S e g u r a n ç a

d a

I n f o r m a ç ã o

2007

"Uma corrente não é mais forte do que seu elo mais fraco."
"Tem medo de ataques ? Tranque sua rede numa sala !".

"Só gerenciamos aquilo que medimos, só medimos aquilo que controlamos" - Axur Information Security

Conceitos

Organização da Segurança da Informação

Tem sido prática comum do mercado, as organizações passarem a considerar o ambiente externo, com suas oportunidades e ameaças e o ambiente interno, com as forças e fraquezas em relação à organização. Como resultado, estabelece-se estratégias de atuação de longo prazo que, para sua eficiente obtenção, devem ser divididos em objetivos de curto prazo e distribuídos em suas linhas de processos, como por exemplo, em desenvolvimento de sistemas, gerenciamento de operações e comunicações, segurança ambiental e física, continuidade de negócios dentre outros citados na ISO/IEC 17799.

Atividades principais

A organização da Segurança da Informação torna-se difícil quando há áreas dentro de uma empresa que não fizeram parcerias com seus pares, nem implantaram iniciativas de educação que ampliem a base da responsabilidade pela segurança, dificultando a implementação das estratégias que é conseguida por meio da gestão da segurança com a definição de um modelo de gestão de segurança corporativa, definindo papéis e atribuições para todos dentro da organização.

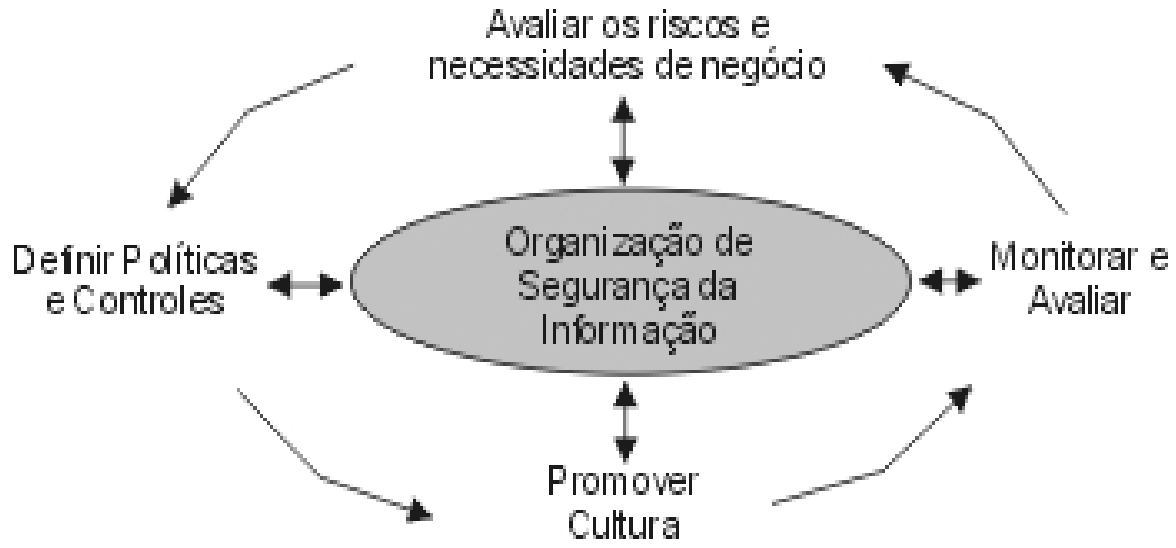
Em geral, é preciso que os profissionais compreendam seus papéis atentando para suas atividades principais.

De modo geral, aos gestores e implementadores da segurança, cabem:
. Definir e manter a estratégia de Segurança da Informação.
. Estruturar e atualizar as políticas, normas, diretrizes, padrões e procedimentos de Segurança da Informação, conforme riscos e necessidades de negócio.
. Desenvolver e implementar processos e componentes/ferramentas de Segurança da Informação.
. Elaborar e monitorar indicadores para avaliação da aderência das ações de Segurança da Informação estabelecidas e atuação preventiva e corretiva.
. Desenvolver a cultura de Segurança da Informação na organização (níveis Estratégico, Tático e Operacional).
. Efetuar mapeamentos contínuos de riscos na organização (riscos surgem e somem a todo momento, temos que mapeá-los sempre).
. Definir e manter o Plano de Continuidade/Recuperação de Desastres da organização.
. Manter a organização atualizada em relação a novas soluções e práticas de Segurança da Informação (Na área de Segurança tudo que é antigo é válido, o que é novo tem se que pesquisar).

Fatores de Sucesso

Quando da gestão da Segurança Organizacional é preciso atentar aos fatores críticos de sucesso, para que as inicitivas de segurança possam atingir seus objetivos internos.

