# Baseline de Segurança para Amazon S3

## Objetivo

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

## Introdução

O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos oferecido pela Amazon Web Services (AWS). Ele é projetado para fornecer armazenamento na internet em grande escala, oferecendo uma interface de armazenamento simples com alta durabilidade, disponibilidade e escalabilidade. O S3 permite armazenar e recuperar qualquer quantidade de dados, a qualquer momento, de qualquer lugar na web.

## Escopo

Este documento se aplica ao Amazon S3 e todos os controles aqui descritos são obrigatórios.

## Visão Geral dos Controles

|  |  |  |  |
| --- | --- | --- | --- |
| Controle | Racional | Aplicabilidade | Local de aplicação do controle |
| Garanta que o acesso ao Amazon S3 seja concedido exclusivamente por meio de IAM Roles. | A utilização de IAM Roles para conceder acesso ao Amazon S3 é uma prática segura e recomendada, garantindo que apenas permissões necessárias sejam atribuídas de forma controlada e auditável. | TBD | TBD |
| Garanta que todo acesso ao Amazon S3 seja realizado via Amazon S3 VPC Endpoints, AWS Direct Connect ou VPN, proibindo o acesso direto via internet. | A utilização de Amazon S3 VPC Endpoints, juntamente com AWS Direct Connect ou VPN, proporciona uma conexão segura e privada, aumentando a segurança ao eliminar a exposição através da internet pública. | TBD | TBD |
| Implemente o uso do Amazon S3 Inventory para facilitar a auditoria de objetos armazenados. | O Amazon S3 Inventory provê relatórios detalhados dos objetos armazenados no S3, possibilitando uma auditoria eficaz e garantindo o cumprimento das políticas de gestão de dados. | TBD | TBD |
| Implemente o monitoramento de acesso aos dados utilizando logs de acesso do servidor S3. | Os logs de acesso do servidor S3 registram detalhadamente as solicitações feitas ao S3, permitindo uma vigilância efetiva e a análise do acesso aos dados, ajudando a detectar e responder a acessos não autorizados. | TBD | TBD |
| Desative as ACLs no Amazon S3 para simplificar o gerenciamento de permissões e reduzir o risco de erros. | Desabilitar as ACLs em favor de políticas de bucket simplifica as configurações de permissão e minimiza a possibilidade de erros que podem levar à exposição não intencional de dados. | TBD | TBD |
| Configure a propriedade do objeto no Amazon S3 para "Bucket Owner Preferred" ou "Object Writer" para desabilitar o uso de ACLs em novos objetos. | Configurar a propriedade do objeto em buckets S3 ajuda a gerenciar as permissões de forma centralizada e segura, eliminando a necessidade de usar ACLs, o que pode reduzir erros de configuração e vazamentos de dados. | TBD | TBD |
| Implemente o bloqueio completo de acesso público aos buckets do Amazon S3, incluindo uma política organizacional para garantir uma abordagem uniforme. | Bloquear o acesso público aos buckets S3 é crucial para prevenir a exposição acidental de dados sensíveis e proteger contra ataques cibernéticos. Aplicar essa política em nível de organização ou conta garante uma proteção abrangente e uniforme. | TBD | TBD |
| Utilize o Amazon Macie para identificar e proteger dados sensíveis nos buckets do S3. | O Amazon Macie é uma ferramenta essencial para a detecção automática de dados sensíveis, auxiliando na prevenção de exposições e vazamentos e na manutenção da conformidade com regulamentos de proteção de dados. | TBD | TBD |
| Ative e configure a proteção do S3 em GuardDuty para monitorar e alertar sobre atividades suspeitas nos buckets do S3. | Utilizar o Amazon GuardDuty para monitorar os buckets do S3 ajuda a identificar atividades suspeitas ou anormais, melhorando significativamente a postura de segurança e prevenindo possíveis ataques. | TBD | TBD |
| Ative o registro de atividades para o S3 usando tanto o AWS CloudTrail quanto o logging de acesso do servidor para criar uma trilha de auditoria detalhada. | A habilitação do registro no S3 usando CloudTrail e logging de acesso do servidor proporciona visibilidade completa sobre as atividades de acesso e modificação, crucial para a detecção e resposta a incidentes de segurança. | TBD | TBD |
| Utilize o AWS Security Hub e o AWS CloudWatch para monitoramento abrangente do Amazon S3, detectando atividades suspeitas e problemas operacionais. | Monitorar o S3 com estas ferramentas permite identificar proativamente eventos de segurança e operacionais, melhorando a segurança e eficiência operacional. | TBD | TBD |
| Assegure que o Grupo de Entrega de Logs S3 não tenha permissão de escrita no bucket de origem do S3, onde o Logging de Acesso do Servidor está ativado. | Prevenir que o Grupo de Entrega de Logs S3 tenha permissões de escrita no bucket de origem ajuda a manter a integridade dos logs ao evitar que sejam alterados ou excluídos após a criação. Isto é essencial para garantir uma trilha de auditoria confiável e para proteger contra manipulações que podem ocultar atividades maliciosas. | TBD | TBD |
| Proíba o acesso 'FULL\_CONTROL' tanto a usuários autenticados quanto a usuários públicos em todos os buckets S3 para prevenir controle total não autorizado e garantir a segurança dos dados. | Limitar o acesso 'FULL\_CONTROL' ajuda a prevenir alterações e exclusões não autorizadas nos buckets S3, protegendo contra acessos maliciosos e garantindo a integridade e segurança dos dados armazenados. Proibir esses acessos tanto para usuários autenticados quanto públicos fortalece a política de segurança e minimiza riscos de exposição e manipulação de dados. | TBD | TBD |
| Proíba o acesso 'READ' tanto a usuários autenticados quanto a usuários públicos em todos os buckets S3 para prevenir leitura não autorizada e garantir a segurança dos dados. | Limitar o acesso 'READ' ajuda a prevenir acessos não autorizados e vazamento de informações nos buckets S3. Proibir esses acessos tanto para usuários autenticados quanto públicos fortalece a política de segurança e minimiza riscos de exposição e manipulação de dados. | TBD | TBD |
| Proíba o acesso 'READ\_ACP' tanto a usuários autenticados quanto a usuários públicos em todos os buckets S3 para impedir o acesso não autorizado às configurações de permissões do bucket. | Limitar o acesso 'READ\_ACP' ajuda a prevenir a exposição não autorizada das configurações de segurança e permissões dos buckets S3. Proibir esses acessos tanto para usuários autenticados quanto públicos fortalece a política de segurança e minimiza riscos de manipulação e vazamentos de informações críticas. | TBD | TBD |
| Proíba o acesso 'WRITE' tanto a usuários autenticados quanto a usuários públicos em todos os buckets S3 para impedir alterações não autorizadas, sobrescrita ou adição de dados. | Limitar o acesso 'WRITE' ajuda a prevenir modificações não autorizadas, adição ou exclusão de dados nos buckets S3. Proibir esses acessos tanto para usuários autenticados quanto públicos fortalece a política de segurança e minimiza riscos de manipulação de dados. | TBD | TBD |
| Proíba o acesso público 'WRITE\_ACP' aos buckets S3 para evitar alterações não autorizadas nas configurações de permissões. | Proibir o acesso público 'WRITE\_ACP' aos buckets S3 é essencial para prevenir modificações não autorizadas nas configurações de permissões e segurança. Isso ajuda a manter o controle sobre quem pode alterar as permissões de acesso, protegendo os dados contra acessos indevidos. | TBD | TBD |
| Implemente criptografia em Buckets S3 usando SSE ou AWS KMS com CMKs | Proteger os dados em repouso nos buckets S3 é crucial para evitar acesso não autorizado e violações de dados. A criptografia SSE-S3 oferece uma solução gerenciada pela AWS, enquanto o AWS KMS com CMKs proporciona controle adicional sobre as chaves de criptografia e segurança melhorada, sendo a opção recomendada para organizações que necessitam de maior controle sobre a segurança dos dados. | TBD | TBD |
| Proibir acesso cross-account desconhecido em todos os buckets S3 através das políticas de bucket para evitar compartilhamento não intencional de dados com entidades externas. | Restringir o acesso cross-account apenas a entidades AWS confiáveis é crucial para proteger os dados contra acessos não autorizados e garantir a conformidade com padrões de segurança como PCI, APRA, MAS, e NIST. A configuração adequada de políticas de bucket impede vazamentos de dados e acesso indevido. | TBD | TBD |
| Garanta Uso de HTTPS/SSL em Todas as Comunicações S3 | Utilizar HTTPS/SSL para comunicações entre clientes e o S3 é essencial para garantir a segurança dos dados em trânsito. Isso protege os dados contra interceptações e adulterações ao criptografá-los durante a transmissão, mantendo a confidencialidade e a integridade dos dados. | TBD | TBD |

