Segurança em Sistemas de Informação

Aula 5

Prof. Luis Gonzaga de Paulo

Conversa inicial

Como já vimos, mesmo havendo um grande esforço e medidas em profusão para garantir a segurança da informação e dos sistemas, nenhuma dessas medidas é infalível. Seja em função do tempo, da complexidade, do valor da informação que visam proteger, da expertise dos atacantes, da extensão ou gravidades dos incidentes, em algum momento haverá uma falha. E esta falha trará consequências para o negócio. O que fazer caso isso ocorra? Como garantir que os efeitos do incidente não comprometam – ou afetem o mínimo – o negócio da organização? A resposta a esta pergunta faz parte das atividades da área de segurança da informação e dos sistemas.

Para dar início às suas reflexões sobre o tema, assista ao vídeo a seguir:

Plano de Continuidade dos Negócios

https://www.youtube.com/watch?v=bq-PjPyHPRI

Acesse o material *on-line* e assista ao vídeo de introdução da aula!

Contextualizando

Apesar de manter-se preparada para enfrentar as ameaças da segurança da informação e de sistemas, a organização deve ter em conta que nenhuma proteção é 100% efetiva, e isso implica em estar sujeita a incidentes que efetivarão o risco, trazendo impactos para o negócio. E é esta inevitabilidade completa de incidentes que requer a adoção das medidas de Gestão da Continuidade dos Negócios (GCN), que é um conjunto de medidas e atividades para serem postas em prática uma vez que ocorrido o incidente e, assim, minimizar ou evitar as perdas decorrentes e o tempo necessário para a retomada da normalidade.

O professor Luis fala um pouco mais sobre isso no vídeo que está disponível no material *on-line*!

Antes de iniciarmos a apresentação do conteúdo, que tal pesquisar um pouco? Acesse a Biblioteca Virtual e leia o conteúdo da Unidade 4 do livro "Fundamentos em Segurança da Informação", de Michele da Costa Galvão. Leia também o capítulo 8 do livro "Tecnologia da Informação e da Comunicação", de Fátima Bayma de Oliveira (org.), da bibliografia básica da disciplina. Pesquise o tema "Gestão da Continuidade de Negócios" e as normas ISO aplicáveis, leia os artigos e textos dos "Materiais complementares" das aulas no UNINVIRTUS e assista aos vídeos recomendados.

Gestão da Continuidade do Negócio

A Gestão da Continuidade dos Negócios (GCN) é um processo diretamente relacionado com a segurança da informação e dos sistemas. Seu objetivo é evitar a interrupção ou reduzir a interferência dos incidentes nos processos críticos e nas informações vitais para a preservação da organização e de seus negócios.

No cenário atual, as áreas das organizações atuam com uma grande diversidade de processos para produzir e entregar produtos e serviços, muitos dos quais de alta complexidade, empregando grande volume de documentos e informações, atendendo a diferentes objetivos e com uma complexa rede de relacionamentos que envolvem considerável número de outras organizações e de pessoas.

Neste ambiente há considerável possibilidade de ocorrerem falhas, a despeito de todas as medidas de proteção. A gestão de riscos busca identificar e propor tratamentos distintos e efetivos para as possibilidades de incidentes, mas e se eles ocorrerem?

Quando um risco se transforma em incidente, ultrapassando todas as defesas projetadas para evitar tal ocorrência, entram em cena os processos de resposta a incidentes, a gestão de crises, o regime de contingência e a recuperação de desastres. Parece dramático, mas não deveria. Todos os riscos para os quais a organização dispôs-se a analisar e tratar devem também ser objetos de uma análise de impacto nos negócios. Esta análise é conhecida como

what-if, ou seja, “e se”? O que acontece se uma informação confidencial for acessada ou divulgada? Ou alterada? O que acontece se um sistema for invadido e tornar-se indisponível ou não-confiável?

A Gestão da Continuidade dos Negócios deve prover a resposta e apontar o direcionamento das ações e providências para as ocorrências que, uma vez não podendo ser evitadas, comprometam as operações da organização e gerem impacto. O planejamento das medidas a serem adotadas compõe o Plano de Continuidade dos Negócios (PCN), ou o *Business Continuity Plan* (BCP).

No que tange à informação e aos sistemas, até pouco tempo imaginava-se que uma cópia de segurança – o *backup* – mantida razoavelmente atualizada era a garantia necessária. Com o avanço da tecnologia e o exponencial aumento dos dados – estimado em 40% ao ano – tanto a complexidade de manter o *backup* atualizado quanto a agilidade necessária para recompor o estado operacional da organização vêm mudando esta percepção. Essa mudança vem exigindo um aprofundamento no conhecimento dos processos estratégicos e informações vitais e um complexo e detalhado planejamento de ações de restabelecimento, que impacta até mesmo nos processos de aquisição e desenvolvimento de *software*.

