# Baseline de Segurança para Athena

## Objetivo

Estabelecer um padrão de segurança consistente para proteger os ativos da organização contra ameaças cibernéticas.

## Introdução

O AWS Athena é um serviço de consulta interativa serverless que permite análise de dados no Amazon S3 usando SQL. Ele oferece análises rápidas e escaláveis sem gerenciamento de infraestrutura, ideal para relatórios e análises ad-hoc diretamente nos dados armazenados no S3.

## Escopo

Este documento se aplica ao Athena e todos os controles aqui descritos são obrigatórios.

## Visão Geral dos Controles

|  |  |  |  |
| --- | --- | --- | --- |
| **Controle** | **Racional** | **Aplicabilidade** | **Local de aplicação do controle** |
| Athena\_001 | A criptografia dos resultados das consultas do AWS Athena ajuda a proteger os dados sensíveis e garante que somente usuários autorizados possam acessar esses resultados. | TBD | TBD |
| Athena\_002 | O uso de serviços de segurança gerenciados avançados, como o Amazon Macie, permite a identificação automática e a proteção contra vazamentos de dados, oferecendo monitoramento contínuo e alertas para configurações de segurança e dados sensíveis. | TBD | TBD |
| Athena\_003 | A criptografia de metadados no AWS Glue Data Catalog é crucial para proteger as informações sensíveis armazenadas nos metadados, prevenindo o acesso não autorizado e garantindo a confidencialidade dos dados. | TBD | TBD |
| Athena\_004 | Criptografar os resultados das consultas armazenados no Amazon S3 assegura a proteção dos dados processados pelo Amazon Athena, evitando a exposição de informações sensíveis e garantindo a confidencialidade dos dados. | TBD | TBD |
| Athena\_005 | Utilizar workgroups no Amazon Athena permite restringir o acesso a consultas salvas, garantindo que apenas usuários autorizados possam visualizar ou executar essas consultas, o que ajuda a proteger as informações sensíveis e a manter a governança de dados. | TBD | TBD |
| Athena\_006 | Restringir o acesso às operações do Amazon Athena com políticas IAM assegura que apenas usuários e sistemas autorizados possam executar operações específicas, protegendo os dados e recursos contra acessos e modificações não autorizadas. | TBD | TBD |
| Athena\_007 | Utilizar políticas gerenciadas pelo Amazon Athena ajuda a simplificar a administração de permissões, assegurando que as atualizações de segurança e de funcionalidades sejam aplicadas de forma consistente e eficiente. | TBD | TBD |
| Athena\_008 | A definição de políticas com permissões granulares para ações específicas do Amazon Athena permite um controle mais preciso sobre o acesso e as operações, garantindo que os usuários tenham apenas as permissões necessárias para realizar suas tarefas. | TBD | TBD |
| Athena\_009 | Conceder acesso apropriado ao local do Amazon S3 onde os dados são armazenados é essencial para garantir que os usuários e serviços do Amazon Athena tenham as permissões necessárias para acessar e processar os dados, sem expor informações sensíveis a entidades não autorizadas. | TBD | TBD |
| Athena\_010 | Proteger os dados armazenados no Amazon S3 e os resultados das consultas do Amazon Athena contra acessos não autorizados, garantindo a confidencialidade e integridade dos dados. | TBD | TBD |
| Athena\_011 | Garantir que os dados transmitidos entre o Amazon Athena e o Amazon S3, bem como entre o Athena e as aplicações dos clientes, estejam protegidos contra interceptações e acessos não autorizados. | TBD | TBD |

## Detalhamento dos Controles

Habilitar Criptografia para Resultados de Consultas do AWS Athena

* Controle ID: Athena\_001
* Racional: A criptografia dos resultados das consultas do AWS Athena ajuda a proteger os dados sensíveis e garante que somente usuários autorizados possam acessar esses resultados.
* Riscos Mitigados: A falta de criptografia pode expor dados sensíveis a acessos não autorizados, comprometendo a confidencialidade e integridade dos dados.
* Auditoria:
  + Faça login no console da AWS e abra o serviço Amazon Athena.
  + Clique em 'Configurações' no painel de navegação à esquerda.
  + Verifique se a opção 'Criptografia das configurações de resultado de consulta' está definida para 'Ativada'.
  + Confirme que o tipo de criptografia (como SSE-S3, SSE-KMS ou CSE-KMS) está especificado e é apropriado para a política de segurança da sua organização.
* Remediação:
  + Acesse o console da AWS e navegue até o serviço Amazon Athena.
  + Clique em 'Configurações' no menu lateral.
  + Na seção 'Configurações de resultado de consulta', escolha 'Editar'.
  + Selecione 'Ativado' na opção de criptografia.
  + Escolha o tipo de criptografia desejado (SSE-S3, SSE-KMS, ou CSE-KMS) e configure os detalhes necessários, como o ARN da chave KMS, se aplicável.
  + Salve as configurações para aplicar a criptografia.
* Referências:
  + [Amazon Athena User Guide - Configuring Encryption Options](https://docs.aws.amazon.com/athena/latest/ug/encryption.html)