## Detalhamento dos Controles

Garanta que o acesso ao Amazon S3 seja concedido exclusivamente por meio de IAM Roles.

* Controle ID: S3\_001
* Racional: A utilização de IAM Roles para conceder acesso ao Amazon S3 é uma prática segura e recomendada, garantindo que apenas permissões necessárias sejam atribuídas de forma controlada e auditável.
* Riscos Mitigados:
  + Concessão de permissões inadequadas ou excessivas.
  + Acesso não autorizado aos recursos do S3.
* Auditoria:
  + Acesse o console do AWS IAM.
  + Na seção de navegação, escolha "Roles" (Funções).
  + Utilize o campo de busca para encontrar roles específicas que possuem permissões para acessar o S3.
  + Selecione uma role para abrir a página de detalhes.
  + Na aba "Permissions" (Permissões), verifique se as políticas anexadas permitem as ações necessárias apenas nos recursos do S3 necessários, sem conceder permissões excessivas.
  + Certifique-se de que não existem políticas que concedam acesso completo ao S3, a menos que seja absolutamente necessário.
* Remediação:
  + No console do AWS IAM, escolha "Roles" (Funções) na seção de navegação.
  + Para editar uma role existente, selecione-a e vá para a aba "Permissions" (Permissões).
  + Clique em "Attach policies" (Anexar políticas) ou "Edit policy" (Editar política) para modificar as permissões.
  + Utilize o editor de políticas para adicionar ou remover permissões específicas para o S3. Garanta que as políticas limitem o acesso apenas aos recursos necessários e às ações específicas exigidas pela aplicação ou usuário.
  + Para criar uma nova role, clique em "Create role" (Criar função), selecione o tipo de serviço que usará a role, por exemplo, EC2, e então configure as permissões específicas para o S3 durante a criação.
* Referências: Amazon S3 Security and Data Protection, AWS - Security best practices for Amazon S3

Garanta que todo acesso ao Amazon S3 seja realizado via Amazon S3 VPC Endpoints, AWS Direct Connect ou VPN, proibindo o acesso direto via internet.

* Controle ID: S3\_002
* Racional: A utilização de Amazon S3 VPC Endpoints, juntamente com AWS Direct Connect ou VPN, proporciona uma conexão segura e privada, aumentando a segurança ao eliminar a exposição através da internet pública.
* Riscos Mitigados:
  + Intercepção de dados durante a transmissão.
  + Acesso não autorizado através de conexões inseguras.
* Auditoria:
  + Acesse o console da Amazon VPC.
  + Na seção de navegação, escolha "Endpoints" (Pontos de extremidade).
  + Verifique na lista de endpoints se existem endpoints do tipo "Gateway" ou "Interface" associados ao Amazon S3.
  + Para cada endpoint do S3 encontrado, selecione-o para visualizar os detalhes, como as sub-redes associadas e as políticas de endpoint.
  + Certifique-se de que os endpoints do S3 estão corretamente associados às sub-redes e VPCs adequadas, e que as políticas de endpoint permitem o acesso apropriado ao S3.
* Remediação:
  + No console da Amazon VPC, escolha "Endpoints" (Pontos de extremidade) na seção de navegação.
  + Clique em "Create Endpoint" (Criar ponto de extremidade).
  + Selecione "AWS Services" (Serviços AWS) para o tipo de serviço e escolha o serviço Amazon S3.
  + Selecione a VPC na qual o endpoint será criado e configure as sub-redes que terão acesso ao endpoint.
  + Configure as configurações de roteamento para permitir a comunicação entre as sub-redes e o endpoint do S3.
  + Revise e aplique as políticas de endpoint, assegurando que elas permitam o acesso necessário ao S3 sem expor recursos desnecessariamente.
  + Clique em "Create" (Criar) para finalizar a configuração do endpoint do S3.
* Referências: Amazon S3 Security and Data Protection, AWS - Security best practices for Amazon S3

Implemente o uso do Amazon S3 Inventory para facilitar a auditoria de objetos armazenados.

