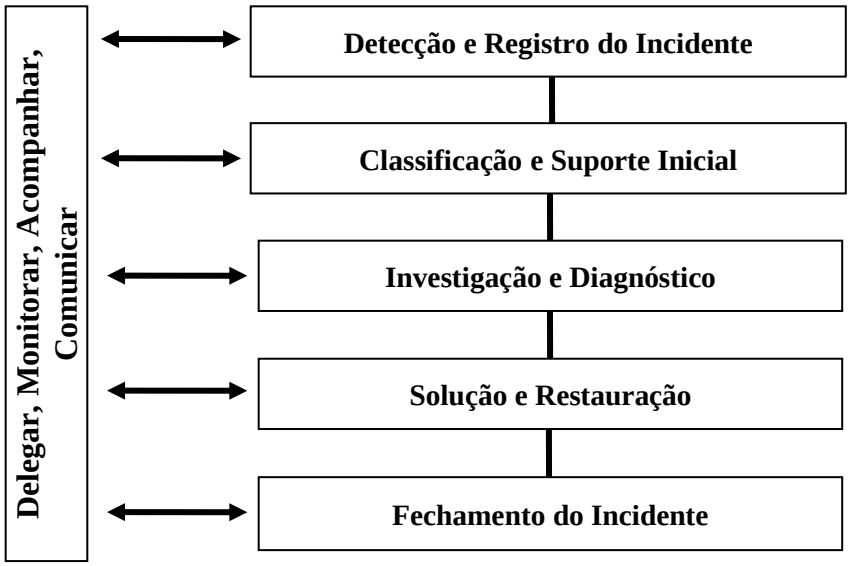
Anexo II da Norma N10/POSIC/MinC – Gestão de Incidentes de Segurança da Informação e Melhorias

PROCESSO DE GERENCIAMENTO DE INCIDENTES

1. **FLUXO**

1.1 O processo de gerenciamento de incidentes deve seguir o seguinte fluxo:



2. **PROCESSO**

2.1 **Detecção e Registro do Incidente**

2.1.1 As entradas para investigação e tratamento de incidentes devem ser realizadas por meio de chamados abertos via Central de Serviços de TI (0800 ou via web), e/ou por meio de ferramentas de monitoramento do ambiente tecnológico da organização.

2.1.2 Todos os incidentes de segurança devem ser registrados, mesmo que estes sejam resolvidos por telefone. O histórico de incidentes registrados ajuda no processo de identificação de tendências de problemas e na extração de informações gerenciais.

2.2 **Classificação e Suporte Inicial**

2.2.1 Os incidentes devem ser classificados visando permitir a identificação de erros conhecidos e a consolidação de informações gerenciais que permitam a identificação dos tipos de incidentes mais frequentes.

2.2.2 Deve ser determinado o Impacto e a Urgência de cada incidente para determinar a sua prioridade. O Impacto deve ser definido conforme a quantidade de pessoas ou de sistemas que possam ser prejudicados pelo incidente. A Urgência deve ser utilizada para determinar a velocidade em que o incidente precisa ser resolvido. Para determinar a prioridade é utilizada a combinação entre Impacto e Urgência do incidente, conforme quadro (onde Impacto = criticidade para o negócio e Urgência = velocidade):

		Impacto		
		Alto	**Médio**	**Baixo**
Urgência	**Alta**	1	2	3
	Média	2	3	4
	Baixa	3	4	5

2.2.3 A prioridade determina qual é a ordem de execução para resolver os incidentes. Os incidentes devem ser classificados de acordo com a Prioridade, que define o tempo para seu atendimento, conforme quadro:

Prioridade	**Descrição**	**Tempo para Atendimento**
1	Crítica	1 hora
2	Alta	4 horas
3	Média	24 horas
4	Baixa	48 horas
5	Planejada	-

2.3 **Investigação e Diagnóstico**

2.3.1 Uma vez registrado o incidente é iniciada a investigação por meio de um conjunto de habilidades e de ferramentas disponíveis e por meio da base de conhecimento de Erros Conhecidos.

2.3.2 Todas as partes que trabalham com os Incidentes devem manter o registro de suas ações, atualizando o registro do incidente.

2.4 **Resolução e Restauração**

2.4.1 Uma vez que uma solução de contorno ou definitiva para o incidente for encontrada, esta será implementada. Se uma mudança for necessária, uma Requisição de Mudança é submetida à área competente.

2.5 **Fechamento do Incidente**

2.5.1 A etapa de fechamento do incidente inclui:

a) atualização dos detalhes do incidente; e
b) comunicação ao usuário sobre a solução.

2.5.2 Durante o ciclo de vida do incidente, a Central de Serviços de TI permanece proprietária do incidente sendo responsável pelo seu fechamento, a fim de permitir ao usuário pronta resposta sobre a situação de seus chamados.