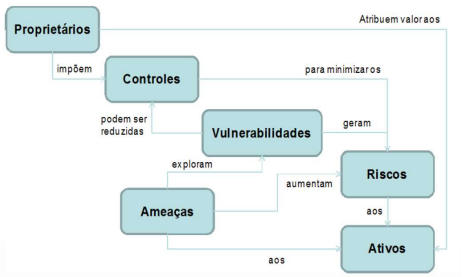
Mitigação do Risco

Prof. Edson Pedro Ferlin

- Objetivos
  - Apresentar os elementos para Mitigação do Risco em termos de Segurança da Informação.
- Conteúdos
  - Análise das situações de aplicação de medidas técnicas ou administrativas
  - Controles técnicos para mitigação do risco
  - Tratamento dos riscos

GESTÃO DE RISCO DE SEGURANÇA

É um processo sistemático da gestão organizacional que determina a aplicação equilibrada de controles de segurança nessa organização, diante do seu perfil de riscos de segurança.



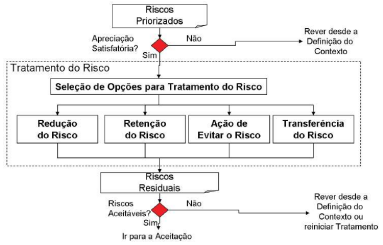
Tratamento dos Riscos

O Tratamento do Risco é a fase da gestão de riscos que envolve a decisão entre reter, evitar, transferir (compartilhar) ou reduzir os riscos.

Objetivos

a. definição de quais controles serão empregados para reduzir alguns destes riscos;
b. retenção ou aceitação de outros riscos;
c. ação de evitar outros riscos;
d. transferência de alguns desses riscos a outros agentes; e
e. definição de um *plano de tratamento do risco.*

Tratamento do Risco



REDUÇÃO DO RISCOS

A Redução do Risco consiste em tomar ações "para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco" [ISO 27005].

A redução envolve a adoção de controles.

É também chamada de mitigação.

Controles

A ISO 27002, também conhecida como ISO 17799, apresenta um guia para implementação de controles de segurança da informação, agrupados por objetivo de controle, num total de 39 objetivos e 133 controles.

Lista de Controles

I. Política de Segurança da Informação (1 objetivo - 2 controles)
II. Organizando a Segurança da Informação (2 objetivos - 11 controles)
III. Gestão de Ativos (2 objetivos - 5 controles)
IV. Segurança em Recursos Humanos (3 objetivos - 9 controles)
V. Segurança Física e do Ambiente (2 objetivos - 13 controles)
VI. Gestão das Operações e Comunicações (10 objetivos - 32 controles)
VII. Controle de Acesso (7 objetivos - 25 controles)
VIII. Aquisição, Desenvolvimento e Manutenção de SI (6 objetivos - 16 controles)
IX. Gestão de Incidentes de Segurança da Informação (2 objetivos - 5 controles)
X. Gestão da Continuidade do Negócio (1 objetivo - 5 controles)
XI. Conformidade (3 objetivos - 10 controles)

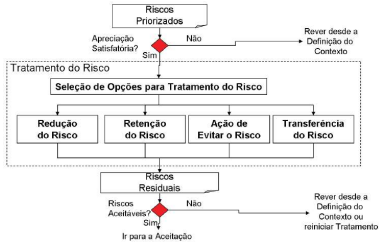
Seleção dos Controles

a. controles apropriados e justificados devem ser selecionados;
b. aspectos normativos e contratuais devem ser considerados quando da aceitação dos riscos;
c. o custo, o tempo e os aspectos técnicos, ambientais e culturais relacionados à seleção do controle devem ser considerados;
d. usualmente, o TCO (custo total de apropriação ou *total cost of ownership*) de um sistema é reduzido por meio da adoção de controles propriamente selecionados;

Efeitos de Controles

a. prevenção
b. conscientização
c. monitoramento
d. detecção
e. detenção
f. eliminação
g. correção
h. minimização de impacto
i. recuperação

Tratamento do Risco



Retenção do Risco

A Retenção do Risco é a decisão de reter ou aceitar o risco sem ações subsequentes.

Se o custo do atacante é menor que o ganho que ele pode ter, e, adicionalmente, se a perda estimada é maior que um limite de tolerância indicada, então o risco é inaceitável. Caso contrário, o risco é retido (aceito).

Evitar o Risco

Uma decisão de evitar o risco completamente pode ser tomada quando os riscos são excessivamente elevados ou os custos de implementação de outras opções excedem os benefícios.

Transferência do Risco

A transferência do risco é o compartilhamento com uma outra entidade do ônus da perda ou do benefício do ganho associado a um risco.

A transferência usualmente transfere a responsabilidade gerencial pelo risco, mas não a responsabilidade jurídica ou contratual pelos impactos.

Contato

eferlin@live.com

(BLOG) professorferlin.blogspot.com

(SITE) professorferlin.com.br

(YOUTUBE) ProfEdsonPedroFerlin