* Controle ID: S3\_003
* Racional: O Amazon S3 Inventory provê relatórios detalhados dos objetos armazenados no S3, possibilitando uma auditoria eficaz e garantindo o cumprimento das políticas de gestão de dados.
* Riscos Mitigados:
  + Não conformidade com as políticas de dados.
  + Falta de visibilidade sobre os dados armazenados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket para o qual você deseja verificar o S3 Inventory.
  + Na aba "Management" (Gerenciamento), procure pela seção "Inventory" (Inventário).
  + Verifique se há configurações de inventário existentes para este bucket. Se houver, analise os detalhes para confirmar que estão configurados para gerar relatórios conforme esperado.
  + Verifique se os relatórios estão sendo entregues no intervalo especificado e se contêm as informações necessárias para a auditoria.
* Remediação:
  + No console do S3, selecione o bucket que você deseja configurar o S3 Inventory.
  + Vá para a aba "Management" (Gerenciamento) e depois para a seção "Inventory" (Inventário).
  + Clique em "Add new" (Adicionar novo) para criar uma nova configuração de inventário.
  + Defina um nome para a configuração do inventário e especifique o formato do arquivo de saída (CSV, ORC ou Parquet).
  + Escolha a frequência de geração do relatório (diária ou semanal) e os campos de objeto que devem ser incluídos no relatório.
  + Configure o bucket de destino onde os relatórios de inventário serão armazenados.
  + Revise as configurações e salve para iniciar a geração regular de relatórios de inventário.
* Referências: Amazon S3 Security and Data Protection

Implemente o monitoramento de acesso aos dados utilizando logs de acesso do servidor S3.

* Controle ID: S3\_004
* Racional: Os logs de acesso do servidor S3 registram detalhadamente as solicitações feitas ao S3, permitindo uma vigilância efetiva e a análise do acesso aos dados, ajudando a detectar e responder a acessos não autorizados.
* Riscos Mitigados:
  + Acesso não autorizado.
  + Falta de visibilidade sobre os padrões de acesso.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket para o qual você deseja verificar o logging de acesso do servidor.
  + Na aba "Properties" (Propriedades), procure pela seção "Server access logging" (Logging de acesso do servidor).
  + Verifique se o logging está habilitado. Se estiver habilitado, você verá o bucket de destino onde os logs estão sendo armazenados.
* Remediação:
  + No console do S3, selecione o bucket para o qual você deseja habilitar o logging de acesso do servidor.
  + Vá para a aba "Properties" (Propriedades) e localize a seção "Server access logging" (Logging de acesso do servidor).
  + Clique em "Edit" (Editar) para modificar as configurações de logging.
  + Habilite o logging, especificando o bucket de destino onde os logs de acesso serão armazenados. É recomendável usar um bucket diferente do bucket de origem para os logs.
  + Opcionalmente, você pode definir um prefixo para os logs, o que ajudará na organização e na identificação dos logs gerados.
  + Salve as configurações para habilitar o logging de acesso do servidor.
* Referências:
  + Amazon S3 Security and Data Protection
  + AWS Security Best Practices and Guidelines for Amazon S3
  + AWS - Security Best Practices for Amazon S3

Desative as ACLs no Amazon S3 para simplificar o gerenciamento de permissões e reduzir o risco de erros.

* Controle ID: S3\_005
* Racional: Desabilitar as ACLs em favor de políticas de bucket simplifica as configurações de permissão e minimiza a possibilidade de erros que podem levar à exposição não intencional de dados.
* Riscos Mitigados:
  + Configuração incorreta de permissões.
  + Exposição potencial de dados sensíveis.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione cada bucket para revisar suas configurações.
  + Verifique na aba "Permissions" (Permissões) de cada bucket se as ACLs estão desativadas. Isto é indicado pela ausência de ACLs listadas ou pela configuração que mostra que as ACLs não estão sendo utilizadas.
  + Repita o processo para todos os buckets da conta para assegurar que nenhuma ACL está ativa.
* Remediação:
  + No console do S3, selecione o bucket para o qual você deseja desabilitar as ACLs.
  + Na aba "Permissions" (Permissões), procure por "Access Control List (ACL)".
  + Se houver opção para desabilitar as ACLs, faça isso. Se não, certifique-se de que nenhuma permissão está concedida através das ACLs.
  + Considere usar a política de bucket para gerenciar as permissões em vez de ACLs, pois isso fornece um modelo de permissão mais simplificado e centralizado.
  + Aplique essa configuração para todos os buckets e objetos no S3 para garantir uma política consistente de não utilização de ACLs.
* Referências: AWS - Security best practices for Amazon S3

Configure a propriedade do objeto no Amazon S3 para "Bucket Owner Preferred" ou "Object Writer" para desabilitar o uso de ACLs em novos objetos.

* Controle ID: S3\_006
* Racional: Configurar a propriedade do objeto em buckets S3 ajuda a gerenciar as permissões de forma centralizada e segura, eliminando a necessidade de usar ACLs, o que pode reduzir erros de configuração e vazamentos de dados.
* Riscos Mitigados:
  + Erros de configuração de ACL.
  + Vazamento de dados devido a permissões mal configuradas.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket desejado e navegue até a aba "Permissions" (Permissões).
  + Procure por uma configuração chamada "Object Ownership" (Propriedade do Objeto) ou similar, que pode estar na seção de permissões avançadas.
  + Verifique se a propriedade do objeto está configurada para "Bucket Owner Preferred" ou "Object Writer" que são as configurações que efetivamente desabilitam o uso de ACLs para novos objetos.
* Remediação:
  + No console do S3, selecione o bucket no qual você deseja desabilitar as ACLs.
  + Vá para a aba "Permissions" (Permissões) e localize a seção "Object Ownership" (Propriedade do Objeto).
  + Escolha a opção "Bucket Owner Preferred" ou "Object Writer" para garantir que as permissões sejam gerenciadas sem a necessidade de ACLs. Esta configuração aplica-se a todos os objetos novos adicionados ao bucket.
  + Salve as alterações para aplicar a configuração. Isso garante que as ACLs não sejam utilizadas para controlar as permissões dos objetos dentro deste bucket.
* Referências: AWS - Security best practices for Amazon S3

Implemente o bloqueio completo de acesso público aos buckets do Amazon S3, incluindo uma política organizacional para garantir uma abordagem uniforme.

