# Baseline de Segurança para Amazon Athena

## Objetivo

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

## Introdução

O Amazon Athena é um serviço interativo de consulta SQL que permite a análise fácil de grandes quantidades de dados diretamente no Amazon Simple Storage Service (Amazon S3). Utilizando o Athena, os usuários podem executar consultas ad-hoc em dados armazenados no formato de arquivos no S3 sem a necessidade de pré-processamento ou movimentação desses dados. Isso é particularmente útil para tarefas de análise de dados, onde a flexibilidade e a escala são cruciais.

## Escopo

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

## Visão Geral dos Controles

|  |  |  |  |
| --- | --- | --- | --- |
| **Controle** | **Racional** | **Aplicabilidade** | **Local de aplicação do controle** |
| Habilitar Criptografia para Resultados de Consultas do AWS Athena | 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 |
| Garanta que o Amazon Macie Esteja Configurado para Monitorar e Proteger Dados Sensíveis Armazenados no S3 | Embora o Amazon Athena permita análises interativas diretamente em dados armazenados no Amazon S3, ele não possui funcionalidades internas para classificação ou proteção detalhada desses dados. A habilitação do Amazon Macie, um serviço de segurança gerenciado avançado, é essencial para complementar o uso do Athena, proporcionando a detecção automática de dados sensíveis e a proteção contra vazamentos de dados. Macie oferece capacidades cruciais de monitoramento contínuo e alertas para configurações inadequadas de segurança e dados sensíveis em S3, assegurando que os dados que o Athena acessa sejam gerenciados de forma segura e conforme as melhores práticas de segurança e conformidade. Essa abordagem integrada fortalece significativamente a postura de segurança ao usar o Athena para análises de dados. | TBD | TBD |
| Criptografar Metadados no AWS Glue Data Catalog | Proteger os metadados armazenados no AWS Glue Data Catalog é essencial para manter a segurança e a confidencialidade das informações. A criptografia desses metadados é fundamental para prevenir acessos não autorizados e garantir a integridade das informações que o Amazon Athena utiliza para executar consultas em dados armazenados no S3. A utilização de criptografia robusta via AWS Key Management Service (KMS) ajuda a assegurar que somente usuários autorizados tenham acesso aos metadados sensíveis. | TBD | TBD |
| Criptografar Resultados de Consultas Armazenados no Amazon S3 | A criptografia dos resultados das consultas armazenados no Amazon S3 é essencial para proteger os dados processados pelo Amazon Athena. Isso evita a exposição de informações sensíveis e garante a confidencialidade dos dados, protegendo contra violações de segurança e exposições inadvertidas de informações críticas ou regulamentadas. | TBD | TBD |
| Implementar Criptografia de Dados em Repouso para Amazon Athena e Amazon S3 | A implementação de criptografia de dados em repouso é vital para proteger os dados armazenados no Amazon S3 usados pelo Amazon Athena, bem como os resultados das consultas gerados por ele. Isso garante a confidencialidade e a integridade dos dados ao prevenir o acesso não autorizado e proteger contra potenciais brechas de segurança. Além disso, a criptografia dos metadados no AWS Glue Data Catalog é essencial para a segurança completa do ecossistema de dados. | TBD | TBD |
| Athena\_011 | Proteger os dados durante a transmissão entre o Amazon Athena e o Amazon S3, e entre o Athena e as aplicações dos clientes, é crucial para evitar interceptações e acessos não autorizados. A utilização de criptografia TLS assegura a integridade e confidencialidade dos dados em trânsito, mitigando o risco de exposição durante a transferência. | 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)

Garanta que o Amazon Macie Esteja Configurado para Monitorar e Proteger Dados Sensíveis Armazenados no S3

