# Documentando as políticas do SOC

As políticas do SOC definem os processos, termos e padrões que a equipe do SOC precisa seguir. Por exemplo, o SOC poderá ser necessário para responder a um incidente dentro de um determinado período dependendo do nível de prioridade do incidente. O Archer Cyber Incident & Breach Response permite documentar todas as políticas do SOC e gerenciar o processo de análise e aprovação com todos os participantes necessários.

O estabelecimento antecipado de políticas do SOC a respeito da lista de assuntos a seguir também ajudará você a gerenciar os processos subsequentes do SOC para tratar incidentes e responder a violações no caso de uso do Archer Cyber Incident & Breach Response.

Nesta página

* [Políticas sugeridas](#Pol%C3%ADticassugeridas)
* [Processo de análise da política do SOC](#X9b70267088ac662d6e3f4980f9cc44523fff007)

## Políticas sugeridas

A tabela a seguir descreve as políticas sugeridas.

| Política | O que ela deve definir |
| --- | --- |
| Classificação de prioridade do incidente | O que cada nível de prioridade significa para sua organização? Como eles devem ser atribuídos aos incidentes? |
| Requisitos de SLA de tratamento de incidentes | Com que rapidez é preciso verificar, investigar e resolver os incidentes? Como isso varia com base na prioridade do incidente? |
| Incidentes declarados | O que um incidente declarado significa para a sua organização? Quando um incidente deve ser declarado? |
| Incidentes confidencias | Quais incidentes devem ser marcados como confidenciais? Quem deve ter acesso aos incidentes confidencias? |
| Requisitos de SLA de remediação de operações de TI | Com que rapidez é preciso resolver um tíquete? Como isso varia com base na relevância? |
| Tratamento de violação | Quem deve ser responsável por gerenciar todo o processo de resposta a violação? |

## Processo de análise da política do SOC

Para cada política de segurança que você deseja documentar no Archer Cyber Incident & Breach Response, crie um novo registro nas Políticas do SOC. Forneça o nome, a descrição, o proprietário e as partes interessadas de uma política.

Quando você cria e salva um novo registro de política do SOC, cada participante designado recebe notificações informando que uma nova política requer sua análise. Cada participante precisa analisar a política e então aprová-la ou rejeitá-la.

Quando todos os participantes tiverem analisado e aprovado a política, o status passará a ser Aprovado. Se nem todos os participantes tiverem analisado a política ou alguns a rejeitaram, o status permanecerá como Em análise.

A figura a seguir mostra o processo de criação e análise de uma política do SOC.

Faça download do arquivo de origem do diagrama aqui: [Diagrama de políticas do SOC de Cyber Incident & Breach Response](../../Resources/Images/Solutions/ITSecRisk/itsrm_cibr_soc_policy_review.vsd)

