

## SUPERIOR TRIBUNAL DE JUSTIÇA

CARGO 14: ANALISTA JUDICIÁRIO – ÁREA DE ATIVIDADE: APOIO ESPECIALIZADO –  
ESPECIALIDADE: SUPORTE EM TECNOLOGIA DA INFORMAÇÃO

PROVA DISCURSIVA

APLICAÇÃO: 27/9/2015

## PADRÃO DE RESPOSTA

O texto deve abordar os itens descritos abaixo:

**Conceito de gestão de riscos de segurança da informação (GRSI):** Um risco de segurança é um evento possível e potencialmente danoso a uma organização, isto é, um evento hipotético, que possui chance de ocorrência futura que não é nula e que apresenta impacto negativo significativo. A gestão de riscos de segurança é um processo sistemático da gestão organizacional que determina a aplicação equilibrada de controles de segurança nessa organização, diante do seu perfil de riscos de segurança. GRSI refere-se a todas as atividades seguintes que devem executadas, segundo a ISO 27005, para gerenciamento destes riscos.

**Estabelecimento do contexto:** cria ou ajusta o contexto para execução da GRSI, produzindo (i) a especificação dos critérios básicos para gestão de riscos; (ii) a especificação do escopo e limites cujos riscos serão geridos e (iii) uma organização preparada para operar a gestão de riscos.

**Avaliação de riscos:** é a atividade responsável por identificar, estimar e avaliar o risco. Envolve várias análises e avaliações, que são agrupadas sobre os processos de análise do risco e de avaliação do risco.

**Tratamento do risco:** tratamento do risco é a fase da GRSI que envolve a decisão entre reter, evitar, transferir (compartilhar) ou reduzir os riscos.

**Aceitação do risco:** aceitação do risco é a fase da GRSI que compreende o registro formal da decisão pelo aceite dos riscos residuais existentes na organização. Essa decisão é tomada pelo gestor responsável pelo escopo de risco.

**Comunicação do risco:** comunicação do risco é um conjunto de atividades continuamente executadas e que envolve a troca de informações sobre riscos entre os tomadores de decisão e todos os envolvidos na organização. O objetivo da comunicação é fazer que as informações sejam trocadas ou compartilhadas entre tomadores de decisão e outros intervenientes.

**Monitoramento e revisão de riscos:** refere-se a um conjunto de atividades continuamente executadas e que envolve o monitoramento dos diversos fatores de caracterização do risco, a fim de identificar quaisquer mudanças no contexto da organização, atualizar o panorama de riscos e aprimorar o processo de gestão desses riscos.