidores com o propósito de detectar a necessidade de atualização técnica e de segurança;
2. Dar aos empregados ou servidores dos grupos de suporte acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança;

A CREDENCIAL DE SEGURANÇA

1. Identificar o empregado por meio de uma credencial, habilitando-o a ter acesso a informações sensíveis, de acordo com a classificação do grau de sigilo da informação e, conseqüentemente, com o grau de sigilo compatível ao cargo e/ou a função a ser desempenhada;
2. A Credencial de Segurança somente será concedida por autoridade competente, ou por ela delegada, e se fundamentará na necessidade de conhecimento técnico dos aspectos inerentes ao exercício funcional e na análise da sensibilidade do cargo e/ou função;

TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

Deve ser definido um processo pelo qual será apresentada aos empregados, servidores e prestadores de serviço a Política de Segurança da Informação e suas normas e

procedimentos relativos ao trato de informações e/ou dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento;

ACOMPANHAMENTO NO DESEMPENHO DA FUNÇÃO

1. Deve ser realizado processo de avaliação de desempenho da função que documente a observação do comportamento pessoal e funcional dos empregados, a ser realizada pela chefia imediata dos mesmos;
2. Deverão ser motivo de registro atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do empregado;
3. Os comportamentos incompatíveis, ou que possam gerar comprometimentos á segurança, deverão ser averiguados e comunicados à chefia imediata;
4. As chefias imediatas assegurarão que todos os empregados ou servidores tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor;

O PROCESSO DE DESLIGAMENTO

1. O acesso de ex-empregados às instalações, quando necessário, será restrito às áreas de acesso público;
2. Sua credencial, identificação, crachá, uso de equipamentos, mecanismos e acessos físicos e lógicos devem ser revogados;

O PROCESSO DE LIBERAÇÃO

O empregado ou servidor firmará, antes do desligamento, declaração de que não possui qualquer tipo de pendência junto aos diversos laboratórios que compõem o CRSPE;

A ENTREVISTA DE DESLIGAMENTO

Deverá ser realizada entrevista de desligamento para orientar o empregado ou servidor sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência nas entidades;

DEVERES

DEVERES DOS EMPREGADOS OU SERVIDORES

1. Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;
2. Cumprir a política de segurança, sob pena de incorrer nas sanções disciplinares e legais cabíveis;
3. Utilizar os Sistemas de Informações dos laboratórios e os recursos a ela relacionados somente para os fins previstos pela Gerência de Segurança;
4. Cumprir as regras específicas de proteção estabelecidas aos ativos de informação;
5. Manter o caráter sigiloso da senha de acesso aos recursos e sistemas das entidades;
6. Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;
7. Responder, por todo e qualquer acesso, aos recursos dos laboratórios bem como pelos efeitos desses acessos efetivados através do seu código de identificação, ou outro atributo para esse fim utilizado;
8. Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente;
9. Comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio;

RESPONSABILIDADE DAS CHEFIAS

A responsabilidade das chefias compreende, dentre outras, as seguintes atividades:

1. Gerenciar o cumprimento da política de segurança, por parte de seus empregados ou servidores;
2. Identificar os desvios praticados e adotar as medidas corretivas apropriadas;
3. Impedir o acesso de empregados demitidos ou demissionários aos ativos de informações, utilizando-se dos mecanismos de desligamento contemplados pelo respectivo plano de desligamento do empregado;
4. Proteger, em nível físico e lógico, os ativos de informação e de processamento dos laboratórios integrantes do CRSPE relacionados com sua área de atuação;
5. Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger a Informação;
6. Comunicar formalmente ao grupo que efetua a concessão de privilégios a usuários de TI, quais os empregados, servidores e prestadores de serviço, sob sua supervisão, que podem acessar as informações disponíveis;
7. Comunicar formalmente ao grupo que efetua a concessão de privilégios aos usuários de TI, quais os empregados, servidores e prestadores de serviço demitidos ou transferidos, para exclusão no cadastro dos usuários;
8. Comunicar formalmente ao grupo que efetua a concessão de privilégios a usuários de TI, aqueles que estejam respondendo a processos, sindicâncias ou que estejam licenciados, para inabilitação no cadastro dos usuários;

