# 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.

Amazon S3 é amplamente utilizado para uma variedade de casos de uso, incluindo backup e recuperação, arquivamento, data lakes, sites de hospedagem, aplicações móveis e aplicações empresariais. Ele se destaca pela sua capacidade de gerenciar grandes volumes de dados, sua segurança robusta, a capacidade de gerenciamento de acesso e a integração com outros serviços da AWS. O serviço é conhecido por sua durabilidade e redundância de dados, garantindo que os objetos de dados sejam armazenados com segurança em múltiplos dispositivos em várias instalações e possam ser acessados a qualquer momento.

## 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 |
| Utilizar IAM roles para acesso ao S3 | As roles do IAM proporcionam uma forma segura de conceder permissões necessárias para que as aplicações e usuários acessem os recursos do S3. | TBD | TBD |
| Utilizar Amazon S3 VPC endpoints | Os VPC endpoints permitem que você conecte sua VPC ao S3 sem precisar atravessar a internet pública, aumentando a segurança da transmissão de dados. | TBD | TBD |
| Empregar AWS IAM Access Analyzer para monitoramento | O AWS IAM Access Analyzer ajuda a identificar as permissões concedidas aos seus buckets S3 e avaliar se elas estão em conformidade com as práticas recomendadas de segurança. | TBD | TBD |
| Utilizar Amazon S3 Inventory para auditoria | O Amazon S3 Inventory fornece relatórios sobre os objetos armazenados no S3, permitindo uma auditoria eficiente e a verificação do cumprimento das políticas de dados. | TBD | TBD |
| Monitorar acesso aos dados com logs de acesso do servidor S3 | Os logs de acesso do servidor S3 fornecem detalhes sobre as solicitações feitas ao S3, ajudando a monitorar e analisar o acesso aos dados. | TBD | TBD |
| Manter estratégia de backup de dados | A estratégia de backup garante a recuperação de dados em caso de perda, corrupção ou desastre, mantendo a continuidade dos negócios. | TBD | TBD |
| Desabilitar listas de controle de acesso (ACLs) no S3 | Desabilitar as ACLs no S3 ajuda a evitar configurações complexas e potenciais erros de permissão que podem levar a exposição de dados. | TBD | TBD |
| Aplicar configuração de propriedade de objeto S3 para desabilitar ACLs | A configuração da propriedade do objeto ajuda a gerenciar as permissões de forma mais eficiente e segura, evitando o uso de ACLs. | TBD | TBD |
| Revisar política de bucket para garantir cobertura completa de acesso | Revisar a política de bucket assegura que apenas os usuários e serviços autorizados tenham acesso ao S3, reduzindo o risco de acesso não autorizado. | TBD | TBD |
| Bloquear acesso público aos buckets S3 | Bloquear o acesso público aos buckets S3 previne a exposição acidental de dados sensíveis na internet. | TBD | TBD |
| Utilizar S3 Object Lock para proteção contra exclusão | O S3 Object Lock protege contra exclusões acidentais ou mal-intencionadas, proporcionando uma camada adicional de segurança para os dados armazenados. | TBD | TBD |
| Habilitar versionamento no S3 | Habilitar o versionamento nos buckets do S3 permite manter diferentes versões de um objeto, facilitando a recuperação de versões anteriores em caso de exclusão ou sobrescrita. | TBD | TBD |
| Usar endpoints VPC para acesso ao S3 | Utilizar VPC endpoints para o S3 permite acesso privado aos buckets S3, melhorando a segurança e reduzindo o tráfego na Internet pública. | TBD | TBD |
| Identificar e auditar todos os buckets S3 | Identificar e auditar regularmente os buckets S3 garante que somente os dados autorizados estão armazenados e acessíveis conforme a política de segurança. | TBD | TBD |
| Habilitar AWS Config para avaliação de configurações | O AWS Config fornece uma visão detalhada das configurações dos recursos da AWS, permitindo avaliação contínua e auditoria da conformidade com as políticas de segurança. | TBD | TBD |
| Descobrir dados sensíveis usando Amazon Macie | Utilizar o Amazon Macie para descobrir dados sensíveis ajuda a identificar e proteger os dados armazenados no S3, reduzindo o risco de exposição e vazamento. | TBD | TBD |
| Utilizar S3 Storage Lens para análise de uso de armazenamento | O S3 Storage Lens oferece insights e análises abrangentes do uso de armazenamento do S3, ajudando a otimizar os custos e melhorar a segurança. | TBD | TBD |
| Bloquear buckets S3 públicos no nível da organização | Bloquear buckets públicos no nível da organização ajuda a prevenir acesso não autorizado, reduzindo o risco de exposição de dados. | TBD | TBD |
| Utilizar políticas de bucket para restringir o acesso de forma específica | Restringir o acesso usando políticas de bucket garante que somente usuários autorizados possam acessar os dados do S3. | TBD | TBD |
| Separar acessos de leitura, escrita e exclusão no S3 | Separar os acessos por tipo de operação ajuda a minimizar o risco de operações não autorizadas ou acidentais. | TBD | TBD |
| Ativar proteção do S3 em GuardDuty para detectar atividades suspeitas | A proteção do S3 em GuardDuty ajuda a identificar e alertar sobre atividades suspeitas, melhorando a postura de segurança. | TBD | TBD |
| Usar Macie para varredura de dados sensíveis fora das áreas designadas | Usar o Macie para varredura de dados sensíveis ajuda a identificar e proteger informações críticas armazenadas no S3. | TBD | TBD |
| Proteger dados no S3 contra exclusão acidental usando Versionamento e Object Lock | O uso de versionamento e Object Lock no S3 previne a exclusão ou alteração acidental de dados, proporcionando uma camada adicional de segurança. | TBD | TBD |
| Habilitar registro para o S3 usando CloudTrail e logging de acesso do servidor | Habilitar o registro para o S3 proporciona uma trilha de auditoria detalhada das atividades de acesso, ajudando a detectar e responder a incidentes de segurança. | TBD | TBD |
| Fazer backup dos dados no S3 | O backup dos dados no S3 assegura a recuperação em caso de perda ou corrupção de dados. | TBD | TBD |
| Monitorar o S3 usando Security Hub e CloudWatch Logs | Monitorar o S3 com Security Hub e CloudWatch Logs permite a detecção proativa de eventos de segurança e operacionais. | TBD | TBD |
| Capturar estatísticas de segurança do Amazon Macie por bucket S3 | Utilizar o Amazon Macie para capturar estatísticas de segurança por bucket S3 ajuda a identificar e mitigar riscos de segurança de dados. | TBD | TBD |
| Configurar bucket S3 diferente para armazenamento de logs de acesso do servidor | Utilizar um bucket S3 separado para logs de acesso do servidor ajuda na organização e segurança dos logs, facilitando a auditoria. | TBD | TBD |
| Configurar propriedade do objeto S3 | Configurar a propriedade do objeto S3 garante que a posse dos dados seja claramente definida e gerenciada. | TBD | TBD |
| Usar nomes de buckets S3 compatíveis com DNS | Usar nomes de buckets compatíveis com DNS assegura que eles podem ser acessados sem problemas e seguem as melhores práticas. | TBD | TBD |
| Negar permissão de escrita do Grupo de Entrega de Logs S3 no bucket de origem | Negar permissão de escrita do Grupo de Entrega de Logs no bucket de origem previne alterações não autorizadas nos logs. | TBD | TBD |
| Ativar bloqueio de acesso público S3 para contas AWS | Ativar o bloqueio de acesso público para contas AWS ajuda a prevenir exposições acidentais de dados. | TBD | TBD |
| Ativar bloqueio de acesso público S3 para buckets S3 | Ativar o bloqueio de acesso público nos buckets S3 previne acessos não autorizados e expõe dados sensíveis. | TBD | TBD |
| Habilitar chaves de bucket S3 | Usar chaves de bucket S3 otimiza a performance da criptografia do lado do servidor, melhorando a segurança. | TBD | TBD |
| Proibir acesso 'FULL\_CONTROL' a usuários autenticados da AWS | Proibir acesso 'FULL\_CONTROL' a usuários autenticados previne controle total indesejado sobre os buckets. | TBD | TBD |
| Proibir acesso 'READ' a usuários autenticados da AWS | Proibir acesso 'READ' a usuários autenticados da AWS reduz o risco de acesso e leitura não autorizados de dados. | TBD | TBD |
| Proibir acesso 'READ\_ACP' a usuários autenticados da AWS | Proibir acesso 'READ\_ACP' a usuários autenticados da AWS evita a exposição das configurações de permissões do bucket. | TBD | TBD |
| Proibir acesso 'WRITE' a usuários autenticados da AWS | Proibir acesso 'WRITE' a usuários autenticados da AWS impede alterações não autorizadas nos buckets S3. | TBD | TBD |
| Proibir acesso 'WRITE\_ACP' a usuários autenticados da AWS | Proibir acesso 'WRITE\_ACP' a usuários autenticados da AWS previne alterações não autorizadas nas configurações do bucket. | TBD | TBD |
| Auditar e Monitorar Atividades nos Buckets S3 Usando AWS CloudTrail e Logs de Acesso | Auditar e monitorar as ações da API e o acesso aos buckets S3 são essenciais para identificar atividades suspeitas, não autorizadas e garantir a segurança dos dados. | TBD | TBD |
| Habilitar MFA Delete nos buckets S3 | Habilitar MFA Delete nos buckets S3 aumenta a segurança exigindo autenticação multifator para deletar objetos ou desativar o versionamento. | TBD | TBD |
| Proibir acesso público 'FULL\_CONTROL' aos buckets S3 | Proibir acesso público 'FULL\_CONTROL' aos buckets S3 evita controle total não autorizado sobre os dados armazenados. | TBD | TBD |
| Proibir acesso público 'READ' aos buckets S3 | Proibir acesso público 'READ' aos buckets S3 previne a leitura não autorizada de dados. | TBD | TBD |
| Proibir acesso público 'READ\_ACP' aos buckets S3 | Proibir acesso público 'READ\_ACP' aos buckets S3 impede o acesso não autorizado às configurações de permissão. | TBD | TBD |
| Proibir acesso público 'WRITE' aos buckets S3 | Proibir acesso público 'WRITE' aos buckets S3 evita que dados não autorizados sejam carregados ou alterados. | TBD | TBD |
| Proibir acesso público 'WRITE\_ACP' aos buckets S3 | Proibir acesso público 'WRITE\_ACP' aos buckets S3 evita alterações não autorizadas nas configurações de permissão. | TBD | TBD |
| Proibir acesso público via políticas de bucket no S3 | Proibir acesso público via políticas de bucket no S3 reduz o risco de exposição e acesso não autorizado aos dados. | TBD | TBD |
| Impor Criptografia em Buckets S3 Usando SSE ou AWS KMS com CMKs | É crucial proteger os dados em repouso nos buckets S3 para evitar acesso não autorizado e violações de dados. | TBD | TBD |
| Configurar políticas de ciclo de vida em buckets S3 | Políticas de ciclo de vida automatizam a gestão de dados, como transição para armazenamento de baixo custo ou exclusão de objetos antigos. | TBD | TBD |
| Revisar configurações de hospedagem de site em buckets S3 | A revisão regular das configurações de hospedagem de site garante que somente o conteúdo apropriado esteja acessível publicamente. | TBD | TBD |
| Monitorar mudanças de configuração no S3 | Monitorar mudanças de configuração no S3 ajuda a identificar alterações não autorizadas ou inadvertidas que possam impactar a segurança dos dados. | TBD | TBD |
| Proibir acesso cruzado desconhecido via políticas de bucket no S3 | Proibir o acesso cruzado desconhecido evita o compartilhamento não intencional de dados com entidades externas. | TBD | TBD |
| Usar bloqueio de objeto no S3 para proteção de dados | O bloqueio de objeto no S3 previne a exclusão ou alteração de objetos durante um período de retenção definido. | TBD | TBD |
| Utilizar aceleração de transferência no S3 para transferências de dados mais rápidas | A aceleração de transferência no S3 pode melhorar a velocidade de upload e download de dados para buckets S3. | TBD | TBD |
| Exigir SSL para proteção de dados em trânsito no S3 | Exigir SSL garante que os dados transmitidos para e do S3 sejam criptografados e protegidos contra interceptação. | TBD | TBD |
| Exigir criptografia do lado do servidor (SSE) no S3 | A criptografia do lado do servidor protege os dados em repouso, garantindo que eles sejam armazenados de forma segura e acessíveis apenas com as chaves de criptografia corretas. | TBD | TBD |
| Criptografar dados em repouso no S3 | Criptografar dados em repouso no S3 ajuda a proteger informações sensíveis contra acesso não autorizado e garantir a conformidade com as regulamentações de privacidade. | TBD | TBD |
| Utilizar o protocolo HTTPS para segurança de dados em trânsito | O uso do protocolo HTTPS assegura que os dados transmitidos entre os clientes e o S3 sejam criptografados, protegendo-os contra interceptação e adulteração. | TBD | TBD |
| Utilizar Amazon CloudWatch para monitoramento unificado | O Amazon CloudWatch permite o monitoramento centralizado de recursos e aplicações na AWS, fornecendo visibilidade em tempo real do estado e desempenho do ambiente AWS. | TBD | TBD |
| Usar AWS CloudTrail para auditoria contínua do uso da AWS | O AWS CloudTrail ajuda a registrar, armazenar e analisar chamadas de API para ações na AWS, proporcionando uma trilha de auditoria completa de atividades de usuário e sistema. | TBD | TBD |
| Implementar ferramentas de terceiros para extensão de segurança na AWS | As ferramentas de segurança de terceiros podem oferecer funcionalidades adicionais para proteger, monitorar e auditar os recursos na AWS, complementando as capacidades nativas da plataforma. | TBD | TBD |

