Segurança da Informação e Proteção ao Conhecimento

Aula 11 – Gestão da continuidade dos negócios

Prof. Dalton Martins
dmartins@gmail.com

Gestão da Informação
Faculdade de Informação e Comunicação
Universidade Federal de Goiás

Gestão de continuidade de negócios

objetivos

Identificar os requisitos e organizar a continuidade de negócios; identificar e selecionar os procedimentos da gestão de incidentes de segurança.

conceitos

Gestão da continuidade de negócios, segurança da informação e continuidade de negócios, plano de continuidade de negócios e gestão de incidentes.

Continuidade de negócios

- Dependência de tecnologia e sistemas computacionais.
- Impactos diversos.
- É preciso considerar:
  - Medidas de recuperação de desastres.
  - Plano de contingências.
  - Plano de continuidade de negócios.
- Preocupação dos dirigentes deve ser constante.

Gestão da continuidade de negócios

- Combina medidas de prevenção e recuperação.
- Aspectos relevantes:
  - Identificar os processos críticos de negócios.
  - Integrar a gestão da segurança da informação.
- O plano de continuidade de negócios deve ser implementado.

Segurança da informação e gestão da continuidade de negócios

A segurança da informação é estratégica. Considerações:

- Compreensão dos riscos.
- Identificação dos processos e ativos críticos.
- Compreensão dos impactos.
- Contratos de seguro.
- Identificação de medidas aplicáveis.
- Identificação dos recursos requeridos.
- Proteção de recursos de processamento.
- Documentação detalhada.
- Testes e manutenção dos planos.

Exemplo de questão a ser considerada no plano de continuidade de negócios:

- “Perda da capacidade de proteção, processamento e recuperação das informações manipuladas nos computadores da organização, podendo ocasionar problemas na realização de seus negócios e no cumprimento de metas previamente estabelecidas em contrato com seus clientes.”

O exemplo apresenta um problema a ser tratado no plano de continuidade de negócios das organizações.

Análise de riscos e continuidade de negócios

Compreende:

- Identificar eventos adversos.
- Analisar riscos (de toda a espécie).

Em função dos resultados da análise, deve-se elaborar um planejamento de estratégias para a continuidade de negócios.

Plano de continuidade de negócios

- Estrutura.
- Desenvolvimento e implementação.
- Testes.
- Manutenção e reavaliação.

Estrutura

Contemplar, pelo menos:

- Responsabilidades individuais requeridas.
- Indicação de gestor.
- Condições para acionamento.
- Procedimentos para operação temporária durante recuperação.
- Procedimentos emergenciais.
- Procedimentos de recuperação.
- Especificação do cronograma de testes e manutenção.
- Treinamentos.

Desenvolvimento e implementação

Considerar, pelo menos:

- Identificação das responsabilidades e procedimentos.
- Identificação do grau aceitável de perdas.
- Implantação dos procedimentos de recuperação.
- Conscientização quanto às responsabilidades.
- Testes.
- Manutenção regular.
- Cópias do plano em locais distintos.

Testes

O plano de testes indica como e quando cada componente do plano deve ser testado.

Técnicas possíveis:

- Testes de cenários.
- Simulações.
- Teste de recuperação técnica.
- Teste de recuperação em local alternativo.
- Testes de facilidade de fornecedores e serviços.
- Ensaio completo.

Manutenção e reavaliação

- Manutenção regular.
- Atualizar o plano em virtude de mudanças.
  - Nos negócios (objetivos e/ou estratégias).
  - Aquisição de novos equipamentos e sistemas.
  - Legislação.
- Deve-se estabelecer responsabilidades para reavaliações regulares.

Exemplo de recomendação para a continuidade de negócios – Comprometimento do ambiente de TI:

- "Em caso de comprometimento comprovado da segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas. Nesses casos, uma versão segura do Sistema Operacional, assim como dos softwares de segurança, deverá ser baixada novamente, e as alterações recentes de usuários e privilégios do sistema devem ser revisadas a fim de detectar modificações não autorizadas de dados."

Exemplo de diretriz para a conscientização em segurança da informação e continuidade de negócios:

- "A divulgação das regras, riscos, procedimentos e políticas de segurança aos usuários finais deve ser objeto de campanhas internas permanentes, seminários de conscientização e quaisquer outros meios ou iniciativas para a consolidação da educação para a segurança da informação."

Notificação de eventos adversos

- Efetuada para acionar as medidas adequadas em tempo aceitável.
- As pessoas devem ser conscientizadas a respeito dos procedimentos de notificação.
- As notificações devem ser emitidas aos responsáveis diretos pela gestão de incidentes.

Procedimentos da gestão de incidentes de segurança

Ações efetivas, rápidas e ordenadas. Compreendem:

- Planos de contingências.
- Identificação e análise da causa do incidente.
- Planejamento e implementação de medidas corretivas.

Planos de contingências

Aspectos importantes:

- Recursos financeiros, humanos e de infraestrutura.

Fases:

- Resposta imediata a desastres.
- Processo de recuperação.

Fases do planejamento

- Atividades preliminares.
- Análise de impactos.
- Análise de alternativas de recuperação.
- Desenvolvimento do plano de contingências.

- Treinamento.
- Testes.
- Avaliação e atualização do plano.

