# Respondendo a incidentes declarados

Nesta página

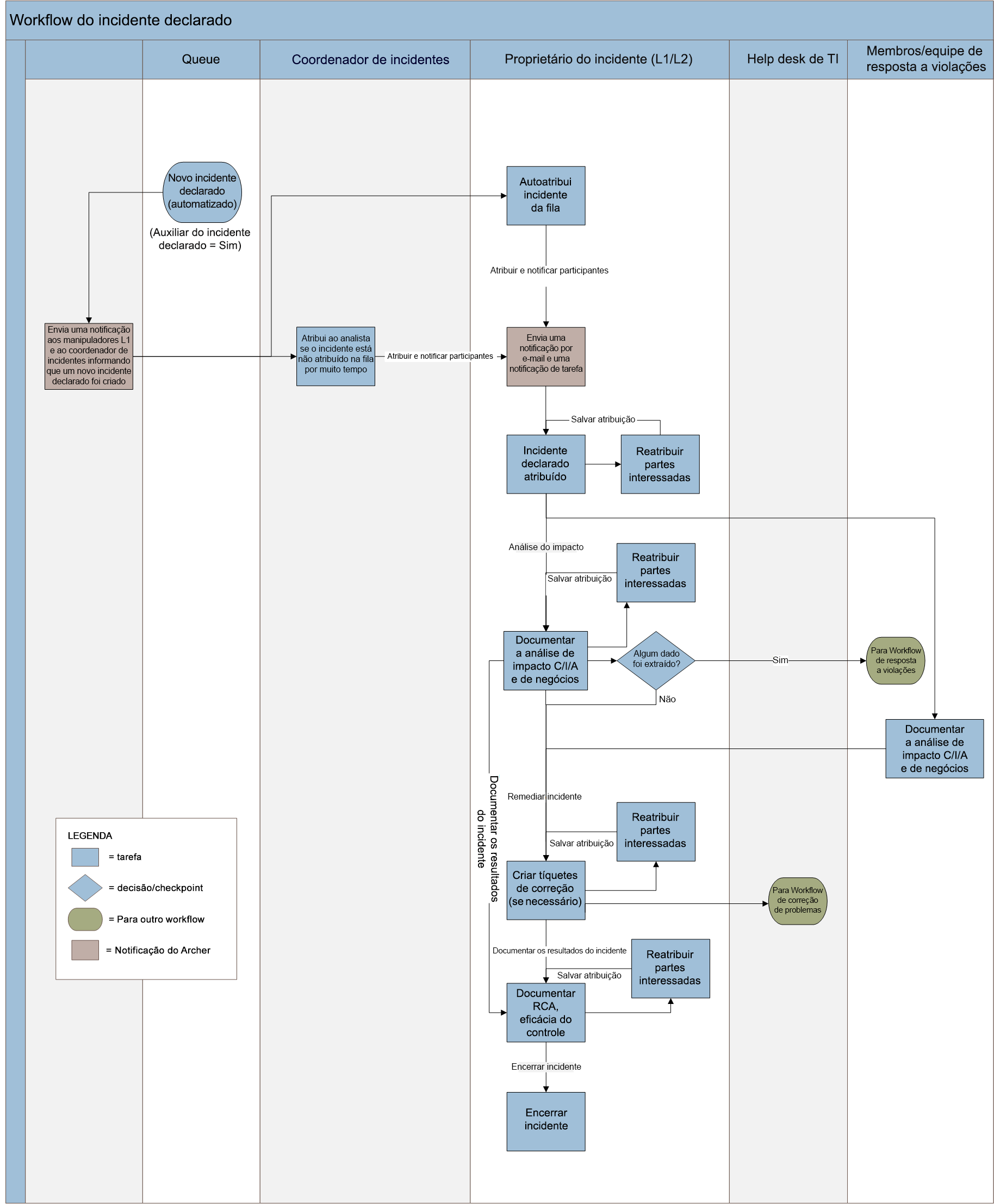
* [Workflow do incidente declarado](#Workflowdoincidentedeclarado)
* [Tarefas para responder a incidentes declarados](#X45b429cacbdc92dcafb5537e4d97ae5c59d0fde)

## Workflow do incidente declarado

O workflow avançado de Incidente declarado oferece a você um processo simplificado para a resolução de incidentes declarados. Usando o workflow de Incidente declarado, você pode envolver diretamente os acionistas dos negócios como parte da análise de impacto e do processo de resposta a violações, além de reduzir o tempo necessário para resolver incidentes declarados críticos.

O caso de uso Cyber Incident & Breach Response foi desenvolvido para dar suporte ao seguinte workflow de Incidente declarado:

Faça download do arquivo de origem do diagrama aqui: [Diagrama de workflow do Incidente declarado de Cyber Incident & Breach Response](../../Resources/Images/Solutions/ITSecRisk/itsrm_cibr_declared_incident_wf.vsd)



Para utilizar o processo de workflow avançado de Incidente declarado, você deverá enviar dados ao Archer usando APIs. Para obter informações sobre os campos obrigatórios, consulte [Habilitando o workflow avançado de Incidente declarado](itsrm_cibr_dec_incd_aw_enabling.htm).

## Tarefas para responder a incidentes declarados

Aqui estão as tarefas para responder a incidentes declarados:

1. Atribua as partes interessadas relevantes, como o proprietário do incidente, o coordenador do incidente e membros adicionais da equipe e vincule às informações relevantes do dispositivo.
2. Comece a análise do incidente. Analise os detalhes do incidente declarado, como nome, prioridade, categoria de ameaça, número de alertas e detalhes do dispositivo. O proprietário do incidente pode, opcionalmente, substituir a prioridade do incidente declarado e gerar automaticamente os procedimentos de resposta ao incidente e as tarefas de resposta ao incidente com base na categoria de ameaça do incidente declarado.
3. Documente a análise de impacto. Envolva a empresa para realizar uma avaliação de impacto e uma análise de impacto de confidencialidade, integridade e disponibilidade sobre o incidente declarado relatado. Além disso, relate quaisquer resultados ao administrador do sistema de TI para fins de remediação e relate uma violação de dados quando a perda de dados é identificada.
4. Para cada problema que precisa de remediação, crie um registro de resultados na guia Remediação do registro de incidente de segurança. Descreva a ação a ser concluída, a relevância para o resultado, uma fila de destino e um tipo de tarefa de remediação.
5. Documenta a análise do incidente. Forneça os resultados do incidente, os atores e as técnicas que contribuíram para o incidente, os detalhes de destino do incidente e adicione os controles de segurança associados à descoberta do incidente.