## Detalhamento dos Controles

Utilizar IAM roles para acesso ao S3

* Controle ID: S3\_001
* Racional: As roles do IAM proporcionam uma forma segura de conceder permissões necessárias para que as aplicações e usuários acessem os recursos do S3.
* Riscos Mitigados:\*\* Concessão excessiva de permissões e acesso não autorizado.
* 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

Utilizar Amazon S3 VPC endpoints

* Controle ID: S3\_002
* Racional: Os VPC endpoints permitem que você conecte sua VPC ao S3 sem precisar atravessar a internet pública, aumentando a segurança da transmissão de dados.
* Riscos Mitigados: Intercepção de dados e acesso não autorizado.
* 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

Empregar AWS IAM Access Analyzer para monitoramento

* Controle ID: S3\_003
* Racional: O AWS IAM Access Analyzer ajuda a identificar as permissões concedidas aos seus buckets S3 e avaliar se elas estão em conformidade com as práticas recomendadas de segurança.
* Riscos Mitigados: Concessão excessiva de permissões e acesso não autorizado.
* Auditoria:
  + Acesse o console do AWS IAM.
  + No painel de navegação, selecione "Access Analyzer".
  + Clique em "Create Analyzer" (Criar Analisador) se ainda não tiver um configurado. Nomeie seu analisador e defina o escopo para a conta ou organização conforme necessário.
  + Uma vez criado o analisador, ele automaticamente começa a analisar as políticas de permissão.
  + Verifique os resultados da análise para identificar quaisquer políticas que permitam acesso não intencional ou excessivo ao S3.
  + Clique nos achados para ver detalhes específicos, como a política e as permissões exatas que estão sendo concedidas.
* Remediação:
  + Baseado nos achados do Access Analyzer, identifique as políticas que necessitam ajuste.
  + No console do IAM, navegue até a seção de políticas ou roles (funções) identificadas pelo Access Analyzer.
  + Revise as políticas de permissão e ajuste-as para limitar o acesso ao S3 apenas ao necessário.
  + Após ajustar as políticas, utilize o Access Analyzer novamente para validar se as permissões agora estão em conformidade com as práticas recomendadas de segurança.
  + Monitore regularmente o Access Analyzer para detectar e remediar qualquer nova concessão excessiva de permissões.
* Referências: Amazon S3 Security and Data Protection

Utilizar Amazon S3 Inventory para auditoria

* Controle ID: S3\_004
* Racional: O Amazon S3 Inventory fornece relatórios sobre os objetos armazenados no S3, permitindo uma auditoria eficiente e a verificação do cumprimento das políticas de dados.
* Riscos Mitigados: Não conformidade com políticas de dados e 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

Monitorar acesso aos dados com logs de acesso do servidor S3

* Controle ID: S3\_005
* Racional: Os logs de acesso do servidor S3 fornecem detalhes sobre as solicitações feitas ao S3, ajudando a monitorar e analisar o acesso aos dados.
* Riscos Mitigados: Acesso não autorizado e análise de 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

Manter estratégia de backup de dados

* Controle ID: S3\_006
* Racional: A estratégia de backup garante a recuperação de dados em caso de perda, corrupção ou desastre, mantendo a continuidade dos negócios.
* Riscos Mitigados: Perda de dados e interrupção do negócio.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que você deseja auditar para verificar a estratégia de backup.
  + Revise as configurações do bucket para verificar se há políticas de ciclo de vida configuradas que movem os dados para o armazenamento de longo prazo, como o S3 Glacier.
  + Verifique se há snapshots ou cópias dos dados armazenados em locais diferentes ou em meios de armazenamento seguros para garantir a recuperação em caso de falha ou perda de dados.
  + Confirme se os backups são realizados em intervalos regulares e se estão em conformidade com as políticas de retenção da empresa.
* Remediação:
  + No console do S3, selecione o bucket para o qual você deseja implementar a estratégia de backup.
  + Configure ou atualize as políticas de ciclo de vida do bucket para automatizar a transferência de dados para o S3 Glacier ou outra solução de armazenamento de longo prazo para backups.
  + Considere o uso de ferramentas de backup de terceiros ou serviços AWS adicionais para criar snapshots e cópias de dados em locais geograficamente distintos para maior resiliência.
  + Defina e aplique políticas de retenção de dados para garantir que os backups sejam mantidos pelo tempo necessário, mas não além do necessário, para otimizar os custos.
  + Teste regularmente a recuperação de dados dos backups para garantir que eles sejam confiáveis e estejam disponíveis quando necessário.
* Referências: Amazon S3 Security and Data Protection, AWS Top 10 security best practices for securing data in Amazon S3

Desabilitar listas de controle de acesso (ACLs) no S3

* Controle ID: S3\_007
* Racional: Desabilitar as ACLs no S3 ajuda a evitar configurações complexas e potenciais erros de permissão que podem levar à exposição de dados.
* Riscos Mitigados: Configuração incorreta de permissões e exposição de dados.
* 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

Aplicar configuração de propriedade de objeto S3 para desabilitar ACLs

* Controle ID: S3\_008
* Racional: A configuração da propriedade do objeto ajuda a gerenciar as permissões de forma mais eficiente e segura, evitando o uso de ACLs.
* Riscos Mitigados: Erros de configuração de ACL e vazamento de dados.
* 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

Revisar política de bucket para garantir cobertura completa de acesso

* Controle ID: S3\_009
* Racional: Revisar a política de bucket assegura que apenas os usuários e serviços autorizados tenham acesso ao S3, reduzindo o risco de acesso não autorizado.
* Riscos Mitigados: Acesso não autorizado e violação de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket cuja política você deseja revisar.
  + Na aba "Permissions" (Permissões), clique em "Bucket Policy" (Política de Bucket).
  + Verifique a política de bucket atual para assegurar que ela limita o acesso aos usuários e serviços autorizados. A política deve explicitar quem pode realizar quais ações (como `GetObject`, `PutObject`, `DeleteObject`, etc.) e em quais recursos.
  + Certifique-se de que não existem permissões excessivas ou abertas que possam permitir acesso não autorizado.
* Remediação:
  + No console do S3, vá para o bucket que requer ajustes na política de bucket.
  + Na aba "Permissions" (Permissões), clique em "Bucket Policy" (Política de Bucket).
  + Revise a política atual e ajuste-a conforme necessário para garantir que apenas entidades autorizadas tenham acesso. Isso pode incluir a restrição de acesso por endereço IP, exigir conexões criptografadas, ou limitar as ações que diferentes usuários ou serviços podem executar.
  + Utilize a ferramenta de validação de política no console do S3, se disponível, para verificar se a política modificada está em conformidade com as práticas recomendadas.
  + Salve as alterações para aplicar a nova política de bucket.
* Referências: AWS - Security best practices for Amazon S3, AWS Security Best Practices and Guidelines for Amazon S3

Bloquear acesso público aos buckets S3

* Controle ID: S3\_010
* Racional: Bloquear o acesso público aos buckets S3 previne a exposição acidental de dados sensíveis na internet.
* Riscos Mitigados: Exposição de dados sensíveis e ataques cibernéticos.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Revise a lista de buckets e selecione cada um para verificar suas configurações.
  + Na aba "Permissions" (Permissões), encontre a seção "Block public access" (Bloquear acesso público).
  + Verifique se todas as opções de bloqueio de acesso público estão habilitadas, o que indica que o acesso público ao bucket está bloqueado.
* Remediação:
  + No console do S3, selecione o bucket para o qual você deseja habilitar o bloqueio de acesso público.
  + Navegue até a aba "Permissions" (Permissões) e localize a seção "Block public access" (Bloquear acesso público).
  + Habilite todas as opções 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 e 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.
* Referências: AWS - Security best practices for Amazon S3, AWS Security Best Practices and Guidelines for Amazon S3

