

# Guia de boas Práticas

Segurança em Armazenamento e  
Compartilhamento de Dados no Amazon S3



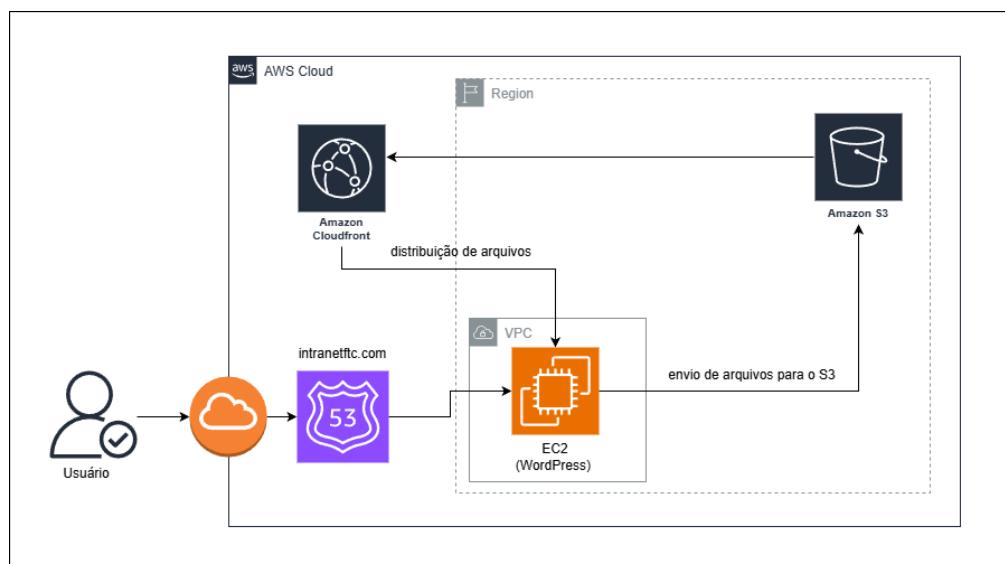
# Guia de boas práticas:

## Segurança em Armazenamento e Compartilhamento de Dados no Amazon S3

Este guia foi desenvolvido a partir de uma análise prática realizada em ambiente AWS, através da integração de serviços para uso interno de uma corporação.

A arquitetura do cenário em questão foi desenvolvida da seguinte forma:

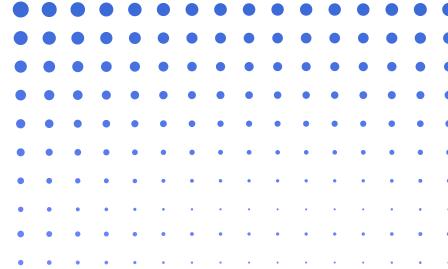
- Uso do S3 para armazenamento de imagens e documentos;
- Os arquivos do S3 são acessados por uma EC2, na qual foi instalado o Wordpress;
- As imagens solicitadas pelos usuários finais são distribuídas pelo CloudFront;
- Nesse cenário, o bucket do S3 pode manter-se privado, enquanto o CloudFront efetua a entrega dos arquivos de forma segura, sem necessidade de exposição pública do bucket.





O Amazon S3 é um serviço de armazenamento disponibilizado pela Amazon Web Services com uma variedade de recursos para controle e segurança dos arquivos armazenados.

O objetivo deste guia é apresentar boas práticas de configuração, armazenamento , compartilhamento e gerenciamento do serviço Amazon S3 para obter um ambiente mais seguro na nuvem.

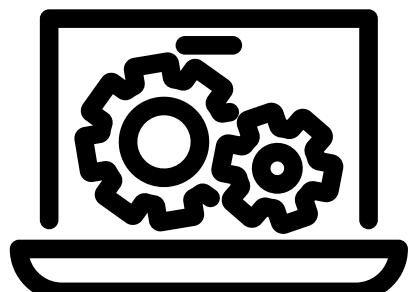


# Boas Práticas de Configuração



Um bucket do Amazon S3, container utilizado para armazenar arquivos, deve ser configurado de acordo com a necessidade a qual vai ser utilizado, visto que as configurações podem variar de acordo com a solução a ser criada.

Ao criar um bucket, os seguintes controles de segurança podem ser utilizados:





## 01 PROPRIEDADE DE OBJETO

Possibilita definir o proprietário dos objetos (arquivos) armazenados no bucket.

- **ACLs desabilitadas:** Todos os objetos do bucket são de propriedade da conta AWS a qual criou o bucket. O acesso ao bucket e aos objetos é definido apenas por políticas.
- **ACLs habilitadas:** Os objetos do bucket podem ser de propriedade de outras contas da AWS. O acesso ao bucket é definido por meio de ACLs e é possível gerenciar o acesso (público ou privado) de cada objeto de maneira individual.



# 01 PROPRIEDADE DE OBJETO

## No cenário desenvolvido:

Foi utilizada a opção de desabilitar as ACLs e gerenciar os objetos por meio de políticas de gerenciamento de acesso da AWS, já que não existe a necessidade de definir o acesso dos objetos de maneira individual.