RESPONSABILIDADES GERAIS

1. Cada área que detém os ativos de processamento e de informação é responsável por eles, devendo prover a sua proteção de acordo com a política de classificação da informação;

2. Todos os ativos de informações deverão ter claramente definidos os responsáveis pelo seu uso;
3. Todos os ativos de processamento das entidades devem estar relacionados no plano de continuidade do negócio;

RESPONSABILIDADES DA GERÊNCIA DE SEGURANÇA

1. Estabelecer as regras de proteção dos ativos dos laboratórios integrantes do CRSPE;
2. Decidir quanto às medidas a serem tomadas no caso de violação das regras estabelecidas;
3. Revisar pelo menos anualmente, as regras de proteção estabelecidas;
4. Restringir e controlar o acesso e os privilégios de usuários remotos e externos;
5. Elaborar e manter atualizado o Plano de Continuidade do negócio;
6. Executar as regras de proteção estabelecidas pela Política de Segurança;
7. Detectar, identificar, registrar e comunicar as violações ou tentativas de acesso não autorizadas;
8. Definir e aplicar, para cada usuário de TI, restrições de acesso à Rede, como horário autorizado, dias autorizados, entre outras;
9. Manter registros de atividades de usuários de TI (logs) por um período de tempo superior a 6 (seis) anos. Os registros devem conter a hora e a data das atividades, a identificação do usuário de TI, comandos (e seus argumentos) executados, identificação da estação local ou da estação remota que iniciou a conexão, número dos processos e condições de erro observadas (tentativas rejeitadas, erros de consistência, etc.);
10. Limitar o prazo de validade das contas de prestadores de serviço ao período da contratação;
11. Excluir as contas inativas;

12. Fornecer senhas de contas privilegiadas somente aos empregados que necessitem efetivamente dos privilégios, mantendo-se o devido registro e controle;

RESPONSABILIDADES DOS PRESTADORES DE SERVIÇO

Devem ser previstas no contrato, cláusulas que contemplem a responsabilidade dos prestadores de serviço no cumprimento desta Política de Segurança da Informação e suas normas e procedimentos;

SANÇÕES

Sanções previstas pela legislação vigente.

6.3.8. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

DEFINIÇÃO

Ambiente físico é aquele composto por todo o ativo permanente dos laboratórios integrantes do CRSPE;

DIRETRIZES GERAIS

1. As responsabilidades pela segurança física dos sistemas dos laboratórios deverão ser definidas e atribuídas a indivíduos claramente identificados na organização;
2. A localização das instalações e o sistema de segurança do perímetro do CRSPE e de seus laboratórios não deverão ser publicamente identificados;
3. Sistemas de segurança para acesso físico deverão ser instalados para controlar e auditar o acesso aos sistemas de TI;
4. Controles duplicados sobre o inventário e cartões/chaves de acesso deverão ser estabelecidos. Uma lista atualizada do pessoal que possui cartões/chaves deverá ser mantida;

5. Chaves criptográficas sob custódia do responsável deverão ser fisicamente protegidas contra acesso não autorizado, uso ou duplicação;
6. Perdas de cartões/chaves de acesso deverão ser imediatamente comunicadas ao responsável pela gerência de segurança do CRSPE. Ele deverá tomar as medidas apropriadas para prevenir acessos não autorizados;
7. Os sistemas de segurança deverão estar localizados em área protegida ou afastada de fontes potentes de magnetismo ou interferência de rádio freqüência;
8. Recursos e instalações críticas ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança e controle de acesso. Elas devem ser fisicamente protegidas de acesso não autorizado, dano, ou interferência. A proteção fornecida deve ser proporcional aos riscos identificados;
9. A entrada e saída, nestas áreas ou partes dedicadas, deverão ser automaticamente registradas com data e hora definidas e serão revisadas diariamente pelo responsável pela gerência de segurança da informação nos laboratórios do CRSPE e mantidas em local adequado e sob sigilo;
10. O acesso aos componentes da infra-estrutura, atividade fundamental ao funcionamento dos sistemas, como painéis de controle de energia, comunicações e cabeamento, deverá ser restrito ao pessoal autorizado;
11. Sistemas de detecção de intrusão deverão ser utilizados para monitorar e registrar os acessos físicos aos sistemas nas horas de utilização;
12. O inventário de todo o conjunto de ativos de processamento deve ser registrado e mantido atualizado, no mínimo, mensalmente;
13. Quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só devem ser utilizados a partir de autorização formal e mediante supervisão;