Utilizar S3 Object Lock para proteção contra exclusão

* Controle ID: S3\_011
* Racional: O S3 Object Lock protege contra exclusões acidentais ou mal-intencionadas, proporcionando uma camada adicional de segurança para os dados armazenados.
* Riscos Mitigados: Exclusão acidental ou maliciosa de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que você deseja verificar.
  + Na aba "Management" (Gerenciamento), procure por "Object Lock" (Bloqueio de Objeto).
  + Verifique se o Object Lock está ativado para o bucket selecionado e revise as configurações para garantir que estejam de acordo com as necessidades de proteção dos dados.
* Remediação:
  + No console do S3, selecione o bucket para o qual você deseja ativar o Object Lock.
  + Vá para a aba "Management" (Gerenciamento) e localize "Object Lock".
  + Ative o Object Lock, se ainda não estiver ativado. Ao habilitar essa opção pela primeira vez, você precisa confirmar que deseja permitir o bloqueio de objetos no bucket.
  + Configure as políticas de retenção e/ou os períodos de legal hold conforme necessário. Isso pode incluir a definição de períodos de retenção que impedem a exclusão de objetos antes do término desse período.
  + Salve as alterações para aplicar a proteção de Object Lock aos dados armazenados no bucket.
* Referências: AWS - Security best practices for Amazon S3

Habilitar versionamento no S3

* Controle ID: S3\_012
* Racional: Habilitar o versionamento nos buckets do S3 permite manter diferentes versões de um objeto, facilitando a recuperação de versões anteriores em caso de exclusão ou sobrescrita.
* Riscos Mitigados: Perda de dados devido a exclusão ou sobrescrita acidental.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket para o qual você deseja verificar o versionamento.
  + Na aba "Properties" (Propriedades), procure pela seção "Versioning" (Versionamento).
  + Verifique se o versionamento está habilitado. Se estiver, o status mostrará "Enabled" (Ativado).
* Remediação:
  + No console do S3, selecione o bucket para o qual você deseja ativar o versionamento.
  + Vá para a aba "Properties" (Propriedades) e localize a seção "Versioning" (Versionamento).
  + Clique em "Enable" (Ativar) para habilitar o versionamento. Se já estiver ativado, não são necessárias mais ações.
  + Confirme a ativação do versionamento, se solicitado.
* Referências: AWS - Security best practices for Amazon S3

Usar endpoints VPC para acesso ao S3

* Controle ID: S3\_013
* Racional: Utilizar VPC endpoints para o S3 permite acesso privado aos buckets S3, melhorando a segurança e reduzindo o tráfego na Internet pública.
* Riscos Mitigados: Interceptação de dados e acesso não autorizado.
* 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 S3 configurados.
  + Para cada endpoint do S3, selecione-o e revise as configurações para garantir que estão associados às tabelas de rotas e sub-redes corretas.
* Remediação:
  + No console da VPC, vá para a seção "Endpoints" (Pontos de extremidade).
  + Clique em "Create Endpoint" (Criar ponto de extremidade) para iniciar o processo de configuração.
  + Selecione o serviço para o qual o endpoint é necessário, neste caso, o S3.
  + Configure o endpoint para ser um "Gateway Endpoint" ou "Interface Endpoint" conforme a necessidade.
  + Associe o endpoint às tabelas de rotas e sub-redes corretas para garantir que o tráfego para o S3 utilize este caminho.
  + Revise e confirme a criação do endpoint.
* Referências: AWS - Security best practices for Amazon S3

Identificar e auditar todos os buckets S3

* Controle ID: S3\_014
* Racional: Identificar e auditar regularmente os buckets S3 garante que somente os dados autorizados estão armazenados e acessíveis conforme a política de segurança.
* Riscos Mitigados: Armazenamento e acesso não autorizado a dados sensíveis.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Navegue pela lista de buckets e selecione cada um individualmente para revisão.
  + Verifique as configurações de permissão de cada bucket na aba "Permissions" (Permissões).
  + Revise as políticas de bucket, as configurações de acesso público, as listas de controle de acesso (ACLs) e quaisquer outras configurações relevantes para garantir conformidade com as políticas de segurança.
  + Use a funcionalidade de relatório do S3 para identificar e revisar todos os objetos armazenados, garantindo que apenas dados autorizados estejam presentes.
* Remediação:
  + Utilize ferramentas de gerenciamento e auditoria da AWS, como AWS Config, para obter uma visão completa do estado de configuração dos buckets S3.
  + Regularmente, use o AWS Config ou ferramentas semelhantes para revisar as configurações e as permissões dos buckets.
  + Corrija qualquer configuração que não esteja em conformidade com as políticas de segurança estabelecidas.
  + Considere a implementação de políticas de ciclo de vida do objeto, criptografia e outras configurações de segurança para garantir a proteção adequada dos dados.
* Referências: AWS - Security best practices for Amazon S3

Habilitar AWS Config para avaliação de configurações

* Controle ID: S3\_015
* Racional: O AWS Config fornece uma visão detalhada das configurações dos recursos da AWS, permitindo avaliação contínua e auditoria da conformidade com as políticas de segurança.
* Riscos Mitigados: Configurações inadequadas e não conformidades.
* Auditoria:
  + Acesse o console do AWS Config.
  + Verifique se o AWS Config está ativado para a conta.
  + Se estiver ativado, revise as regras do AWS Config para garantir que elas estejam configuradas para avaliar as configurações dos recursos do S3.
* Remediação:
  + Se o AWS Config não estiver ativado, no console do AWS Config, inicie o processo de configuração clicando em “Get started” (Iniciar).
  + Siga as instruções para configurar o AWS Config, incluindo a especificação dos recursos que deseja monitorar, como buckets do S3.
  + Configure regras específicas do AWS Config para avaliar as configurações dos recursos do S3, como políticas de bucket, versionamento, e bloqueio de acesso público.
  + Ative o monitoramento contínuo para receber avaliações automáticas e relatórios sobre o estado das configurações dos recursos do S3 em sua conta.
* Referências: AWS - Security best practices for Amazon S3

Descobrir dados sensíveis usando Amazon Macie

* Controle ID: S3\_016
* Racional: Utilizar o Amazon Macie para descobrir dados sensíveis ajuda a identificar e proteger os dados armazenados no S3, reduzindo o risco de exposição e vazamento.
* Riscos Mitigados: Vazamento de dados sensíveis e 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

Utilizar S3 Storage Lens para análise de uso de armazenamento

* Controle ID: S3\_017
* Racional: O S3 Storage Lens oferece insights e análises abrangentes do uso de armazenamento do S3, ajudando a otimizar os custos e melhorar a segurança.
* Riscos Mitigados: Uso ineficiente de recursos e potenciais riscos de segurança devido à falta de visibilidade.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Procure por S3 Storage Lens no painel de navegação ou na seção de gerenciamento.
  + Verifique se há painéis do S3 Storage Lens configurados e ativos.
  + Analise os relatórios e métricas disponíveis para entender o uso do armazenamento nos seus buckets do S3.
* Remediação:
  + No console do S3, navegue até a seção S3 Storage Lens.
  + Se ainda não estiver ativo, ative o S3 Storage Lens criando um novo painel de controle.
  + Configure o painel com as métricas e insights que deseja monitorar, abrangendo todos os buckets do S3 ou grupos específicos de buckets.
  + Defina as preferências de análise, como frequência de atualização dos dados, granularidade das métricas, e opções de exportação dos dados para análise externa.
  + Salve e ative o painel de controle do S3 Storage Lens para começar a receber análises sobre o uso do armazenamento.
* Referências: AWS - Security best practices for Amazon S3

Bloquear buckets S3 públicos no nível da organização

* Controle ID: S3\_018
* Racional: Bloquear buckets públicos no nível da organização ajuda a prevenir acesso não autorizado, reduzindo o risco de exposição de dados.
* Riscos Mitigados: Exposição não intencional de dados e acesso não autorizado.
* Auditoria:
  + Acesse o console de gerenciamento da AWS.
  + Navegue até a seção de configurações da organização ou conta.
  + Verifique nas configurações de serviço do Amazon S3 se o bloqueio de acesso público está ativado para a organização ou conta.
* Remediação:
  + No console de gerenciamento da AWS, vá para as configurações de serviço do S3.
  + Encontre a opção para bloquear o acesso público no nível da conta ou organização.
  + Ative o bloqueio de acesso público para todos os buckets S3, garantindo que esta política seja aplicada em toda a organização ou conta.
  + Salve as configurações para garantir que nenhum bucket S3 possa ser configurado como público inadvertidamente.
* Referências: AWS Top 10 security best practices for securing data in Amazon S3

Utilizar políticas de bucket para restringir o acesso de forma específica

* Controle ID: S3\_019
* Racional: Restringir o acesso usando políticas de bucket garante que somente usuários autorizados possam acessar os dados do S3.
* Riscos Mitigados: Acesso não autorizado e vazamento de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket cuja política de acesso você deseja revisar.
  + Na aba "Permissions" (Permissões), clique em "Bucket Policy" (Política de Bucket).
  + Revise a política atual para verificar se existem restrições específicas de acesso, como limitações por IP, negação de ações não autorizadas, ou requisitos de criptografia.
* Remediação:
  + No console do S3, selecione o bucket para o qual você deseja configurar a política.
  + Na aba "Permissions" (Permissões), clique em "Bucket Policy" (Política de Bucket).
  + Utilize o editor de políticas para adicionar ou modificar regras que restrinjam o acesso. Isso pode incluir:
  + - Especificar quais contas ou usuários podem acessar o bucket.
  + - Definir quais ações estão permitidas ou negadas (como `s3:GetObject`, `s3:PutObject`).
  + - Restringir o acesso por endereço IP, VPC ou através de endpoints VPC.
  + - Exigir o uso de conexões HTTPS para acesso ao bucket.
  + Valide a política para garantir que está correta e não bloqueia acessos legítimos.
  + Salve a política para aplicar as restrições ao bucket.
* Referências: AWS Top 10 security best practices for securing data in Amazon S3

Separar acessos de leitura, escrita e exclusão no S3

* Controle ID: S3\_020
* Racional: Separar os acessos por tipo de operação ajuda a minimizar o risco de operações não autorizadas ou acidentais.
* Riscos Mitigados: Modificação ou exclusão acidental ou maliciosa de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket para o qual você deseja verificar as permissões.
  + Na aba "Permissions" (Permissões), clique em "Bucket Policy" (Política de Bucket) ou verifique as permissões das ACLs (se aplicável).
  + Analise a política e as ACLs para assegurar que as permissões de leitura, escrita e exclusão estejam claramente separadas e atribuídas somente aos usuários ou grupos necessários.
* Remediação:
  + No console do S3, vá até o bucket que precisa de ajuste nas permissões.
  + Na aba "Permissions" (Permissões), acesse "Bucket Policy" (Política de Bucket) para modificar as políticas de acesso.
  + Crie ou modifique a política para definir explicitamente as permissões de leitura (`s3:GetObject`), escrita (`s3:PutObject`) e exclusão (`s3:DeleteObject`) e assegure que elas sejam atribuídas a entidades específicas.
  + Por exemplo, para separar as permissões:
  + - Leitura: permita `s3:GetObject` para grupos ou usuários que necessitam apenas visualizar os dados.
  + - Escrita: permita `s3:PutObject` para grupos ou usuários que devem adicionar ou modificar dados.
  + - Exclusão: permita `s3:DeleteObject` apenas para administradores ou usuários específicos com essa necessidade.
  + Certifique-se de que as permissões estejam de acordo com o princípio de menor privilégio, concedendo acesso somente conforme necessário para a função do usuário ou sistema.
* Referências: AWS Top 10 security best practices for securing data in Amazon S3

