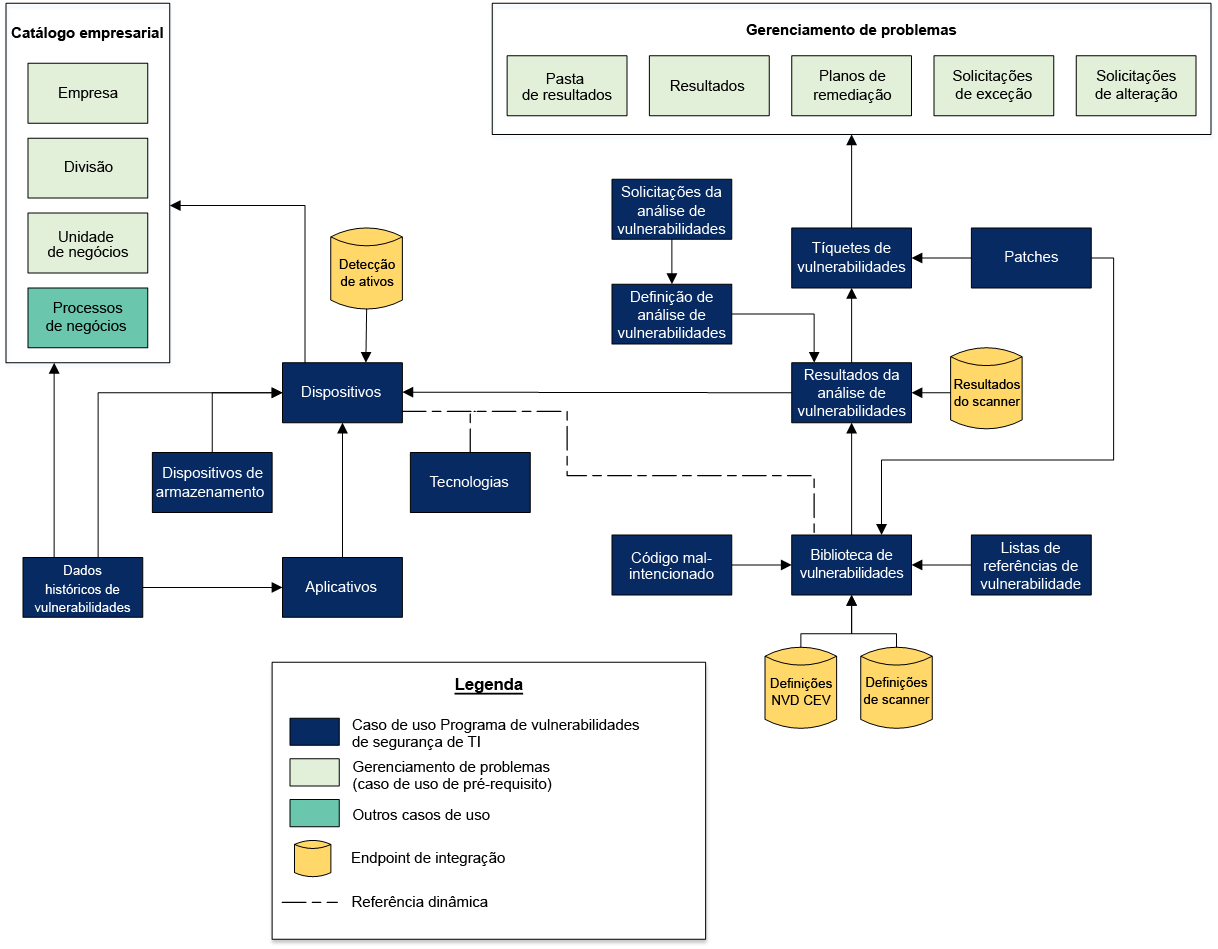
# Design de caso de uso Programa de vulnerabilidades de segurança de TI

Este tópico explica o design de caso de uso do Programa de vulnerabilidades de segurança de TI.

Nesta página

* [Diagrama da arquitetura](#Diagramadaarquitetura)
* [Aplicativos](#Aplicativos)
* [Funções de acesso e permissões de registro](#Xa9bdac9233b6c432b99b795538546de4bb4a338)
* [Painéis de controle](#Pain%C3%A9isdecontrole)
* [Feeds de dados](#Feedsdedados)
  + [Integrações disponíveis](#Integra%C3%A7%C3%B5esdispon%C3%ADveis)
* [Dicionário de dados](#Dicion%C3%A1riodedados)

## Diagrama da arquitetura

O diagrama a seguir mostra os aplicativos em relação ao caso de uso Programa de vulnerabilidades de segurança de TI (ITSVP).