* Controle ID: S3\_007
* Racional: Bloquear o acesso público aos buckets S3 é crucial para prevenir a exposição acidental de dados sensíveis e proteger contra ataques cibernéticos. Aplicar essa política em nível de organização ou conta garante uma proteção abrangente e uniforme.
* Riscos Mitigados:
  + Exposição acidental de dados sensíveis.
  + Ataques cibernéticos resultantes de acessos públicos não autorizados.
* Procedimento de Auditoria:
  + Acesse o console de gerenciamento da AWS.
  + Verifique se a política de bloqueio de acesso público está configurada e ativa para a organização ou conta.
  + Revise a lista de buckets individualmente no console do Amazon S3.
  + Na aba "Permissions" (Permissões), verifique em cada bucket se todas as opções de bloqueio de acesso público estão habilitadas.
* Procedimento de Remediação:
  + No console de gerenciamento da AWS, configure a política de bloqueio de acesso público em nível de conta ou organização para garantir que todos os buckets sejam protegidos por padrão.
  + No console do Amazon S3, selecione cada bucket individualmente para revisão:
    - Navegue até a aba "Permissions" (Permissões) e localize a seção "Block public access" (Bloquear acesso público).
    - Habilite todas as opções disponíveis para garantir que nenhum acesso público seja possível. Isso inclui:
      * Bloquear novas permissões de ACL públicas.
      * Remover permissões de ACL públicas existentes.
      * Bloquear novas políticas de bucket públicas.
      * Remover políticas de bucket públicas existentes.
  + Salve as configurações para aplicar o bloqueio de acesso público. Repita esse processo para todos os buckets na sua conta para garantir que nenhum deles esteja exposto ao acesso público inadvertidamente.
* Referências:
  + AWS - Security Best Practices for Amazon S3
  + AWS Security Best Practices and Guidelines for Amazon S3
  + AWS Top 10 security best practices for securing data in Amazon S3

Utilize o Amazon Macie para identificar e proteger dados sensíveis nos buckets do S3.

* Controle ID: S3\_008
* Racional: O Amazon Macie é uma ferramenta essencial para a detecção automática de dados sensíveis, auxiliando na prevenção de exposições e vazamentos e na manutenção da conformidade com regulamentos de proteção de dados.
* Riscos Mitigados:
  + Vazamento de dados sensíveis.
  + Não conformidade com regulamentos de proteção de dados.
* Auditoria:
  + Acesse o console do Amazon Macie.
  + Verifique se o serviço está ativado para sua conta AWS.
  + Confira se há trabalhos de varredura criados e em execução que monitoram os buckets do S3 para detectar dados sensíveis.
  + Revise os resultados das varreduras para identificar quaisquer dados sensíveis ou padrões de uso que possam representar riscos.
* Remediação:
  + No console do Amazon Macie, ative o serviço, se ainda não estiver ativo.
  + Configure o Macie para iniciar a varredura dos buckets do S3 em busca de dados sensíveis. Isso inclui a criação de trabalhos de descoberta de dados que especificam quais buckets do S3 devem ser varridos.
  + Defina parâmetros de varredura, como frequência de varredura e tipos de dados a serem identificados.
  + Monitore os resultados das varreduras de dados sensíveis fornecidos pelo Macie para tomar ações corretivas, como mover dados sensíveis para locais mais seguros, aplicar criptografia adicional ou ajustar as políticas de acesso.
* Referências: AWS - Security best practices for Amazon S3, AWS Top 10 security best practices for securing data in Amazon S3

Ative e configure a proteção do S3 em GuardDuty para monitorar e alertar sobre atividades suspeitas nos buckets do S3.

* Controle ID: S3\_009
* Racional: Utilizar o Amazon GuardDuty para monitorar os buckets do S3 ajuda a identificar atividades suspeitas ou anormais, melhorando significativamente a postura de segurança e prevenindo possíveis ataques.
* Riscos Mitigados:
  + Atividades suspeitas nos buckets do S3.
  + Ataques potenciais que podem comprometer a integridade e a segurança dos dados.
* Auditoria:
  + Acesse o console do Amazon GuardDuty.
  + Verifique se o serviço está ativado e operando na conta AWS.
  + Na seção de configurações ou no painel de controle do GuardDuty, procure por uma opção relacionada à proteção do S3 ou integrações específicas com o S3.
  + Confirme se a proteção do S3 está ativada e configurada corretamente para monitorar os buckets de interesse.
* Remediação:
  + Se ainda não estiver ativado, inicie o Amazon GuardDuty no console AWS.
  + Navegue até a seção específica do S3 dentro das configurações do GuardDuty.
  + Ative a funcionalidade de proteção do S3 para começar a monitorar atividades suspeitas, como acesso anormal, deletação em massa ou download incomum de dados.
  + Configure as notificações ou alertas para ser informado imediatamente sobre qualquer atividade suspeita detectada.
  + Revise regularmente os achados do GuardDuty para assegurar que você está ciente e pode responder a possíveis ameaças de segurança.
* Referências: AWS Top 10 security best practices for securing data in Amazon S3

Ative o registro de atividades para o S3 usando tanto o AWS CloudTrail quanto o logging de acesso do servidor para criar uma trilha de auditoria detalhada.

* Controle ID: S3\_010
* Racional: A habilitação do registro no S3 usando CloudTrail e logging de acesso do servidor proporciona visibilidade completa sobre as atividades de acesso e modificação, crucial para a detecção e resposta a incidentes de segurança.
* Riscos Mitigados:
  + Atividades maliciosas envolvendo dados no S3.
  + Acesso não autorizado aos buckets do S3.
  + Não conformidade com as políticas de segurança e regulamentações de proteção de dados.
* Auditoria:
  + Acesse o console do AWS CloudTrail.
  + Verifique se o CloudTrail está configurado e ativado.
  + Confirme se os trails estão configurados para registrar eventos do S3.
  + Acesse o console do Amazon S3.
  + Selecione cada bucket para verificar se o logging de acesso do servidor está ativado na aba "Properties" (Propriedades).
* Remediação:
  + No console do CloudTrail:
  + Verifique se existe um trail que inclui eventos de nível de API do S3. Se não, crie um novo trail e certifique-se de incluir os eventos relacionados ao S3.
  + No console do S3, para cada bucket:
  + Vá para a aba "Properties" (Propriedades) e clique em "Server access logging" (Logging de acesso do servidor).
  + Habilite o logging e especifique o bucket onde os logs de acesso devem ser armazenados.
  + Configure opções adicionais, como o prefixo do log, se necessário.
  + Garanta que as configurações de registro no CloudTrail e no S3 sejam suficientes para capturar todas as atividades relevantes e que os logs estejam sendo armazenados de forma segura e acessíveis para análise e auditoria.
* Referências:
* Amazon S3 Security and Data Protection
* AWS Security Best Practices and Guidelines for Amazon S3
* AWS Top 10 security best practices for securing data in Amazon S3
* Trend Micro Best practice rules for Amazon S3

Utilize o AWS Security Hub e o AWS CloudWatch para monitoramento abrangente do Amazon S3, detectando atividades suspeitas e problemas operacionais.