Ativar proteção do S3 em GuardDuty para detectar atividades suspeitas

* Controle ID: S3\_021
* Racional: A proteção do S3 em GuardDuty ajuda a identificar e alertar sobre atividades suspeitas, melhorando a postura de segurança.
* Riscos Mitigados: Atividades suspeitas e ataques potenciais.
* 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

Usar Macie para varredura de dados sensíveis fora das áreas designadas

* Controle ID: S3\_022
* Racional: Usar o Macie para varredura de dados sensíveis ajuda a identificar e proteger informações críticas armazenadas no S3.
* Riscos Mitigados: Vazamento de dados sensíveis e não conformidade regulatória.
* Auditoria:
  + Acesse o console do Amazon Macie.
  + Verifique se o serviço Macie está ativado para a sua conta AWS.
  + Revise as configurações dos trabalhos de varredura no Macie para garantir que eles estão configurados para analisar os buckets do S3 apropriados.
  + Certifique-se de que os trabalhos de varredura estão procurando por dados sensíveis fora das áreas designadas, como informações pessoalmente identificáveis (PII) ou informações financeiras em locais inesperados.
* Remediação:
  + No console do Amazon Macie, ative o serviço se ainda não estiver ativado.
  + Configure novos trabalhos de varredura, selecionando os buckets do S3 que você deseja analisar.
  + Defina critérios de varredura para identificar dados sensíveis, focando em áreas onde esses dados não deveriam estar presentes.
  + Determine a frequência da varredura, que pode ser diária, semanal ou conforme necessário para a sua organização.
  + Ative as notificações para ser alertado imediatamente se o Macie identificar dados sensíveis fora das áreas designadas.
  + Regularmente, revise os resultados das varreduras para tomar ações corretivas se dados sensíveis forem encontrados em locais não autorizados.
* Referências: AWS Top 10 security best practices for securing data in Amazon S3

Proteger dados no S3 contra exclusão acidental usando Versionamento e Object Lock

* Controle ID: S3\_023
* Racional: O uso de versionamento e Object Lock no S3 previne a exclusão ou alteração acidental de dados, proporcionando uma camada adicional de segurança.
* Riscos Mitigados: Exclusão ou alteração acidental ou maliciosa de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione cada bucket para verificar suas configurações.
  + Na aba "Properties" (Propriedades), verifique se o versionamento está ativado.
  + Na aba "Management" (Gerenciamento), procure por "Object Lock" e verifique se está ativado.
* Remediação:
  + No console do S3, para cada bucket:
  + Vá para "Properties" (Propriedades) e ative o versionamento se ainda não estiver ativado.
  + Em "Management" (Gerenciamento), configure e ative o Object Lock.
  + No caso do Object Lock, defina a política de retenção que proíba a exclusão dos objetos durante o período definido.
  + Para versionamento, assegure-se de que está ativado para manter as versões anteriores dos objetos, permitindo a recuperação em caso de exclusão ou alteração.
  + Teste as configurações de versionamento e Object Lock para garantir que estão funcionando como esperado e protegendo os dados contra exclusões e alterações acidentais ou mal-intencionadas.
* Referências: AWS Top 10 security best practices for securing data in Amazon S3

Habilitar registro para o S3 usando CloudTrail e logging de acesso do servidor

* Controle ID: S3\_024
* Racional: Habilitar o registro para o S3 proporciona uma trilha de auditoria detalhada das atividades de acesso, ajudando a detectar e responder a incidentes de segurança.
* Riscos Mitigados: Atividades maliciosas, acesso não autorizado e não conformidade com políticas de segurança.
* 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: AWS Top 10 security best practices for securing data in Amazon S3

Fazer backup dos dados no S3

* Controle ID: S3\_025
* Racional: O backup dos dados no S3 assegura a recuperação em caso de perda ou corrupção de dados.
* Riscos Mitigados: Perda de dados e interrupção dos negócios.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione cada bucket para analisar suas configurações.
  + Verifique se as políticas de ciclo de vida estão configuradas para criar backups automaticamente ou se há algum outro processo de backup configurado.
* Remediação:
  + No console do S3, para cada bucket relevante:
  + Configure ou revise as políticas de ciclo de vida para assegurar que os backups sejam realizados regularmente. Isso pode incluir mover os dados para o S3 Glacier ou S3 Glacier Deep Archive para armazenamento de longo prazo.
  + Considere o uso de soluções de backup da AWS, como o AWS Backup, para gerenciar e automatizar os backups do S3.
  + Assegure que os backups sejam criptografados e armazenados em uma localização segura, possivelmente em uma região diferente para proteção contra desastres.
  + Defina e teste políticas de retenção para garantir que os dados antigos sejam preservados pelo tempo necessário e excluídos de forma segura após esse período.
* Referências: AWS Top 10 security best practices for securing data in Amazon S3

Monitorar o S3 usando Security Hub e CloudWatch Logs

* Controle ID: S3\_026
* Racional: Monitorar o S3 com Security Hub e CloudWatch Logs permite a detecção proativa de eventos de segurança e operacionais.
* Riscos Mitigados: Ameaças de segurança, atividades suspeitas e problemas operacionais.
* Auditoria:
  + Acesse o AWS Security Hub para verificar se está integrado e monitorando os buckets S3 para atividades suspeitas ou problemas de segurança.
  + No AWS CloudWatch, verifique se os logs de eventos do S3 estão sendo capturados e monitorados. Isso inclui logs de acesso ao S3 e outras atividades operacionais relevantes.
* Remediação:
  + No AWS Security Hub:
  + Certifique-se de que o Security Hub está ativado e configurado para integrar com o S3.
  + Utilize as funcionalidades do Security Hub para avaliar e monitorar a configuração e atividades do S3 contra benchmarks de segurança e práticas recomendadas.
  + No AWS CloudWatch:
  + Configure o logging para os buckets S3, ativando o registro de logs de acesso e operações.
  + Crie log groups e streams no CloudWatch para capturar e armazenar esses logs.
  + Defina métricas e alarmes baseados em logs para identificar comportamentos anormais ou indicadores de possíveis ameaças de segurança.
  + Regularmente, revise os logs e alertas gerados por essas ferramentas para tomar ações corretivas e ajustar as configurações de monitoramento conforme necessário.
* Referências: AWS Top 10 security best practices for securing data in Amazon S3

Capturar estatísticas de segurança do Amazon Macie por bucket S3

* Controle ID: S3\_027
* Racional: Utilizar o Amazon Macie para capturar estatísticas de segurança por bucket S3 ajuda a identificar e mitigar riscos de segurança de dados.
* Riscos Mitigados: Exposição de dados sensíveis e não conformidade regulatória.
* Auditoria:
  + Acesse o console do Amazon Macie.
  + Verifique se o Macie está ativado e configurado para a sua conta AWS.
  + Revise os trabalhos de descoberta de dados existentes para garantir que eles estejam configurados para analisar todos os buckets S3 relevantes.
  + Confira se as estatísticas de segurança, como a detecção de dados sensíveis e padrões de acesso, estão sendo capturadas e registradas para cada bucket.
* Remediação:
  + No console do Amazon Macie, ative o serviço, se necessário.
  + Configure trabalhos de descoberta de dados no Macie para analisar automaticamente todos os buckets S3. Isso inclui:
  + - Selecionar os buckets S3 que você deseja monitorar.
  + - Definir a frequência de análise (diária, semanal, mensal ou conforme necessário).
  + Certifique-se de que as análises do Macie estão capturando dados relevantes, como tipos de dados sensíveis armazenados, volume de dados, padrões de acesso e qualquer outra métrica de segurança crítica.
  + Revise os resultados fornecidos pelo Macie regularmente para identificar e mitigar potenciais riscos de segurança nos dados armazenados.
* Referências: Trend Micro Best practice rules for Amazon S3

Configurar bucket S3 diferente para armazenamento de logs de acesso do servidor

* Controle ID: S3\_028
* Racional: Utilizar um bucket S3 separado para logs de acesso do servidor ajuda na organização e segurança dos logs, facilitando a auditoria.
* Riscos Mitigados: Alteração ou exclusão não autorizada de logs e dificuldade no rastreamento de atividades.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Verifique os buckets existentes para determinar se existe um dedicado exclusivamente ao armazenamento de logs de acesso.
  + Selecione o bucket que armazena logs de acesso e verifique nas configurações de logging se ele aponta para si mesmo ou para um bucket separado especificamente para logs.
* Remediação:
  + No console do S3, identifique ou crie um bucket dedicado exclusivamente para armazenar logs de acesso do servidor.
  + Para cada bucket que está sendo monitorado, configure o logging de acesso do servidor para que os logs sejam direcionados ao bucket dedicado de logs.
  + Certifique-se de que as políticas de permissão no bucket de logs estão configuradas para prevenir alterações não autorizadas ou exclusão dos logs.
  + Aplique medidas de segurança, como criptografia e controle de acesso, para proteger os dados do log.
* Referências: Trend Micro Best practice rules for Amazon S3

Configurar propriedade do objeto S3

* Controle ID: S3\_029
* Racional: Configurar a propriedade do objeto S3 garante que a posse dos dados seja claramente definida e gerenciada.
* Riscos Mitigados: Disputas de propriedade de dados e problemas de acesso.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket desejado e verifique a configuração da propriedade do objeto.
  + Na aba "Permissions" (Permissões), procure por "Object Ownership" (Propriedade do Objeto) e verifique se a configuração reflete a estrutura de propriedade desejada.
* Remediação:
  + No console do S3, selecione o bucket em questão.
  + Na aba "Permissions" (Permissões), localize a seção "Object Ownership" (Propriedade do Objeto).
  + Ajuste as configurações de propriedade do objeto para garantir que reflitam a posse correta, escolhendo entre as opções como "Bucket Owner Preferred" (Preferência do Proprietário do Bucket) ou "Object Writer" (Escritor do Objeto).
  + Salve as configurações para assegurar que a propriedade dos objetos no bucket esteja corretamente atribuída e gerenciada.
* Referências: Trend Micro Best practice rules for Amazon S3