Utilizar Serviços de Segurança Gerenciados Avançados como Amazon Macie

* Controle ID: Athena\_002
* Racional: O uso de serviços de segurança gerenciados avançados, como o Amazon Macie, permite a identificação automática e a proteção contra vazamentos de dados, oferecendo monitoramento contínuo e alertas para configurações de segurança e dados sensíveis.
* Riscos Mitigados: A falta de visibilidade e monitoramento pode levar a exposições de dados não detectadas, comprometendo a segurança e a privacidade dos dados armazenados.
* Auditoria:
  + Acesse o console da AWS e verifique se o Amazon Macie está ativado.
  + Revise as configurações do Macie para garantir que ele esteja configurado corretamente para monitorar os recursos desejados, como buckets do S3.
  + Verifique os alertas e relatórios gerados pelo Macie para identificar possíveis riscos ou incidentes de segurança.
* Remediação:
  + No console da AWS, acesse o serviço Amazon Macie e ative-o, caso ainda não esteja.
  + Configure o Amazon Macie para monitorar automaticamente os buckets do S3 e outros recursos AWS para dados sensíveis e configurações de segurança.
  + Defina parâmetros de classificação e políticas de auditoria para ajustar a sensibilidade do monitoramento às necessidades específicas da organização.
  + Monitore os alertas e análises fornecidos pelo Macie regularmente para responder rapidamente a potenciais vulnerabilidades ou exposições de dados.
* Referências:
  + [Amazon Macie User Guide](https://docs.aws.amazon.com/macie/latest/userguide/what-is-macie.html)
  + [AWS Security Services](https://aws.amazon.com/products/security/)

Criptografar Metadados no AWS Glue Data Catalog

* Controle ID: Athena\_003
* Racional: A criptografia de metadados no AWS Glue Data Catalog é crucial para proteger as informações sensíveis armazenadas nos metadados, prevenindo o acesso não autorizado e garantindo a confidencialidade dos dados.
* Riscos Mitigados: A falta de criptografia pode resultar na exposição de informações sensíveis contidas nos metadados, levando a riscos de segurança e privacidade.
* Auditoria:
  + Acesse o console da AWS e navegue até o AWS Glue.
  + Selecione o Data Catalog e verifique as configurações de segurança para confirmar que a criptografia está habilitada para os metadados.
  + Assegure-se de que a criptografia utiliza o AWS Key Management Service (KMS) para gerenciar as chaves de criptografia.
* Remediação:
  + No console da AWS, vá até o AWS Glue.
  + Acesse as configurações do Data Catalog.
  + Habilite a criptografia de metadados e selecione o AWS Key Management Service (KMS) para gerenciar as chaves de criptografia.
  + Configure a chave de criptografia do KMS, selecionando uma chave existente ou criando uma nova específica para o Glue Data Catalog.
* Referências:
  + [AWS Glue Documentation - Encrypting Data Written by Crawlers, Jobs, and Development Endpoints](https://docs.aws.amazon.com/glue/latest/dg/encryption-security-configuration.html)
  + [AWS Key Management Service (KMS) Documentation](https://docs.aws.amazon.com/kms/latest/developerguide/overview.html)

