# Caso de uso Cyber Incident & Breach Response

Este tópico explica o design de caso de uso Cyber Incident & Breach Response.

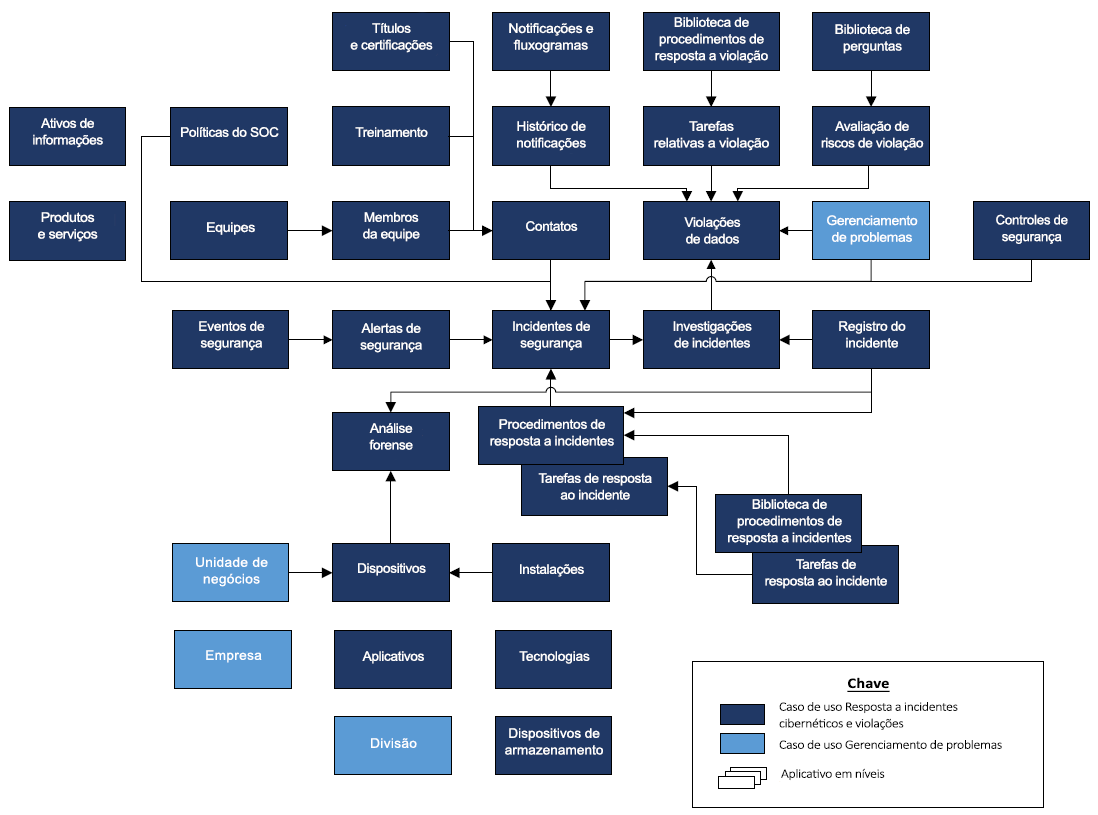
Nesta página

* [Diagrama da arquitetura](#Diagramadaarquitetura)
* [Aplicativos](#Aplicativos)
* [Personas e funções de acesso](#Personasefun%C3%A7%C3%B5esdeacesso)
* [Painéis de controle](#Pain%C3%A9isdecontrole)
* [Feeds de dados](#Feedsdedados)
* [Dicionário de dados](#Dicion%C3%A1riodedados)

## Diagrama da arquitetura

O diagrama a seguir mostra os relacionamentos entre os aplicativos no caso de uso Resposta a incidentes cibernéticos e violações.