* Controle ID: S3\_011
* Racional: Monitorar o S3 com estas ferramentas permite identificar proativamente eventos de segurança e operacionais, melhorando a segurança e eficiência operacional.
* Riscos Mitigados:
  + Ameaças de segurança e atividades suspeitas envolvendo o S3.
  + Problemas operacionais que podem afetar a integridade e disponibilidade dos dados.
* Auditoria:
  + AWS Security Hub:
    - Acesse o AWS Security Hub.
    - Verifique se está ativado e se há integração com o Amazon S3.
    - Confirme que os benchmarks de segurança específicos para o S3 estão sendo monitorados.
  + AWS CloudWatch:
    - Acesse o AWS CloudWatch.
    - Verifique se os logs de eventos do S3, incluindo logs de acesso e operações via CloudTrail, estão sendo capturados e analisados.
* Remediação:
  + No AWS Security Hub:
    - Ative o AWS Security Hub, caso ainda não esteja ativado.
    - Configure a integração com o Amazon S3.
    - Utilize o AWS Foundational Security Best Practices para configurar benchmarks de segurança que incluam o monitoramento das configurações e atividades do S3.
  + No AWS CloudWatch:
    - Garanta que o AWS CloudTrail está habilitado para capturar eventos de nível de API do S3.
    - Ative o logging de acesso do S3 para todos os buckets relevantes.
    - No CloudWatch, configure grupos de logs e streams para armazenar esses logs.
    - Crie métricas e alarmes com base nos logs para identificar comportamentos anormais, como:
    - Aumento inesperado nas operações de `PutObject` ou `GetObject`.
    - Erros `AccessDenied` que indicam tentativas de acesso não autorizado.
    - Use o CloudWatch Logs Insights para executar consultas ad-hoc em busca de padrões suspeitos ou problemas.
* Referências:
  + AWS Top 10 Security Best Practices for Securing Data in Amazon S3

Assegure que o Grupo de Entrega de Logs S3 não tenha permissão de escrita no bucket de origem do S3, onde o Logging de Acesso do Servidor está ativado.

* Controle ID: S3\_012
* Racional: Prevenir que o Grupo de Entrega de Logs S3 tenha permissões de escrita no bucket de origem ajuda a manter a integridade dos logs ao evitar que sejam alterados ou excluídos após a criação. Isto é essencial para garantir uma trilha de auditoria confiável e para proteger contra manipulações que podem ocultar atividades maliciosas.
* Riscos Mitigados:
  + Alteração ou exclusão maliciosa de logs de acesso.
  + Comprometimento da capacidade de rastrear acessos não autorizados ou outras atividades suspeitas.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket de origem que está armazenando os logs.
  + Na aba "Permissions" (Permissões), verifique as ACLs (Listas de Controle de Acesso) e políticas de bucket para assegurar que as permissões de escrita para o Grupo de Entrega de Logs estejam explicitamente negadas.
* Remediação:
  + No console do S3, selecione o bucket de origem onde os logs são armazenados.
  + Acesse a aba "Permissions" (Permissões) e então vá para "Bucket Policy" (Política de Bucket).
  + Adicione uma política para negar explicitamente as permissões de escrita (`s3:PutObject`) para o Grupo de Entrega de Logs do S3.

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Deny",  "Principal": {  "Service": "delivery.logs.amazonaws.com"  },  "Action": "s3:PutObject",  "Resource": "arn:aws:s3:::nome-do-bucket/\*"  }  ]  } |

* + Substitua `nome-do-bucket` pelo nome real do seu bucket de logs.
  + Salve as alterações na política de bucket para garantir que as permissões de escrita sejam negadas ao Grupo de Entrega de Logs.
* Referências: Trend Micro Best practice rules for Amazon S3

Proíba o acesso 'FULL\_CONTROL' tanto a usuários autenticados quanto a usuários públicos em todos os buckets S3 para prevenir controle total não autorizado e garantir a segurança dos dados.

* Controle ID: S3\_013
* Racional: Limitar o acesso 'FULL\_CONTROL' ajuda a prevenir alterações e exclusões não autorizadas nos buckets S3, protegendo contra acessos maliciosos e garantindo a integridade e segurança dos dados armazenados. Proibir esses acessos tanto para usuários autenticados quanto públicos fortalece a política de segurança e minimiza riscos de exposição e manipulação de dados.
* Riscos Mitigados:
  + Acesso não autorizado aos dados.
  + Alterações não autorizadas nos buckets S3.
  + Exclusão de dados críticos.
* Auditoria:
  + Acesse o console do Amazon S3 em https://console.aws.amazon.com/s3/.
  + Selecione cada bucket para revisar suas permissões.
  + Na aba "Permissions", verifique as políticas de bucket e ACLs para garantir que não concedam acesso 'FULL\_CONTROL' a usuários autenticados ou públicos.
  + Especificamente, verifique as configurações em "Block public access" (Bloquear acesso público) para confirmar que estão ativadas, proibindo qualquer acesso público.
* Remediação:
  + No console do Amazon S3, para cada bucket:
    - Acesse a aba "Permissions".
    - Ative todos os bloqueios em "Block public access" (Bloquear acesso público) e revise as ACLs e políticas de bucket.
    - Assegure que as políticas de bucket neguem explicitamente o acesso 'FULL\_CONTROL' tanto a usuários autenticados quanto públicos, utilizando a seguinte política:

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Deny",  "Principal": "\*",  "Action": "s3:\*",  "Resource": "arn:aws:s3:::<nome-do-bucket>/\*",  "Condition": {"StringEquals": {"aws:PrincipalType": ["AuthenticatedUser", "Public"]}}  }  ]  } |

* + - Substitua `<nome-do-bucket>` pelo nome real do seu bucket.
    - Salve as modificações para garantir que as restrições de acesso sejam aplicadas.
* Referências:
  + Trend Micro Best Practice Rules for Amazon S3

Proíba o acesso 'READ' tanto a usuários autenticados quanto a usuários públicos em todos os buckets S3 para prevenir leitura não autorizada e garantir a segurança dos dados.