Criptografar Resultados de Consultas Armazenados no Amazon S3

* Controle ID: Athena\_004
* Racional: Criptografar os resultados das consultas armazenados no Amazon S3 assegura a proteção dos dados processados pelo Amazon Athena, evitando a exposição de informações sensíveis e garantindo a confidencialidade dos dados.
* Riscos Mitigados: A ausência de criptografia pode levar ao acesso não autorizado ou à exposição de dados confidenciais armazenados no S3, resultando em possíveis violações de segurança e de privacidade.
* Auditoria:
  + Acesse o console da AWS e navegue até o Amazon S3.
  + Verifique os buckets que armazenam os resultados das consultas do Athena para garantir que a criptografia está ativada.
  + Confirme que os dados estão sendo criptografados usando o AWS Key Management Service (KMS) ou a criptografia do lado do servidor fornecida pela Amazon S3 (SSE-S3).
* Remediação:
  + No console da AWS, acesse o Amazon S3.
  + Selecione o bucket que armazena os resultados das consultas do Athena.
  + Ative a criptografia do lado do servidor (SSE) utilizando o AWS Key Management Service (KMS) ou SSE-S3.
  + Se optar pelo AWS KMS, selecione uma chave de criptografia existente ou crie uma nova.
  + Assegure que as configurações de criptografia estejam aplicadas a todos os objetos novos e existentes no bucket.
* Referências:
  + [Amazon S3 Documentation - Using Server-Side Encryption](https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html)
  + [AWS Key Management Service (KMS) Documentation](https://docs.aws.amazon.com/kms/latest/developerguide/overview.html)

Restringir Acesso a Consultas Salvas Usando Workgroups

* Controle ID: Athena\_005
* Racional: Utilizar workgroups no Amazon Athena permite restringir o acesso a consultas salvas, garantindo que apenas usuários autorizados possam visualizar ou executar essas consultas, o que ajuda a proteger as informações sensíveis e a manter a governança de dados.
* Riscos Mitigados: Sem a restrição adequada, as consultas salvas podem ser acessadas ou executadas por usuários não autorizados, potencialmente levando à exposição de dados sensíveis.
* Auditoria:
  + Acesse o console da AWS e vá para o serviço Amazon Athena.
  + Verifique se os workgroups estão configurados e sendo utilizados para gerenciar o acesso a consultas e resultados.
  + Confira as políticas de permissão associadas a cada workgroup para garantir que apenas os usuários e grupos autorizados tenham acesso às consultas salvas.
* Remediação:
  + No console da AWS, navegue até o Amazon Athena.
  + Crie ou configure um workgroup existente.
  + Defina as configurações de permissão do workgroup para controlar quem pode acessar e executar as consultas salvas.
  + Aplique políticas de IAM para restringir o acesso ao workgroup a apenas usuários e grupos específicos.
  + Certifique-se de que todas as consultas salvas estejam associadas ao workgroup correto com as permissões apropriadas.
* Referências:
  + [Amazon Athena User Guide - Working with Workgroups](https://docs.aws.amazon.com/athena/latest/ug/workgroups.html)
  + [AWS Identity and Access Management (IAM) User Guide](https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html)

Restringir Acesso às Operações do Athena com Políticas IAM

* Controle ID: Athena\_006
* Racional: Restringir o acesso às operações do Amazon Athena com políticas IAM assegura que apenas usuários e sistemas autorizados possam executar operações específicas, protegendo os dados e recursos contra acessos e modificações não autorizadas.
* Riscos Mitigados: Acesso não restrito ou mal configurado ao Athena pode levar a exposições de dados, manipulações indevidas ou uso abusivo dos recursos, comprometendo a segurança dos dados.
* Auditoria:
  + Revise as políticas IAM associadas ao Amazon Athena para verificar se elas estão corretamente configuradas para limitar as operações com base no princípio do menor privilégio.
  + Utilize o AWS CloudTrail para auditar o uso do Athena e verificar se as políticas IAM estão sendo efetivamente aplicadas e respeitadas.
* Remediação:
  + No console da AWS, acesse o serviço IAM.
  + Crie ou revise as políticas IAM para restringir as operações no Amazon Athena, especificando as ações permitidas e os recursos acessíveis.
  + Associe as políticas IAM aos usuários, grupos ou funções que necessitam de acesso ao Athena, garantindo que as permissões sejam concedidas estritamente conforme necessário.
  + Regularmente revise e ajuste as políticas IAM com base nas mudanças de requisitos de acesso e no princípio do menor privilégio.
* Referências:
  + [Amazon Athena Documentation - IAM Policies for Amazon Athena](https://docs.aws.amazon.com/athena/latest/ug/security-iam.html)
  + [AWS IAM User Guide](https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html)

Utilizar Políticas Gerenciadas pelo Athena para Facilitar a Atualização de Permissões

