–

RISI Nº xxxx/2018

Descrição	*identificar resumidamente o que ocorreu - p.ex. defacement do site internet*
Período em que ocorreu o incidente	**Data/hora início:**
	Data/hora fim:
Severidade do Incidente	**( ) Alta ( ) Média ( ) Baixa**
Tipo de Impacto	**( ) Confidencialidade ( ) Integridade ( ) Disponibilidade**
Origem do alerta	*informar quem ou qual sistema alertou sobre o incidente*
Comunicação do incidente	*informar a quem ou a quais setores o incidente foi informado*

Detalhamento do Incidente

<informar a categoria do incidente. Ex.: Alteração não planejada, Ataque DDoS, Não Conformidade com a PSI, etc>

<descrever o que ocorreu, extensão e impactos do incidente, bem como detalhar as causas do incidente, áreas envolvidas na investigação do incidente, etc>

Tratamento do Incidente

<descrever ações executadas para contenção e/ou contorno do problema/incidente, equipes/pessoas envolvidas, se houve acionamento de PCOs/PRDs, etc. Atentar ao fato de que determinadas ações de contenção/contorno podem demandar sua prévia comunicação (à SAU, à SETIC, à Presidência, aos usuários internos/externos, etc) e/ou prévia autorização de instâncias superiores (SETIC, Presidência, etc)>

Análise e Encerramento do Incidente

<descrever se necessárias outras ações e recursos necessários para finalizar o tratamento do incidente e/ou para evitar que o incidente volte a ocorrer, informando, se possível, prazos e responsáveis para execução.>
<lições aprendidas>
<informar identificador do chamado/problema vinculado ao incidente, se houver>

Considerar também a necessidade de:

- *reversão da solução de controle/contorno*
- *implementação de uma correção para a causa-raiz do problema;*
- *implantação de um novo serviço/sistema;*
- *substituição do ativo/sistema afetado;*
- *revisão de procedimentos/processos/PRDs ou PCOs;*