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



## Aplicativos

A tabela a seguir descreve os aplicativos de casos de uso.

| Aplicativo | Descrição |
| --- | --- |
| Incidentes de segurança | O aplicativo Incidentes de segurança oferece um local central para gerenciamento de incidentes, tanto os criados a partir de alertas de segurança agregadas e aqueles que são relatados manualmente. Com o aplicativo Incidentes de segurança, é possível:   * Capturar informações sobre o incidente, inclusive os fatores que contribuíram para ele, os ativos e as informações visadas, além da eficácia dos controles de segurança. * Gerenciar o workflow completo de tratamento de incidentes, desde atribuir um manipulador de incidentes L1 para analisar e avaliar o incidente até escalonar um incidente a um manipulador de incidentes L2 para mais investigação e análise e criar e atribuir tarefas de resposta e de remediação. * Capturar a análise de impacto e forense. |
| Alertas de segurança | O aplicativo Alertas de segurança armazena os alertas individuais relatados por uma ferramenta SIEM que compõem um incidente. Com o aplicativo Alertas de segurança, você pode visualizar os detalhes sobre o alerta de segurança, como os endereços IP de origem e destino e o nível de severidade, abrir o Bing Maps para exibir a cidade ou o país de origem e a cidade ou o país de destino no alerta de segurança e iniciar o NetWitness para exibir o alerta de segurança em contexto. |
| Eventos de segurança | O aplicativo Eventos de segurança armazena os eventos individuais que compõem um alerta. Com ele, você pode visualizar os detalhes do evento de segurança, como os endereços IP de origem e de destino e os endereços MAC de origem e de destino. |
| Investigações de incidentes | O aplicativo Investigações de incidentes permite associar vários incidentes relacionados para agilizar a manipulação e a resolução. Você pode documentar a análise de impacto, as tarefas de resposta e remediação necessárias, e os resultados da investigação, assim como em um incidente.  É possível também criar um registro de investigação para examinar uma atividade suspeita, a inteligência contra ameaças ou outras informações relatadas fora de Resposta a incidentes de segurança e violações. |
| Análise jurídica | O aplicativo Análise forense permite que um manipulador de incidente capture os detalhes sobre qualquer host relevante ou análise forense de rede realizada no decorrer da investigação de um incidente. |
| Registro do incidente | O aplicativo Registro do incidente permite que um manipulador de incidentes registre anotações sobre cada ação que tomar enquanto estiver trabalhando em um incidente, investigação ou violação. |
| Procedimentos de resposta a incidentes | Procedimentos de resposta a incidentes é um aplicativo em níveis que permite documentar, gerenciar e rastrear todas as tarefas específicas que devem ser concluídas em um incidente ou investigação. O primeiro nível, Procedimentos de resposta a incidentes, descreve o procedimento geral, incluindo as categorias de ameaças e respostas às quais ele se aplica. O segundo nível, Tarefas de resposta a incidentes, descreve as tarefas individuais que um manipulador de incidentes deve concluir. |
| Biblioteca de procedimentos de resposta a incidentes | A Biblioteca de procedimentos de resposta a incidentes é um aplicativo em níveis e oferece um repositório de modelos de tarefas de resposta que devem ser concluídas para um incidente. O primeiro nível, Procedimentos de resposta a incidentes, permite documentar o procedimento geral, inclusive as categorias de ameaça e resposta às quais ele se aplica. O segundo nível, Tarefas de resposta a incidentes, permite documentar as tarefas individuais que devem ser concluídas pelo manipulador do incidente. |
| Tarefas relativas a violação | O aplicativo Tarefas relativas a violação permite documentar, gerenciar e rastrear todas as tarefas específicas que devem ser concluídas caso ocorra uma violação. Algumas tarefas podem ser criadas manualmente por outra pessoa atribuída para trabalhar na violação, como um diretor de conformidade ou manipulador de incidentes, enquanto outras podem ser criadas automaticamente com base nos modelos armazenados no aplicativo Biblioteca de procedimentos de resposta a violação. |