### Propriedade de objeto Informações

Controle a propriedade de objetos gravados nesse bucket a partir de outras contas da AWS e o uso de listas de controle de acesso (ACLs). A propriedade

#### Propriedade do objeto

##### ACLs desabilitadas (recomendado)

Todos os objetos nesse bucket são de propriedade dessa conta. O acesso a esse bucket e seus objetos é especificado usando apenas políticas.

##### ACLs habilitadas

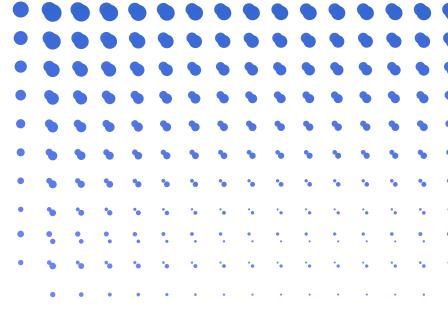
Os objetos nesse bucket podem ser de propriedade de outras contas da AWS. O acesso a esse bucket e seus objetos pode ser especificado usando ACLs.

#### Propriedade do objeto

Imposto pelo proprietário do bucket

# 02

## CONFIGURAÇÕES DE BLOQUEIO DO ACESSO PÚBLICO AO BUCKET



É a opção que permite gerenciar o acesso público aos objetos do bucket criado. Os objetos podem ser públicos ou privados de acordo com a necessidade do projeto.

- **Bloquear acesso público:** Os objetos não podem ser acessados de maneira pública diretamente pela URL do objeto.
  - **Exemplo de uso:** Um bucket para armazenar logs
- **Não bloquear acesso público:** Os objetos podem ser acessados de maneira pública diretamente pela URL do objeto.
  - **Exemplo de uso:** Um bucket para hospedagem de site estático



# 02

## CONFIGURAÇÕES DE BLOQUEIO DO ACESSO PÚBLICO AO BUCKET

### No cenário desenvolvido:

Foi utilizada a opção de bloquear o acesso público, já que os arquivos contidos no bucket não devem ser acessados diretamente, e sim através da distribuição CloudFront criada.

#### Configurações de bloqueio do acesso público deste bucket

O acesso público é concedido a buckets e objetos por meio de listas de controle de acesso (ACLs), políticas de bucket, políticas de ponto de acesso ou se o objeto seja bloqueado, ative a opção de Bloquear todo o acesso público. Essas configurações serão aplicadas apenas a este bucket e aos respectivos objetos. Porém, antes de aplicar qualquer uma dessas configurações, verifique se as aplicações funcionarão corretamente sem acesso público. Caso precise, é possível personalizar as configurações individuais abaixo para que atendam aos seus casos de uso de armazenamento específicos. [Saiba mais](#)

**Bloquear todo o acesso público**

Ativar essa configuração é o mesmo que ativar todas as quatro configurações abaixo. Cada uma das configurações a seguir são independentes uma da outra.





## 03 VERSIONAMENTO DO BUCKET

Permite manter diferentes versões de um mesmo objeto no bucket, armazenando todas as alterações desse objeto e facilitando a recuperação de todas as versões.

- **Desativar versionamento:** Não mantém versões de um mesmo objeto.
  - **Exemplo de uso:** Utilizado em buckets onde os objetos podem ser sobreescritos várias vezes ao dia, para evitar um aumento significativo do custo de armazenamento.
- **Ativar versionamento:** Mantém versões de um mesmo objeto.
  - **Exemplo de uso:** Deve ser ativado quando o bucket contém objetos importantes para evitar exclusões e modificações acidentais de arquivos.



## 03 VERSIONAMENTO DE BUCKET

### No cenário desenvolvido:

O versionamento foi ativado para que caso necessário, seja possível recuperar arquivos modificados acidentalmente.

#### Versionamento de bucket

O versionamento é um meio de manter múltiplas variantes de um objeto no mesmo bucket. Você pode usar o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. Com o versionamento, você pode recuperar facilmente ações não intencionais do usuário e falhas da aplicação. [Saiba mais ↗](#)

#### Versionamento de bucket

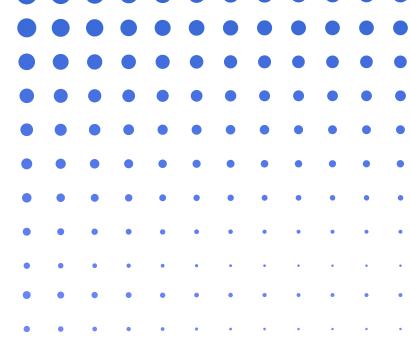
- Desativar
- Ativar

# 04 TIPO DE CRIPTOGRAFIA

- **Criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3):** Criptografia padrão dos buckets
- **Criptografia do lado do servidor com chaves do AWS Key Management Service (SSE-KMS):** A criptografia é aplicada de acordo com uma chave disponibilizada pelo serviço Key Management Service (KMS), gerenciada pelo cliente.
- **Criptografia de duas camadas no lado do servidor com chaves do AWS Key Management Service (DSSE-KMS):** Duas camadas individuais de criptografia são aplicadas, geralmente é utilizado para atender os requisitos de conformidade de regulamentações.