14. Nas instalações dos laboratórios integrantes do CRSPE, todos deverão utilizar alguma forma visível de identificação (por exemplo: crachá), e devem informar à segurança sobre a presença de qualquer pessoa não identificada ou de qualquer estranho não acompanhado;
15. Visitantes das áreas de segurança devem ser supervisionados. Suas horas de entrada e saída e o local de destino devem ser registrados. Essas pessoas devem obter acesso apenas às áreas específicas, com propósitos autorizados, e esses acessos devem seguir instruções baseadas nos requisitos de segurança da área visitada;
16. Os ambientes onde ocorrem os processos críticos do sistema de TI do CRSPE deverão ser monitorados, em tempo real, com as imagens registradas por meio de sistemas de CFTV;
17. Sistemas de detecção de intrusos devem ser instalados e testados regularmente de forma a cobrir os ambientes, as portas e janelas acessíveis, nos ambientes onde ocorrem processos críticos. As áreas não ocupadas devem possuir um sistema de alarme que permaneça sempre ativado.

6.3.9. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

DEFINIÇÃO

Ambiente lógico é composto por todo o ativo de informações dos laboratórios;

DIRETRIZES GERAIS

1. A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, deve ser elaborado um sistema de classificação da informação;
2. Os dados, as informações e os sistemas de informação dos laboratórios e sob sua guarda, devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens;

3. As violações de segurança devem ser registradas e esses registros devem ser analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria. Os registros devem ser protegidos e armazenados de acordo com a sua classificação;
4. Os sistemas e recursos que suportam funções críticas para operação das entidades, devem assegurar a capacidade de recuperação nos prazos e condições definidas em situações de contingência;
5. O inventário sistematizado de toda a estrutura que serve como base para manipulação, armazenamento e transmissão dos ativos de processamento, deve estar registrado e mantido atualizado em intervalos de tempo definidos pelo Grupo de Suporte do CRSPE.

DIRETRIZES ESPECÍFICAS

SISTEMAS

1. As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis nos laboratórios. A documentação dos sistemas deve ser mantida atualizada. A cópia de segurança deve ser testada e mantida atualizada;
2. Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado;
3. Os arquivos de *logs* devem ser criteriosamente definidos para permitir recuperação nas situações de falhas, auditoria nas situações de violações de segurança e contabilização do uso de recursos. Os *logs* devem ser periodicamente analisados, para identificar tendências, falhas ou usos indevidos. Os *logs* devem ser protegidos e armazenados de acordo com sua classificação;

4. Devem ser estabelecidas e mantidas medidas e controles de segurança para verificação crítica dos dados e configuração de sistemas e dispositivos quanto a sua precisão, consistência e integridade;
5. Os sistemas devem ser avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção. As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas;

MÁQUINAS SERVIDORAS

1. O acesso lógico, ao ambiente ou serviços disponíveis em servidores, deve ser controlado e protegido. As autorizações devem ser revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado;
2. Os acessos lógicos devem ser registrados em *logs*, que devem ser analisados periodicamente. O tempo de retenção dos arquivos de *logs* e as medidas de proteção associadas devem estar precisamente definidos;
3. Devem ser adotados procedimentos sistematizados para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração do Sistema Operacional e de outros arquivos críticos. Os eventos devem ser armazenados em relatórios de segurança (*logs*) de modo que sua análise permita a geração de trilhas de auditoria a partir destes registros;
4. As máquinas devem estar sincronizadas para permitir o rastreamento de eventos;
5. Proteção lógica adicional (criptografia) deve ser adotada para evitar o acesso não autorizado às informações;
6. A versão do Sistema Operacional, assim como outros *softwares* básicos instalados em máquinas servidoras, devem ser mantidos atualizados, em conformidade com as recomendações dos fabricantes;

7. Devem ser utilizados somente *softwares* autorizados pelo próprio INPE/CRSPE em seus equipamentos. Deve ser realizado o controle da distribuição e instalação dos mesmos;
8. O acesso remoto a máquinas servidoras deve ser realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço;
9. Os procedimentos de cópia de segurança (*backup*) e de recuperação devem estar documentados, mantidos atualizados e devem ser regularmente testados, de modo a garantir a disponibilidade das informações;