Usar nomes de buckets S3 compatíveis com DNS

* Controle ID: S3\_030
* Racional: Usar nomes de buckets compatíveis com DNS assegura que eles podem ser acessados sem problemas e seguem as melhores práticas.
* Riscos Mitigados: Problemas de conectividade e acesso.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Revise a lista de buckets e verifique se os nomes estão em conformidade com os padrões de nomenclatura DNS, o que inclui não ter espaços, caracteres especiais (exceto hífens), e começar com uma letra ou número.
  + Os nomes dos buckets devem ser únicos globalmente e devem aderir ao padrão de DNS de não ter letras maiúsculas.
* Remediação:
  + Caso algum bucket não esteja em conformidade com as normas de nomenclatura DNS, você precisará criar um novo bucket com o nome correto.
  + Mova os dados do bucket antigo para o novo bucket com o nome compatível com DNS.
  + Atualize quaisquer configurações ou referências ao nome antigo para usar o novo nome de bucket.
  + Depois de garantir que o novo bucket está funcionando corretamente e todos os dados foram transferidos, você pode deletar o bucket antigo.
* Referências: Trend Micro Best practice rules for Amazon S3

Negar permissão de escrita do Grupo de Entrega de Logs S3 no bucket de origem

* Controle ID: S3\_031
* Racional: Negar permissão de escrita do Grupo de Entrega de Logs no bucket de origem previne alterações não autorizadas nos logs.
* Riscos Mitigados: Alteração ou exclusão maliciosa de logs de acesso.
* 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

Ativar bloqueio de acesso público S3 para contas AWS

* Controle ID: S3\_032
* Racional: Ativar o bloqueio de acesso público para contas AWS ajuda a prevenir exposições acidentais de dados.
* Riscos Mitigados: Exposição acidental de dados sensíveis e violações de segurança.
* Auditoria:
  + Acesse o console AWS.
  + Navegue até a seção de gerenciamento de S3.
  + Verifique se o bloqueio de acesso público está ativado para toda a conta, o que previne a configuração de qualquer bucket S3 para permitir acesso público.
* Remediação:
  + No console AWS, vá até a página de gerenciamento do S3.
  + Localize a seção que gerencia o bloqueio de acesso público.
  + Ative o bloqueio de acesso público para toda a conta, assegurando que nenhuma configuração de bucket S3 individual possa sobrescrever esta política.
  + Aplique e salve as configurações para garantir que todos os buckets S3 existentes e futuros na conta tenham o acesso público bloqueado por padrão.
* Referências: Trend Micro Best practice rules for Amazon S3

Ativar bloqueio de acesso público S3 para buckets S3

* Controle ID: S3\_033
* Racional: Ativar o bloqueio de acesso público nos buckets S3 previne acessos não autorizados e expõe dados sensíveis.
* Riscos Mitigados: Acesso não autorizado e vazamento de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione cada bucket individualmente para revisar as configurações.
  + Verifique na aba "Permissions" (Permissões) se a opção "Block public access" (Bloquear acesso público) está ativada para cada bucket.
* Remediação:
  + No console do S3, selecione o bucket que você deseja configurar.
  + Vá para a aba "Permissions" (Permissões).
  + Localize a seção "Block public access" (Bloquear acesso público) e ative todas as opções disponíveis para garantir que o bucket não esteja acessível publicamente.
  + Repita o processo para cada bucket no S3, garantindo que o bloqueio de acesso público esteja ativado para prevenir acessos não autorizados e vazamento de dados.
* Referências: Trend Micro Best practice rules for Amazon S3

Habilitar chaves de bucket S3

* Controle ID: S3\_034
* Racional: Usar chaves de bucket S3 otimiza a performance da criptografia do lado do servidor, melhorando a segurança.
* Riscos Mitigados: Desempenho reduzido devido à sobrecarga de criptografia e vulnerabilidades de segurança.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione cada bucket e verifique nas configurações de criptografia se as chaves de bucket S3 (SSE-KMS) estão habilitadas.
* Remediação:
  + No console do S3, selecione o bucket que você deseja configurar.
  + Vá para a aba "Properties" (Propriedades) e depois para a seção "Default encryption" (Criptografia padrão).
  + Escolha a opção de criptografia que utiliza o AWS Key Management Service (AWS KMS) e selecione uma chave de bucket específica ou crie uma nova chave KMS para esse propósito.
  + Salve as configurações para habilitar a criptografia do lado do servidor usando a chave de bucket S3, o que melhora a eficiência da criptografia e o desempenho de acesso aos dados.
* Referências: Trend Micro Best practice rules for Amazon S3

Proibir acesso 'FULL\_CONTROL' a usuários autenticados da AWS

* Controle ID: S3\_035
* Racional: Proibir acesso 'FULL\_CONTROL' a usuários autenticados previne controle total indesejado sobre os buckets.
* Riscos Mitigados: Alterações não autorizadas e exclusão de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione cada bucket para revisar suas permissões.
  + Na aba "Permissions" (Permissões), verifique as ACLs (Listas de Controle de Acesso) e as políticas de bucket para garantir que não concedem acesso 'FULL\_CONTROL' a usuários autenticados da AWS.
* Remediação:
  + No console do S3, para cada bucket:
  + Acesse a aba "Permissions" (Permissões).
  + Revise e modifique as ACLs e políticas de bucket para garantir que o acesso 'FULL\_CONTROL' não seja concedido a usuários autenticados.
  + As políticas de bucket devem especificar claramente que o acesso 'FULL\_CONTROL' é negado a `AuthenticatedUsers`, o que impede qualquer usuário autenticado da AWS de ter controle total sobre o bucket.

|  |
| --- |
| * { * "Version": "2012-10-17", * "Statement": [ * { * "Effect": "Deny", * "Principal": "\*", * "Action": "s3:\*", * "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 aplicar a política.
* Referências: Trend Micro Best practice rules for Amazon S3

Proibir acesso 'READ' a usuários autenticados da AWS

* Controle ID: S3\_036
* Racional: Proibir acesso 'READ' a usuários autenticados da AWS reduz o risco de acesso e leitura não autorizados de dados.
* Riscos Mitigados: Acesso não autorizado e vazamento de informações.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione cada bucket e revise as ACLs (Listas de Controle de Acesso) e políticas de bucket para verificar se o acesso 'READ' está proibido para usuários autenticados da AWS.
* Remediação:
  + No console do S3, para cada bucket:
  + Acesse a aba "Permissions" (Permissões).
  + Revise e ajuste as ACLs e as políticas de bucket para garantir que o acesso 'READ' não seja permitido a usuários autenticados da AWS.
  + Utilize a política de bucket para negar explicitamente o acesso 'READ' a todos os usuários autenticados. Exemplo de política:

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "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 alterações para aplicar a nova configuração e efetivar a proibição de acesso 'READ' para usuários autenticados.
* Referências: Trend Micro Best practice rules for Amazon S3

Proibir acesso 'READ\_ACP' a usuários autenticados da AWS

* Controle ID: S3\_037
* Racional: Proibir acesso 'READ\_ACP' a usuários autenticados da AWS evita a exposição das configurações de permissões do bucket.
* Riscos Mitigados: Divulgação não autorizada de configurações de permissões.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione cada bucket e examine as ACLs (Listas de Controle de Acesso) e políticas de bucket para assegurar que o acesso 'READ\_ACP' (leitura da ACL) não está permitido para usuários autenticados da AWS.
* Remediação:
  + No console do S3, para cada bucket:
  + Acesse a aba "Permissions" (Permissões).
  + Revise as ACLs e políticas de bucket para garantir que não concedam acesso 'READ\_ACP' a usuários autenticados.
  + Modifique as políticas de bucket para negar explicitamente o acesso 'READ\_ACP' a todos os usuários autenticados. Um exemplo de política que nega esse acesso:

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "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 alterações para aplicar as restrições e impedir o acesso 'READ\_ACP' por usuários autenticados.
* Referências: Trend Micro Best practice rules for Amazon S3

Proibir acesso 'WRITE' a usuários autenticados da AWS

* Controle ID: S3\_038
* Racional: Proibir acesso 'WRITE' a usuários autenticados da AWS impede alterações não autorizadas nos buckets S3.
* Riscos Mitigados: Modificação não autorizada e sobrescrita de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Revise as configurações de cada bucket para verificar se o acesso 'WRITE' está proibido para usuários autenticados da AWS, analisando as ACLs e políticas de bucket.
* Remediação:
  + No console do S3, para cada bucket:
  + Acesse a aba "Permissions" (Permissões).
  + Revise as ACLs e políticas de bucket para garantir que não concedam acesso 'WRITE' a usuários autenticados.
  + Modifique as políticas de bucket para negar explicitamente o acesso 'WRITE' a todos os usuários autenticados. Exemplo de política que impede esse acesso:

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

* + Substitua `nome-do-bucket` pelo nome real do seu bucket.
  + Salve as alterações para aplicar as restrições e evitar o acesso 'WRITE' por usuários autenticados.
* Referências: Trend Micro Best practice rules for Amazon S3

Proibir acesso 'WRITE\_ACP' a usuários autenticados da AWS

* Controle ID: S3\_039
* Racional: Proibir acesso 'WRITE\_ACP' a usuários autenticados da AWS previne alterações não autorizadas nas configurações do bucket.
* Riscos Mitigados: Modificação não autorizada de permissões e configurações do bucket.
* Auditoria:
  + Acesse o console do Amazon S3 na AWS.
  + Na lista de buckets, selecione o bucket que deseja auditar.
  + Vá para a aba 'Permissões' do bucket.
  + Verifique nas ACLs (Listas de Controle de Acesso) e nas políticas de bucket se o acesso 'WRITE\_ACP' está explicitamente negado para usuários autenticados da AWS.
  + - Para ACLs, verifique se não há permissões de 'WRITE\_ACP' para `Authenticated Users` grupo.
  + - Para políticas de bucket, procure por declarações que concedem ação `s3:PutBucketAcl` e certifique-se de que `Condition` inclui uma negação para usuários autenticados.
* Remediação:
  + No console do Amazon S3, vá até o bucket que precisa de correção.
  + Na aba 'Permissões', modifique as ACLs e políticas de bucket:
  + - Para ACLs, remova qualquer permissão 'WRITE\_ACP' para o grupo de `Authenticated Users`.
  + - Para políticas de bucket, adicione uma declaração que explicitamente negue a ação `s3:PutBucketAcl` para `aws:Group` como `Authenticated Users`.
  + A política deve parecer algo assim:

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Deny",  "Principal": "\*",  "Action": "s3:PutBucketAcl",  "Resource": "arn:aws:s3:::SEU\_BUCKET",  "Condition": {  "StringEquals": {  "aws:PrincipalOrgID": "ID\_ORGANIZACAO"  }  }  }  ]  } |

* + Substitua `SEU\_BUCKET` pelo nome do seu bucket e `ID\_ORGANIZACAO` pelo ID da sua organização AWS.
* Referências: Trend Micro Best practice rules for Amazon S3