Aspectos de governança e *compliance*, legislação e necessidade de retenção de dados por longos períodos também devem ser considerados e agregam complexidade a esta capacidade de reação a incidentes.

No mundo dos negócios eletrônicos e em tempo real, itens como a alta disponibilidade, tolerância a falhas, *site backup* e procedimentos regulares de teste compõem o conjunto de temas pertinentes à gestão da continuidade do negócio.

Em suma, é necessária a GCN para reduzir, a um nível aceitável, qualquer interferência nos processos de negócio da organização, causados por desastres ou falhas na segurança, sejam estes naturais, acidentais, tecnológicos ou intencionais. Para isso devem ser combinadas as atividades e processos de

prevenção e de recuperação. Também é recomendável que haja um registro histórico destes eventos, com as medidas adotadas e as lições aprendidas.

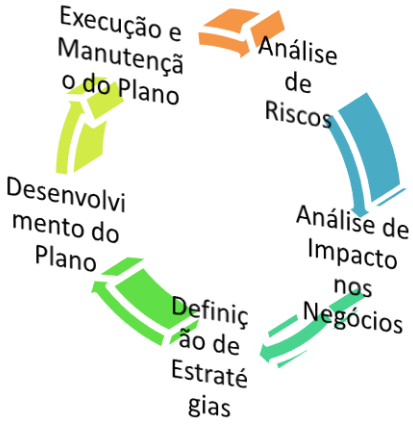
O propósito supremo da GCN na segurança da informação e dos sistemas é restabelecer a normalidade da operação em tempo adequado, *Recovery Time Objective* (RTO), e garantir o mínimo de perda de informação, o *Recovery Point Objective* (RPO).

Para mais informações sobre a Gestão da Continuidade dos Negócios, acesse o material *on-line* e assista ao vídeo que está disponível para você!

Análise de impacto nos negócios

A análise de impacto nos negócios ou *Business Impact Analisys* (BIA) é uma ferramenta essencial para a Gestão da Continuidade dos Negócios. O propósito da BIA é o conhecimento dos processos de negócio e a avaliação dos mesmos quanto às possibilidades de incidentes que possam interrompê-los, considerando o tempo de interrupção, o tempo para a retomada à normalidade e os recursos necessários para isso. Desta forma pode-se planejar e priorizar as ações de recuperação em função de critérios objetivos como tempo, esforço, recursos e custos envolvidos, isto é, elaborar o *Business Continuity Plan* (BCP) ou Plano de Continuidade dos Negócios (PCN).

Figura 1 – A BIA no contexto do BCP



Leitura recomendada

Para saber mais sobre o assunto, leia o texto que está disponível a seguir:

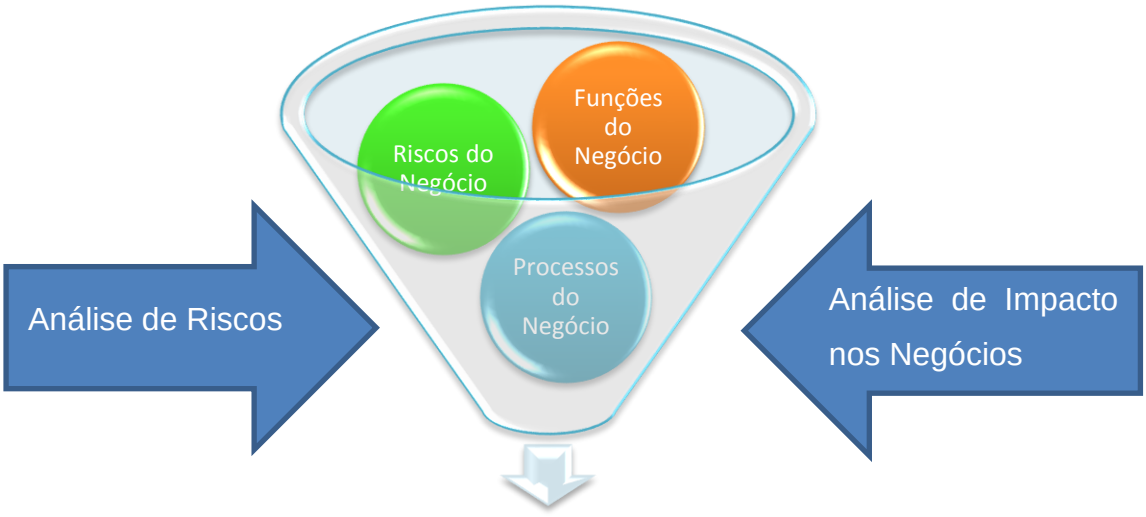
BIA – Uma visão conceitual

http://www.portalgsti.com.br/2013/07/business-impact-analysis-uma-visao.html

A BIA é apoiada nas normas ISO/IEC 27005 e ISO/IEC 22301 e é um componente de suma importância para a segurança da informação e dos sistemas, abordando e visando principalmente os aspectos de integridade e disponibilidade da informação. Os dois insumos básicos para a BIA são:

- O mapeamento dos processos do negócio da organização – geralmente obtidos por meio de atividades do *Business Process Management* (BPM) ou gerenciamento dos processos de negócio;
- A análise de riscos do negócio, parte do processo de gerenciamento de riscos.

Figura 2 – BIA na apuração dos processos críticos do negócio



É bom ressaltar que a análise de riscos aqui trata das perdas ou interrupções da capacidade produtiva da organização, isto é, da sua incapacidade de entregar produtos e serviços devido a incidentes, e não das

ameaças em si, que devem ser devidamente abordadas pelos processos de gerenciamento de riscos. Riscos de negócios, portanto, não são necessariamente as ameaças, mas a possibilidade de perda de recursos requeridos para a entrega de produtos e serviços, por exemplo, pessoal, instalações, equipamentos, fornecedores e tecnologia.

O professor Luis fala mais sobre análise de impacto nos negócios no vídeo que está disponível no material *on-line*!

Plano de Continuidade dos Negócios

O Plano de Continuidade dos Negócios (PCN), ou *Business Continuity Plan (*BCP), é um documento ou conjunto de documentos que estabelece as estratégias e planos de ação para o enfrentamento de situações de emergência que afetem a operação normal da organização. Do ponto de vista da segurança da informação e dos sistemas o PCN aborda os sistemas críticos e seus componentes, além dos processos de negócio dos quais fazem parte.

Leitura recomendada

Quer aprofundar mais seus conhecimentos? Então faça a leitura indicada a seguir:

A importância do PCN

http://iso27000.com.br/index.php?option=com_content&view=article&id=52:importpcn&catid=34:seginfartgeral&Itemid=53

O PCN é a principal ferramenta da Gestão da Continuidade dos Negócios. É por meio dele que a organização espera assegurar a continuidade das suas operações, mantendo os seus negócios em funcionamento, na eventualidade de uma indisponibilidade prolongada dos recursos que dão suporte à realização das suas operações, isto é, dos equipamentos, dos sistemas de informação, das instalações, do pessoal e das informações.

Todas as atividades de uma organização estão sujeitas a ameaças que podem causar sua interrupção, e isto inclui as atividades que dependem de

sistemas de informação. Um PCN define como reagir de forma adequada a estas interrupções, preservando o máximo possível do conjunto de componentes dos processos de negócio, ativando os recursos de contingência e recuperando a normalidade operacional no mais breve espaço de tempo possível.

Um PCN geralmente inclui a identificação de situações no qual deva ser ativado e também contempla os seguintes aspectos:

- Identificação e administração de crises;
- Contingência;
- Recuperação de desastres;
- Continuidade operacional.

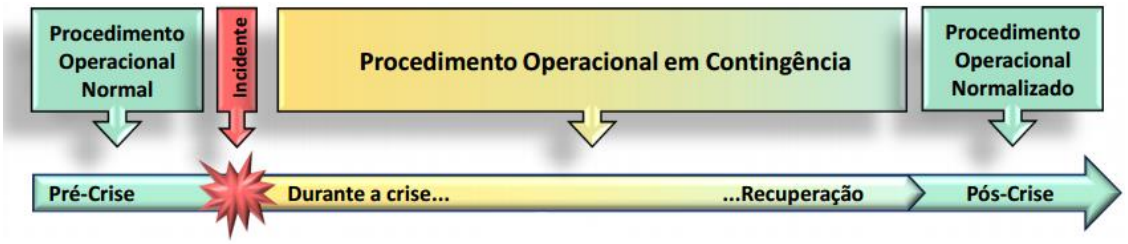
Dependendo do porte da organização e da complexidade e abrangência de seus negócios, pode ser necessário subdividir o PCN por áreas.

Figura 3 – O ambiente do PCN

Importante

- **Crise** é a situação a partir da ocorrência de um incidente que afeta de modo significativo a operação normal da organização ou de uma de suas áreas críticas.
- **Contingência** é ativação de processos e recursos em resposta ao incidente para garantir a continuidade operacional durante a ocorrência.