REDES DOS LABORATÓRIOS DO CRSPE

1. O tráfego das informações no ambiente de rede deve ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos;
2. Componentes críticos da rede local devem ser mantidos em salas protegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries;
3. Devem ser adotadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede;
4. A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação;
5. Serviços vulneráveis devem receber nível de proteção adicional;
6. O uso de senhas deve estar submetido a uma política específica para sua gerência e utilização;
7. O acesso lógico aos recursos da rede local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela administração da rede, baseado nas responsabilidades e tarefas de cada usuário;

8. A utilização de qualquer mecanismo capaz de realizar testes de qualquer natureza, como por exemplo, monitoração sobre os dados, os sistemas e dispositivos que compõem a rede, só devem ser utilizado à partir de autorização formal e mediante supervisão;
9. A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração devem ser formalmente documentadas e mantidas, de forma a permitir registro histórico, e devem ter a autorização da administração da rede e da gerência de segurança. O diagrama topológico, a configuração e o inventário dos recursos devem ser mantidos atualizados;
10. Devem ser definidos relatórios de segurança (*logs*) de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria. Os *logs* devem ser analisados periodicamente e o período de análise estabelecido deve ser o menor possível;
11. Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos;
12. Proteção lógica adicional deve ser adotada para evitar o acesso não-autorizado às informações;
13. A infra-estrutura de interligação lógica deve estar protegida contra danos mecânicos e conexão não autorizada;
14. A alimentação elétrica para a rede local deve ser separada da rede convencional, devendo ser observadas as recomendações dos fabricantes dos equipamentos utilizados, assim como as normas ABNT aplicáveis;
15. O tráfego de informações deve ser monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança;
16. Devem ser observadas as questões envolvendo propriedade intelectual quando da cópia de software ou arquivos de outras localidades;

17. Informações sigilosas, corporativas ou que possam causar prejuízo às entidades devem estar protegidas e não devem ser enviadas para outras redes, sem proteção adequada;
18. Todo serviço de rede não explicitamente autorizado deve ser bloqueado ou desabilitado;
19. Mecanismos de segurança baseados em sistemas de proteção de acesso (*firewall*) devem ser utilizados para proteger as transações entre redes externas e a rede interna da entidade;
20. Os registros de eventos devem ser analisados periodicamente, no menor prazo possível e em intervalos de tempo adequados;
21. Deve ser adotado um padrão de segurança para todos os tipos de equipamentos servidores, considerando aspectos físicos e lógicos;
22. Todos os recursos considerados críticos para o ambiente de rede, e que possuam mecanismos de controle de acesso, deverão fazer uso de tal controle;
23. A localização dos serviços baseados em sistemas de proteção de acesso (*firewall*) deve ser resultante de uma análise de riscos. No mínimo, os seguintes aspectos devem ser considerados: requisitos de segurança definidos pelo serviço, objetivo do serviço, público alvo, classificação da informação, forma de acesso, freqüência de atualização do conteúdo, forma de administração do serviço e volume de tráfego;
24. Ambientes de rede considerados críticos devem ser isolados de outros ambientes de rede, de modo a garantir um nível adicional de segurança;
25. Conexões entre as redes dos laboratórios do CRSPE e redes externas deverão estar restritas somente àquelas que visem efetivar os processos;
26. Sistemas que executam funções especificas deverão estar isolados para minimizar a exposição contra tentativas de comprometer o sigilo, a integridade e a disponibilidade das informações armazenadas;

27. A segurança das comunicações intra-rede e inter-rede, entre os sistemas deverão ser garantidas pelo uso de mecanismos que assegurem o sigilo e a integridade das informações trafegadas;
28. As ferramentas de detecção de intrusos devem ser implantadas para monitorar as redes críticas, alertando periodicamente os administradores das redes sobre as tentativas de intrusão;

CONTROLE DE ACESSO LÓGICO (BASEADO EM SENHAS)