Auditar e Monitorar Atividades nos Buckets S3 Usando AWS CloudTrail e Logs de Acesso

* Controle ID: S3\_040
* Racional: Auditar e monitorar as ações da API e o acesso aos buckets S3 são essenciais para identificar atividades suspeitas, não autorizadas e garantir a segurança dos dados. AWS CloudTrail e os logs de acesso do servidor no S3 oferecem visibilidade completa das operações realizadas, possibilitando uma análise de segurança e auditoria eficaz.
* Riscos Mitigados: Acesso não autorizado, atividades maliciosas, alterações indevidas em dados ou configurações e falta de visibilidade nas atividades de acesso.
* Auditoria:
  + No console do AWS CloudTrail, verifique se o rastreamento para o S3 está habilitado e as atividades da API relacionadas ao S3 estão sendo registradas.
  + Vá para o console do CloudTrail e selecione “Trails”.
  + Verifique se existe um trail configurado para registrar as atividades do S3. Se não, crie um novo trail e assegure que os eventos de dados do S3 estejam sendo capturados.
  + No console do Amazon S3, confirme se os logs de acesso ao servidor estão habilitados para os buckets desejados.
  + Selecione o bucket desejado e vá para a aba ‘Propriedades’.
  + Na seção ‘Logs de acesso ao servidor’, verifique se o registro está ativado. Se não, habilite-o e especifique o bucket onde os logs devem ser armazenados.
* Remediação:
  + Para configurar o AWS CloudTrail para capturar todas as atividades da API relacionadas ao S3:
    - No console do CloudTrail, crie um novo trail ou edite um existente.
    - Na configuração do trail, assegure-se de incluir eventos de dados para o S3, selecionando todas as operações de leitura e escrita.
  + Para ativar os registros de acesso ao servidor nos buckets S3:
    - No console do S3, selecione o bucket para o qual deseja ativar os logs.
    - Na aba ‘Propriedades’, localize e ative a opção ‘Logs de acesso ao servidor’.
    - Configure o bucket de destino para os logs, assegurando que este tenha as permissões corretas para permitir que o S3 escreva os logs nele.
  + Recomendação: Utilize ambos, AWS CloudTrail para registro de atividades da API e logs de acesso ao servidor S3, para obter uma visão integrada e completa das operações nos buckets, facilitando a detecção e investigação de incidentes de segurança.
* 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

Habilitar MFA Delete nos buckets S3

* Controle ID: S3\_041
* Racional: Habilitar MFA Delete nos buckets S3 aumenta a segurança exigindo autenticação multifator para deletar objetos ou desativar o versionamento.
* Riscos Mitigados: Exclusão acidental ou maliciosa de dados.
* Auditoria:
* Acesse o console do Amazon S3 na AWS.
* Na lista de buckets, selecione o bucket que deseja auditar.
* Vá para a aba 'Propriedades' do bucket.
* No painel 'Versionamento', verifique se o MFA Delete está habilitado. O status de MFA Delete é exibido juntamente com o status do versionamento.
* Remediação:
* No console do Amazon S3, selecione o bucket que você deseja configurar.
* Vá para a aba 'Propriedades' e encontre a seção 'Versionamento'.
* Clique em 'Editar' no painel de versionamento.
* Ative o versionamento, se ainda não estiver ativo.
* Para habilitar o MFA Delete, você precisa usar a AWS CLI porque essa opção não está disponível no console AWS. Execute o seguinte comando na AWS CLI:

|  |
| --- |
| aws s3api put-bucket-versioning --bucket NOME\_DO\_BUCKET --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "ARN\_DO\_MFA CODIGO\_MFA |

* + Substitua `NOME\_DO\_BUCKET` pelo nome do seu bucket, `ARN\_DO\_MFA` pelo ARN do dispositivo MFA, e `CODIGO\_MFA` pelo código MFA atual.
* Referências: Trend Micro Best practice rules for Amazon S3

Proibir acesso público 'FULL\_CONTROL' aos buckets S3

* Controle ID: S3\_042
* Racional: Proibir acesso público 'FULL\_CONTROL' aos buckets S3 evita controle total não autorizado sobre os dados armazenados.
* Riscos Mitigados: Acesso não autorizado e manipulação de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que deseja verificar.
  + Vá para a aba 'Permissões' do bucket.
  + Na seção 'Controle de acesso público', verifique se as opções 'Bloquear acesso público' estão todas ativadas, o que impede qualquer acesso público, incluindo 'FULL\_CONTROL'.
  + Revise também as ACLs e políticas do bucket para assegurar que não concedam permissões 'FULL\_CONTROL' a qualquer usuário público.
* Remediação:
  + No console do Amazon S3, selecione o bucket que precisa de ajustes.
  + Na aba 'Permissões', vá para 'Controle de acesso público' e ative todos os bloqueios para garantir que o acesso público 'FULL\_CONTROL' seja proibido.
  + Modifique as ACLs do bucket para remover quaisquer permissões 'FULL\_CONTROL' que possam estar concedidas a usuários públicos.
  + Revise as políticas do bucket para garantir que nenhuma política permita explicitamente 'FULL\_CONTROL' a usuários públicos. Se houver, modifique as políticas para remover ou negar tais permissões.
  + Referências: Trend Micro Best practice rules for Amazon S3

Proibir acesso público 'READ' aos buckets S3

* Controle ID: S3\_043
* Racional: Proibir acesso público 'READ' aos buckets S3 previne a leitura não autorizada de dados.
* Riscos Mitigados: Vazamento de dados e acesso não autorizado.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que deseja auditar.
  + Vá para a aba 'Permissões' do bucket.
  + Na seção 'Controle de acesso público', verifique se as configurações 'Bloquear acesso público' estão habilitadas para evitar qualquer acesso 'READ' público.
  + Confirme que as ACLs (Listas de Controle de Acesso) e políticas do bucket não concedem permissão de leitura ('READ') a qualquer usuário público.
* Remediação:
  + No console do Amazon S3, acesse o bucket que precisa de ajuste.
  + Na aba 'Permissões', ajuste as configurações em 'Controle de acesso público' para garantir que todas as formas de acesso público estejam bloqueadas.
  + Modifique as ACLs do bucket para remover qualquer permissão 'READ' que possa estar concedida a usuários públicos.
  + Verifique e ajuste as políticas do bucket para garantir que elas não permitam acesso 'READ' público. Se alguma política conceder acesso 'READ' a usuários públicos, modifique-a para remover essa permissão ou inclua uma cláusula de negação para tal acesso.
  + Referências: Trend Micro Best practice rules for Amazon S3

Proibir acesso público 'READ\_ACP' aos buckets S3

* Controle ID: S3\_044
* Racional: Proibir acesso público 'READ\_ACP' aos buckets S3 impede o acesso não autorizado às configurações de permissão.
* Riscos Mitigados: Exposição de configurações de segurança e permissões.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que deseja auditar.
  + Vá para a aba 'Permissões' do bucket.
  + Na seção 'Controle de acesso público', verifique se as configurações 'Bloquear acesso público' estão ativadas, impedindo o acesso público 'READ\_ACP'.
  + Verifique também as ACLs (Listas de Controle de Acesso) e as políticas do bucket para confirmar que não há permissões de 'READ\_ACP' concedidas ao público.
* Remediação:
  + No console do Amazon S3, vá até o bucket em questão.
  + Na aba 'Permissões', ajuste as configurações em 'Controle de acesso público' para garantir que todas as formas de acesso público, incluindo 'READ\_ACP', estejam bloqueadas.
  + Modifique as ACLs do bucket para remover quaisquer permissões 'READ\_ACP' que possam estar concedidas a usuários públicos.
  + Revise e ajuste as políticas do bucket para assegurar que não permitam acesso público 'READ\_ACP'. Se alguma política conceder tal acesso, modifique-a para remover essa permissão ou adicione uma cláusula de negação específica para isso.
* Referências: Trend Micro Best practice rules for Amazon S3

Proibir acesso público 'WRITE' aos buckets S3

* Controle ID: S3\_045
* Racional: Proibir acesso público 'WRITE' aos buckets S3 evita que dados não autorizados sejam carregados ou alterados.
* Riscos Mitigados: Sobrescrita, exclusão ou adição não autorizada de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que deseja verificar.
  + Na aba 'Permissões' do bucket, verifique a seção 'Controle de acesso público'.
  + Assegure-se de que as opções para bloquear acesso público estejam todas ativadas, o que inclui proibir acesso 'WRITE' público.
  + Revise as ACLs e políticas do bucket para verificar que não existem permissões 'WRITE' concedidas a usuários públicos.
* Remediação:
  + No console do Amazon S3, vá ao bucket que necessita ajuste.
  + Na aba 'Permissões', ative os bloqueios em 'Controle de acesso público' para evitar qualquer acesso 'WRITE' público.
  + Modifique as ACLs do bucket para remover qualquer permissão 'WRITE' que possa ter sido concedida a usuários públicos.
  + Verifique e ajuste as políticas do bucket para garantir que não permitem acesso 'WRITE' público. Se necessário, atualize as políticas para remover explicitamente essas permissões ou incluir negações para o acesso 'WRITE' público.
* Referências: Trend Micro Best practice rules for Amazon S3

Proibir acesso público 'WRITE\_ACP' aos buckets S3

* Controle ID: S3\_046
* Racional: Proibir acesso público 'WRITE\_ACP' aos buckets S3 evita alterações não autorizadas nas configurações de permissão.
* Riscos Mitigados: Alterações não autorizadas de permissões e configurações de segurança.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que deseja verificar.
  + Na aba 'Permissões' do bucket, verifique a seção 'Controle de acesso público'.
  + Certifique-se de que as opções para bloquear acesso público estão ativadas, impedindo especificamente o acesso 'WRITE\_ACP' público.
  + Analise as ACLs e as políticas do bucket para garantir que não concedem permissão 'WRITE\_ACP' a usuários públicos.
* Remediação:
  + No console do Amazon S3, navegue até o bucket em questão.
  + Na aba 'Permissões', ative os bloqueios em 'Controle de acesso público' para proibir qualquer acesso 'WRITE\_ACP' público.
  + 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. Se alguma política conceder esse acesso, atualize-a para remover essa permissão ou adicionar uma negação explícita para tal.
* Referências: Trend Micro Best practice rules for Amazon S3

Proibir acesso público via políticas de bucket no S3

* Controle ID: S3\_047
* Racional: Proibir acesso público via políticas de bucket no S3 reduz o risco de exposição e acesso não autorizado aos dados.
* Riscos Mitigados: Acesso não autorizado e exposição de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que deseja verificar.
  + Na aba 'Permissões', vá para 'Políticas de bucket'.
  + Revise a política de bucket para verificar se não há declarações que permitem acesso público.
* Remediação:
  + No console do Amazon S3, selecione o bucket que precisa de correção.
  + Acesse 'Permissões' e depois 'Políticas de bucket'.
  + Modifique a política de bucket para remover quaisquer declarações que permitam acesso público. Isso pode ser feito adicionando uma declaração de negação para `Principal` como `"\*"` ou removendo qualquer declaração que conceda acesso público.
  + Assegure-se de que a política final não contém nenhuma declaração que permita explicitamente o acesso público.
* Referências: Trend Micro Best practice rules for Amazon S3

