eSecurity

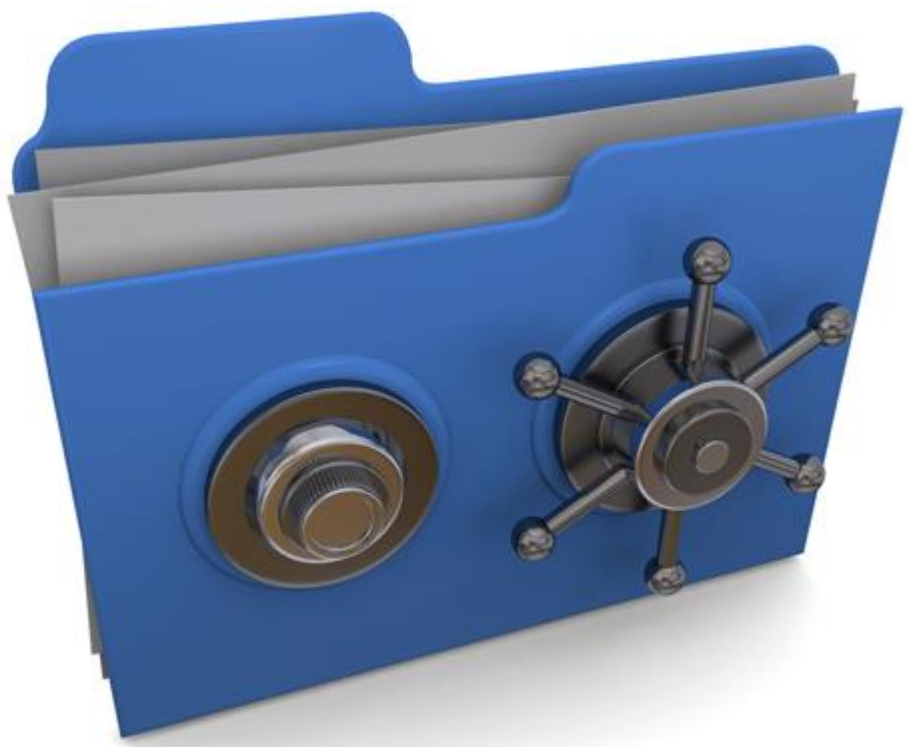
Treinamentos em Segurança da Informação

O que temos para hoje?

Politica de Segurança da Informação:

- ✓Definição
- ✓Maturidade de Segurança da Informação
  - ✓ Segurança Reativa
  - ✓ Políticas, Normas e Acordos (ou fase documental)
  - ✓ Análise de Risco
  - ✓ Gestão do Risco
  - ✓ Implementando um Sistema de Gestão de SegInfo
- ✓Tipificando Riscos
- ✓O que é um Risco?
- ✓Conquistando a aceitação da PSI

Políticas de SegInfo - PSI



PSI: Definição

A informação é um dos principais bens de qualquer organização. Assim, a Instituição estabelece a presente Política de Segurança da Informação, a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações da organização, dos clientes e do público em geral.

A política de segurança se aplica aos empregados, estagiários, contratados, prestadores de serviços, parceiros e fornecedores que utilizam as informações da Empresa.

As medidas de segurança da informação visam proteger a informação de diversos tipos de ameaças, para garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

PSI: Definição

Pode-se definir a política de segurança como um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades sobre o que deve ser feito para alcançar um padrão desejável de proteção para as informações.

Ela é basicamente um manual de procedimentos que descreve como os recursos de TI da empresa devem ser protegidos e utilizados e é o pilar da eficácia da segurança da informação. Sem regras pré-estabelecidas, ela torna-se inconsistentes e vulnerabilidades podem surgir.

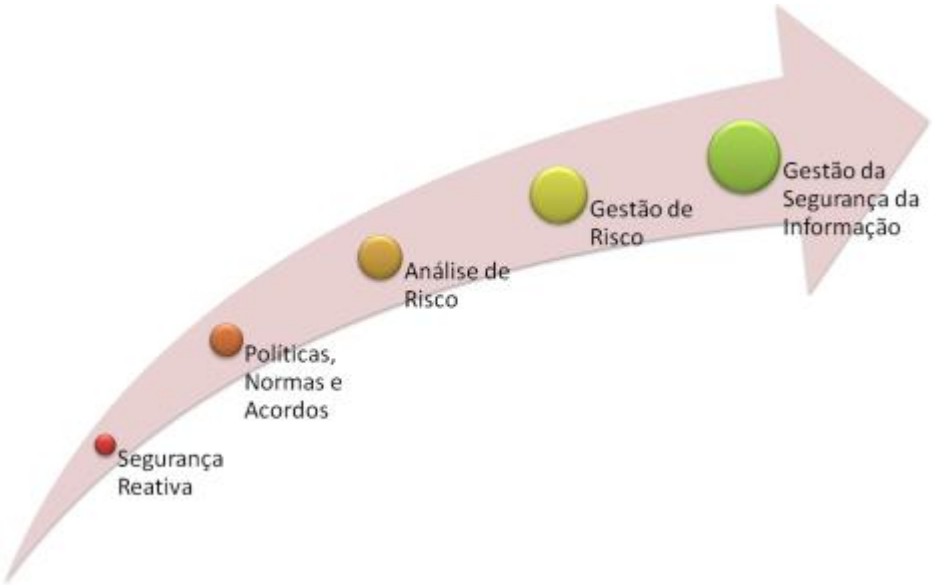
A política tende a estabelecer regras e normas de conduta com o objetivo de diminuir a probabilidade da ocorrência de incidentes que provoquem, por, exemplo a indisponibilidade do serviço, furto ou até mesmo a perda de informações.