1. Usuários e aplicações que necessitem ter acesso a recursos dos laboratórios do CRSPE devem ser identificados e autenticados;
2. O sistema de controle de acesso deve manter as habilitações atualizadas e registros que permitam a contabilização do uso, auditoria e recuperação nas situações de falha;
3. Nenhum usuário deve ser capaz de obter os direitos de acesso de outro usuário;
4. A informação que especifica os direitos de acesso de cada usuário ou aplicação deve ser protegida contra modificações não autorizadas;
5. O arquivo de senhas deve ser criptografado e ter o acesso controlado;
6. As autorizações devem ser definidas de acordo com a necessidade de desempenho das funções (acesso motivado) e considerando o princípio dos privilégios mínimos (ter acesso apenas aos recursos ou sistemas necessários para a execução de tarefas);
7. As senhas devem ser individuais, secretas, intransferíveis e ser protegidas com grau de segurança compatível com a informação associada;
8. O sistema de controle de acesso deve possuir mecanismos que impeçam a geração de senhas fracas ou óbvias;

9. As seguintes características das senhas devem estar definidas de forma adequada: conjunto de caracteres permitidos, tamanho mínimo e máximo, prazo de validade máximo, forma de troca e restrições específicas;
10. A distribuição de senhas aos usuários de TI (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário de TI, no primeiro acesso;
11. O sistema de controle de acesso deve permitir ao usuário alterar sua senha sempre que desejar. A troca de uma senha bloqueada só deve ser executada após a identificação positiva do usuário. A senha digitada não deve ser exibida;
12. Devem ser adotados critérios para bloquear ou desativar usuários de acordo com período pré-definido sem acesso e tentativas sucessivas de acesso mal sucedidas;
13. O sistema de controle de acesso deve solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*);
14. O sistema de controle de acesso deve exibir, na tela inicial, mensagem informando que o serviço só pode ser utilizado por usuários autorizados. No momento de conexão, o sistema deve exibir para o usuário informações sobre o último acesso;
15. O registro das atividades (*logs*) do sistema de controle de acesso deve ser definido de modo a auxiliar no tratamento das questões de segurança, permitindo a contabilização do uso, auditoria e recuperação nas situações de falhas. Os *logs* devem ser periodicamente analisados;
16. Os usuários e administradores do sistema de controle de acesso devem ser formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso;

COMPUTAÇÃO PESSOAL

1. As estações de trabalho, incluindo equipamentos portáteis ou stand alone, e informações devem ser protegidos contra danos ou perdas, bem como acesso, uso ou exposição indevidos;
2. Equipamentos que executem operações sensíveis devem receber proteção adicional, considerando os aspectos lógicos (controle de acesso e criptografia) e físicos (proteção contra furto ou roubo do equipamento ou componentes);
3. Devem ser adotadas medidas de segurança lógica referentes a combate a vírus, *backup*, controle de acesso e uso de software não autorizado;
4. As informações armazenadas em meios eletrônicos devem ser protegidas contra danos, furtos ou roubos, devendo ser adotados procedimentos de b*ackup*, definidos em documento específico;
5. O acesso às informações deve atender aos requisitos de segurança, considerando o ambiente e forma de uso do equipamento (uso pessoal ou coletivo);
6. Os usuários de TI devem utilizar apenas *softwares* licenciados pelo fabricante nos equipamentos dos laboratórios, observadas as normas do CRSPE e legislação de *software*;
7. O Grupo de Gerencia de Software deverá estabelecer os aspectos de controle, distribuição e instalação de *softwares* utilizados;
8. A impressão de documentos sigilosos deve ser feita sob supervisão do responsável. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não-autorizado;
9. O inventário dos recursos deve ser mantido atualizado;
10. Os sistemas em uso devem solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*);

11. As mídias devem ser eliminadas de forma segura, quando não forem mais necessárias. Procedimentos formais para a eliminação segura das mídias devem ser definidos, para minimizar os riscos;

COMBATE A VÍRUS DE COMPUTADOR

Os procedimentos de combate a processos destrutivos (*vírus, cavalo-de-tróia e worms*) devem estar sistematizados e devem abranger máquinas servidoras, estações de trabalho, equipamentos portáteis e microcomputadores *stand alone*.