## Aplicativos

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

| Aplicativo | Descrição |
| --- | --- |
| 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. |
| Tíquetes de vulnerabilidades | O aplicativo Tíquetes de vulnerabilidades fornece um método de criação e atribuição de tíquetes para resultados específicos de análise de vulnerabilidades. O aplicativo permite que tíquetes sejam atribuídos a um proprietário específico, que tem 1 de 4 maneiras de tratar de um tíquete:   * Criar uma solicitação de exceção * Abrir resultados * Criar um plano de remediação simples * Criar um plano de remediação formal   Cada tíquete inclui informações do resultado da análise de vulnerabilidade e de dispositivos relacionados, bem como patches usados para concluir a remediação simples. As medições monitoradas automaticamente pelo aplicativo de tíquetes incluem o número de dias abertos, o status dos tíquetes, a verificação do scanner e o status dos resultados da análise de vulnerabilidade associados. |
| Resultados da análise de vulnerabilidades | O aplicativo Resultados da análise de vulnerabilidades armazena os problemas resultantes de cada registro criado pelo scanner de vulnerabilidades, como nome do dispositivo, IP, proprietário, departamento, descrição, anotações, recomendações e muito mais. Esses registros contêm a recomendação técnica de cada resultado da análise e permitem a geração de relatórios contendo o número total de problemas, independentemente do sistema que os detectou. |
| Dados históricos de vulnerabilidades | O aplicativo Dados históricos de vulnerabilidade fornece um método para monitorar tendências históricas no aplicativo Resultados da análise de vulnerabilidade. As seguintes medições são registradas e monitoradas:   * Vulnerabilidades por severidade * Vulnerabilidades por status geral do VSR * Número de dispositivos * Número de dispositivos analisados (últimos 30 dias)   Os resultados da análise de vulnerabilidade são agrupados nas seguintes dimensões:   * Todas as dimensões * Aplicativo * Processo de negócios * Unidade de negócios * Tecnologias – Produto * Tecnologias – Fornecedor   Os registros no aplicativo Dados históricos de vulnerabilidade representam um snapshot de um point-in-time para uma dimensão e um dispositivo específicos. As informações são preenchidas no Dados históricos de vulnerabilidade diariamente por meio de um feed de dados que agrega dados estatísticos do aplicativo Resultados da análise de vulnerabilidade.  **Importante:** Os campos Status geral do VSR e Severidade localizados no aplicativo Resultados da análise de vulnerabilidade estão intimamente vinculados aos feeds de dados Dados históricos de vulnerabilidade. Alterar os valores ou a configuração desses campos pode fazer com que o feed de dados não funcione adequadamente ou causar uma perda de transferência de dados. |
| 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. |
| 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. |
| Definição de análise de vulnerabilidades | O aplicativo Definição de análises de vulnerabilidades documenta análises de vulnerabilidades ocasionais ou recorrentes para fins de geração de relatórios. As análises de vulnerabilidades podem ser conduzidas de modo regular ou periódico como parte do programa de gerenciamento de ameaças, por exemplo, análises trimestrais de PCI ou análises de servidores externos. As análises de vulnerabilidades também podem ser conduzidas de modo "transacional" para um só fim, como uma análise de aplicativo ou como parte de uma avaliação de ameaça.  Com o aplicativo Definição de análises de vulnerabilidades, é possível:   * Definir análises operacionais recorrentes, incluindo escopo, propriedade, frequência e outros atributos. * Documentar análises "únicas" individuais como documentação de outros processos de ameaça, como análises anteriores ou posteriores à implementação e avaliações de ameaça. * Relacionar resultados individuais do aplicativo Definições de análises de vulnerabilidades por meio de Resultados da análise de vulnerabilidades. * Estabelecer a relação com projetos de ameaça para documentar a execução de análises individuais como parte de um projeto de ameaça. |
| Biblioteca de vulnerabilidades | O aplicativo Biblioteca de vulnerabilidades representa um catálogo de dados de vulnerabilidades coletados das ofertas de integração do Archer Exchange. A Biblioteca de vulnerabilidades é atualizada a cada semana ou mês por feeds de dados dependendo da origem. A biblioteca inclui pontos de dados, como:   * Data de publicação da vulnerabilidade * Título * Consequência * Solução recomendada * Severidade * Pontuação de CVSS   Os registros podem ser vinculados a dispositivos afetados, resultados de análises de vulnerabilidades e código mal-intencionado encontrado para explorar a vulnerabilidade. A Biblioteca de vulnerabilidades também fornece um método para gerar solicitações de exceção, identificar estratégias atenuantes e identificar portas afetadas.  Vinculando vulnerabilidades a ativos, você pode analisar e priorizar as ameaças aos ativos vulneráveis, além de respondê-las de maneira adequada e proativa. A biblioteca de vulnerabilidades fornece a capacidade de:   * Importar dados automaticamente das ofertas de integração do Archer Exchange. * Notificar a equipe adequada automaticamente quando novas vulnerabilidades forem identificadas. * Pesquisar possíveis ameaças e produzir relatórios em tempo real que facilitam a criação de planos de ação. |