* Controle ID: S3\_014
* Racional: Limitar o acesso 'READ' ajuda a prevenir acessos não autorizados e vazamento de informações nos buckets S3. Proibir esses acessos tanto para usuários autenticados quanto públicos fortalece a política de segurança e minimiza riscos de exposição e manipulação de dados.
* Riscos Mitigados:
  + Acesso não autorizado a dados sensíveis.
  + Vazamento de informações.
* Auditoria:
  + Acesse o console do Amazon S3 em https://console.aws.amazon.com/s3/.
  + Selecione cada bucket e revise as políticas de bucket e ACLs para verificar se o acesso 'READ' está proibido para usuários autenticados e usuários públicos.
  + Na aba "Permissions", verifique a seção "Block public access" para confirmar que todas as opções de bloqueio de acesso público 'READ' estão ativadas.
* Remediação:
  + No console do Amazon S3, para cada bucket:
    - Acesse a aba "Permissions".
    - Ajuste as configurações em "Block public access" para garantir que todas as formas de acesso público 'READ' estejam bloqueadas.
    - Revise e ajuste as ACLs e políticas de bucket para garantir que o acesso 'READ' não seja permitido a usuários autenticados ou públicos.
    - Implemente políticas de bucket para negar explicitamente o acesso 'READ' a todos os usuários autenticados e públicos, utilizando a seguinte política:

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Deny",  "Principal": "\*",  "Action": "s3:GetObject",  "Resource": "arn:aws:s3:::<nome-do-bucket>/\*",  "Condition": {"Bool": {"aws:public": "true"}}  },  {  "Effect": "Deny",  "Principal": "\*",  "Action": "s3:GetObject",  "Resource": "arn:aws:s3:::<nome-do-bucket>/\*",  "Condition": {"StringEquals": {"aws:PrincipalType": "AuthenticatedUser"}}  }  ]  } |

* + - Substitua `<nome-do-bucket>` pelo nome real do seu bucket.
    - Salve as modificações para garantir que as restrições de acesso sejam aplicadas.
* Referências:
  + Trend Micro Best Practice Rules for Amazon S3

Proíba o acesso 'READ\_ACP' tanto a usuários autenticados quanto a usuários públicos em todos os buckets S3 para impedir o acesso não autorizado às configurações de permissões do bucket.

* Controle ID: S3\_015
* Racional: Limitar o acesso 'READ\_ACP' ajuda a prevenir a exposição não autorizada das configurações de segurança e permissões dos buckets S3. Proibir esses acessos tanto para usuários autenticados quanto públicos fortalece a política de segurança e minimiza riscos de manipulação e vazamentos de informações críticas.
* Riscos Mitigados:
  + Exposição das configurações de segurança e permissões.
  + Acesso não autorizado às configurações de ACL, que pode levar a brechas de segurança.
* Auditoria:
  + Acesse o console do Amazon S3 em https://console.aws.amazon.com/s3/.
  + Selecione cada bucket e revise as políticas de bucket e ACLs para verificar se o acesso 'READ\_ACP' está proibido para usuários autenticados e usuários públicos.
  + Na aba "Permissions", verifique a seção "Block public access" para confirmar que todas as opções de bloqueio de acesso público 'READ\_ACP' estão ativadas.
* Remediação:
  + No console do Amazon S3, para cada bucket:
    - Acesse a aba "Permissions".
    - Ajuste as configurações em "Block public access" para garantir que todas as formas de acesso público e autenticado 'READ\_ACP' estejam bloqueadas.
    - Revise e ajuste as ACLs e políticas de bucket para garantir que o acesso 'READ\_ACP' não seja permitido a usuários autenticados ou públicos.
    - Implemente políticas de bucket para negar explicitamente o acesso 'READ\_ACP' a todos os usuários autenticados e públicos, utilizando a seguinte política:

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Deny",  "Principal": "\*",  "Action": "s3:GetBucketAcl",  "Resource": "arn:aws:s3:::<nome-do-bucket>/\*",  "Condition": {"Bool": {"aws:public": "true"}}  },  {  "Effect": "Deny",  "Principal": "\*",  "Action": "s3:GetBucketAcl",  "Resource": "arn:aws:s3:::<nome-do-bucket>/\*",  "Condition": {"StringEquals": {"aws:PrincipalType": "AuthenticatedUser"}}  }  ]  } |

* + - Substitua `<nome-do-bucket>` pelo nome real do seu bucket.
    - Salve as modificações para garantir que as restrições de acesso sejam aplicadas.
* Referências:
  + Trend Micro Best Practice Rules for Amazon S3

Proíba o acesso 'WRITE' tanto a usuários autenticados quanto a usuários públicos em todos os buckets S3 para impedir alterações não autorizadas, sobrescrita ou adição de dados.

* Controle ID: S3\_016
* Racional: Limitar o acesso 'WRITE' ajuda a prevenir modificações não autorizadas, adição ou exclusão de dados nos buckets S3. Proibir esses acessos tanto para usuários autenticados quanto públicos fortalece a política de segurança e minimiza riscos de manipulação de dados.
* Riscos Mitigados:
  + Modificação não autorizada de dados.
  + Sobrescrita e adição não autorizada de arquivos.
  + Exposição de dados sensíveis devido ao acesso não autorizado.
* Auditoria:
  + Acesse o console do Amazon S3 em https://console.aws.amazon.com/s3/.
  + Selecione cada bucket e revise as políticas de bucket e ACLs para verificar se o acesso 'WRITE' está proibido tanto para usuários autenticados quanto para usuários públicos.
  + Na aba "Permissions", verifique a seção "Block public access" para confirmar que todas as opções de bloqueio de acesso público 'WRITE' estão ativadas.
* Remediação:
  + No console do Amazon S3, para cada bucket:
    - Acesse a aba "Permissions".
    - Ajuste as configurações em "Block public access" para garantir que todas as formas de acesso público e autenticado 'WRITE' estejam bloqueadas.
    - Revise e ajuste as ACLs e políticas de bucket para garantir que o acesso 'WRITE' não seja permitido a usuários autenticados ou públicos.
    - Implemente políticas de bucket para negar explicitamente o acesso 'WRITE' a todos os usuários autenticados e públicos, utilizando a seguinte política:

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Deny",  "Principal": "\*",  "Action": ["s3:PutObject", "s3:DeleteObject"],  "Resource": "arn:aws:s3:::<nome-do-bucket>/\*",  "Condition": {"StringEquals": {"aws:PrincipalType": "AuthenticatedUser"}}  },  {  "Effect": "Deny",  "Principal": "\*",  "Action": ["s3:PutObject", "s3:DeleteObject"],  "Resource": "arn:aws:s3:::<nome-do-bucket>/\*",  "Condition": {"Bool": {"aws:public": "true"}}  }  ]  } |

* + - Substitua `<nome-do-bucket>` pelo nome real do seu bucket.
    - Salve as modificações para garantir que as restrições de acesso sejam aplicadas.
* Referências:
  + Trend Micro Best Practice Rules for Amazon S3

Proíba o acesso público 'WRITE\_ACP' aos buckets S3 para evitar alterações não autorizadas nas configurações de permissões.

