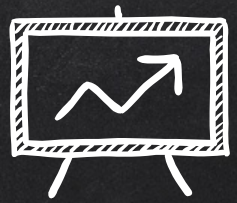
UNAERP

Universidade de Ribeirão Preto

Campus Ribeirão Preto - Campus Guarujá



Segurança da Informação

Tópicos Especiais em Engenharia
Política de Seg. da Informação
Gestão de Incidentes

Política de Seg. da informação

Declaração formal geral da alta direção da organização, definindo o papel da SI dentro da organização

Objetivos da PSI

- ✘ Prover orientação da direção e apoio para a SI
  - Requisitos de Negócio
  - Leis e Regulamentações relevantes
- ✘ Alinhada com o propósito da organização
- ✘ Comprometimento com requisitos aplicáveis
- ✘ Comprometimento com a melhoria contínua do SGSI

Requisitos

Estratégia da organização

Regulamentações, legislação e contratos

Perfil de ameaças a SI

PERFIL ESPECÍFICO DA ORGANIZAÇÃO

Tópicos da PSI

- ✘ Introdução
- ✘ Propósito
- ✘ Escopo
- ✘ Diretrizes
- ✘ Papéis e Responsabilidades
- ✘ Sanções e punições
- ✘ Casos omissos
- ✘ Glossário / Acrônimos

Características da PSI

- ✘ Ser aprovada pela alta diretoria
- ✘ Estabelecer abordagem da organização para gestão dos objetivos da SI
- ✘ Publicação e divulgação adequada
- ✘ Apoiada por políticas específicas
- ✘ Revisada periodicamente

https://www.trt4.jus.br/portais/governanca/politica-seguranca-informacao

Níveis

Estratégico

Direcionamento e Governança

Porque?
Quando?

Política Geral de SI

Tático

Autoridade Formalizada

O que?

Políticas Específicas

Operacional

SI na prática

Como?

Procedimentos

Exemplos da PSI

- ✘ Política de uso aceitável de ativos de informação
- ✘ Política de gestão de riscos
- ✘ Política de controle de acesso
- ✘ Política de desenvolvimento seguro de apps
- ✘ Política de continuidade de negócios
- ✘ Política de resposta a incidentes
- ✘ Política de privacidade

Somente políticas resolve?


ORGANIZAÇÃO

Organização da S.I.

- ✘ Papéis e Responsabilidades
  - S.I. é multidisciplinar (Juridico, RH, etc)
- ✘ Segregação de Funções
  - Acumulo de funções: Risco (dev+sysadmin)
- ✘ Contato com autoridades
  - Bombeiros, PF, etc
- ✘ Contato com grupos especiais
  - CSIRT, Fóruns
- ✘ Segurança na Gestão/Desenvolvimento de Projetos
  - NOT cereja-do-bolo


E SE DER
RUIM?

Gestão de Incidentes

Ocorrência de um único evento ou uma série de eventos de SI indesejados/inesperados, que têm uma probabilidade significativa de comprometer as operações do negócio e ameaçar a segurança das informações

Exemplos de Incidentes de S.I.

- ✘ Colaborador usa dados reais da empresa numa apresentação
- ✘ Gerente recebe e-mail com PDF e ransomware infecta computador
- ✘ Estagiário executa Drop Database
- ✘ Colaborador recebe ligação fingindo ser representante de banco da empresa


Qual Impacto que o incidente pode trazer à sua organização?

Impacto Financeiro

Custo para tratar o incidente ou repor item destruído ou danificado

Consequência após incidente

Impacto Operacional

Serviços indisponíveis (Continuidade)

Retrabalho após recuperação

Impacto Legal

Violação de Contratos (Fornec. / Clientes)

Violação de Leis / Regulamentações

Impacto de Reputação

Divulgação do incidente

Fuga de novos negócios

Qual melhor forma de se tratar um incidente de S.I.?

Gestão de Incidentes de S.I. é o conjunto de processos para detectar, relatar, avaliar, responder, lidar e aprender com incidentes de S.I.

(ISO 27000)

Gestão de Incidentes de S.I.

- (ITIL) O Gerenciamento de Incidentes tem como foco principal restabeler o serviço o mais rápido possível minimizando o impacto negativo no negócio, uma solução de contorno ou reparo rápido fazendo com que o cliente volte a trabalhar de modo alternativo.
- Considerações adicionais:
  - Controlar divulgação de informações relacionadas ao incidente
  - Evitar danos desnecessários e propagação
  - Análise e estimativa de dados
  - Checar implicações legais

Fases Gestão de Incidentes de S.I.

- ✘ Identificação (automática / manual)
- ✘ Registro (formulário / ferramenta SD)
- ✘ Classificação
- ✘ Priorização
- ✘ Diagnóstico inicial
- ✘ Escalamento (Funcional / Hierárquica)
- ✘ Investigação e diagnóstico

Impacto Urgência	Alto	Médio	Baixo
Alto	1	2	3
Média	2	3	4
Baixa	3	4	5

Lições Aprendidas

O que deu bom

O que deu ruim

O que precisa de correção

O que precisa de melhoria

Como evitar nova ocorrência do incidente

Notificação de Incidentes de S.I.

- ✘ Quem precisa ser notificado
  - Interna, acionistas, autoridades, clientes
- ✘ Forma
  - Oficial, site, report, nota
- ✘ Quem
  - Técnicos / Rel. Pub. / Diretoria

https://minutodaseguranca.blog.br/posicionamento-tivit-sobre-vazamento-de-dados-de-clientes/

Atividade!!!

Elaborar uma Política Geral de Segurança de Informação para sua (futura) empresa

Em dupla

Entrega 13/03/2020

https://forms.gle/6XyusvhYaA9ZzRWS9

Dúvidas?

Não esqueça de enviar sua maior dúvida pelo link que está no github.

ezarpelao@unaerp.br

https://github.com/elizarp/unaerp

Credits

Special thanks to all the people who made and released these awesome resources for free:

- ✘ Presentation template by SlidesCarnival
- ✘ Photographs by Unsplash