Anexo I da Norma N02/POSIC/MinC – Análise dos Riscos de Segurança da Informação
CONTROLES E INDICADORES DO PROCESSO DE GRSIC

1.1 Todos os controles de segurança devem ser avaliados quanto à sua aplicabilidade, antes da implementação em ambiente de produção, em conformidade com as diretrizes descritas na ABNT NBR ISO/IEC 27002, ABNT NBR ISO/IEC 27001 e ABNT ISO GUIA 73.

1.1.1 O valor PSR (Indicador de Risco Absoluto) representa o grau de risco associado à ausência de um controle, calculado pela equação Risco = Probabilidade x Severidade x Relevância, onde os fatores da Probabilidade e Severidade são pontuados durante as análises técnicas e a Relevância pontuada considerando-se a visão do negócio, em termos da relevância do ativo para o MinC.

1.1.2 A Gestão de controles por indicadores é calculada pelos seguintes critérios:

a) Indicador de Conformidade – Este indicador é calculado dividindo-se a quantidade total de controles implementados pela quantidade total de controles aplicáveis. Ele é expresso em números percentuais e pode variar de 0% a 100%.
b) Indicador de Segurança – Este indicador é calculado dividindo-se o total de riscos dos controles implementados (PSR evitado) pelo total de riscos dos controles aplicáveis (PSR total). Ele também é expresso em números percentuais e pode variar de 0% a 100%.
c) PSR (Indicador de Risco Absoluto) – Este indicador é calculado através da soma dos resultados de PSR (multiplicação dos fatores P, S e R em cada controle) dos controles que não estão implementados.

1.2 A implementação das ações do MinC - quer sejam políticas, planos, treinamento, soluções customizadas ou outras necessárias – deve ser organizada por atividades em projetos, acrescida do gerenciamento e revisão periódica do nível de segurança.

1.2.1 Para o processo de trabalho, os critérios iniciais para atuação das ações podem partir de três opções distintas:

a) com base nos ativos - orientação pelos ativos de maior risco;
b) com base na visão do negócio - componentes de negócio com maior risco;
c) com base nos componentes dos ativos – componentes com maior risco;

1.3 Após a escolha do critério de atuação, os seguintes passos operacionais devem ser executados:

a) identificar os controles com Risco Alto e Muito Alto;
b) verificar os possíveis impactos da implementação dos controles na operação dos ativos, sistemas e negócio;
c) implementar imediatamente os controles com Risco Alto e Muito Alto;
d) identificar os controles com Risco Médio;
e) verificar os possíveis impactos da implementação dos controles na operação dos ativos e sistemas;
f) avaliar a necessidade de Implementar em curto prazo os controles com Risco Médio;
g) apresentar o benefício da redução dos riscos nos Componentes de Negócio onde os ativos apoiam;
h) apresentar o benefício da redução dos riscos na empresa;
i) verificar se os riscos residuais são satisfatórios;
j) refazer a análise de risco e continuar o processo cíclico.