| Violações de dados | O aplicativo Violações de dados permite gerenciar o processo de manipulação de uma violação relacionada a dados de privacidade, dados de cartão de crédito, propriedade intelectual e segredos comerciais. No aplicativo Violações de dados, é possível:   * Capturar informações sobre os ativos e os dados envolvidos em uma violação. * Visualizar a investigação ou os incidentes que resultaram na descoberta da violação. * Rastrear as atividades necessárias de equipes interfuncionais e instruir os membros da equipe multifuncional a fornecer avaliações de impacto da violação. |
| Títulos e certificações | O aplicativo Títulos e certificações permite capturar informações sobre treinamento, certificações e graduações dos membros da equipe. Você poderá rastrear problemas e datas de expiração, se o treinamento profissional contínuo (CPE, Continuing Professional Education) for necessário, e outras informações. |
| Histórico de notificações | O aplicativo Histórico de notificações permite documentar a execução manual de fluxogramas. Ele captura o número de pessoas contatadas e atingidas, bem como a duração da atividade. |
| Notificação e fluxogramas | O aplicativo Notificações e árvores de chamadas permite gerenciar notificações usando um fluxograma (uma rede de pessoas organizadas de modo que possam disseminar informações com rapidez e facilidade entre si).  Com o aplicativo Notificações e árvores de chamadas, é possível:   * Documentar notificações (mensagens específicas). * Documentar iniciadores e destinatários de árvore de chamadas. * Criar mensagens personalizadas para enviar aos destinatários. |
| Avaliação de riscos de violação | O questionário de avaliação de riscos de violação permite calcular para sua organização os riscos causados por uma violação, tendo como base o tipo de dados divulgados, o risco de danos a pessoas e se a divulgação foi acidental ou intencional. |
| Biblioteca de procedimentos de resposta a violação | O aplicativo Procedimento de resposta a violação oferece um repositório para modelos de tarefas de resposta que devem ser concluídas caso ocorra uma violação. |
| Biblioteca de perguntas | A Biblioteca de perguntas é um aplicativo que armazena perguntas de avaliação que você pode consultar e copiar em um questionário. Cada pergunta é armazenada em um registro individual, e cada registro contém informações inclusive o texto de pergunta e resposta, bem como informações necessárias para exibir e pontuar sua pergunta. Dependendo da solução que você licenciou, a Biblioteca de perguntas contém um grande conjunto de perguntas previamente criadas por padrão. Além disso, você pode adicionar novas perguntas e armazená-las na Biblioteca de perguntas. |
| Controles de segurança | O aplicativo Controles de segurança permite documentar informações sobre os controles de segurança da organização, incluindo nomes e descrições, a ferramenta de segurança que fornece o controle, os custos associados ao controle e o proprietário do controle. |
| Políticas do SOC | O aplicativo Políticas de SOC permite documentar as políticas de segurança da organização, incluindo nomes e descrições, proprietários de política e as partes interessadas. |
| Equipes | O aplicativo Equipes permite que você capture informações sobre suas equipes de manipuladores de incidentes, como nome da equipe, gerente e uma descrição das responsabilidades da equipe. |
| Membros da equipe | O aplicativo Membros da equipe permite capturar informações sobre cada membro da equipe, como seus nomes e funções. |
| Treinamento | O aplicativo Treinamento permite capturar o histórico do treinamento dos membros da equipe e os créditos do CPE (Continuing Professional Education, treinamento profissional contínuo) obtidos para renovação das certificações profissionais. |
| Aplicativos | O aplicativo Aplicativos armazena todos os aplicativos de software usados pela organização para executar operações de negócios. Você pode visualizar como um aplicativo é utilizado, as pessoas que o utilizam e os dispositivos no qual o aplicativo está instalado. Você também pode rastrear o impacto nos negócios, o impacto no cliente e os detalhes do licenciamento e associar isso a outros aspectos da infraestrutura corporativa.  **Observação:** O aplicativo Aplicativos está incluído no pacote Catálogo corporativo. |
| Dispositivos | O aplicativo Dispositivos serve como repositório central de conhecimentos, como relevância, dispositivos de TI e a quais aplicativos eles dão suporte. É possível gerenciar dispositivos para garantir que eles sejam protegidos de acordo com as expectativas do gerenciamento. O aplicativo também está associado a outros aspectos da infraestrutura corporativa.  **Observação:** o aplicativo Dispositovos está incluído no pacote Catálogo corporativo. |