Figura 4 – Operação em contingência



A elaboração de um PCN e sua manutenção pode basear-se em experiências anteriores e estudos do mercado ou estudos científicos, e orienta-se pelo modelo PDCA (*Plan, Do, Check, Act*), como mostra a Figura 5.

Figura 5 – O ciclo PDCA aplicado ao PCN

Devido à complexidade e abrangência de um PCN, geralmente sua elaboração e aprimoramento são levados a termo por um grupo multidisciplinar

ou comitê, sendo inicialmente abordado como um projeto da organização. Este projeto inicia-se com a análise dos riscos e a análise do impacto nos negócios, como já vimos, e avança com a definição de estratégias de abordagem e elaboração dos planos de ação. Estes planos, bem como sua aplicação, devem então ser testados, avaliados e melhorados ou adaptados às mudanças de cenário, uma vez que os negócios, a conjuntura e o ambiente da organização estão em constante evolução, bem como as ameaças às quais a organização, seus componentes e seus negócios estão expostos.

Agora, veja o que o professor Luis tem a dizer sobre o Plano de Continuidade dos Negócios no vídeo que está disponível no material *on-line*!

Gestão de Crises

Para começarmos, o que é uma crise? Crise é uma ocorrência que impede ou dificulta que a organização atinja seus objetivos, colocando em risco sua reputação e até mesmo sua existência.

Para pensar: você consegue enumerar situações de crise atuais ou recentes? Já participou de atividades de simulação de incêndio ou treinamento de primeiros socorros? O que achou da(s) experiência(s)?

A gestão de crises é um plano ou conjunto de medidas estratégicas que, em situações de anormalidade e alto risco, visa coordenar as ações para:

1. Identificar e tratar impactos na vida e na segurança das pessoas;
2. Evitar que a situação piore;
3. Prover a comunicação adequada no nível interno e externo à organização;
4. Preservar as evidências para averiguações das causas e reavaliação dos riscos;
5. Propiciar condições para a retomada da normalidade.

Para isso é necessário planejamento, treinamento e preparação contínuos, de modo a capacitar as pessoas da organização para a ação pronta

e coordenada. E é importante o trabalho em equipe e colaborativo: em situação de crise as decisões individuais podem ser catastróficas!

A sequência de atividades conduzida pelo grupo de gestão de crise inclui, geralmente:

1. Providenciar a primeira resposta – resposta de emergência – frente à situação de desastre ou incidente;
2. Identificar, avaliar, classificar e declarar o cenário ou situação de desastre;
3. Prover as informações relacionadas ao incidente / desastre para os interessados (comunicação da crise);
4. Tomar a decisão de fazer a declaração de desastre e ativar o BCP.

No caso da segurança da informação e de sistemas, é recomendada a criação e manutenção de um *Computer Security Incident Response Team* (CSIRT) ou Time de Resposta a Incidentes de Segurança de Computadores.

Vídeo recomendado

Quer saber mais? Então assista ao vídeo indicado a seguir:

Tratamento de Incidentes de Segurança na Internet, explicado pelo NIC.br

https://youtu.be/flu6JPRHW04?list=UUscVLgae-2f9baEXhVbM1ng

Além dos procedimentos de contingência, um aspecto muito importante da gestão de crises é o processo de comunicação. É recomendável que esta seja unificada (por um porta-voz, por exemplo), baseada em uma estratégia (quem comunica, o que comunica e em quais intervalos). Geralmente nas situações de crise todos – inclusive a mídia – querem saber:

1. O que aconteceu?
2. Por que aconteceu?
3. De quem é a culpa?
4. O que está sendo feito para cessar a crise?
5. Pode haver novas ocorrências? Com serão evitadas?

Caso informações incompletas, falsas, erradas ou dissimuladas sejam fornecidas, isso pode agravar a crise. A comunicação deve ser, à medida do possível, simples, direta e honesta. Informações devem ser divulgadas constantemente para dar clareza e transparência à situação. Porém, a regra é divulgar somente informações das quais se tenha certeza absoluta, mesmo que isso prejudique a agilidade. Informações contraditórias contribuem para agravar a situação de crise. Contatos com autoridades e órgãos de segurança, defesa e proteção também são recomendados o quanto antes.

Outro aspecto importante a ser considerado na elaboração de um plano de gestão de crises é que crises não seguem um *script*, isto é, não têm padrões. Por isso as ações tomadas nos minutos iniciais críticos geralmente determinam o impacto final. E somente uma organização bem treinada para enfrentar uma crise, com estratégias e táticas pré-determinadas, pode salvaguardar seus empregados, o negócio, os ativos e a sua imagem.