Impor Criptografia em Buckets S3 Usando SSE ou AWS KMS com CMKs

* Controle ID: S3\_048
* Racional: É crucial proteger os dados em repouso nos buckets S3 para evitar acesso não autorizado e violações de dados. A criptografia do lado do servidor (SSE-S3) oferece uma solução gerenciada pela AWS, enquanto o uso de chaves de gerenciamento de cliente (CMKs) no AWS KMS proporciona controle e segurança adicionais, sendo a opção recomendada.
* Riscos Mitigados: Acesso não autorizado a dados em repouso, violações de dados e falhas de compliance.
* 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

Configurar políticas de ciclo de vida em buckets S3

* Controle ID: S3\_049
* Racional: Políticas de ciclo de vida automatizam a gestão de dados, como transição para armazenamento de baixo custo ou exclusão de objetos antigos.
* Riscos Mitigados: Custos elevados de armazenamento e retenção de dados desnecessária.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que deseja verificar.
  + Vá para a aba 'Gerenciamento' do bucket.
  + Verifique se existem políticas de ciclo de vida configuradas e se estão alinhadas com as práticas de gestão de dados desejadas.
* Remediação:
  + No console do Amazon S3, selecione o bucket para o qual deseja configurar a política de ciclo de vida.
  + Acesse a aba 'Gerenciamento' e selecione 'Políticas de ciclo de vida'.
  + Clique em 'Adicionar política de ciclo de vida' para criar uma nova política.
  + Defina regras para transição de objetos para diferentes classes de armazenamento (como S3 Standard-IA, S3 One Zone-IA, S3 Intelligent-Tiering ou Glacier) após um número específico de dias após a criação.
  + Configure a expiração para deletar objetos automaticamente após um período determinado de tempo.
  + Siga as instruções para nomear a política, configurar as regras e salvá-la.
* Referências: Trend Micro Best practice rules for Amazon S3

Revisar configurações de hospedagem de site em buckets S3

* Controle ID: S3\_050
* Racional: A revisão regular das configurações de hospedagem de site garante que somente o conteúdo apropriado esteja acessível publicamente.
* Riscos Mitigados: Exposição não intencional de dados sensíveis e violação de segurança.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket usado para hospedar o site.
  + Vá para a aba 'Propriedades' do bucket.
  + Na seção 'Hospedagem de site estático', verifique se as configurações, como o documento de índice e o documento de erro, estão corretamente definidas.
  + Certifique-se de que não há permissões excessivas que possam expor dados sensíveis.
* Remediação:
  + No console do Amazon S3, vá até o bucket que está sendo usado para hospedagem de site.
  + Na aba 'Propriedades', localize a seção 'Hospedagem de site estático'.
  + Revise as configurações de hospedagem, incluindo o documento de índice, documento de erro e redirecionamentos, para garantir que estejam corretas e seguras.
  + Ajuste as políticas de bucket e as ACLs para assegurar que apenas o conteúdo apropriado esteja acessível publicamente e que os dados sensíveis estejam protegidos.
  + Se necessário, desabilite a hospedagem de site estático até que todas as revisões de segurança sejam concluídas e as configurações apropriadas estejam em vigor.
* Referências: Trend Micro Best practice rules for Amazon S3

Monitorar mudanças de configuração no S3

* Controle ID: S3\_051
* Racional: Monitorar mudanças de configuração no S3 ajuda a identificar alterações não autorizadas ou inadvertidas que possam impactar a segurança dos dados.
* Riscos Mitigados: Alterações de configuração não autorizadas e potenciais violações de segurança.
* Auditoria:
  + Utilize o AWS CloudTrail para verificar se os logs de eventos para as atividades do S3 estão sendo capturados. No console do CloudTrail, confirme que o trail está configurado para registrar eventos relacionados ao S3.
  + Use o AWS Config para monitorar e avaliar as configurações dos buckets S3. No console do AWS Config, verifique se as regras estão configuradas para avaliar as alterações nas configurações dos buckets S3.
* Remediação:
  + No AWS CloudTrail, certifique-se de que os eventos relacionados ao S3 estão sendo registrados. Se necessário, crie um novo trail que inclua eventos do S3.
  + No AWS Config, configure regras para monitorar as configurações específicas dos buckets S3 que você deseja rastrear. Isso pode incluir mudanças nas políticas de bucket, ACLs, configurações de criptografia, e outras configurações relevantes.
  + Configure notificações ou alertas no AWS Config e CloudTrail para ser notificado sobre mudanças importantes. Isso pode ser feito integrando com serviços como o Amazon SNS, Amazon CloudWatch Events ou Amazon EventBridge para disparar alertas ou ações automatizadas em resposta a mudanças de configuração.
* Referências: Trend Micro Best practice rules for Amazon S3

Proibir acesso cruzado desconhecido via políticas de bucket no S3

* Controle ID: S3\_052
* Racional: Proibir o acesso cruzado desconhecido evita o compartilhamento não intencional de dados com entidades externas.
* Riscos Mitigados: Vazamento de dados e acesso não autorizado.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que deseja auditar.
  + Vá para a aba 'Permissões' e depois para 'Políticas de bucket'.
  + Revise a política do bucket para verificar se há alguma permissão que permita acesso cruzado (cross-account) que não seja conhecido ou intencional.
* 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 cruzado desconhecido. Isto pode ser feito adicionando uma declaração de `Deny` na política do bucket para entidades externas não autorizadas.
  + Certifique-se de que todas as permissões de acesso cruzado na política do bucket são necessárias e autorizadas, e qualquer acesso não reconhecido ou não autorizado seja claramente negado.
* Referências: Trend Micro Best practice rules for Amazon S3

Usar bloqueio de objeto no S3 para proteção de dados

* Controle ID: S3\_053
* Racional: O bloqueio de objeto no S3 previne a exclusão ou alteração de objetos durante um período de retenção definido.
* Riscos Mitigados: Exclusão ou alteração acidental ou maliciosa de objetos.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que deseja verificar.
  + Vá para a aba 'Gerenciamento' e depois para 'Bloqueio de objeto'.
  + Verifique se o bloqueio de objeto está habilitado e se as políticas de retenção e/ou bloqueio legal estão configuradas corretamente.
* Remediação:
  + No console do Amazon S3, selecione o bucket em que deseja habilitar o bloqueio de objeto.
  + Vá para a aba 'Gerenciamento' e selecione 'Bloqueio de objeto'.
  + Habilite o bloqueio de objeto, se ainda não estiver ativo.
  + Configure as políticas de retenção conforme necessário para proteger os dados contra exclusões e alterações. Isso pode incluir a definição de períodos de retenção e/ou a aplicação de bloqueio legal em objetos específicos.
* Referências: Trend Micro Best practice rules for Amazon S3

Utilizar aceleração de transferência no S3 para transferências de dados mais rápidas

* Controle ID: S3\_054
* Racional: A aceleração de transferência no S3 pode melhorar a velocidade de upload e download de dados para buckets S3.
* Riscos Mitigados: Latência elevada e atrasos na transferência de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que deseja verificar.
  + Vá para a aba 'Propriedades'.
  + Verifique se a aceleração de transferência está habilitada na seção 'Aceleração de transferência do S3'.
* Remediação:
  + No console do Amazon S3, selecione o bucket que precisa de otimização na transferência de dados.
  + Acesse a aba 'Propriedades'.
  + Na seção 'Aceleração de transferência do S3', habilite a aceleração de transferência.
  + Siga as instruções para completar a configuração, o que pode incluir a escolha de um nome de endpoint que será usado para acelerar as transferências.
* Referências: Trend Micro Best practice rules for Amazon S3

Exigir SSL para proteção de dados em trânsito no S3

* Controle ID: S3\_055
* Racional: Exigir SSL garante que os dados transmitidos para e do S3 sejam criptografados e protegidos contra interceptação.
* Riscos Mitigados: Interceptação de dados e comprometimento da integridade dos dados em trânsito.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione o bucket que deseja verificar.
  + Vá para a aba 'Permissões' e depois para 'Políticas de bucket'.
  + Revise a política de bucket para garantir que exista uma condição que exija conexões SSL para todas as transferências de dados.
* Remediação:
  + No console do Amazon S3, selecione o bucket que necessita de configuração.
  + Acesse a aba 'Permissões' e selecione 'Políticas de bucket'.
  + Adicione ou modifique a política de bucket para incluir uma condição que exija o uso de SSL para todas as transferências de dados. Isso pode ser feito usando uma declaração na política do bucket que nega o acesso se a conexão não estiver usando SSL.
  + Exemplo de condição na política do bucket:

|  |
| --- |
| {  "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.
* Referências: Trend Micro Best practice rules for Amazon S3

Exigir criptografia do lado do servidor (SSE) no S3

* Controle ID: S3\_056
* Racional: A criptografia do lado do servidor protege os dados em repouso, garantindo que eles sejam armazenados de forma segura e acessíveis apenas com as chaves de criptografia corretas.
* Riscos Mitigados: Acesso não autorizado a dados em repouso e vazamento de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Para cada bucket, selecione-o e vá para a aba 'Propriedades'.
  + Verifique na seção de criptografia se a criptografia do lado do servidor está habilitada, seja com SSE-S3 (chaves gerenciadas pela AWS) ou SSE-KMS (chaves gerenciadas pelo cliente).
* Remediação:
  + No console do Amazon S3, selecione o bucket que precisa ser configurado.
  + Acesse a aba 'Propriedades' e localize a seção de criptografia.
  + Para habilitar a criptografia SSE-S3, escolha 'Amazon S3-managed keys (SSE-S3)' como opção de criptografia.
  + Para usar a criptografia SSE-KMS, escolha 'AWS Key Management Service key (SSE-KMS)' e selecione a chave gerenciada pelo cliente ou permita que a AWS crie uma para você.
  + Salve as configurações para garantir que todos os dados novos e existentes no bucket sejam criptografados usando o método escolhido.
* Referências: Trend Micro Best practice rules for Amazon S3