Os fatores críticos para o sucesso da gestão da segurança organizacional são:
. Suporte a participação executiva.
. Interagir com todos os níveis e áreas da organização (entendendo e incorporando os riscos e necessidades do negócio nas diretrizes e soluções de Segurança da Informação).
. Transformar o comportamento das pessoas/usuários.
. Identificar e implementar soluções técnicas adequadas ao nível de riscos, e que viabilizem o negócio, ao invés de limitá-lo.



Resumindo...
. Avaliar os riscos.
. Definir políticas.
. Cultura da SI.
. Monitorar e avaliar.

Security Officer

Security Officer é o equivalente a Gerente de Segurança da Informação e possui hoje, variações como CSO – Chief Security Officer, em suma, este profissional é responsável pela gestão da Segurança da Informação.

Atualmente, cresce o número de SO (Security Officer) que não são responsáveis somente pela segurança em tecnologia da informação, acumulando também funções de segurança no controle de acesso lógico.

Existe muita dificuldade em esclarecer como este se enquadra na hierarquia de uma empresa. No modelo ideal, posiciona-se este profissional de forma que possa se reportar diretamente a alta administração. A independência é fator fundamental.

Sua função é fazer a segurança da informação na organização acontecer. Este perfil demanda um conhecimento generalista de tecnologia, visão do negócio da empresa e suas responsabilidades básicas são:

. Manter a análise de risco atualizada, refletindo o estado corrente da organização.
. Identificar controles físicos, administrativos e tecnológicos para mitigação do risco.
. Aprovar junto a alta administração o nível de aceitação do risco.
. Desenvolver, implementar e gerenciar um programa de conscientização e treinamento com base na Política de Segurança da empresa.
. Trabalhar lado a lado com consultores externos e auditores independentes quando for necessário.

As qualificações desejadas são:
. Deve possuir experiência em Gestão de Risco, Política de Segurança, Plano de Continuidade de Negócios, Auditoria e padrões internacionais de segurança.

. Deve estar capacitado a desenvolver acordos de níveis de serviço com terceiros, para estabelecer um bom controle de segurança nas interfaces externas à organização.
. Apresentar conhecimento de aspectos legais relacionados à segurança da informação.
. Conhecimento técnico e entendimento acerca dos controles tecnológicos.
. Conhecimento do negócio, visão de sua tendência e visão estruturada da proteção da informação são ações básicas para ter condições de priorizar o que deve ser implementado.

Trabalho paralelo ao da Auditoria

A função de auditor não deve ser confundida com o trabalho do Security Officer. Eles devem operar em paralelo. No momento em que um dos dois começa a realizar o trabalho do outro, quem sai perdendo é a organização. Além do mais, o Security Officer precisa ser auditado e a auditoria precisa seguir as políticas de segurança da informação.

Comitê de Segurança

Aconselha-se a formação de um Comitê de Segurança da Informação para que haja a melhor gestão das questões relacionadas à segurança dentro da organização.

O comitê, basicamente, tem o objetivo de atuar com as áreas associadas, definir indicadores e metas, coordenar as medidas de segurança, avaliar os resultados, promover palestras (conscientização e manutenção da Política de Segurança), gerir ações de auditoria e monitoramento, entre outras responsabilidades. Ele deve ser criado com representatividade das áreas técnicas, de gestão e de negócios.

A primeira atividade é definir as responsabilidades de planejamento, execução, monitoração, seu posicionamento dentro do organograma da empresa, garantindo que tenham acesso a esferas decisivas que possam atuar sobre toda a corporação. Seguido da divulgação interna e sua oficialização.

Integrantes do Comitê de Segurança

Composto por profissionais com larga experiência em diversas áreas de atividades da empresa, o Comitê de Segurança deve ser responsável por orientar todos os protocolos de segurança e planos de emergência internos, que visam assegurar a integridade, confidencialidade e disponibilidade das informações manipuladas pela empresa.

Indica-se que este Comitê seja liderado pelo responsável pela área de segurança ou Security Officer, entretanto essa liderança não significa que este tenha um poder de decisão superior aos demais integrantes do Comitê.

O Comitê de Segurança pode ser composto por pessoas de diversas áreas, desde a cozinha até o jurídico, mas por pessoas com larga experiência.

Ele tem a finalidade de dividir (também) a responsabilidade da criação da Política.

Grupos de Ação

O Grupo de Ação será formado temporariamente por integrantes do comitê e das áreas envolvidas para atacar um ou mais problemas identificados pelo comitê. Quando o Grupo de Ação não for composto por profissionais da área de segurança, ou em situações em que os projetos sejam executados por outros grupos, deverão ser supervisionados pela área de

segurança.

A partir de problemas identificados ou reportados para o comitê de segurança, o Grupo de Ação deverá estudar o problema e confeccionar até 3 propostas de soluções com todas as informações – planejamento, custos, impactos e riscos – para que o comitê tenha subsídios suficientes para escolher e aprovar a proposta.

Área de Segurança da Informação

A Área de Segurança da Informação será responsável por toda orientação estratégia na área de segurança, indicando melhorias e endereçando a resolução de incidentes, problemas em potencial ou problemas existentes.