6.3.10. AUDITORIA

INTRODUÇÃO

1. Deverão ser realizadas auditorias periódicas nos sistemas dos laboratórios do CRSPE, pelo Grupo de Segurança;
2. As atividades dos laboratórios integrantes do CRSPE estão associadas ao conceito de confiança. O processo de auditoria periódica representa um dos instrumentos que facilita a percepção e transmissão de confiança à comunidade de usuários;

OBJETIVO DA AUDITORIA

Verificar a capacidade dos Grupos, laboratórios, e repositórios em atender os requisitos do CRSPE. O resultado da auditoria é um item fundamental a ser considerado no processo de melhora continuada adotada pelo modelo de Gerencia do CRSPE, assim como, para a manutenção da condição de Segurança;

ABRANGÊNCIA

A auditoria deve abordar os aspectos relativos ao ambiente de operação e ciclo de vida da informação. Os seguintes tópicos devem ser verificados:

1. Ambiente de operação;
2. Segurança da operação;

3. Segurança de pessoal;
4. Segurança física;
5. Segurança lógica;
6. Segurança de telecomunicações;
7. Segurança de recursos criptográficos;
8. Plano de contingência;

DOCUMENTOS DE REFERÊNCIA

A auditoria deve ser realizada tendo como orientação básica os atos normativos que disciplinam as atividades exercidas no âmbito do CRSPE;

IDENTIDADE E QUALIFICAÇÃO DO AUDITOR

A auditoria dos Grupos e laboratórios do CRSPE atenderá aos seguintes requisitos mínimos:

1. Corpo técnico com comprovada experiência nas áreas de segurança da informação (ambientes físico e lógico), criptografia, infra-estrutura de chaves pública e sistemas críticos;
2. Experiência em serviços de auditoria dessa mesma natureza e referências de outros serviços de auditoria similares;
3. Utilização de padrões internacionais (ISO 17799) que serviu de base para a confecção deste documento, ou padrão similar como referência de melhores práticas e procedimentos;

O RESULTADO DA AUDITORIA PODE CONTER AS SEGUINTES RECOMENDAÇÕES

1. Suspender temporariamente os serviços nos laboratórios ou Grupos do CRSPE até correção dos problemas;
2. Revogar a conta do usuário, grupo do CRSPE;
3. Substituir / treinar pessoal;

FREQÜÊNCIA DAS AUDITORIAS

O processo de auditoria deve ser realizado nas seguintes situações e respectivas freqüências:

1. Credenciamento inicial – antes do credenciamento e do início de suas atividades no âmbito do CRSPE;
2. Auditoria periódica anual – para manutenção do credenciamento;
3. Por determinação do Gerente de Segurança, a qualquer tempo.

6.3.11. GERENCIAMENTO DE RISCOS

DEFINIÇÃO

Processo que visa a proteção dos serviços dos laboratórios integrantes do CRSPE, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) mais viável. Os seguintes pontos principais devem ser identificados:

1. O que deve ser protegido;
2. Análise de riscos (Contra quem ou contra o quê deve ser protegido);
3. Avaliação de riscos (Análise da relação custo/benefício);

FASES PRINCIPAIS

O gerenciamento de riscos consiste das seguintes fases principais:

1. Identificação dos recursos a serem protegidos – hardware, rede, software, dados, informações pessoais, documentação, suprimentos;
2. Identificação dos riscos (ameaças) - que podem ser naturais (tempestades, inundações), causadas por pessoas (ataques, furtos, vandalismos, erros ou negligências) ou de qualquer outro tipo (incêndios);
3. Análise dos riscos (vulnerabilidades e impactos) - identificar as vulnerabilidades e os impactos associados;

4. Avaliação dos riscos (probabilidade de ocorrência) - levantamento da probabilidade da ameaça vir a acontecer, estimando o valor do provável prejuízo. Esta avaliação pode ser feita com base em informações históricas ou em tabelas internacionais;
5. 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;
6. Monitoração da eficácia dos controles adotados para minimizar os riscos identificados;
7. Reavaliação periódica dos riscos em intervalos de tempo não superiores a 6 (seis) meses;

RISCOS RELACIONADOS AOS LABORATÓRIOS DO CRSPE

Os riscos a serem avaliados para os laboratórios integrantes do CRSPE compreendem, dentre outros, os seguintes:

Segmento	Riscos
Dados e Informação	Indisponibilidade, Interrupção (perda), Interceptção, Modificação, Fabricação, Destruição
Pessoas	Omissão, Erro, Negligencia, Imprudência, Imperícia, Desídia, Sabotagem, Perda de Conhecimento
Rede	Hacker, Acesso Desautorizado, Interceptação, Engenharia Social, Identidade Forjada, Reenvio de Mensagem, Violação de Integridade, Indisponibilidade e Recusa de Serviço
Hardware	Indisponibilidade, Interceptação (furto ou roubo), Falha
Softwares e Sistemas	Interrupção (apagamento), Interceptação, Modificação, Desenvolvimento, Falha
Recursos Criptográficos	Gerenciamento das chaves criptográficas, Ciclo de vida de Certificados, Hardware criptográficos, Algoritmos

CONSIDERAÇÕES GERAIS

1. Os riscos que não puderem ser eliminados devem ter seus controles documentados e devem ser levados ao conhecimento do Gerente de Segurança do CRSPE;
2. 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);
3. É necessária a participação e o envolvimento da alta administração das entidades;

IMPLEMENTAÇÃO DO GERENCIAMENTO DE RISCOS

O gerenciamento de riscos nos laboratórios do CRSPE pode ser conduzido de acordo com a metodologia padrão ou proprietária, desde que atendidos todos os tópicos relacionados.

6.3.12. PLANO DE CONTINUIDADE DO NEGÓCIO

DEFINIÇÃO

Plano cujo objetivo é manter em funcionamento os serviços e processos críticos dos laboratórios integrantes do CRSPE, na eventualidade da ocorrência de desastres, atentados, falhas e intempéries;

DIRETRIZES GERAIS

Sistemas e dispositivos redundantes devem estar disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna;

Todos os laboratórios integrantes do CRSPE deverão apresentar um Plano de Continuidade do Negócio que estabelecerá, no mínimo, o tratamento adequado dos seguintes eventos de segurança:

1. Invasão do sistema e da rede interna do laboratório;

2. Incidentes de segurança física e lógica;
3. Indisponibilidade da Infra-estrutura; e
4. Fraudes ocorridas no registro do usuário, na emissão, expedição, distribuição, revogação e no gerenciamento de usuários;

Todo pessoal envolvido com o Plano de Continuidade do Negócio deve receber um treinamento específico para poder enfrentar estes incidentes;

Um plano de ação de resposta a incidentes deverá ser estabelecido para todos os laboratórios integrantes do CRSPE. Este plano deve prever, no mínimo, o tratamento adequado dos seguintes eventos:

1. Comprometimento de controle de segurança em qualquer evento referenciado no Plano de Continuidade do Negócio;
2. Notificação à comunidade de usuários, se for o caso;
3. Revogação dos certificados afetados, se for o caso;
4. Procedimentos para interrupção ou suspensão de serviços e investigação;
5. Análise e monitoramento de trilhas de auditoria; e
6. Relacionamento com o público e com meios de comunicação, se for o caso.

7. CONCLUSÃO

Atualmente, a informação é tratada como um ativo pelas organizações. E, como qualquer outro ativo importante para os negócios, ela precisa ser devidamente protegida para garantir a continuidade dos negócios. Mas isso não é tão simples como parece, pois o avanço tecnológico, que ao mesmo tempo agiliza e simplifica os trabalhos aumentando a produtividade, tem tornado as organizações mais vulneráveis às ameaças de segurança. A conexão com redes públicas e privadas, o compartilhamento de recursos e o aumento da computação distribuída dificultam cada vez mais a implementação de controles de acesso à informação, realmente eficientes. A maioria dos Ambientes Computacionais não foi projetada para serem seguros. Ademais, a segurança que pode ser alcançada por meios estritamente técnicos é limitada. É importante lembrar também que, na implementação e manutenção de sistemas de segurança da informação, o apoio da direção da organização e a participação de todos os funcionários são fundamentais. Além disso, pode ser que seja necessária ainda a participação de terceiros, como clientes e fornecedores, bem como a contratação de uma consultoria externa. Por tudo isso, tornar seguro este ambiente pode ser uma tarefa bastante complexa, requerendo gestão e procedimentos apropriados.

A função deste trabalho foi justamente o de fornecer subsídios para o gerenciamento da implementação de controles de segurança apropriados no CRSPE, ou de qualquer outra organização, visto que foi desenvolvida no decorrer deste trabalho uma interpretação da norma ISO17799 para o ambiente em estudo.