Criptografar dados em repouso no S3

* Controle ID: S3\_057
* Racional: Criptografar dados em repouso no S3 ajuda a proteger informações sensíveis contra acesso não autorizado e garantir a conformidade com as regulamentações de privacidade.
* Riscos Mitigados: Acesso não autorizado a dados em repouso e vazamento de dados.
* Auditoria:
  + Acesse o console do Amazon S3.
  + Selecione cada bucket para verificar.
  + Na aba 'Propriedades' de cada bucket, verifique se a criptografia em repouso está habilitada, procurando pela seção de criptografia.
* Remediação:
  + No console do Amazon S3, vá para cada bucket que necessita de criptografia.
  + Na aba 'Propriedades', encontre a seção de criptografia.
  + Escolha entre habilitar a criptografia SSE-S3 (chaves gerenciadas pela AWS) ou SSE-KMS (chaves gerenciadas pelo cliente).
  + Para SSE-S3, selecione 'Amazon S3-managed keys (SSE-S3)'. Para SSE-KMS, selecione 'AWS Key Management Service key (SSE-KMS)' e escolha uma chave gerenciada pelo cliente ou permita que a AWS crie uma.
  + Aplique as mudanças para garantir que a criptografia em repouso seja ativada para todos os dados armazenados nos buckets.
* Referências: Trend Micro Best Practices for Keeping Amazon S3 Buckets Secure

Utilizar o protocolo HTTPS para segurança de dados em trânsito

* Controle ID: S3\_058
* Racional: O uso do protocolo HTTPS assegura que os dados transmitidos entre os clientes e o S3 sejam criptografados, protegendo-os contra interceptação e adulteração.
* Riscos Mitigados: Interceptação e modificação de dados em trânsito.
* Auditoria:
  + Acesse o console do Amazon 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 para todas as conexões.
* 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. Isso pode ser feito com uma declaração na política que nega o acesso se a conexão não for feita via HTTPS.
  + Exemplo de condição na política de bucket:

|  |
| --- |
| {  "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 bucket.
* Referências: Trend Micro Best Practices for Keeping Amazon S3 Buckets Secure

Utilizar Amazon CloudWatch para monitoramento unificado

* Controle ID: S3\_059
* Racional: O Amazon CloudWatch permite o monitoramento centralizado de recursos e aplicações na AWS, fornecendo visibilidade em tempo real do estado e desempenho do ambiente AWS.
* Riscos Mitigados: Indisponibilidade de sistema, desempenho inadequado e falhas não detectadas.
* Auditoria:
  + Acesse o console do Amazon CloudWatch.
  + Verifique se existem métricas e logs configurados para os recursos do S3.
  + Na seção de alarmes do CloudWatch, confira se existem alarmes ativos que monitoram condições específicas dos buckets S3, como uso de armazenamento, atividades de acesso e erros.
* Remediação:
  + No console do Amazon CloudWatch, configure a coleta de métricas e logs para os recursos do S3.
  + - Isso pode incluir a ativação do logging de acesso do S3 e a integração com o CloudWatch para métricas específicas.
  + Crie alarmes no CloudWatch com base nas métricas do S3 para notificar proativamente sobre atividades anormais, como picos de tráfego, alterações na utilização de armazenamento, ou erros de acesso.
  + Configure as notificações de alarme para enviar mensagens a um tópico do Amazon SNS ou a outros endpoints de notificação para alertar a equipe de operações ou segurança sobre possíveis problemas.
* Referências: Trend Micro Best Practices for Keeping Amazon S3 Buckets Secure

Usar AWS CloudTrail para auditoria contínua do uso da AWS

* Controle ID: S3\_060
* Racional: O AWS CloudTrail ajuda a registrar, armazenar e analisar chamadas de API para ações na AWS, proporcionando uma trilha de auditoria completa de atividades de usuário e sistema.
* Riscos Mitigados: Atividades maliciosas, erros de configuração e violação de políticas de compliance.
* Auditoria:
  + Acesse o console do AWS CloudTrail.
  + Verifique se os trails estão configurados para registrar as chamadas de API do S3.
  + Confira se os logs do CloudTrail estão sendo armazenados em um bucket S3 e se medidas de segurança adequadas estão aplicadas ao bucket de log.
  + Certifique-se de que os logs estão sendo analisados, seja através de ferramentas nativas da AWS como o AWS CloudWatch Logs ou soluções de terceiros para detecção de atividades suspeitas.
* Remediação:
  + No console do AWS CloudTrail, crie ou atualize um trail para incluir as chamadas de API do S3.
  + Configure o trail para armazenar os logs em um bucket S3 dedicado e seguro, aplicando políticas de bucket apropriadas para proteger os logs.
  + Ative a integração com o AWS CloudWatch Logs para análise contínua ou utilize outras ferramentas de análise de log para monitorar e alertar sobre atividades suspeitas.
  + Estabeleça mecanismos para a revisão regular dos logs e para a resposta a incidentes com base nas descobertas dos logs.
* Referências: Trend Micro Best Practices for Keeping Amazon S3 Buckets Secure

Implementar ferramentas de terceiros para extensão de segurança na AWS

* Controle ID: S3\_061
* Racional: As ferramentas de segurança de terceiros podem oferecer funcionalidades adicionais para proteger, monitorar e auditar os recursos na AWS, complementando as capacidades nativas da plataforma.
* Riscos Mitigados: Ameaças avançadas, lacunas de segurança e conformidade.
* Auditoria:
  + Avalie quais ferramentas de segurança de terceiros estão em uso e como estão integradas com a AWS, especialmente com o S3.
  + Verifique a configuração dessas ferramentas para garantir que estão adequadamente configuradas para monitorar e proteger os recursos do S3.
  + Revise os registros e alertas gerados pelas ferramentas para avaliar sua eficácia na identificação de riscos e ameaças.
* Remediação:
  + Identifique e avalie ferramentas de segurança de terceiros que possam complementar as medidas de segurança da AWS para seus buckets S3.
  + Implemente ferramentas que ofereçam monitoramento avançado, detecção de ameaças, análise de vulnerabilidades, e gestão de conformidade.
  + Configure as ferramentas para se integrarem com os serviços da AWS, garantindo que tenham acesso necessário para monitorar e auditar os recursos do S3 de forma eficaz.
  + Teste e valide a integração das ferramentas de terceiros para garantir que elas funcionem conforme o esperado, fornecendo visibilidade e controle adicionais sobre a segurança dos recursos do S3.
* Referências: Trend Micro Best Practices for Keeping Amazon S3 Buckets Secure

## Histórico de alterações

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data de Publicação** | **Descrição** | **Alterações** |
| 1.0 | 04/04/2024 | Criação do documento | * Controles incluídos: * Utilizar IAM roles para acesso ao S3 (S3\_001) * Utilizar Amazon S3 VPC endpoints (S3\_002) * Empregar AWS IAM Access Analyzer para monitoramento (S3\_003) * Utilizar Amazon S3 Inventory para auditoria (S3\_004) * Monitorar acesso aos dados com logs de acesso do servidor S3 (S3\_005) * Manter estratégia de backup de dados (S3\_006) * Desabilitar listas de controle de acesso (ACLs) no S3 (S3\_007) * Aplicar configuração de propriedade de objeto S3 para desabilitar ACLs (S3\_008) * Revisar política de bucket para garantir cobertura completa de acesso (S3\_009) * Bloquear acesso público aos buckets S3 (S3\_010) * Utilizar S3 Object Lock para proteção contra exclusão (S3\_011) * Habilitar versionamento no S3 (S3\_012) * Usar endpoints VPC para acesso ao S3 (S3\_013) * Identificar e auditar todos os buckets S3 (S3\_014) * Habilitar AWS Config para avaliação de configurações (S3\_015) * Descobrir dados sensíveis usando Amazon Macie (S3\_016) * Utilizar S3 Storage Lens para análise de uso de armazenamento (S3\_017) * Bloquear buckets S3 públicos no nível da organização (S3\_018) * Utilizar políticas de bucket para restringir o acesso de forma específica (S3\_019) * Separar acessos de leitura, escrita e exclusão no S3 (S3\_020) * Ativar proteção do S3 em GuardDuty para detectar atividades suspeitas (S3\_021) * Usar Macie para varredura de dados sensíveis fora das áreas designadas (S3\_022) * Proteger dados no S3 contra exclusão acidental usando Versionamento e Object Lock (S3\_023) * Habilitar registro para o S3 usando CloudTrail e logging de acesso do servidor (S3\_024) * Fazer backup dos dados no S3 (S3\_025) * Monitorar o S3 usando Security Hub e CloudWatch Logs (S3\_026) * Capturar estatísticas de segurança do Amazon Macie por bucket S3 (S3\_027) * Configurar bucket S3 diferente para armazenamento de logs de acesso do servidor (S3\_028) * Configurar propriedade do objeto S3 (S3\_029) * Usar nomes de buckets S3 compatíveis com DNS (S3\_030) * Negar permissão de escrita do Grupo de Entrega de Logs S3 no bucket de origem (S3\_031) * Ativar bloqueio de acesso público S3 para contas AWS (S3\_032) * Ativar bloqueio de acesso público S3 para buckets S3 (S3\_033) * Habilitar chaves de bucket S3 (S3\_034) * Proibir acesso 'FULL\_CONTROL' a usuários autenticados da AWS (S3\_035) * Proibir acesso 'READ' a usuários autenticados da AWS (S3\_036) * Proibir acesso 'READ\_ACP' a usuários autenticados da AWS (S3\_037) * Proibir acesso 'WRITE' a usuários autenticados da AWS (S3\_038) * Proibir acesso 'WRITE\_ACP' a usuários autenticados da AWS (S3\_039) * Auditar e Monitorar Atividades nos Buckets S3 Usando AWS CloudTrail e Logs de Acesso (S3\_040) * Habilitar MFA Delete nos buckets S3 (S3\_041) * Proibir acesso público 'FULL\_CONTROL' aos buckets S3 (S3\_042) * Proibir acesso público 'READ' aos buckets S3 (S3\_043) * Proibir acesso público 'READ\_ACP' aos buckets S3 (S3\_044) * Proibir acesso público 'WRITE' aos buckets S3 (S3\_045) * Proibir acesso público 'WRITE\_ACP' aos buckets S3 (S3\_046) * Proibir acesso público via políticas de bucket no S3 (S3\_047) * Impor Criptografia em Buckets S3 Usando SSE ou AWS KMS com CMKs (S3\_048) * Configurar políticas de ciclo de vida em buckets S3 (S3\_049) * Revisar configurações de hospedagem de site em buckets S3 (S3\_050) * Monitorar mudanças de configuração no S3 (S3\_051) * Proibir acesso cruzado desconhecido via políticas de bucket no S3 (S3\_052) * Usar bloqueio de objeto no S3 para proteção de dados (S3\_053) * Utilizar aceleração de transferência no S3 para transferências de dados mais rápidas (S3\_054) * Exigir SSL para proteção de dados em trânsito no S3 (S3\_055) * Exigir criptografia do lado do servidor (SSE) no S3 (S3\_056) * Criptografar dados em repouso no S3 (S3\_057) * Utilizar o protocolo HTTPS para segurança de dados em trânsito (S3\_058) * Utilizar Amazon CloudWatch para monitoramento unificado (S3\_059) * Usar AWS CloudTrail para auditoria contínua do uso da AWS (S3\_060) * Implementar ferramentas de terceiros para extensão de segurança na AWS (S3\_061) * 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