COLOMBIA POTENCIA DE LA VIDA

TIC

# LECCIÓN 2: CÓMO SE PROTEGEN LOS DATOS EN REPOSO

TALENTO TECH | AZ PROYECTOS EDUCATIVOS | UTP Universidad Tecnológica de Pereira

# ¿POR QUÉ SE DEBEN PROTEGER LOS DATOS EN REPOSO?

## ESCENARIOS COMUNES

- **Divulgación de información**
- **Peligro para la integridad de IOS datos**
- **Eliminación accidental o malintencionada**
- **Disponibilidad del sistema, del hardware y del software**

## CAPA ADICIONAL DE PROTECCIÓN SI SU SISTEMA ESTÁ EN PELIGRO

Es importante cifrar los datos en reposo. Esto garantiza la seguridad de los datos, incluso si una persona no autorizada obtiene acceso a ellos. El cifrado de datos en reposo hace que sea mucho más difícil para los atacantes poner en peligro los datos, incluso si pueden comprometer un punto de enlace. Además, es posible que deba proteger sus datos en reposo debido a los requisitos empresariales o de cumplimiento.

En la siguiente lista, se identifican los problemas más comunes que hacen que sea necesario proteger los datos en reposo. También se describe cómo protegerse contra cada problema:

# DIVULGACIÓN DE INFORMACIÓN

**Limite la cantidad de usuarios que pueden acceder a los datos y utilice políticas para administrar el acceso a los recursos. Utilice el cifrado para proteger los datos confidenciales.**

# PELIGRO PARA LA INTEGRIDAD DE LOS DATOS

**Utilice permisos en el nivel de recursos para limitar el acceso de los usuarios que pueden modificar datos. Implemente la firma digital y el cifrado. Restaure los datos de una copia de seguridad o, en el caso de Amazon S3, de una versión del objeto anterior.**

# ELIMINACIÓN ACCIDENTAL O MALICIOSA

**Utilice los permisos correctos y el principio de mínimo privilegio. Restaure los datos de una copia de seguridad o, en el caso de Amazon S3, de una versión del objeto anterior.**

# DISPONIBILIDAD DEL SISTEMA, EL HARDWARE Y EL SOFTWARE:

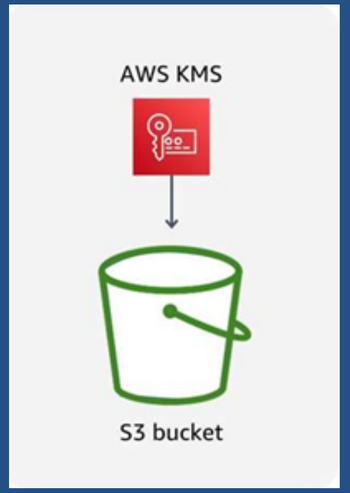
**En caso de un error del sistema o de un desastre natural, restaure los datos desde las réplicas.**

# DATOS EN REPOSO EN AMAZON S3

**Los datos almacenados en Amazon S3 son privados de forma predeterminada y requieren credenciales De AWS para el acceso**

**UTILICE POLÍTICAS DE BUCKET PARA OBTENER ACCESO GRANULAR A LOS OBJETOS.**

**CONSIDERE CIFRAR LOS DATOS EN REPOSO.**



De forma predeterminada, todos los recursos de Amazon S3 (buckets, objetos y subrecursos relacionados; por ejemplo, la configuración del ciclo de vida y la configuración del sitio web) son privados. Solo el propietario del recurso, la cuenta de AWS que lo creó, puede acceder a él. El propietario del recurso puede conceder permisos de acceso a otros mediante la escritura de una política de acceso.

Puede modificar las políticas de bucket para permitir acceso adicional, mientras que AWS proporciona una serie de herramientas a fin de configurar buckets para una amplia variedad de cargas de trabajo. Por ejemplo, la función Block Public Access de S3 actúa como una capa adicional de protección para evitar la exposición accidental de datos.

