M03 - Caso de Estudio: Plataforma Escolar EduNova

Descripción General

"EduNova" es una plataforma de gestión escolar SaaS utilizada por colegios privados para facilitar:

- Control de asistencia y calificaciones.
- Emisión de boletas y certificados.
- Interacción entre padres y docentes.
- Carga y descarga de archivos (boletas, fotos, informes).

La plataforma opera sobre AWS y ha crecido rápidamente en el último año. Sin embargo, la organización enfrenta problemas importantes en dos dimensiones:

1. Vulnerabilidades de seguridad relacionadas al almacenamiento de archivos escolares.
2. Configuración débil de políticas de acceso y monitoreo en su infraestructura cloud.

Arquitectura Actual

Servicios Usados

- Frontend: Aplicación React alojada en un bucket S3 sin CloudFront.
- Backend: API REST sobre AWS Lambda + Amazon API Gateway.
- Base de datos: DynamoDB (estudiantes, docentes, calificaciones).
- Autenticación: AWS Cognito parcialmente integrado.
- Almacenamiento de archivos: Buckets S3 con carpetas por institución (sin control granular).
- Logs y métricas: CloudWatch básico; sin CloudTrail habilitado para S3.

Infraestructura

- Buckets de S3 configurados con acceso público habilitado.
- Rutas públicas que permiten descargar archivos PDF sin autenticación.
- IAM con políticas excesivamente permisivas (s3:* en múltiples roles).
- Ausencia de cifrado obligatorio en S3 (ni en tránsito ni en reposo).
- Ausencia de herramientas como Access Analyzer, Macie, o políticas de expiración de objetos.
- No se usa presigned URLs para compartir archivos.
- Enlaces a documentos compartidos por correo sin control de acceso temporal o

individual.

Problemas Identificados

Seguridad

● Archivos personales de estudiantes expuestos (DNI, certificados, boletas, evaluaciones).
● URLs públicas copiables por cualquier usuario sin restricción.
● Buckets configurados sin “block public access” habilitado.
● Roles IAM mal definidos y sin rotación de credenciales.
● Falta de segregación de ambientes (producción, pruebas).
● No se implementan prácticas de seguridad mínimas como el principio de menor privilegio.

Actividad

1. Identificar vulnerabilidades en la arquitectura desde la perspectiva de seguridad.
2. Evaluar los riesgos asociados a cada punto de exposición o mala configuración.
3. Proponer mejoras que integren prácticas de seguridad desde el diseño.
4. Recomendar herramientas y servicios de AWS para monitoreo, cifrado, acceso restringido y trazabilidad.
5. Redactar una lista priorizada de acciones para EduNova que puedan implementarse en dos fases: urgentes y evolutivas.

Recursos a Entregar

● Documento con análisis de vulnerabilidades.
● Tabla de medidas de mitigación recomendadas (urgentes / evolutivas).
● Diagrama esquemático de arquitectura segura y segregada.
● Propuesta de políticas IAM y estrategia de control de acceso sobre S3.