Modelo de caso de negócios para um Sistema de Gestão de Segurança da Informação (SGSI) com base nas normas da série ISO 27000 / IEC (ISO27k)

por Gary Hinson - Versão 2, 2012

Resumo executivo

Benefícios

Um SGSI trará segurança da informação com o controle gerencial da empresa, provendo orientação e melhoria quando necessário. A gestão da SegInfo reduz o risco (probabilidade de ocorrência e/ou impactos adversos) de incidentes, redução de perdas e custos relacionados com o incidente.

Outros benefícios do SGSI incluem:

• Uma abordagem estruturada, coerente e profissional para a gestão da segurança da informação, alinhada com outros sistemas de gestão ISO

• Avaliação global do risco de segurança da informação e tratamento de acordo com as prioridades do negócio e da segurança

• Concentra-se o investimento de segurança da informação para melhor administração

• Governança empresarial utilizando boas práticas de segurança internacionalmente reconhecidas

Custos

A maior parte dos custos associados com a segurança da informação ocorreriam de qualquer maneira desde que a segurança da informação é um imperativo do negócio e de conformidade. Os custos adicionais especificamente relacionadas com o SGSI são principalmente:

• Recursos necessários para projetar, implementar e operar o SGSI, incluindo a gestão de projeto para o projeto de implementação

• Mudanças necessárias para modificar diversos processos e atividades de negócios de acordo com as normas ISO

• Auditorias de conformidade de terceiros

Introdução, âmbito e finalidade

Adotar as normas 27000 da ISO / IEC geralmente começa com um projeto de implementação para especificar, projetar, desenvolver e lançar o Sistema de Gestão da Segurança da Informação (SGSI). Uma vez em funcionamento, o SGSI opera por tempo indeterminado, incorporando a gestão da segurança da informação nos processos de governança e de gestão da empresa.

Este trabalho identifica e categoriza as implicações financeiras da implementação de um SGSI ISO27k como um conjunto de benefícios e custos típicos ou comuns. É claro que é genérico, uma vez que não tem conhecimento de sua situação de segurança da informação específica ou riscos.

Benefícios do SGSI

Estas são as maneiras pelas quais um SGSI normalmente beneficia a organização.

Redução de riscos de segurança da informação

- Fortalece ambiente de controle de segurança da informação existente, (re) enfatizando os requisitos de controle de segurança de informação de negócios, atualização de políticas de segurança de informações atuais, os controles *etc.* e dar um estímulo para rever e, se necessário, melhorar os controles de segurança da informação periodicamente **- redução do risco**
- Abordagem abrangente e bem estruturada, que aumenta a probabilidade de que todas as ameaças de segurança da informação relevantes, vulnerabilidades e impactos serão identificados, avaliados e tratados de forma racional **- redução do risco**
- Abordagem de gestão de risco profissional, padronizada e racional, que dá consistência entre vários sistemas de informação / comunicação (TIC) e os processos de negócio ao longo do tempo, e aborda os riscos de segurança da informação de acordo com suas prioridades relativas **- redução do risco**
- Aumenta a capacidade de transferir certos riscos seletivamente para as seguradoras ou outros terceiros, e pode facilitar a negociação de redução dos prémios de seguro de acordo como controles-chave são implementados e gerenciados **- economia de custos**
- Gerentes e funcionários tornam-se cada vez mais familiarizados com os termos de segurança da informação, riscos e controles **- redução do risco**

Benefícios da padronização em torno da séria ISO27K

- Fornece um *exemplo* de linha de base de segurança. Uma plataforma sólida de controles de segurança da informação quase universalmente exigidos serve de base que para implementar controles adicionais específicos conforme o caso **- poupança de custos**
- Uma adoção de boas práticas, evita 'reinventar a roda' **- redução de custos**
- Evita ter de especificar os mesmos controles básicos repetidamente em todas as situações **- poupança de custos**
- São geralmente aplicáveis e, portanto, re-utilizáveis em vários departamentos, funções, unidades de negócios e organizações sem alterações significativas **- poupança de custos**
- Permite que a organização concentre esforços e recursos em requisitos de segurança adicionais específicos necessárias para proteger determinados ativos de informação **- redução de custos**
- São baseados nas normas de segurança reconhecidas e respeitadas globalmente **- O valor da marca**
- As normas ISO27k vem sendo desenvolvidas e mantidas pelos organismos de normalização, refletindo novos desafios de segurança (tais como BYOD e computação em nuvem) **- o valor da marca**
- Definem formalmente os termos especializados, permitindo que as questões de segurança da informação sejam discutidas, analisadas e tratadas de forma consistente por várias pessoas em diferentes épocas **- economia de custos**

- Permite controles desnecessários, inapropriados ou excessivos sejam relaxados ou removidos sem comprometer indevidamente valiosos ativos de informação **- redução de custos**
- Sendo baseada no risco, a abordagem ISO27k é flexível o suficiente para se adequar a *qualquer* organização, em oposição às normas mais rígidas e prescritivas, como PCI-DSS **- poupança de custos**