Antes do planejamento, é importante responder às seguintes questões:

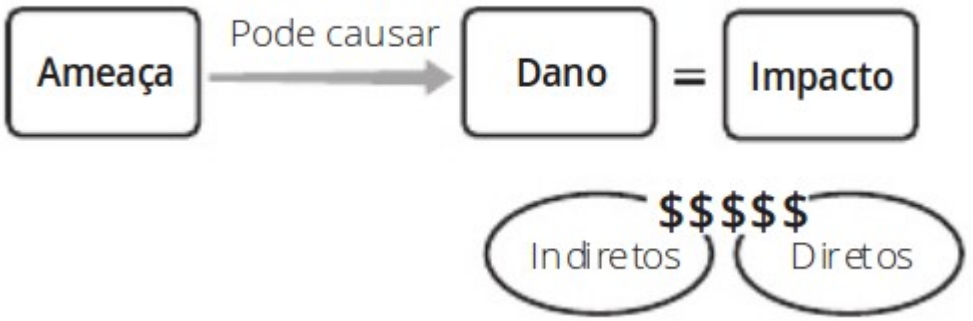
- Quais são os objetivos?
- Qual é o orçamento?
- Quais são os prazos?
- Quais são os recursos humanos disponíveis?
- Quais são os equipamentos e demais suprimentos necessários?
- Quais são as responsabilidades da equipe responsável pelo planejamento?

Com todas as respostas, pode-se iniciar o planejamento de contingências, seguindo as fases

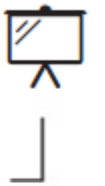
Análise de impacto

Atividade importante para a tomada de decisões estratégicas. Subfases:

- Identificação e classificação dos recursos, sistemas e funções críticas.
- Definição do tempo para recuperação.
- Elaboração de relatório específico.



Identificação dos recursos, funções e sistemas críticos



- Identificar e classificar segundo as prioridades para os negócios.
- Essencial à tomada de decisões quanto a contingências.

Nesta subfase, deve-se considerar tanto a identificação de recursos, funções e sistemas críticos, quanto sua classificação. Segue uma proposta para classificação que pode ser usada em organizações reais:

- Altamente importantes (essenciais);
- De importância média;
- De baixa importância.

Definição do tempo para recuperação e elaboração de relatório

Determinar o intervalo de tempo aceitável para paradas. No relatório, destacar:

- Recursos, sistemas e funções identificadas e classificadas.
- Descrição das potenciais ameaças.
- Intervalo de tempo aceitável para recuperação.
- Levantamento de recursos necessários à recuperação após desastres.

Análise de alternativas de recuperação

Considerar necessidades reais da organização. Existem várias alternativas:

- Prevenção e detecção de acidentes.
- Política adequada de backup.
- Armazenamento e recuperação de dados.
- Seguros.

Relatório de alternativas de recuperação

- Descrição das opções.
- Estimativas de custos.
- Vantagens e desvantagens.
- Recursos necessários.

Desenvolvimento do plano de contingências

- Designar equipe responsável.
- Determinar como responder a desastres.
- Identificar aplicativos críticos.
- Manter inventário de arquivos, dados, Sis tema Operacional e utilitários.
- Levantar necessidades especiais.

Treinamentos e testes

- Treinamentos devem ser regulares e compreender teoria, práticas e simulações.
- Testes podem ser feitos nas categorias:
  - Integral.
  - Parcial.
  - Simulado.

Avaliação e atualização do plano

A avaliação e atualização do plano devem ser contínuas e refletir mudanças:

- Nos negócios.
- No ambiente.
- Em questões administrativas.

Exemplos de recomendações para a prevenção de incidentes de segurança da informação:

- "Não é permitido, a menos que com a devida autorização, interferir, sobrecarregar ou desativar um serviço, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos."
- "É vetada aos usuários a execução de testes ou tentativas de comprometimento de controles internos. Esta prática é permitida apenas a pessoas com competência e função técnica na organização, durante atividades de monitoramento e análise de riscos, com a autorização legítima para tal."

Boas práticas

- Documentar incidentes de segurança.
- Identificar recursos, sistemas e funções críticas.
- Analisar impactos.
- Avaliar alternativas e selecionar as adequadas.
- Elaborar o plano segundo as necessidades reais.
- Promover treinamentos periódicos.
- Efetuar testes regulares.
- Manter o plano atualizado.

Atividade 9.1 – Entendendo os conceitos de Gestão de Continuidade de Negócios

1. Explique o que é a Gestão de Continuidade de Negócios.

2. Que considerações devem ser atendidas no tratamento da segurança da informação no contexto da continuidade de negócios?

Atividade 9.2 – Executando a continuidade de negócios

1. Qual a estrutura mínima de um Plano de Continuidade de Negócios (PCN)?

2. O que a gestão de incidentes de segurança deve contemplar?

3. Qual a importância da notificação de eventos adversos?

4. Quais devem ser os procedimentos da gestão de incidentes de segurança?

5. Descreva o que deve ser feito durante a análise de impacto no decorrer das fases do planejamento de contingências.

6. Explique o que é o "tempo de recuperação" e, através de um exemplo prático, indique como ele deve ser empregado.

Atividade 9.3 – Executando a continuidade de negócios e a gestão de incidentes na sua organização

1. Como integrante do comitê de segurança da informação, você foi indicado(a) para apresentar um plano de Continuidade de Negócios (PCN) para sua organização. Durante a apresentação do tema, considerando a atual estrutura e objetivos da sua instituição, que atividades devem ser listadas para desenvolver este plano?

2. Você assumiu a responsabilidade de estruturar uma equipe de Tratamento e Respostas a Incidentes para redes computacionais (ETIR) para sua organização. Como você vai estruturar esta equipe? Que profissionais da sua organização integrarão o ETIR? Quais serão os objetivos do ETIR?