| Patches | O aplicativo Patches contém informações de patch, que são preenchidas pelos feeds de ameaças. |
| 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. |
| Solicitações da análise de vulnerabilidades | O aplicativo Solicitação de análise de vulnerabilidades permite solicitar uma análise de vulnerabilidades em determinado dispositivo, aplicativo, segmento de rede ou intervalo de IPs. Ele contém campos para documentar a solicitação, inclusive informações sobre o solicitante e o gerente, escopo da análise, data/hora, tipo de análise e prioridade. |
| Código mal-intencionado | O aplicativo Código mal-intencionado coleta dados de malware relacionados a worms, cavalos de troia, rootkits, spyware, crimeware, vírus e outros códigos de programa hostis ou invasivos. Vinculando códigos mal-intencionados a dados de ativos, você pode analisar, priorizar e determinar de maneira adequada a remediação necessária com base na classificação de relevância do ativo. Com o aplicativo Código mal-intencionado, é possível:   * Importar dados automaticamente de um feed de inteligência. * Notificar as equipes adequadas automaticamente quando um novo código mal-intencionado for identificado. * Pesquisar possíveis ameaças e produzir relatórios em tempo real que facilitam a criação de planos de ação. |
| Resultados | O aplicativo Resultados permite documentar lacunas,deficiências ou problemas detectados por meio de avaliações e testes de controle. Os resultados são gerados automaticamente a partir de questionários, incluindo links que levam ao questionário, ao destino e a quaisquer padrões de controle aplicáveis e fontes confiáveis, ou são gerados manualmente pelos usuários. Você pode resolver os resultados por meio de tarefas de remediação e/ou solicitações de exceção.  Com o aplicativo Resultados, é possível:   * Minimizar resultados gerados automaticamente com base nos resultados de avaliações e testes de controle. * Usar um workflow automatizado para rotear resultados ao pessoal apropriado. * Minimizar resultados por meio de tarefas de remediação e/ou solicitações de exceção. O sistema calcula o risco residual e o status de conformidade com base na resolução dos resultados. * Relacionar vários resultados no contexto de um plano de remediação. * Rastrear tarefas associadas à resolução dos resultados. |
| Solicitações de exceção | O aplicativo Solicitações de exceção permite gerenciar o processo de concessão, negação e expiração de exceções na remediação necessária em um resultado. Com o workflow integrado, o aplicativo garante que todas as exceções sejam devidamente revisadas. A ferramenta também pode relatar exceções em toda a empresa, monitorando-as por controle, departamento ou severidade.  Com o aplicativo Solicitações de exceção, é possível:   * Permitir que os funcionários enviem as próprias solicitações de exceção por meio de uma interface Web fácil de usar. * Permitir que pessoas designadas avaliem as solicitações de exceção e as aprovem ou neguem com base no risco apresentado aos negócios. * Conceder exceções por um período específico e notificar os funcionários apropriados conforme a data de expiração se aproxima. * Permitir que a gerência rastreie exceções concedidas, facilitando revisões periódicas de exceções e o impacto das exceções. * Permitir que os funcionários rastreiem os status das próprias solicitações de exceção à política por meio dos relatórios Minhas solicitações. * Compreender as políticas ou normas padrão com as exceções mais aprovadas e usar essas informações para dar suporte a programas de treinamento e conscientização. |
| Planos de remediação | O aplicativo Planos de remediação permite documentar ações específicas que a gerência pretende executar para resolver problemas e lacunas identificados. Você pode capturar os principais detalhes sobre as iniciativas de remediação, incluindo custos estimados e reais, prazos, proprietários e ações detalhadas. Você pode associar vários planos de remediação a um só resultado e rastrear cada iniciativa individualmente. Também é possível relacionar um único plano de remediação a vários resultados, caso uma ação seja desenvolvida para resolver vários problemas. |
| 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. |
| 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. |
| 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. |
| Listas de referências de vulnerabilidade | O aplicativo Listas de referências de vulnerabilidades fornece um repositório de referências públicas de vulnerabilidades coletadas das ofertas de integração do Archer Exchange, com base no fornecedor que você está usando para analisar. A Lista de referências de vulnerabilidades é atualizada com base em um agendamento definido pelo usuário para considerar ameaças emergentes. O aplicativo fornece uma lista de entradas, cada uma contendo um número de identificação de vulnerabilidade, um tipo e uma referência pública para vulnerabilidades conhecidas de segurança cibernética. A URL encontrada no aplicativo contém uma lista de referências públicas detalhando informações sobre a vulnerabilidade, como uma descrição, consequências da vulnerabilidade e possíveis estratégias de mitigação. |