Recuperação de desastres

A recuperação de desastres é o conjunto de procedimentos que, após um incidente, visa restabelecer a normalidade da operação da organização no menor espaço de tempo possível e minimizando os danos. A regra é retomar a normalidade o quanto antes e com o menor prejuízo possível.

Para que isto seja possível é necessário a elaboração de um Plano de Recuperação de Desastres, ou *Disaster Recovery Plan* (DRP), com base em um questionamento bem simples: o que fazer se...? O DRP para a área de TI e sistemas compreende o desenho das atividades do planejamento e a recuperação do ambiente e da infraestrutura de tecnologia da informação, promovido por um grupo especificamente constituído para esta tarefa na organização.

De acordo com uma metodologia bastante utilizada, conhecida por *7-step methodology*, um DRP, especialmente com o enfoque em segurança da informação e de sistemas, necessita considerar os seguintes aspectos e etapas:

1. A política de segurança da informação da organização;

2. A análise de impacto nos negócios – BIA;
3. A identificação dos controles preventivos e corretivos;
4. O desenvolvimento de estratégias de recuperação;
5. A documentação do plano de recuperação de desastres;
6. O teste e o treinamento para a operacionalização do plano;
7. A revisão e a manutenção do plano e dos recursos necessários para suportá-lo.

Figura 6 – O ciclo de vida do DRP

Os principais benefícios de um DRP bem elaborado, como é típico de medidas de segurança em geral, são:

- Prover uma melhor sensação de segurança, o que reforça a tranquilidade necessária para enfrentar situações críticas;
- Minimizar o tempo de resposta aos incidentes e desastres;
- Garantir a confiabilidade dos mecanismos e sistemas em *stand-by* ou prontidão;
- Propiciar padrões para os testes necessários para garantir a confiabilidade no plano;

- Minimizar a necessidade da tomada de decisão durante um incidente ou operação de contingência;
- Reduzir os potenciais riscos de responsabilização legal;
- Diminuir o já elevado estresse do ambiente de trabalho, especialmente durante as crises.

Leitura recomendada

Para saber mais, leia a elaboração do Plano de Recuperação de Desastres, no Material Complementar da disciplina, no UNIVIRTUS.

Trocando ideias

Acesse o fórum “DRP” no UNIVIRTUS e converse com seus colegas de turma, discorrendo sobre os seguintes pontos:

1. Quais incidentes recentes divulgados pela mídia podem ser considerados desastres?
2. Qual foi a resposta das organizações afetadas?
3. Existiram pontos falhos nessas respostas? O que poderia ser feito diferente ou melhorado?
4. Existem paralelos na história? Comparando esses incidentes, houve uma melhora na resposta e recuperação ou ocorreu o contrário?

Na prática

Para avaliar e aplicar seus conhecimentos, busque na mídia notícias recentes sobre incidentes de segurança da informação, avalie-os sob os pontos de vista dos temas estudados e discuta com seus colegas:

1. As organizações demonstraram preparo para tratar os incidentes?
2. Qual foi o impacto do incidente nos negócios?
3. Que medidas poderiam ser adotadas ou melhoradas nesses casos?

4. Discuta com seus colegas no fórum “DRP” da disciplina, no Ambiente Virtual de Aprendizagem UNIVIRTUS, e compare com os estudos dos demais colegas;
5. Em caso de dúvidas ou dificuldades, faça uso do canal de Tutoria do UNIVIRTUS.

Síntese

Nesta aula foram apresentadas as temáticas relativas à continuidade dos negócios com o foco na segurança da informação e dos sistemas. Tratamos da Gestão da Continuidade do Negócio ou *Business Continuity Management* (BCM), da Análise de Impacto nos Negócios ou *Business Impact Analisys* (BIA), do Plano de Continuidade dos Negócios ou *Business Continuity Plan* (BCP), da gestão de crises e do Plano de Recuperação de Desastres ou *Disaster Recovery Plan* (DRP).

Todas essas questões são de primordial importância para a segurança da informação e dos sistemas, pois visam, em primeiro plano, a perenização do negócio da organização e, em um segundo plano, a preservação das características básicas da segurança da informação e dos sistemas.

Referências

ABNT. **Segurança da Informação:** Coletânea eletrônica. Rio de Janeiro: ABNT, 2014.

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

GALVÃO, M. C. **Fundamentos em Segurança da Informação.** São Paulo: Pearson Education, 2015.

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.