* Controle ID: Athena\_007
* Racional: Utilizar políticas gerenciadas pelo Amazon Athena ajuda a simplificar a administração de permissões, assegurando que as atualizações de segurança e de funcionalidades sejam aplicadas de forma consistente e eficiente.
* Riscos Mitigados: A gestão ineficiente de permissões pode levar a configurações incorretas ou excesso de privilégios, aumentando o risco de exposição de dados e de acessos não autorizados.
* Auditoria:
  + Revise as políticas de IAM no console da AWS para verificar se as políticas gerenciadas pelo Athena estão sendo utilizadas.
  + Garanta que as permissões concedidas através dessas políticas estejam em conformidade com o princípio do menor privilégio e sejam adequadas às necessidades operacionais.
* Remediação:
  + No console da AWS, acesse o serviço IAM.
  + Navegue até a seção de políticas e filtre por políticas gerenciadas pela AWS específicas para o Athena.
  + Associe essas políticas gerenciadas aos usuários, grupos ou funções que necessitam de acesso ao Athena.
  + Regularmente revise as permissões para garantir que elas continuem adequadas às necessidades e conformes às práticas recomendadas de segurança.
* Referências:
  + [Amazon Athena Documentation - Access Management](https://docs.aws.amazon.com/athena/latest/ug/access.html)
  + [AWS IAM User Guide - Managed Policies and Inline Policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/access\_policies\_managed-vs-inline.html)

Afinar Políticas com Permissões Granulares para Ações do Athena

* Controle ID: Athena\_008
* Racional: A definição de políticas com permissões granulares para ações específicas do Amazon Athena permite um controle mais preciso sobre o acesso e as operações, garantindo que os usuários tenham apenas as permissões necessárias para realizar suas tarefas.
* Riscos Mitigados: Permissões amplas podem permitir acesso não intencional ou malicioso a dados e recursos, aumentando o risco de comprometimento de dados e de segurança.
* Auditoria:
  + Examine as políticas de IAM aplicadas ao Athena para garantir que elas especificam ações individuais, em vez de conceder permissões amplas.
  + Verifique se as permissões estão alinhadas com o princípio do menor privilégio, permitindo aos usuários realizar apenas as tarefas necessárias.
* Remediação:
  + No console da AWS, acesse o serviço IAM e edite ou crie políticas de IAM que se aplicam ao Athena.
  + Especifique ações individuais nas políticas (como `athena:startQueryExecution`, `athena:getQueryResults`, etc.) para controlar o acesso a operações específicas.
  + Aplique estas políticas aos usuários, grupos ou funções que necessitam de acesso ao Athena, assegurando que cada entidade tenha apenas as permissões necessárias para suas funções.
  + Regularmente revise e atualize as políticas de IAM para refletir mudanças nas necessidades de acesso e operações.
* Referências:
  + [Amazon Athena Documentation - IAM Policies for Amazon Athena](https://docs.aws.amazon.com/athena/latest/ug/security-iam-athena.html)
  + [AWS IAM User Guide - Example Policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/access\_policies\_examples.html)

Conceder Acesso Apropriado ao Local do Amazon S3 dos Dados

* Controle ID: Athena\_009
* Racional: Conceder acesso apropriado ao local do Amazon S3 onde os dados são armazenados é essencial para garantir que os usuários e serviços do Amazon Athena tenham as permissões necessárias para acessar e processar os dados, sem expor informações sensíveis a entidades não autorizadas.
* Riscos Mitigados: Acesso inadequado aos dados armazenados no S3 pode levar a vazamentos de dados, acesso não autorizado e comprometimento da integridade dos dados.
* Auditoria:
  + Verifique as políticas de acesso do Amazon S3 para assegurar que os buckets e objetos estão corretamente configurados para permitir o acesso apenas às entidades autorizadas.
  + Revise as políticas de IAM e as configurações de permissão do S3 para confirmar que elas estão alinhadas com o uso pretendido no Athena e com as práticas de segurança recomendadas.
* Remediação:
  + No console da AWS, acesse o serviço Amazon S3.
  + Identifique os buckets utilizados pelo Amazon Athena e revise suas políticas de acesso.
  + Aplique políticas de bucket do S3 para garantir que o acesso seja restrito a usuários, grupos ou funções do IAM que requerem acesso para suas operações no Athena.
  + Configure as permissões em nível de objeto, se necessário, para controlar o acesso a dados específicos dentro dos buckets.
  + Utilize as melhores práticas de segurança, como a criptografia dos dados e o logging do acesso, para proteger as informações armazenadas.
* Referências:
  + [Amazon S3 Documentation - Managing Access Permissions to Your Amazon S3 Resources](https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-access-control.html)
  + [AWS Documentation on Access Management for Amazon S3](https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-overview.html)