| Dispositivos de armazenamento | O aplicativo Dispositivos de armazenamento serve como um repositório central dos dispositivos de armazenamento usados na infraestrutura.  **Observação:** o aplicativo Dispositivos de armazenamento está incluído no pacote Catálogo corporativo. |
| Tecnologias | O aplicativo Tecnologias oferece um repositório pesquisável e ampliável de informações sobre versões de tecnologia que podem ser aproveitadas para relacionar dispositivos com tecnologia semelhante. Os dispositivos podem ser identificados e agrupados usando 1 das listas detalhadas de valores hierárquicos de 3 níveis:   * Tecnologia do sistema operacional. Essa lista detalha informações como o fornecedor do sistema operacional, produto e versão do sistema operacional. * Tecnologia de aplicativo. Essa lista contém informações como o fornecedor do aplicativo, nome e versão. * Tecnologia de hardware. Essa lista descreve informações relacionadas ao fornecedor do hardware, inclusive nome, descrição e convenções de nomenclatura da versão da tecnologia.   Os usuários podem filtrar tecnologias que foram aprovadas pela empresa e exibir relatórios detalhando as vulnerabilidades conhecidas que ameaçam suas tecnologias.  **Observação:** o aplicativo Tecnologias está incluído no pacote Catálogo corporativo. |
| Unidade de negócios | O aplicativo Unidade de negócios apresenta uma visão detalhada de todas as atividades relacionadas a uma unidade de negócios específica.  **Observação:** o aplicativo Unidade de negócios está incluído no pacote Catálogo corporativo. |
| Empresa | O aplicativo Empresa armazena informações gerais, financeiras e de conformidade de uma empresa. Combinado com os aplicativos Divisão e Unidade de negócios, esse aplicativo oferece suporte à geração de relatórios cumulativos sobre iniciativas de governança, riscos e conformidade em toda a empresa.  **Observação:** o aplicativo Empresa está incluído no pacote Catálogo corporativo. |
| Contatos | O aplicativo Contatos serve como um repositório central para informações de contato, é utilizado em várias áreas do Archer e contém informações que são frequentemente utilizadas por outros casos de uso. As atualizações realizadas em um registro de perfil nesse aplicativo se propagam automaticamente para todos os registros com informações de contato exibidas.  **Observação:** o aplicativo Contatos está incluído no pacote Catálogo corporativo. |
| Divisão | O aplicativo Divisão representa a unidade intermediária na hierarquia de negócios que está um nível abaixo da empresa e um nível acima da unidade de negócios individual. Use esse aplicativo para documentar melhor os relacionamentos em seus negócios e avaliar a eficiência e a conformidade das divisões individuais da empresa.  **Observação:** o aplicativo Divisão está incluído no pacote Catálogo corporativo. |
| Instalações | O aplicativo Instalações mantém uma lista de todas as instalações da organização, como data centers e filiais. Você pode documentar e analisar todas as informações associadas a uma instalação, como pessoal de contato, informações sobre o local e tecnologias associadas ao local.  **Observação:** o aplicativo de Instalações está incluído no pacote Catálogo corporativo. |
| Produtos e serviços | O aplicativo Produtos e serviços mantém todos os produtos e serviços oferecidos em uma organização. Por exemplo, uma empresa de serviços financeiros oferece uma variedade de produtos e serviços, como serviços bancários, de corretagem e de empréstimo.  **Observação:** o aplicativo Produtos e serviços está incluído no pacote Catálogo corporativo. |
| Ativos de informações | O aplicativo Ativos de informações permite gerenciar um repositório de ativos de informações, como dados de cartão de crédito, previsões financeiras, números de seguro social de funcionários e marcas comerciais. Use esse aplicativo para fazer avaliações on-line e assim determinar classificações de informações e períodos de retenção necessários. Vincule ativos de informações aos processos de negócios relacionados, aos aplicativos em que são gerenciados e às instalações onde estão armazenados.  **Observação:** o aplicativo de Ativos de informações está incluído no pacote Catálogo corporativo. |