As políticas de segurança geralmente são construídas a partir das necessidades do negócio e eventualmente aperfeiçoadas pele experiência do gestor.

PSI: Maturidade de SegInfo

É possível medir, acompanhar e administrador o processo de maturidade da Segurança da Informação de uma determinada empresa.

Esse processo passa por algumas fases, e essas fases podem dizer em que pé está a Segurança de Informação de uma determinada empresa.



PSI: Maturidade de SegInfo

Segurança Reativa

A segurança reativa é a fase onde a empresa está focada apenas nas soluções de tecnologia, e onde os controles técnicos básicos fundamentais de SI são implementados, destacando-se os três controles mais difundidos e implementados: backup, antimalware e firewall.

Existe também nessa fase uma preocupação com o conteúdo acessado pelos usuários, através soluções (ainda técnicas) de controle de conteúdo web (filtro de URL) e antispam, com enfoque maior em produtividade da força de trabalho do que na SI propriamente dita.

PSI: Maturidade de SegInfo

Políticas, Normas e Acordos (ou fase documental)

Nessa fase tem-se um entendimento maior de que a SI não será administrada apenas com tecnologia; começa-se a perceber a importância do fator humano, jurídico e normativo.

Já fica evidente a necessidade de instrumentos de comunicação com os usuários, respaldo jurídico e processos internos de responsabilização e punição.

Muitas empresas despertam para o fato que a informação a ser protegida não está apenas em formato eletrônico, mas encontra-se em mesas, gavetas, armários e nas mentes das pessoas.

PSI: Maturidade de SegInfo

Análise de Risco

A Análise de Risco tem o potencial para ser um divisor de águas na gestão da segurança da informação da empresa.

A Análise (ou Avaliação) de Risco difere da Análise de Vulnerabilidade pois leva em consideração a importância do ativo analisado para os processos de negócio e os objetivos da organização. Em termos simples, como diferenciamos o risco entre, por exemplo, dois servidores de arquivos (file servers) que tem o mesmo sistema operacional, estão no mesmo ambiente físico, possuem os mesmos patches, mas um é utilizado apenas para armazenar documentos históricos para uma consulta eventual, e o outro armazena documentos utilizado no dia-a-dia dos processos, com milhares de acessos e atualizações por dia? Nesse caso o risco é calculado através do impacto de negócio em caso do comprometimento da disponibilidade, integridade ou confidencialidade desses servidores. Eles tem a mesma probabilidade de sofrer um ataque de hacker ou uma falha física, mas cada um trará um impacto diferente para a organização.

PSI: Maturidade de SegInfo

Gestão do Risco

Por Gestão do Risco entende-se não apenas a implementação de controles para mitigar os riscos identificados na Análise de Risco, mas também calcular o risco residual e até mesmo permitir que a direção da empresa aceite riscos, ou seja, formalize o conhecimento dos riscos identificados e que não pretende no momento investir recursos na mitigação do risco, mas conviver com o mesmo temporariamente ou indefinidamente.

Obviamente só é possível para a Direção da empresa assumir riscos caso exista uma visão clara e transparente do impacto dos mesmos ao negócio, o que é uma premissa da Análise de Risco.

PSI: Sistema de Gestão

Implementando um Sistema de Gestão de Segurança da Informação

1. Definir Política de Segurança da Informação
2. Definir escopo do SGSI
3. Executar Avaliação do SGSI
4. Gerenciar Risco
5. Selecionar controles a serem implementados
6. Preparar a declaração de aplicabilidade

PSI: Tipificação de Riscos

Os riscos típicos em Tecnologia de Informação que esta política procura evitar são:

- Revelação de informações sensíveis;
- Modificações indevidas de dados e programas;
- Perda de dados e programas;
- Destruição ou perdas de recursos e instalações;
- Interdições ou interrupções de serviçosessenciais;
- Roubo de propriedades.

Estes riscos ocorrem pelos seguintes principais motivos:

- Negligência – atos não intencionais de funcionários;
- Subversão – ataques disfarçados, por funcionários;
- Acidentes – ocorrências acidentais, por fatores alheios;
- Ataques furtivos – ataques praticados por pessoas estranhas;
- Ataques forçados – ataques às claras, praticados por funcionários ou estranhos;

PSI: O que é um risco?

Com relação a segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas. É medido pela possibilidade de um evento vir a acontecer e produzir perdas.

Para evitar possíveis perdas de informações, que dependendo do seu grau de sigilo, poderá levar a empresa à falência, é necessário a elaboração de uma gestão de riscos, onde os riscos são determinados e classificados, sendo depois especificado um conjunto equilibrado de medidas de segurança que permitirá reduzir ou eliminar os riscos a que a empresa se encontra sujeita.

A norma NBR ISO 27002 nos oferece uma métrica, em que o risco pode ser calculado pela seguinte formula:

RISCO = (Ameaça) x (Vulnerabilidade) x (Valor do Risco)

PSI: Conquistando a aceitação

Após a elaboração das PSIs, é extremamente importante que ela seja assinada por todos os funcionários e terceiros, de todas as classes hierárquicas dentro da empresa.

Este trabalha deve ser realizado de cima para baixo, ou seja, começando com o presidente e conselho, depois as mais altas cúpulas da organização e descendo hierarquicamente todos os cargos, departamentos e sessões da instituição.

Após esse processo, as PSIs deve ficar sempre disponíveis e de fácil consulta para todos os colaboradores, de forma digital e física.

Uma excelente maneira de aplicar e realizar o aceite desse processo, são através de reuniões e apresentações das necessidades de sua implementação.

É importante ressaltar que as PSIs não deve impactar no negócio, mas sim, deve protege-la de qualquer ameaça.

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker