# Usando o Cyber Incident & Breach Response

O Archer Cyber Incident & Breach Response oferece suporte aos processos a seguir.

Nesta página

* [Gerenciando a equipe e os contatos do SOC](#GerenciandoaequipeeoscontatosdoSOC)
* [Documentando as políticas do SOC](#Documentandoaspol%C3%ADticasdoSOC)
* [Documentando procedimentos de resposta a incidentes](#X6d42085f4d41c44e30fa3ddbdd3c552c757721a)
* [Configurando fluxogramas](#Configurandofluxogramas)
* [Usando controles de segurança](#Usandocontrolesdeseguran%C3%A7a)
* [Respondendo a incidentes e incidentes declarados](#Xff6394ae7ed79b5b1a368962b6f2b692bd790a3)
* [Documentando procedimentos de resposta a violações](#X31c73fa7c84c707f3965dbb3a5abc83dbfecb6c)
* [Respondendo a violações de dados](#Respondendoaviola%C3%A7%C3%B5esdedados)

## Gerenciando a equipe e os contatos do SOC

A Cyber Incident & Breach Response do Archer utiliza o aplicativo Contatos para criar um catálogo dos membros da equipe do SOC e suas diferentes habilidades, treinamentos e recursos. Isso ajuda o gerente do SOC a atribuir os vários incidentes aos membros da equipe do SOC com base em seus pontos fortes e sua experiência. Além disso, o gerente do SOC pode usar o aplicativo Equipes para criar as equipes de resposta a violação e atribuir membros da equipe a elas.

## Documentando as políticas do SOC

As políticas do SOC definem os processos, termos e padrões que a equipe do SOC precisa seguir. O aplicativo Políticas do SOC auxilia o gerente do SOC ou o coordenador de incidentes na escolha de uma política certa para a equipe do SOC e o que cada política deve definir como parte de sua implementação.

## Documentando procedimentos de resposta a incidentes

O aplicativo Biblioteca de procedimentos de resposta a incidentes abriga um catálogo de informações que os manipuladores de incidentes podem usar quando responderem a um incidente. Este catálogo inclui as seguintes informações: tarefas recomendadas, diretrizes e checklists.

Quando um manipulador de incidentes categoriza um incidente, todos os procedimentos de resposta que correspondem a essa categoria são automaticamente copiados da biblioteca de procedimentos de resposta a incidentes para o aplicativo Procedimentos de resposta a incidentes e vinculados ao registro de incidente.

## Configurando fluxogramas

A Cyber Incident & Breach Response inclui o aplicativo Notificações e árvores de chamadas. Um fluxograma é uma lista de pessoas, funções e/ou organizações que você pode precisar notificar em uma sequência específica no caso de uma violação.

## Usando controles de segurança

Controles de segurança são todas as ferramentas ou tecnologias que o seu SOC usa para detectar, impedir e investigar incidentes de segurança. Controles de segurança podem ser tecnologia (como ferramentas, plataformas e sistemas), bem como controles manuais (como um processo de análise de registro manual). A Cyber Incident & Breach Response permite documentar todos os controles de segurança, inclusive cada proprietário de controle, status de implementação, categoria do controle e custos operacionais anuais e fixos.

## Respondendo a incidentes e incidentes declarados

O caso de uso Cyber Incident & Breach Response inclui um workflow avançado que oferece aos usuários um fluxo de processo detalhado para o gerenciamento de incidentes de segurança e um processo simplificado para o gerenciamento de incidentes declarados.

O Archer Cyber Incident & Breach Response também fornece aos usuários percepções adicionais sobre quanto tempo é gasto em determinada fase do processo do incidente.

## Documentando procedimentos de resposta a violações

Os procedimentos de resposta definem as tarefas que os manipuladores de incidentes devem concluir ou as diretrizes ou checklists que devem seguir ao responder a uma violação. Definindo procedimentos de resposta, você consegue fornecer manipuladores de incidentes com orientação e processos consistentes para analisar incidentes e tratar violações. O aplicativo Biblioteca de procedimentos de resposta a violação contém todos os seus procedimentos de resposta padrão.

## Respondendo a violações de dados

Responder a violações de dados é crucial para o sucesso de qualquer empresa. A Cyber Incident & Breach Response do Archer inclui um workflow em várias etapas projetado para ajudar todos os membros da equipe do SOC a responder rapidamente a uma violação de segurança para garantir que a empresa tenha total conhecimento sobre o que ocorreu e quais dados podem ter sido transferidos de maneira não autorizada.