Además, considere cifrar los datos en reposo en Amazon S3.

# CONCESIÓN DE PERMISOS

## CON BASE EN LA IDENTIDAD
**Adjunta a una entidad principal de IAM**

Bob

| Recurso | Get | Put | List |
|---|---|---|---|
| Bucket X | PERMITIR | PERMITIR | PERMITIR |
| Bucket Y | N/A | N/A | PERMITIR |

## CON BASE EN LOS RECURSOS
**Adjunta a un recurso de AWS**

Bucket X

| Usuario | Get | Put | List |
|---|---|---|---|
| Bob | PERMITIR | DENEGAR | PERMITIR |

Bucket Y

| Usuario | Get | Put | List |
|---|---|---|---|
| Bob | PERMITIR | N/A | PERMITIR |

**¿PUEDE BOB GET, PUT O LIST PARA EL BUCKET X?**

**¿PUEDE BOB GET O LIST PARA EL BUCKET Y?**

## NOTA

**En las tablas de la diapositiva, N/A significa que no se aplica porque la política no especifica permisos para esa acción en particular.**

**Amazon S3 admite dos tipos de mecanismos de control de acceso: con base en la identidad (o en el usuario) y con base en los recursos.**

# ¿CUÁLES SON LAS DIFERENCIAS ENTRE LAS POLÍTICAS BASADAS EN LA IDENTIDAD Y AQUELLAS BASADAS EN LOS RECURSOS?

Son casi idénticas en apariencia y función, pero presentan algunas pequeñas diferencias de sintaxis. La mayor diferencia radica en dónde se aplican. Los permisos basados en la identidad se adjuntan a un usuario de AWS Identity and Access Management (IAM) e indican lo que se le permite hacer al usuario.

Los permisos basados en los recursos se adjuntan a un recurso e indican lo que un usuario específico (o grupo de usuarios) puede hacer con el recurso. Por ejemplo, puede adjuntar políticas basadas en los recursos a buckets de S3, puntos de enlace de nube virtual privada (VPC) y claves de cifrado de AWS Key Management Service (AWS KMS). Las políticas basadas en los recursos son una forma de restringir el acceso según los recursos.

En el ejemplo de la diapositiva, un usuario de IAM llamado Bob tiene adjunta una política basada en identidad. La política le permite usar las API GET, PUT y LIST para el bucket X. Sin embargo, la política basada en los recursos para el bucket X le permite usar GET y LIST y niega la capacidad de usar PUT. Esto significa que, si bien su política basada en la identidad lo permite, Bob no puede colocar objetos en el bucket X mediante la acción PUT.

Para el bucket Y, la política basada en la identidad de Bob permite la acción LIST. La política no permite ni deniega explícitamente las acciones GET y PUT en el bucket Y. La política basada en los recursos para el bucket Y le permite usar GET y LIST, pero no especifica la acción PUT. Por lo tanto, Bob puede leer objetos del bucket, aunque su política basada en la identidad no lo permita explícitamente.

Para algunos servicios de AWS, puede conceder acceso entre cuentas a sus recursos al colocar una política directamente en el recurso que desea compartir, en lugar de utilizar un rol como proxy. El recurso que quiere compartir debe admitir las políticas basadas en los recursos. La política especifica quién (como una lista de ID de cuenta de AWS) puede acceder a ese recurso.


Además de las políticas de bucket e IAM, Amazon S3 admite un mecanismo de permisos conocido como lista de control de acceso (ACL). Una ACL es independiente de las políticas y los permisos de IAM, pero se puede usar en combinación con ellos. Sin embargo, la mayoría de los casos prácticos modernos en Amazon S3 ya no requieren el uso de ACL. AWS recomienda que desactive las ACL, excepto en circunstancias inusuales en las que necesite controlar el acceso de cada objeto individualmente. Con las ACL desactivadas, la política del bucket de S3 se convierte en la única superficie de auditoría.