## Funções de acesso e permissões de registro

A tabela a seguir descreve as funções de acesso de casos de uso.

| Função de acesso | Descrição |
| --- | --- |
| ITSVP: Analistas | Essa função fornece os níveis de acesso apropriados para analistas dentro do caso de uso ITSVP para executar a análise e classificar as vulnerabilidades corretamente. |
| ITSVP: Operações | Esta função fornece os níveis de acesso adequados a Operadores no caso de uso ITSVP. |
| ITSVP: Gerenciamento executivo | Esta função estabelece os direitos para Gerenciamento executivo no caso de uso ITSVP. Os usuários com essa função recebem acesso de leitura a aplicativos ITSVP. |
| ITSVP: Gerenciamento de negócios | Esta função fornece os níveis de acesso à linha de negócios adequada no caso de uso ITSVP. |
| ITSVP: Administração | Esta função serve como o administrador do caso de uso ITSVP, fornecendo privilégios de acesso, criação, leitura, atualização e exclusão. |

**Observação:** para conhecer os direitos de acesso detalhados no nível da página, 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 |
| --- | --- |
| ITSVP – Gerenciamento executivo e de negócios | O painel de controle ITSVP – Gerenciamento executivo e de negócios fornece uma visão geral de alto nível do caso de uso ITSVP. Este painel exibe informações sobre resultados de análise de vulnerabilidades, dispositivos e tíquetes de vulnerabilidades. Os usuários também podem classificar planos de remediação de vulnerabilidade, detecções e solicitações de exceção por status para ver quais estão em andamento, encerrados, aprovados ou expirados.  Somente os usuários atribuídos às funções ITSVP: Gerenciamento de negócios ou ITSVP: Gerenciamento executivo podem exibir o painel de controle ITSVP – Gerenciamento executivo e de negócios. |
| ITSVP – Analista | O painel de controle ITSVP – Analista apresenta informações sobre a severidade e o status de definições de vulnerabilidade e resultados da análise de vulnerabilidade. Esse painel de controle organiza definições de vulnerabilidade por mês para ajudar os analistas a traçar comparações. Os analistas também podem exibir tíquetes de vulnerabilidades abertos atribuídos a eles.  Somente os usuários atribuídos à função ITSVP: Analista podem exibir o painel de controle ITSVP – Analista. |
| ITSVP – Operações | O painel de controle ITSVP – Operações apresenta informações sobre resultados da análise de vulnerabilidade e tíquetes de vulnerabilidades. Os usuários atribuídos à função Operações podem usar esse painel de controle para exibir os tíquetes de vulnerabilidades em aberto atribuídos a eles e ver quais dispositivos estão associados aos resultados da análise de vulnerabilidade em aberto. Este painel de controle também realça as solicitações de exceção de vulnerabilidade a expirar.  Somente os usuários atribuídos à função ITSVP: Operações podem exibir o painel de controle ITSVP – Operações. |

## Feeds de dados

A tabela a seguir descreve o feed de dados do caso de uso.