Caberá a área de segurança, supervisionar ou implementar os processos operacionais que implementem as resoluções definidas pelo Grupo de Ação e aprovadas pelo Comitê.

Esta área de segurança da informação terá a seguinte responsabilidade:
. Responderá pela implementação de medidas e execução de trabalhos que aumentem a disponibilidade, integridade, confidencialidade e legalidade das informações manipuladas através de sistemas computadorizados de propriedade da empresa (medidas que aumentam o CID).
. Tratará do estabelecimento de regras de acesso aos recursos existentes nos sistemas computadorizados (Estabelecer regras de acesso).
. Coordenará, cuidará da assessoria e integração dos diversos planos de continuidade que envolva o ambiente computadorizado da empresa (gerir os planos de continuidade).
. Pesquisar e implementar ferramentas de procedimentos, buscando garantir a integridade, disponibilidade e confidencialidade (CID) da informação.
. Planejamento, elaboração, delegação e acompanhamento dos diversos planos de ação, visando a aderência da empresa às diretrizes desta política e do Termo de Responsabilidade e Sigilo.
. Atribuição de responsabilidades de segurança da informação de cada área funcional da empresa.
. Fornecimento de suporte e assessoria em temas de segurança da informação e seus controles associados.
. Difundir a cultura de segurança da informação na empresa.

Papéis de Atuação

A estrutura organizacional de segurança da empresa deverá apresentar profissionais que supram os principais papéis de atuação relacionados à tecnologia da informação. É através destes papéis que as ações de segurança poderão ser implementadas.

Todos os papéis de atuação devem estar alinhados com as necessidades de segurança da empresa.

Papel: Continuidade do Negócio

Responsabilidades:
. Dividido em profissionais que assumem o plano de continuidade do negócio e o time que assume o plano de recuperação (Disaster Recovery), são responsáveis pela análise de impactos, testes do ambiente e implementação do plano de continuidade do negócio.

Papel: Security Officer

Responsabilidades:
. Liderar o fórum de segurança e preparar os temas de debate.
. Liderar o help-desk no que tange aos incidentes de segurança.
. Manter o SMS – Security Manager System.
. Estabelecer e revisar o levantamento de risco.
. Coordenar a seleção de controles e a mitigação de risco.
. Monitorar a compatibilidade com os padrões de segurança.
. Abrir e manter o canal de comunicação com recursos de segurança externos.
. Avaliar e validar as mudanças e resultados de implicações de segurança.
. Aconselhar a organização no que se refere a segurança.

Papel: Gerenciamento de Segurança

Responsabilidades:
. Prover suporte aos processos de segurança.
. Servir de canal alternativo para discussões de pontos de segurança.
. Desenvolver objetivos, estratégias e políticas de segurança.
. Discutir as iniciativas de segurança.
. Revisar os relatórios de incidente de segurança e suas soluções.
. Formular pontos de gerenciamento de riscos e requerimentos de seguro.
. Revisar periodicamente e aprovar a Política de Segurança da Informação.

Papel: Help Desk

Responsabilidades:
. Estar preparado para os incidentes.
. Identificar, registrar, direcionar e redirecionar incidentes de segurança.
. Solucionar operacionalmente os incidentes de segurança.
. Manter a segurança da organização.

Papel: Questões Legais

Responsabilidades:
. Estar alinhado com as agências legais (nacionais e internacionais).

Papel: Manutenção de Incidentes de Segurança

Responsabilidades:
. Rastrear e reportar informações referentes à segurança.
. Gerenciar mudanças.
. Procedimentos de recuperação.

Papel: Infra-estrutura de Segurança

Responsabilidades:
. Transformar as metas da empresa em normas da Política de Segurança.
. Proceder com os esforços de implementação da Política de Segurança.
. Endereçar padrões e tomar ações referente à:
- .Segurança de pessoal
- .Conduta do usuário
- .Classificação, manuseio, transmissão de dados
- .Controle de acesso
- .Padrões de firewall
- .Segurança da rede
- .Segurança da aplicação
- .Log
- .Segurança física de dados e recursos tecnológicos
- .Manutenção da Segurança
- .Gerenciamento de risco
- .Gerenciamento de contas e senhas de usuários
- .Testes de aceite
- .Detecção de intrusão
- .Proteção da rede (antivírus, intrusão, etc)
- .Plano de continuidade
- .Resposta a incidentes

Papel: Compliance

Responsabilidades:
. Endereçar os requerimentos de padrões da ISO 17799.
. Detalhar como identificar riscos através de levantamento de riscos.
. Mitigar riscos através de controles.
. Definir quando é mais aceitável assumir os riscos do que assumir os custos de mitigação.

Papel: Educação para a Segurança

Responsabilidades:
. Divulgar a importância da segurança e utilização de seus controles.
. Divulgar as responsabilidades de segurança dos usuários.
. Servir como fórum de discussão às questões de segurança.
. Orientar novos contratados.