#### Ibmec Business School

## Especialização em Segurança da Informação

**IBMEC - Petrobras**

**Disciplina: Tratamento de Incidentes de Segurança**

Professor

Frederico Sauer, D.Sc.

fred@sauersecurity.com.br

Exercício: Elaboração de um GRIS e um PRI

**Templates**

**Template para o esboço do GRIS**

**Passo 1: Obter apoio da Direção e recursos para operação**

**Passo 2: Determinar o plano estratégico do GRIS**

**Passo 3: Reunir informações relevantes**

**Passo 4: Criar a visão do GRIS**

**Passo 5: Comunicar a visão do GRIS e o plano operacional**

**Passo 6: Iniciar a implementação do GRIS**

**Passo 7: Anunciar a operacionalidade do GRIS**

**Passo 8: Avaliar a eficácia do GRIS**

1. Quem são as partes interessadas alvo das ações de motivação e financiadores ?
2. Como eles serão motivados a apoiar a criação e financiamento do GRIS ?
3. Que ações serão empreendidas para tornar transparente este apoio ?
4. Quem serão os responsáveis pelo desenvolvimento do Plano Estratégico do GRIS, e quais serão as suas funções ?
5. Quais são as informações extraídas do caso apresentado que serão usadas como base para a criação do GRIS ?
6. Qual será a comunidade apoiada ?
7. Qual será a missão do GRIS ?
8. Quais serão os objetivos do GRIS ?
9. Quais serão os serviços prestados pelo GRIS à comunidade ?
10. Qual é a função/capacitação desejada da equipe (por membro) ?
11. Quais são os recursos estimados necessários para o cumprimento da missão ?
12. Qual será a Política de Comunicação de Incidentes entre a comunidade e o GRIS ?
13. Quais serão os recursos utilizados para realizar o marketing do GRIS ?
14. Quais serão as métricas para avaliação da eficiência do GRIS ? e da eficácia ?

**Template para o esboço do PRI**

**Passo 1: PREPARAR-SE para os incidentes**

**Passo 2: Capacitar-se para DETECTAR a ocorrência de eventos e incidentes**

**Passo 3: Capacitar-se para ANALISAR uma ocorrência de incidente**

**Passo 4: Ser capaz de Implementar medidas para CONTER o incidente**

**Passo 5: Assegurar-se que se possa ERRADICAR as causas de um incidente**

**Passo 6: Certificar-se que se possa RECUPERAR as condições originais dos processos**

**Passo 7: Garantir que existam mecanismos para se APRENDER LIÇÕES com o incidente**

**Passo 8: Descrever e registrar INDICADORES que possam aferir a qualidade da RI**

**Passo 9: Buscar sempre MELHORAR a qualidade dos serviços de RI**

1. Qual será o tipo de incidente com alta probabilidade de ocorrência que vai ser o foco do PRI em discussão ?
2. Com base nisso, quais serão os controles e defesas a serem adotados ?
3. Quais recursos específicos para Resposta a um Incidente esta ameaça são necessários ?
4. Qual será a metodologia de detecção do incidente ?
5. Quais serão os parâmetros utilizados para se avaliar a severidade e a criticidade do incidente[[1]](#footnote-1) ?
6. Quais serão as medidas de contenção a usar ?
7. Qual será o *checklist* de erradicação da ameaça e das vulnerabilidades ?
8. Quais serão as ações para se certificar que os processos voltaram ao seu status quo ?
9. Quais informações devem ter sido documentadas durante a RI para uso na reunião de Lições Aprendidas ?
10. Quais serão os parâmetros indicadores usados para aferir a eficiência da RI ?
11. Quais serão os parâmetros indicadores usados para aferir a eficácia da RI ?
1. Considerando-se que C (criticidade) = E (efeito / severidade) + A (Abrangência / Importância) [↑](#footnote-ref-1)