Cabe ressaltar que os produtos desenvolvidos ao longo deste trabalho, são artefatos gerenciais, isto é, são, na verdade, documentos (como relatórios e planos), em vez de produtos de natureza muito técnica (como, por exemplo, instalar e configurar um *firewall*). Este fato demonstra a preocupação em desenvolver o esboço de *framework* segundo uma linha mais gerencial do que técnica. A abordagem do esboço de *framework* tem, portanto, um enfoque voltado para os resultados (expressos através dos produtos) ao final de cada fase. Dessa forma, a abordagem utilizada segue o que parece ser uma tendência das modernas técnicas de gestão, que focalizam mais os resultados obtidos em detrimento dos processos empregados para obtê-los.

Como passo inicial, este trabalho preocupou-se em montar um *framework* onde fosse possível aprofundar os conhecimentos necessários para a implementação de um modelo de segurança completo, com todo embasamento teórico e normativo desenvolvidos, iniciamos o processo de segurança com uma análise de riscos mais abrangente, gerando um relatório de sugestões de segurança e após, geramos uma política de segurança.

A continuidade desse trabalho como fases seguintes a adoção de uma Política de Segurança, pode ser iniciada com uma análise de riscos mais detalhada, ou mesmo a implementação das medidas indicadas na política, dentre elas o Plano de Contingência, e ações de monitoramento do modelo de segurança, que somados, podem minimizar os riscos de um incidente de segurança no CRSPE.

BIBLIOGRAFIA

NBR/ISO/IEC 17799. Tecnologia da Informação: Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas ABNT, 2001.

MOREIRA, Nilton Stringasci; Segurança Mínima – Uma Visão Corporativa da Segurança de Informações, Editora Axcel Books, 2001.

NORTHCUTT, Stephen; ZELTSER, Lenny; WINTERS, Scott; Desvendando Segurança em Redes, Editora Campus, 2002.

HEFFERAN, Rossylenne; BS 7799 – Information Security Management, 2000, disponível em http://www.istc.org.uk.

KRAUSE TIPON, Handbook of Information Security Management 1999, Editora Auerback, 1999.

NIMER, Fernando. Segurança da Informação em Ambientes Distribuídos. Developers Magazine, vol.24, p.22-24, ago 1998.

SCHNEIER, B. Segurança.com: segredos e mentiras sobre a proteção na vida digital: Rio de Janeiro: Campus, 2001.

KURTZ, George; LEE, James; HATCH, Brian. Hachers Expostos – Linux, Segredos e Soluções para a Segurança do Linux. São Paulo: Editora MAKRON BOOKS, 2002.

KURTZ, George; MCCLURE, Stuart; SCAMBRAY, Joel. Hachers Expostos – Segunda Edição, Segredos e Soluções para a Segurança de Redes. São Paulo: Editora MAKRON BOOKS, 2001.

MUTSAERS, E.J. et al. The evolution of information technology. Information Management & Computer Security, v 6, n 3.1998.

RITCHEY, Ronald; FREDERICK, Karen; NORTHCUTT, Stephen. Desvendando Segurança em Redes. Rio de Janeiro: Editora CAMPUS, 2002.

CARUSO, C.A.A.; STEFFEN, F.D. Segurança em Informática e de Informações. São Paulo: Ed. Senac. 1999.

TANENBAUM, Andrew S. Redes de Computadores. Rio de Janeiro: Editora Campus, 3ª edição, 1999, 948 pp. ISBN 8535201572.

OLIVEIRA, Wilson José. Segurança da Informação: Florianópolis: Visual Books, 2001.

MÓDULO Security Solutions S.A. Available: MÓDULO Security Solutions S.A. disponível em: http://www.modulo.com.br, acesso Dez 2004.

LAUDON, K.C.; LAUDON, J.P. Sistemas de informação. 4a Ed. Rio de Janeiro, Ed. Livros Técnicos e Científicos. 1999.

SÊMOLA, Marcos. Gestão da Segurança da Informação – Uma visão executiva. 2ª Ed. Editora Campus. 2001.

PUTTINI, Ricardo S.; SOUZA, Rafael T. de. Principais Aspectos da Seguraça, disponível em: http://webserver.redes.unb.br/security/introducao/aspectos.html, fev 2004.