Benefícios de uma abordagem estruturada

- Fornece um quadro / estrutura logicamente consistente e razoavelmente abrangente para diferentes controles de segurança da informação **- economia de custos**
- Fornece o impulso para análise de sistemas, dados e fluxos de informação com potencial para reduzir a sobrecarga de desnecessários sistemas / dados / processos duplicados e outros e melhorar a qualidade da informação (processos de negócios re-engenharia) **- redução de custos**
- Fornece um mecanismo para medir o desempenho e gradativamente elevar o status de segurança da informação a longo prazo **- economia de custos e redução de riscos**
- Constrói um conjunto coerente de políticas de segurança da informação, procedimentos e diretrizes, adaptados para a organização e formalmente aprovados pela administração **- benefícios a longo prazo**

Benefícios da certificação eventual

- A confirmação formal por um avaliador independente, competente que SGSI da organização cumpre os requisitos da norma ISO / IEC 27001 **- a redução do risco**
- Fornece garantia sobre as capacidades de uma organização de gestão de segurança da informação (e, por implicação, seu status de segurança da informação) para funcionários, proprietários, parceiros de negócios, fornecedores, reguladores, auditores e outras partes interessadas, sem a necessidade de inúmeras avaliações individuais, avaliações ou auditorias, ou ter que confiar exclusivamente em afirmações e premissas de gestão **- economia de custos e redução de riscos**
- Posiciona a organização como um parceiro de negócios confiável (semelhante ao selo ISO 9000 de garantia de qualidade) **- o valor da marca**
- Demonstra claramente o compromisso da gestão de segurança da informação para a governança corporativa, *compliance* ou fins de *due diligence* **- economia de custos e redução de riscos**

Benefícios da conformidade

- A ISO27k fornece um quadro abrangente para a gestão de segurança da informação, que abrange uma ampla gama de requisitos externos e internos, aproveitando os elementos comuns **- economia de custos e redução de riscos**
- As partes interessadas ou autoridades podem, em algum momento insistir que a organização cumpra a ISO27k como condição do negócio ou para satisfazer a privacidade e outras leis, ao passo que a sua aplicação em nossos próprios termos e prazos é provável que seja mais rentável **- redução de custos**

- Adotar boas práticas geralmente reconhecidas fornecer uma defesa válida em caso de ações de execução legal / regulamentar, após os incidentes de segurança da informação **- de redução de custos e de redução de riscos**

Custos SGSI

Estes são os principais custos associados com os elementos do sistema de gestão de um SGSI ISO27k [3] .

Custos de gerenciamento de projetos de implementação do SGSI

- Encontrar um gerente de projeto adequado (geralmente, mas não necessariamente, a pessoa que acabará por se tornar o CISO - Gestor de Segurança da Informação)
- Preparar uma estratégia de gestão de segurança da informação em geral, alinhada com outras estratégias de negócio, objetivos e imperativos, bem como as ISO27k
- Planejar o projeto de implementação
- Obter a aprovação da gerência de alocar os recursos necessários para estabelecer a equipe do projeto de implementação
- Empregar / ceder, administrar, dirigir e controlar vários recursos do projeto
- Realizar reuniões regulares de gerenciamento de projetos que envolvem os principais interessados
- Acompanhar o progresso real contra os planos e fazer circular atualizações regulares relatórios de status / progresso
- Identificar e lidar com os riscos do projeto, de preferência com antecedência
- Articular, se necessário com várias outras partes interessadas, projetos paralelos, gestores, parceiros de *negócios, etc.*

Outros custos de implementação do SGSI

- Compilar um inventário dos ativos de informação
- Avaliar riscos de segurança para os ativos de informação, e priorizá-los
- Determinar como tratar os riscos de informação *(ou seja,* mitigá-los usando os controles de segurança adequados, evitá-los, transferi-los ou aceitá-las)
- (Re) desenhar a arquitetura de segurança e base de segurança
- Revisão/atualização da PolSeg existente e preparar/emitir novas políticas de segurança da informação, normas, procedimentos, diretrizes, as cláusulas contratuais *etc.*
- Racionalizar, implementar, atualizar, complementar ou aposentar os controles de segurança existentes e outros tratamentos de risco, conforme apropriado
- Realizar sensibilização / formação sobre o SGSI, como a introdução de novas políticas e procedimentos de segurança [4]
- Pode ser necessário demitir ou aplicar outras sanções em caso de descumprimento

Os custos de certificação - eventual

- Avaliar e selecionar um organismo de certificação adequado

- Visitas de pré-certificação e auditoria de certificação / inspeção por uma norma ISO / IEC 27001 organismo de certificação acreditado
- Risco de não obter a certificação na primeira aplicação, demandando revisão e novos custos
- Tempo da equipe / gestão gasto durante as visitas anuais de vigilância
- Re-certificação tri-anual
- Todos estes custos serão todos minimizado se alcançar a implementação de alta qualidade através de nossos próprios esforços

Custos de operação e manutenção do SGSI

- Auditorias internas periódicas para verificar se os procedimentos do SGSI estão sendo seguidos corretamente
- Ações preventivas e corretivas completas para resolver os problemas potenciais e reais
- Revisão periódica e manutenção de políticas de segurança da informação, normas, procedimentos, diretrizes, as cláusulas contratuais *etc.*