Implementar Criptografia de Dados em Repouso para Amazon Athena e Amazon S3

* Controle ID: Athena\_010
* Racional: Proteger os dados armazenados no Amazon S3 e os resultados das consultas do Amazon Athena contra acessos não autorizados, garantindo a confidencialidade e integridade dos dados.
* Riscos Mitigados: Mitiga o risco de exposição de dados sensíveis devido a acessos não autorizados ou brechas de segurança em armazenamentos de dados.
* Auditoria:
  + Acesse o console do Amazon S3 e verifique se os buckets utilizados pelo Athena estão configurados com SSE-S3 ou SSE-KMS para criptografia de dados em repouso.
  + No console do Amazon Athena, confirme se os resultados das consultas são armazenados em locais do S3 com a criptografia habilitada.
  + No console do AWS Glue Data Catalog, verifique se os metadados estão configurados para criptografia.
* Remediação:
  + No console do Amazon S3, selecione o bucket relevante e habilite a criptografia usando SSE-S3 ou SSE-KMS.
  + No Amazon Athena, assegure que os resultados das consultas sejam armazenados em buckets do S3 com criptografia habilitada.
  + No AWS Glue Data Catalog, ative a criptografia de metadados.
* Referências:
  + [Proteção de dados no Amazon Athena](https://docs.aws.amazon.com/athena/latest/ug/security-data-protection.html)
  + [Criptografia de resultados de consultas no Amazon S3](https://docs.aws.amazon.com/athena/latest/ug/encryption.html)

Implementar Criptografia de Dados em Trânsito para Amazon Athena

* Controle ID: Athena\_011
* Racional: Garantir que os dados transmitidos entre o Amazon Athena e o Amazon S3, bem como entre o Athena e as aplicações dos clientes, estejam protegidos contra interceptações e acessos não autorizados.
* Riscos Mitigados: Mitiga o risco de interceptação de dados sensíveis durante a transmissão.
* Auditoria:
  + Verifique se as conexões entre o Amazon Athena e o Amazon S3 estão usando TLS.
  + Confirme que todas as conexões cliente-Athena estão utilizando HTTPS (TLS), verificando as políticas do IAM dos buckets do S3.
  + Para conexões JDBC ou ODBC, assegure-se de que a criptografia TLS está sendo utilizada.
* Remediação:
  + Garanta que as políticas do IAM dos buckets do S3 incluam a condição `aws:SecureTransport` para forçar conexões criptografadas via HTTPS (TLS).
  + Atualize e configure os drivers JDBC e ODBC do Athena para utilizar a criptografia TLS.
  + Para fontes de dados federadas do Athena, verifique a documentação dos conectores específicos para assegurar o suporte à criptografia em trânsito.
* Referências:
  + [Proteção de dados no Amazon Athena](https://docs.aws.amazon.com/athena/latest/ug/security-data-protection.html)
  + [Criptografia em trânsito no Amazon Athena](https://docs.aws.amazon.com/athena/latest/ug/encryption-in-transit.html)
  + [Conectando ao Amazon Athena com JDBC](https://docs.aws.amazon.com/athena/latest/ug/connect-with-jdbc.html)
  + [Conectando ao Amazon Athena com ODBC](https://docs.aws.amazon.com/athena/latest/ug/connect-with-odbc.html)
  + [Data protection in Athena](<https://docs.aws.amazon.com/athena/latest/ug/security-data-protection.html>)

## Histórico de alterações

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data de Publicação** | **Descrição** | **Alterações** |
| 1.0 | 09/04/2024 | Breve descrição do que foi realizado | * Controles Incluídos:   + Athena\_001 - Criptografia de resultados de consultas   + Athena\_002 - Uso do Amazon Macie para monitoramento   + Athena\_003 - Criptografia de metadados no AWS Glue   + Athena\_004 - Criptografia de resultados de consultas no S3   + Athena\_005 - Restrição de acesso usando Workgroups   + Athena\_006 - Restrição de acesso com IAM   + Athena\_007 - Uso de políticas gerenciadas do Athena   + Athena\_008 - Permissões granulares no IAM   + Athena\_009 - Acesso apropriado ao S3   + Athena\_010 - Criptografia em repouso para Athena e S3   + Athena\_011 - Criptografia em trânsito para Athena * Controles Excluídos: None * Controles Alterados: None |