* Controle ID: S3\_017
* Racional: Proibir o acesso público 'WRITE\_ACP' aos buckets S3 é essencial para prevenir modificações não autorizadas nas configurações de permissões e segurança. Isso ajuda a manter o controle sobre quem pode alterar as permissões de acesso, protegendo os dados contra acessos indevidos.
* Riscos Mitigados:
  + Alterações não autorizadas nas permissões e configurações de segurança dos buckets.
  + Potencial comprometimento das políticas de segurança do bucket.
* Auditoria:
  + Acesse o console do Amazon S3 em https://console.aws.amazon.com/s3/.
  + Selecione o bucket que deseja verificar.
  + Na aba "Permissions", verifique a seção "Block public access" para certificar-se de que todas as opções para bloquear acesso público estão ativadas, incluindo as que impedem especificamente o acesso 'WRITE\_ACP' público.
  + Analise as ACLs e as políticas do bucket para garantir que não concedam permissão 'WRITE\_ACP' a usuários públicos.
* Remediação:
  + No console do Amazon S3, navegue até o bucket em questão.
  + Na aba "Permissions", ative os bloqueios em "Block public access" para garantir que qualquer forma de acesso 'WRITE\_ACP' público esteja proibida.
  + Modifique as ACLs do bucket para eliminar qualquer permissão 'WRITE\_ACP' que possa ter sido concedida a usuários públicos.
  + Verifique e ajuste as políticas do bucket para assegurar que não permitam acesso 'WRITE\_ACP' público. Adicione ou atualize políticas de bucket para incluir uma negação explícita para esse acesso, por exemplo:

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Deny",  "Principal": "\*",  "Action": "s3:PutBucketAcl",  "Resource": "arn:aws:s3:::<nome-do-bucket>/\*",  "Condition": {"Bool": {"aws:public": "true"}}  }  ]  } |

* + Substitua `<nome-do-bucket>` pelo nome real do seu bucket.
  + Salve as alterações para aplicar as restrições e impedir o acesso 'WRITE\_ACP' público.
* Referências:
  + Trend Micro Best Practice Rules for Amazon S3

Implemente criptografia em Buckets S3 usando SSE ou AWS KMS com CMKs

* Controle ID: S3\_018
* Racional: Proteger os dados em repouso nos buckets S3 é crucial para evitar acesso não autorizado e violações de dados. A criptografia SSE-S3 oferece uma solução gerenciada pela AWS, enquanto o AWS KMS com CMKs proporciona controle adicional sobre as chaves de criptografia e segurança melhorada, sendo a opção recomendada para organizações que necessitam de maior controle sobre a segurança dos dados.
* Riscos Mitigados:
  + Acesso não autorizado a dados em repouso.
  + Violações de dados.
  + Falhas de compliance relacionadas à segurança dos dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que deseja verificar.
  + Na aba 'Propriedades', verifique a seção de criptografia para confirmar se a criptografia está habilitada.
  + Determine se o bucket usa SSE-S3 ou AWS KMS com CMKs, de acordo com as necessidades de segurança e compliance da organização.
* Remediação:
  + Para SSE-S3:
    - No console do S3, selecione o bucket desejado.
    - Vá até a aba 'Propriedades'.
    - Na seção de criptografia, ative a opção 'Amazon S3-managed keys (SSE-S3)'.
  + Para AWS KMS com CMKs:
    - No console do S3, selecione o bucket desejado.
    - Acesse a aba 'Propriedades'.
    - Na seção de criptografia, escolha 'AWS Key Management Service key (SSE-KMS)'.
    - Selecione uma CMK gerenciada pelo cliente para a criptografia ou crie uma nova CMK.
  + Recomendação: Apesar de a criptografia SSE-S3 atender a muitos cenários, a utilização de AWS KMS com CMKs é aconselhada para organizações que buscam maior controle sobre a criptografia, incluindo rotação de chaves e definição de políticas de acesso detalhadas.
* Referências:
  + Amazon S3 Security and Data Protection
  + Trend Micro Best practice rules for Amazon S3

Proibir acesso cross-account desconhecido em todos os buckets S3 através das políticas de bucket para evitar compartilhamento não intencional de dados com entidades externas.

* Controle ID: S3\_019
* Racional: Restringir o acesso cross-account apenas a entidades AWS confiáveis é crucial para proteger os dados contra acessos não autorizados e garantir a conformidade com padrões de segurança como PCI, APRA, MAS, e NIST. A configuração adequada de políticas de bucket impede vazamentos de dados e acesso indevido.
* Riscos Mitigados:
  + Vazamento de dados.
  + Acesso não autorizado.
  + Não conformidade com regulamentações de proteção de dados.
* Auditoria:
  + Acesse o console do Amazon S3 em https://console.aws.amazon.com/s3/.
  + Selecione o bucket que deseja auditar.
  + Na aba 'Permissões', vá para 'Políticas de bucket'.
  + Revise a política do bucket para verificar se há alguma permissão que permita acesso cross-account que não seja de entidades conhecidas e autorizadas. Verifique especialmente por declarações `Allow` que não incluam os AWS account IDs ou ARNs confiáveis.
* Remediação:
  + No console do Amazon S3, selecione o bucket que precisa de ajustes nas políticas.
  + Acesse a aba 'Permissões' e depois 'Políticas de bucket'.
  + Modifique a política do bucket para remover ou explicitamente negar permissões que permitam acesso cross-account desconhecido. Adicione uma declaração de `Deny` para entidades externas não autorizadas, considerando os AWS account IDs ou ARNs confiáveis definidos previamente na sua configuração de conformidade. Por exemplo:

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Deny",  "Principal": {  "AWS": "\*"  },  "Action": "s3:\*",  "Resource": "arn:aws:s3:::<nome-do-bucket>/\*",  "Condition": {  "StringNotEquals": {  "aws:PrincipalAccount": ["123456789012", "210987654321"]  }  }  }  ]  } |

* + Substitua `<nome-do-bucket>` pelo nome real do seu bucket e inclua os IDs de conta AWS confiáveis.
  + Salve as alterações para garantir que todas as permissões de acesso cross-account na política do bucket sejam necessárias, autorizadas, e qualquer acesso não reconhecido ou não autorizado seja claramente negado.
* Referências:
  + Trend Micro Best Practice Rules for Amazon S3
  + AWS Documentation on S3 Security and Data Protection
  + Compliance standards documentation (PCI, APRA, MAS, NIST)
  + AWS Well-Architected Framework