# 04 TIPO DE CRIPTOGRAFIA



## No cenário desenvolvido:

Foi utilizada a criptografia SSE-S3 por ter um gerenciamento simplificado em relação as outras opções, mas ainda seguro.

### Criptografia padrão [Informações](#)

A criptografia no lado do servidor é aplicada automaticamente a novos objetos armazenados nesse bucket.

#### Tipo de criptografia [Informações](#)

Proteja seus objetos com duas camadas separadas de criptografia. Para obter detalhes sobre a precificação, consulte os [preços do Amazon S3](#).

- Criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3)
- Criptografia do lado do servidor com chaves do AWS Key Management Service (SSE-KMS)
- Criptografia de duas camadas no lado do servidor com chaves do AWS Key Management Service (DSSE-KMS)





# 05

## BLOQUEIO DE OBJETOS

Permite bloquear a exclusão de objetos do bucket por períodos específicos ou indefinidos, sendo necessária a remoção manual do bloqueio caso utilizado com período indefinido.

- **Desativar:** Não ativa o bloqueio de objetos no bucket
  - **Exemplo de uso:** Deve ser utilizado em cenários onde não é necessária a retenção de arquivos.
- **Ativar:** Ativa o bloqueio de objetos no bucket
  - **Exemplo de uso:** Deve ser utilizado quando arquivos devem ser retidos por tempo determinado para seguir exigências de regulamentações.





# 05

## BLOQUEIO DE OBJETOS

### No exemplo desenvolvido:

A opção de bloqueio de objeto não foi ativada, já que não é necessária a retenção de nenhum arquivo.

#### ▼ Configurações avançadas

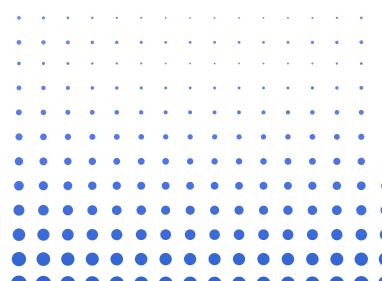
##### Bloqueio de objeto

Armazene objetos usando um modelo write-once-read-many (WORM).

Desativar

Ativar

Permite sempre que os objetos neste bucket sejam bloqueados contidos nele contra exclusão ou substituição.



# Boas Práticas de Armazenamento e Compartilhamento de arquivos

## 1. Utilizar buckets diferentes para armazenar objetos públicos e privados

Prefira utilizar buckets com acesso público bloqueado, caso não seja possível, evite misturar arquivos com acesso público e acesso privado em um mesmo bucket. A gestão individual do acesso de cada arquivo dificulta o processo de gerenciamento do bucket e possibilita que erros ocorram de maneira mais fácil.

## 2. Utilizar versionamento de objetos

O versionamento é indicado para a maioria dos casos, sendo uma maneira fácil de restaurar versões de um mesmo objeto.

## 3. Definir bloqueio de objetos

O recurso de bloqueio de objetos pode ser uma ferramenta importante para atender questões de conformidade com políticas, normas e legislações, de maneira a impedir que os arquivos bloqueados sejam excluídos indevidamente.

## 4. Utilize o CloudFront e Pre-Signed URLs, se possível

O CloudFront é um importante recurso de segurança para utilizar em conjunto ao S3 já que pode acessar um bucket privado e distribuir seus objetos publicamente, além de ocultar a URL original do objeto armazenado.

Ao ser combinado com o uso de Pre-Signed URLs, que gera URLs temporárias de acesso ao arquivo, esses dois recursos trazem uma camada extra de segurança ao bucket.

# Boas Práticas de Gerenciamento

## Privilégio de mínimo acesso

O conceito de privilégio mínimo, conceder permissões de acesso somente a quem necessita, deve ser utilizado com os serviços e usuários da AWS, é recomendável que o acesso ao Amazon S3 só seja concedido a quem realmente utiliza e o administra.

O IAM (Identity and Access Management) permite que os privilégios de acesso ao S3 possam ser liberados de forma modular, controlando quais ações um usuário ou serviço pode realizar.

## Cloudtrail para auditoria e monitoramento

O CloudTrail deve ser utilizado para gerar e armazenar registros, que podem ser utilizados para auditar acessos. Os registros gerados armazenam informações importantes para manter a rastreabilidade da ação registrada, como endereço de IP, qual solicitação foi feita e quando a solicitação foi feita.

O CloudTrail pode armazenar os seguintes tipos de eventos:

- Eventos de gerenciamento: Registra eventos de administração do bucket como alteração de políticas, ativação de versionamento;
- Eventos de dados: Registra ações de solicitação, envio e exclusão dos objetos do bucket;
- Eventos de insights: Analisa eventos para estabelecer uma linha base de ações, registrando quando uma atividade incomum é detectada.