Aula 5

Segurança em Sistemas de Informação

Prof. Me. Luis Gonzaga de Paulo

A Continuidade dos Negócios

Agenda

- Gestão da continuidade dos negócios
- Análise de impacto nos negócios
- Plano de continuidade dos negócios
- Gestão de crises
- Recuperação de desastres

Contextualizando

- Nenhuma proteção é 100% efetiva
- Incidentes podem – e vão – ocorrer
- Diminuir o impacto
- Minimizar ou evitar perdas
- Reduzir o tempo de retomada

Gestão da Continuidade dos Negócios

- Objetivos
  - Evitar a interrupção
  - Reduzir a interferência

- Respostas a incidentes
- Gestão de crises
- Contingência
- Recuperação de desastres

- **A GCN busca orientar as ações e definir as providências a serem adotadas quando da ocorrência de um incidente, fazendo uso de:**
  - **alta disponibilidade**
  - **tolerância a falhas**
  - ***site backup***
  - **testes regulares**

- **A GCN é necessária para reduzir a um nível aceitável o resultado de uma ocorrência. Contempla, além dos processos de prevenção e contenção:**
  - **o registro histórico**
  - **as medidas adotadas**
  - **as lições aprendidas**

- **Alguns aspectos ligados à TI são fatores de maior complexidade nos processos de GCN, tais como:**
  - **as questões da legislação**
  - **governança**
  - ***compliance***
  - **necessidade de retenção dos dados por longos períodos**

- **Como o propósito da GCN está diretamente ligado ao tempo e aos recursos, os principais indicadores dela (KPI – *Key Process Indicator*) são:**
  - **RTO – *Recovery Time Objective* → quanto tempo foi perdido**
  - **RPO – *Recovery Point Objective* → qual o valor da perda**

Análise do Impacto nos Negócios

- **O tempo de interrupção**
- **O tempo para a retomada**
- **Os recursos necessários para a retomada**

- **A análise de impacto nos negócios ou BIA (*Business Impact Analysis*) é essencial para a GCN. A BIA visa conhecer os processos do negócio e o risco de incidentes para:**
  - **planejar e priorizar ações de recuperação**
  - **elaborar o BCP (*Business Continuity Plan*)**

- **A BIA objetiva identificar as perdas e interrupções, e medir o impacto destas para os negócios. Para isso, considera todos os recursos, tais como:**
  - **pessoal**
  - **instalações**
  - **equipamentos**
  - **fornecedores**
  - **tecnologia**

- **Os riscos, para efeito da BIA, não referem-se às ameaças em si, mas à perda da capacidade produtiva ou de operação e dos recursos mencionados anteriormente**
  - **A perda de recursos resulta na incapacidade de entregar produtos e serviços**

Plano de Continuidade dos Negócios

- **Estratégias para enfrentar os incidentes e as emergências**
- **Considera os sistemas críticos e todos os seus componentes**

- **Avalia os processos de negócio**
- **Provê os recursos mínimos necessários para a operação continuada dos negócios**

- **O PCN é a base da GCN, e objetiva assegurar a continuidade das operações da organização, de modo a manter os negócios após a ocorrência de incidentes**

- **Implica em manter:**
  - **equipamentos**
  - **sistemas**
  - **instalações**
  - **pessoal**
    - ✓ **Todos os recursos em condições de operar**

- **O PCN deve orientar a ação da organização nas interrupções causadas pelos incidentes. Isso requer preparo, capacidade e habilidade para:**

- **preservar os processos críticos**
- **ativar a contingência**
- **recuperar a normalidade operacional**

- ✓ **E tudo isso no menor tempo e com o menor esforço possível**

- **O PCN também contempla a identificação de situações nas quais deve ser ativado, levando em consideração os seguintes aspectos:**

- **identificação e administração de crises**
- **contingência**
- **recuperação de desastres**
- **continuidade operacional**
  - ✓ **Por área de negócio ou abrangência geográfica**

Gestão de Crises

- **Crise é uma situação que impede ou dificulta a organização de atingir seus objetivos**

- **A gestão de crises propõe:**
  - **identificar e tratar os impactos**
  - **conter os danos**
  - **comunicação adequada**
  - **preservar evidências**
  - **retomar a normalidade**

- **Uma crise é algo que afeta de modo muito significativo a organização. Para enfrentá-la é necessário:**
  - **planejamento**
  - **treinamento**
  - **preparação**

- ✓ **Capacitando, portanto, as pessoas da organização para uma ação em equipe, pronta e coordenada**

- **A gestão de crises, a depender do porte da organização, pode requerer a criação e a manutenção de um CSIRT ou de um CERT:**

- ***Computer Security Incident Response Team* – Time de Resposta a Incidentes de Segurança da Computação**
- ***Computer Emergency Response Team* – Time de Resposta a Emergências da Computação**

- **Um aspecto crucial na gestão de crises é o processo de comunicação, que deve ser único e planejado. Em uma crise todos buscam saber:**

- o que ocorreu
- por que ocorreu
- quem são os culpados
- quais as medidas adotadas
- como serão evitadas novas ocorrências

Recuperação de Desastres

- Restabelecer a normalidade
- Reduzir o tempo de parada
- Minimizar os danos
- Encerrar a ocorrência
- Documentar e revisar

- A recuperação de desastres requer procedimentos ativados após um incidente para restabelecer a normalidade no menor tempo e minimizando os dados. Para isso, demanda um DRP (*Disaster Recovery Plan* – Plano de Recuperação de Desastres)

- A premissa do DRP é: "o que fazer se...", cuja resposta deve alinhar-se com:
  1) a política de segurança da informação
  2) a BIA

3) as estratégias de recuperação
4) a DRP
5) teste e treinamento
6) revisão e manutenção

- Com um DRP bem elaborado é possível obter vários benefícios:
  1) aumentar a percepção de segurança e a tranquilidade para enfrentar as crises

2) reduzir o tempo de resposta
3) garantir a confiabilidade
4) prover padrões para os testes

- Além dos benefícios citados, um DRP também mitiga alguns riscos:
  1) minimiza a necessidade da tomada de decisão

2) reduz o risco de responsabilização legal
3) diminui o estresse no ambiente de trabalho, especialmente durante as crises

Síntese

- BCM
- BIA
- BCP
- Gestão de crises
- DRP

Referências de Apoio

- GALVÃO, M. C. Fundamentos em Segurança da Informação. São Paulo: Pearson Education, 2015.
- ABNT. Segurança da Informação – Coletânea eletrônica. Rio de Janeiro: ABNT, 2014.

- **COSTA, G. C. G. Negócios eletrônicos: uma abordagem estratégica e gerencial. Curitiba: Intersaberes, 2013.**

- **OLIVEIRA, F. B. (Org). Fundação Getúlio Vargas. Tecnologia da Informação e da Comunicação: a busca de uma visão ampla e estruturada. São Paulo: Pearson Education, 2007.**