| Feed de dados | Descrição |
| --- | --- |
| Vulnerability\_Historical\_Data.dfx5 | O feed de dados Dados históricos de vulnerabilidade captura no aplicativo Dados históricos de vulnerabilidade as métricas preenchidas em Resultados da análise de vulnerabilidades. O feed de dados é baseado em vários relatórios estatísticos e captura as seguintes medições para cada registro de análise de vulnerabilidade:   * Vulnerabilidades por severidade * Vulnerabilidades por status geral do VSR * Número de dispositivos * Número de dispositivos analisados (últimos 30 dias)   se um dispositivo estiver vinculado a várias dimensões ou valores de dimensão, os relatórios agregados no aplicativo Dados históricos de vulnerabilidade refletirão o mesmo resultado de análise várias vezes.  **Importante:** o feed de dados Dados históricos de vulnerabilidade só está disponível no idioma inglês. |

### Integrações disponíveis

O caso de uso Programa de vulnerabilidades de segurança de TI tem várias integrações disponíveis no Archer Exchange que permitem alimentar dados de vulnerabilidade no Archer.

**Observação:** Não é necessário instalar nenhuma integração para usar o caso de uso de ITSVP.

A tabela a seguir descreve as integrações disponíveis para o caso de uso.

| Integração | Descrição |
| --- | --- |
| NVD (National Vulnerability Database, banco de dados nacional de vulnerabilidades) do NIST | A integração NVD do NIST faz o seguinte:   * Cataloga vulnerabilidades usando o padrão CVE (Common Vulnerability Enumeration) definido pelo governo dos EUA * Constrói uma biblioteca de vulnerabilidades de base reconhecida como o padrão do setor de segurança * Suporta formato de feed de dados JSON CVE do NVD   Para obter mais informações sobre NVD do NIST, incluindo como configurar os feeds de dados de integração, consulte "NIST National Vulnerability Database Integration" no Archer Exchange at <https://www.archerirm.community/t5/exchange-overviews/nist-national-vulnerability-database-integration/ta-p/564705>. |
| Qualys Vulnerability Management | A integração com o Qualys Vulnerability Management faz o seguinte:   * Cataloga dispositivos de rede em uma rede corporativa * Descobre vulnerabilidades de dispositivos de rede usando tecnologia de varredura * Complementa o aplicativo Biblioteca de vulnerabilidades com a base de conhecimento Qualys   Para obter mais informações sobre o Qualys, incluindo como configurar os feeds de dados de integração, consulte "Qualys Vulnerability Management Integration" no Archer Exchange em <https://www.archerirm.community/t5/exchange-overviews/qualys-vulnerability-management-integration/ta-p/573408>. |
| Tenable.sc Vulnerability Management | A integração com o Tenable.sc Vulnerability Management faz o seguinte:   * Cataloga dispositivos de rede em uma rede corporativa * Descobre vulnerabilidades de dispositivos de rede usando tecnologia de varredura * Complementa o aplicativo Biblioteca de vulnerabilidades Library com plug-ins da Tenable para informações de vulnerabilidade, um conjunto simplificado de ações de remediação e um algoritmo para testar problemas de segurança atuais   Para obter mais informações sobre Tenable.sc, incluindo como configurar os feeds de dados de integração, consulte "Tenable.sc Vulnerability Management Integration" no Archer Exchange no <https://www.archerirm.community/t5/exchange-overviews/tenable-sc-vulnerability-management-integration/ta-p/573423>. |
| RiskRecon Own Enterprise Monitoring | A integração do RiskRecon Own Enterpise Monitoring permite que você monitore de modo independente a postura de segurança externa de sua empresa. Essa integração fornece às organizações visibilidade, percepção e inteligência acionável sobre ambientes de risco.  Para obter mais informações sobre o RiskRecon Own Enterprise Monitoring, incluindo como configurar os feeds de dados de integração, consulte "RiskRecon Own Enterprise Monitoring Integration" no Archer Exchange no <https://www.archerirm.community/t5/exchange-overviews/riskrecon-own-enterprise-monitoring-integration/ta-p/571193>. |

## Dicionário de dados

O Dicionário de dados do Programa de vulnerabilidades de segurança de TI contém as informações de configuração do caso de uso.

Você pode obter o Dicionário de dados da solução entrando em contato com o representante de contas do Archer.