Garanta Uso de HTTPS/SSL em Todas as Comunicações S3

* Controle ID: S3\_020
* Racional: Utilizar HTTPS/SSL para comunicações entre clientes e o S3 é essencial para garantir a segurança dos dados em trânsito. Isso protege os dados contra interceptações e adulterações ao criptografá-los durante a transmissão, mantendo a confidencialidade e a integridade dos dados.
* Riscos Mitigados:
  + Interceptação de dados em trânsito.
  + Comprometimento da integridade e confidencialidade dos dados.
* Auditoria:
  + Acesse o console do Amazon S3 em https://console.aws.amazon.com/s3/.
  + Para cada bucket, vá para a aba 'Permissões' e depois 'Políticas de bucket'.
  + Verifique as políticas de bucket para assegurar que haja uma condição que exija o uso de HTTPS/SSL para todas as transferências de dados.
* Remediação:
  + No console do Amazon S3, acesse cada bucket que precisa ser configurado.
  + Na aba 'Permissões', selecione 'Políticas de bucket'.
  + Adicione ou modifique as políticas de bucket para incluir uma condição que força o uso de HTTPS/SSL para todas as comunicações. Isso pode ser feito adicionando uma declaração que nega o acesso quando a conexão não estiver usando HTTPS/SSL, como:

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Deny",  "Principal": "\*",  "Action": "s3:\*",  "Resource": "arn:aws:s3:::<nome-do-bucket>/\*",  "Condition": {"Bool": {"aws:SecureTransport": "false"}}  }  ]  } |

* + Substitua `<nome-do-bucket>` pelo nome real do seu bucket.
  + Salve as alterações para garantir que todas as conexões com o S3 sejam realizadas exclusivamente via HTTPS/SSL.
* Referências:
  + Trend Micro Best Practices for Keeping Amazon S3 Buckets Secure

## Histórico de alterações

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data de Publicação** | **Descrição** | **Alterações** |
| 1.0 | 14/04/2024 | Inclusão inicial de controles de segurança para S3 | * Controles incluídos:   + Garanta que o acesso ao Amazon S3 seja concedido exclusivamente por meio de IAM Roles. - Controle ID: S3\_001   + Garanta que todo acesso ao Amazon S3 seja realizado via Amazon S3 VPC Endpoints, AWS Direct Connect ou VPN, proibindo o acesso direto via internet. - Controle ID: S3\_002   + Implemente o uso do Amazon S3 Inventory para facilitar a auditoria de objetos armazenados. - Controle ID: S3\_003   + Implemente o monitoramento de acesso aos dados utilizando logs de acesso do servidor S3. - Controle ID: S3\_004   + Desative as ACLs no Amazon S3 para simplificar o gerenciamento de permissões e reduzir o risco de erros. - Controle ID: S3\_005   + Configure a propriedade do objeto no Amazon S3 para "Bucket Owner Preferred" ou "Object Writer" para desabilitar o uso de ACLs em novos objetos. - Controle ID: S3\_006   + Implemente o bloqueio completo de acesso público aos buckets do Amazon S3, incluindo uma política organizacional para garantir uma abordagem uniforme. - Controle ID: S3\_007   + Utilize o Amazon Macie para identificar e proteger dados sensíveis nos buckets do S3. - Controle ID: S3\_008   + Ative e configure a proteção do S3 em GuardDuty para monitorar e alertar sobre atividades suspeitas nos buckets do S3. - Controle ID: S3\_009   + Ative o registro de atividades para o S3 usando tanto o AWS CloudTrail quanto o logging de acesso do servidor para criar uma trilha de auditoria detalhada. - Controle ID: S3\_010   + Utilize o AWS Security Hub e o AWS CloudWatch para monitoramento abrangente do Amazon S3, detectando atividades suspeitas e problemas operacionais. - Controle ID: S3\_011   + Assegure que o Grupo de Entrega de Logs S3 não tenha permissão de escrita no bucket de origem do S3, onde o Logging de Acesso do Servidor está ativado. - Controle ID: S3\_012   + Proíba o acesso 'FULL\_CONTROL' tanto a usuários autenticados quanto a usuários públicos em todos os buckets S3 para prevenir controle total não autorizado e garantir a segurança dos dados. - Controle ID: S3\_013   + Proíba o acesso 'READ' tanto a usuários autenticados quanto a usuários públicos em todos os buckets S3 para prevenir leitura não autorizada e garantir a segurança dos dados. - Controle ID: S3\_014   + Proíba o acesso 'READ\_ACP' tanto a usuários autenticados quanto a usuários públicos em todos os buckets S3 para impedir o acesso não autorizado às configurações de permissões do bucket. - Controle ID: S3\_015   + Proíba o acesso 'WRITE' tanto a usuários autenticados quanto a usuários públicos em todos os buckets S3 para impedir alterações não autorizadas, sobrescrita ou adição de dados. - Controle ID: S3\_016   + Proíba o acesso público 'WRITE\_ACP' aos buckets S3 para evitar alterações não autorizadas nas configurações de permissões. - Controle ID: S3\_017   + Implemente criptografia em Buckets S3 usando SSE ou AWS KMS com CMKs - Controle ID: S3\_018   + Proibir acesso cross-account desconhecido em todos os buckets S3 através das políticas de bucket para evitar compartilhamento não intencional de dados com entidades externas. - Controle ID: S3\_019   + Garanta Uso de HTTPS/SSL em Todas as Comunicações S3 - Controle ID: S3\_020 * Controles excluídos: <TBD> * Controles alterados: <TBD> |

## Referencias para consulta

* Amazon S3 Security and Data Protection: https://d1.awsstatic.com/product-marketing/S3/Amazon\_s3\_Security\_and\_Data\_Protection\_Tools\_and\_Best\_Practices.pdf
* AWS Security Best Practices and Guidelines for Amazon S3: https://d1.awsstatic.com/product-marketing/S3/Amazon\_S3\_Security\_eBook\_2020.pdf
* Trend Micro Best practice rules for Amazon S3: https://www.trendmicro.com/cloudoneconformity-staging/knowledge-base/aws/S3/
* AWS - Security best practices for Amazon S3: https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html
* Trend Micro 10 best practices for S3 bucket security configuration: https://www.trendmicro.com/pt\_br/devops/22/c/best-practices-s3-buckets-security-configurations.html
* AWS - Top 10 security best practices for securing data in Amazon S3: https://aws.amazon.com/pt/blogs/security/top-10-security-best-practices-for-securing-data-in-amazon-s3/
* Trend Micro Best Practices for Keeping Amazon S3 Buckets Secure: https://www.trendmicro.com/en\_us/devops/21/b/best-practices-for-keeping-amazon-s3-buckets-secure.html
* AWS repost How can I secure the files in my Amazon S3 bucket?: https://repost.aws/knowledge-center/secure-s3-resources