## Personas e funções de acesso

A tabela a seguir descreve as funções gerais que compõem a organização do SOC de uma empresa. Dependendo da organização de sua empresa, essas funções e responsabilidades podem variar.

| Função de acesso | Descrição |
| --- | --- |
| Analista L1 de resposta a incidentes | Manipuladores de incidentes N1 são responsáveis por analisar e responder aos incidentes em sua fila e é seu trabalho reunir informações sobre os ativos, dados e usuários envolvidos no incidente e determinar se eles podem fornecer uma solução ou se é preciso escalar o incidente para um manipulador de incidentes N2. Os manipuladores de incidentes N1 também podem relatar violações que eles descobrem no decorrer da investigação de um incidente e documentar os resultados e as tarefas que é preciso tratar para resolver o incidente. |
| Analista L2 de resposta a incidentes | Manipuladores de incidentes N2 têm habilidades avançadas em perícia forense de rede/host e engenharia reversa de malware, e são responsáveis por tratar incidentes mais complexos que são escalados de manipuladores de incidentes N1. Os manipuladores de incidentes N2 também conduzem investigações em vários incidentes relacionados, podem relatar violações que descobrem no decorrer da investigação de um incidente e documentam os resultados e as tarefas que precisam ser tratados para resolver o incidente. |
| Coordenador de incidentes | Os coordenadores de incidentes gerenciam uma equipe de manipuladores de incidentes N1 e N2 e é seu trabalho garantir o cumprimento de SLAs (acordos de nível de serviço) de resposta a incidentes. Os coordenadores de incidentes monitoram filas de incidentes e relatórios de medição de SLA e atribuem incidentes a manipuladores de incidentes conforme apropriado, com base em suas habilidades e disponibilidade. |
| Gerente do SOC | Os gerentes do SOC são responsáveis pelo centro de resposta a incidentes críticos e é seu trabalho garantir que o SOC esteja pronto para evitar e responder a incidentes. Os gerentes do SOC também precisam fornecer à gerência relatórios semanais sobre o estado atual do SOC. |
| CISO/CSO | O CISO/CSO recebe relatórios semanais de resumo de incidentes e precisa receber notificação de incidentes de alta importância. |
| Administrador de solução | O administrador de solução é responsável por instalar, configurar e manter o caso de uso Cyber Incident & Breach Response. |
| Jurídico | A consultoria jurídica participa das investigações dos incidentes e é responsável por fornecer uma análise de impacto jurídica de todas as violações relatadas. A consultoria jurídica determina quais tarefas jurídicas é preciso concluir quando ocorre uma violação. |
| RH | O analista de RH participa de investigações de incidentes que também exigem uma investigação de políticas de RH, assédio ou ética e é responsável por fornecer todos os comentários de recursos humanos sobre todas as violações relatadas, além de determinar quais tarefas de RH devem ser concluídas quando ocorre uma violação. |
| Gerente de negócios | O gerente de negócios é envolvido nas investigações de incidentes. O gerente de negócios é responsável por uma linha de negócios e pode incluir o gerente geral, o chefe da unidade de negócios ou um representante. Os gerentes de negócios também são responsáveis por executar uma avaliação de impacto nos negócios para a respectiva linha de negócios quando ocorre uma violação. |
| Responsável pela conformidade | O diretor de conformidade ou privacidade participa das investigações de incidentes que exigem uma investigação de conformidade regulamentar ou corporativa e é responsável por fornecer uma análise de impacto sobre a conformidade regulamentar em todas as violações relatadas. O diretor de conformidade ou privacidade determina quais tarefas de conformidade é preciso concluir quando ocorre uma violação. Eles podem assumir a função de liderança no gerenciamento de violações quando elas ocorrem. |
| Help desk de TI | O analista de help desk de TI é responsável por tratar os tíquetes de remediação atribuídos pelo manipulador de incidentes N1 ou N2 durante o curso de uma resposta a incidente ou violação. |

Para obter uma lista completa de funções de acesso e privilégios de acesso detalhados em nível de página, consulte o *Dicionário de dados*.

Para obter a lista completa dos campos de permissão de registro do aplicativo, inclusive quais campos de usuários/grupos preenchem os campos e de onde os campos herdam as permissões, consulte o *Dicionário de dados*.

## Painéis de controle

A tabela a seguir descreve os painéis de controle do caso de uso.