* Controle ID: Athena\_002
* Racional: Embora o Amazon Athena permita análises interativas diretamente em dados armazenados no Amazon S3, ele não possui funcionalidades internas para classificação ou proteção detalhada desses dados. A habilitação do Amazon Macie, um serviço de segurança gerenciado avançado, é essencial para complementar o uso do Athena, proporcionando a detecção automática de dados sensíveis e a proteção contra vazamentos de dados. Macie oferece capacidades cruciais de monitoramento contínuo e alertas para configurações inadequadas de segurança e dados sensíveis em S3, assegurando que os dados que o Athena acessa sejam gerenciados de forma segura e conforme as melhores práticas de segurança e conformidade. Essa abordagem integrada fortalece significativamente a postura de segurança ao usar o Athena para análises de dados.
* 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: Proteger os metadados armazenados no AWS Glue Data Catalog é essencial para manter a segurança e a confidencialidade das informações. A criptografia desses metadados é fundamental para prevenir acessos não autorizados e garantir a integridade das informações que o Amazon Athena utiliza para executar consultas em dados armazenados no S3. A utilização de criptografia robusta via AWS Key Management Service (KMS) ajuda a assegurar que somente usuários autorizados tenham acesso aos metadados sensíveis.
* Riscos Mitigados:
  + Exposição de informações estruturais e sensíveis sobre os dados, aumentando o risco de ataques direcionados e violação de dados.
  + Acesso não autorizado aos metadados, o que pode comprometer toda a cadeia de análise de dados, incluindo as operações do Amazon Athena.
* 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: A criptografia dos resultados das consultas armazenados no Amazon S3 é essencial para proteger os dados processados pelo Amazon Athena. Isso evita a exposição de informações sensíveis e garante a confidencialidade dos dados, protegendo contra violações de segurança e exposições inadvertidas de informações críticas ou regulamentadas.
* Riscos Mitigados:
  + Acesso não autorizado a dados confidenciais resultantes de consultas, potencialmente expondo informações sensíveis.
  + Violações de políticas de conformidade de dados que requerem criptografia de dados sensíveis, tanto em repouso quanto em trânsito.
* 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)

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

* Controle ID: Athena\_006
* Racional: A implementação de criptografia de dados em repouso é vital para proteger os dados armazenados no Amazon S3 usados pelo Amazon Athena, bem como os resultados das consultas gerados por ele. Isso garante a confidencialidade e a integridade dos dados ao prevenir o acesso não autorizado e proteger contra potenciais brechas de segurança. Além disso, a criptografia dos metadados no AWS Glue Data Catalog é essencial para a segurança completa do ecossistema de dados.
* Riscos Mitigados:
  + Exposição de dados sensíveis devido a acessos não autorizados, potencialmente levando a violações de dados.
  + Comprometimento da integridade dos dados e metadados armazenados, afetando a confiabilidade e a segurança das operações 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\_007
* Racional: Proteger os dados durante a transmissão entre o Amazon Athena e o Amazon S3, e entre o Athena e as aplicações dos clientes, é crucial para evitar interceptações e acessos não autorizados. A utilização de criptografia TLS assegura a integridade e confidencialidade dos dados em trânsito, mitigando o risco de exposição durante a transferência.
* Riscos Mitigados:
  + Interceptação de dados sensíveis durante a transmissão, o que pode levar a vazamentos de informações e comprometimento da segurança.
  + Acesso não autorizado a dados em trânsito, aumentando o risco de ataques de "man-in-the-middle".
* 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 | 14/04/2024 | Inclusão de novos controles de segurança para AWS Athena e serviços relacionados. | * Controles incluídos:   + Habilitar Criptografia para Resultados de Consultas do AWS Athena - Athena\_001   + Garanta que o Amazon Macie Esteja Configurado para Monitorar e Proteger Dados Sensíveis Armazenados no S3 - Athena\_002   + Criptografar Metadados no AWS Glue Data Catalog - Athena\_003   + Criptografar Resultados de Consultas Armazenados no Amazon S3 - Athena\_004   + Restringir Acesso a Consultas Salvas Usando Workgroups - Athena\_005   + Implementar Criptografia de Dados em Repouso para Amazon Athena e Amazon S3 - Athena\_006   + Implementar Criptografia de Dados em Trânsito para Amazon Athena - Athena\_007 * Controles excluídos: None * Controles alterados: None" |