| Painel de controle | Descrição |
| --- | --- |
| Manipulador de incidentes N1 | O painel de controle Manipulador de incidentes N1 exibe informações sobre incidentes de segurança. Os manipuladores de incidentes N1 podem ver os itens atualmente atribuídos a eles, itens em fila nos quais podem começar a trabalhar, tarefas abertas e outras métricas.  Somente os usuários designados para a função de manipulador de incidentes N1 podem visualizar o painel de controle Manipulador de incidentes N1. |
| Manipulador de incidentes N2 | Esse painel de controle exibe informações sobre incidentes de segurança e investigações de incidentes. Os manipuladores de incidentes N2 podem ver os itens atualmente atribuídos a eles, itens em fila nos quais podem começar a trabalhar, tarefas abertas e outras métricas.  Somente os usuários designados para a função de manipulador de incidentes N2 podem visualizar o painel de controle Manipulador de incidentes N2. |
| Coordenador de incidentes | O painel de controle Coordenador de incidentes apresenta informações resumidas sobre todos os incidentes e investigações abertos, mostra a carga de trabalho atual de cada manipulador de incidentes, mostra todos os incidentes não atribuídos que o coordenador de incidentes precisa atribuir e exibe relatórios de medição de SLA recentes para o coordenador de incidentes analisar no início de um turno.  Somente os usuários designados para a função de coordenador de incidentes podem visualizar o painel de controle Coordenador de incidentes. |
| Resposta a violações | O painel de controle Resposta a violações fornece uma visualização de alto nível de todo o seu programa de resposta a violações. Você pode exibir todas as violações de dados ativas, qualquer tarefa aberta que é preciso concluir como parte de uma resposta a violação, quais normas foram mais afetadas por violações de dados e qual tipo de dados foi divulgado.  Somente os usuários designados às funções de diretor de conformidade/privacidade, gerente do SOC ou CISO/CSO podem exibir o painel de controle Resposta a violações. |
| Help desk de TI | O painel de controle Help desk de TI fornece uma exibição resumida de todos os tíquetes (resultados) que é preciso remediar em relação a um incidente ou uma violação. Você pode exibir todos os tíquetes abertos, todos os tíquetes que correspondem a uma ação ou um tipo específico de remediação e os tíquetes abertos mais críticos.  Somente os usuários atribuídos à função Help desk de TI podem exibir o painel de controle Help desk de TI. |
| Gerente do SOC | O painel de controle Gerente do SOC fornece informações resumidas sobre todas as violações de dados e incidentes ativos, exibe mapas de alertas de segurança recentes provenientes de recursos e destinos externos, mostra métricas sobre as categorias de ameaça e impactos dos incidentes sobre os negócios e exibe os controles de segurança mais eficazes no SOC.  Somente os usuários designados à função de gerente do SOC podem exibir o painel de controle Gerente do SOC. |

## Feeds de dados

A tabela a seguir descreve os feeds de dados dos casos de uso.

| Feed de dados | Descrição |
| --- | --- |
| CI&BR\_-\_Generate\_Incident\_Response\_Procedures\_and\_Tasks | O feed de dados Generate Incident Response Procedures and Tasks cria tarefas automaticamente, com base nos modelos de resposta associados a um registro. Por exemplo, quando um manipulador de incidentes seleciona uma categoria para um incidente, o feed de dados Generate Incident Response Procedures and Tasks copia todos os procedimentos de resposta a incidente que correspondem a essa categoria e os associa ao incidente. |
| CI&BR\_-\_Not\_Applicable\_Incident\_Response\_Procedures\_and\_Tasks | Se uma tarefa se torna desnecessária devido a uma alteração na norma afetada relacionada, o feed de dados Not Applicable faz uma cópia dessa tarefa e a relaciona na seção Não se aplica do registro da tarefa de resposta a incidente. |
| CI&BR\_-\_Generate\_Breach\_Tasks | O feed de dados Breach Response Tasks cria tarefas automaticamente, com base nos modelos de resposta associados a um registro. Por exemplo, quando o líder de resposta a violação seleciona as normas afetadas por uma violação, o feed de dados Generate Breach Tasks copia todos os procedimentos de resposta que correspondem às normas selecionadas e os associa ao registro de violação. |
| CI&BR\_-\_Not\_Applicable\_Breach\_Tasks | Se uma tarefa se torna desnecessária devido a uma alteração na norma afetada relacionada, o feed de dados Not Applicable fará uma cópia dessa tarefa e a listará na seção Não se aplica do registro da tarefa de resposta a violação. |

## Dicionário de dados

O *Dicionário de dados* de Cyber Incident & Breach Response contém a informação sobre configuração do caso de uso.

Você pode obter o *Dicionário de dados* do caso de uso entrando em contato com o representante de contas do Archer.