Estrategia de Ciberseguridad en la Nube (AWS) para EduTech Global

Sámuel Muñoz Gómez
Grado en Ciberseguridad

ENTI / UB

18 de mayo de 2025

Índice

1. Introducción

EduTech Global, una empresa educativa ficticia con un entorno Moodle crítico (anteriormente on-premise), planea migrar toda su infraestructura de TI a la nube pública de Amazon Web Services (AWS). Este informe presenta una estrategia completa de ciberseguridad en AWS, abordando los desafíos específicos del cloud y garantizando la protección de datos, aplicaciones y servicios clave. La estrategia se estructura en torno a los cuatro pilares de seguridad en la nube – gestión de identidades y accesos (IAM), protección de datos, protección de la infraestructura y detección y respuesta – e incluye políticas, herramientas y procedimientos para asegurar la plataforma Moodle y los activos en la nube.

A continuación, se detallan la infraestructura cloud propuesta en AWS, los principales retos y riesgos, la política básica de seguridad cloud (quién accede, cuándo y desde dónde), las herramientas y servicios de seguridad recomendados, una implementación práctica de medidas de seguridad (opcional) y las directrices de monitorización continua, respuesta a incidentes y mejores prácticas.

Cabe destacar que toda la estrategia está centrada en AWS y aprovecha sus servicios nativos de seguridad.

2. Infraestructura Cloud propuesta en AWS

La nueva arquitectura en AWS se diseña para alojar la plataforma Moodle de forma segura, escalable y altamente disponible. Se propone separar claramente las capas de aplicación, datos y red para mejorar la elasticidad y la seguridad docs.aws.amazon.com . La infraestructura aprovecha múltiples zonas de disponibilidad (AZ) de AWS para tolerancia a fallos, junto con autoescalado para ajustar los recursos según la demanda. A continuación, describimos los activos y servicios de AWS más relevantes en la arquitectura de EduTech Global, junto con su papel y consideraciones de seguridad:

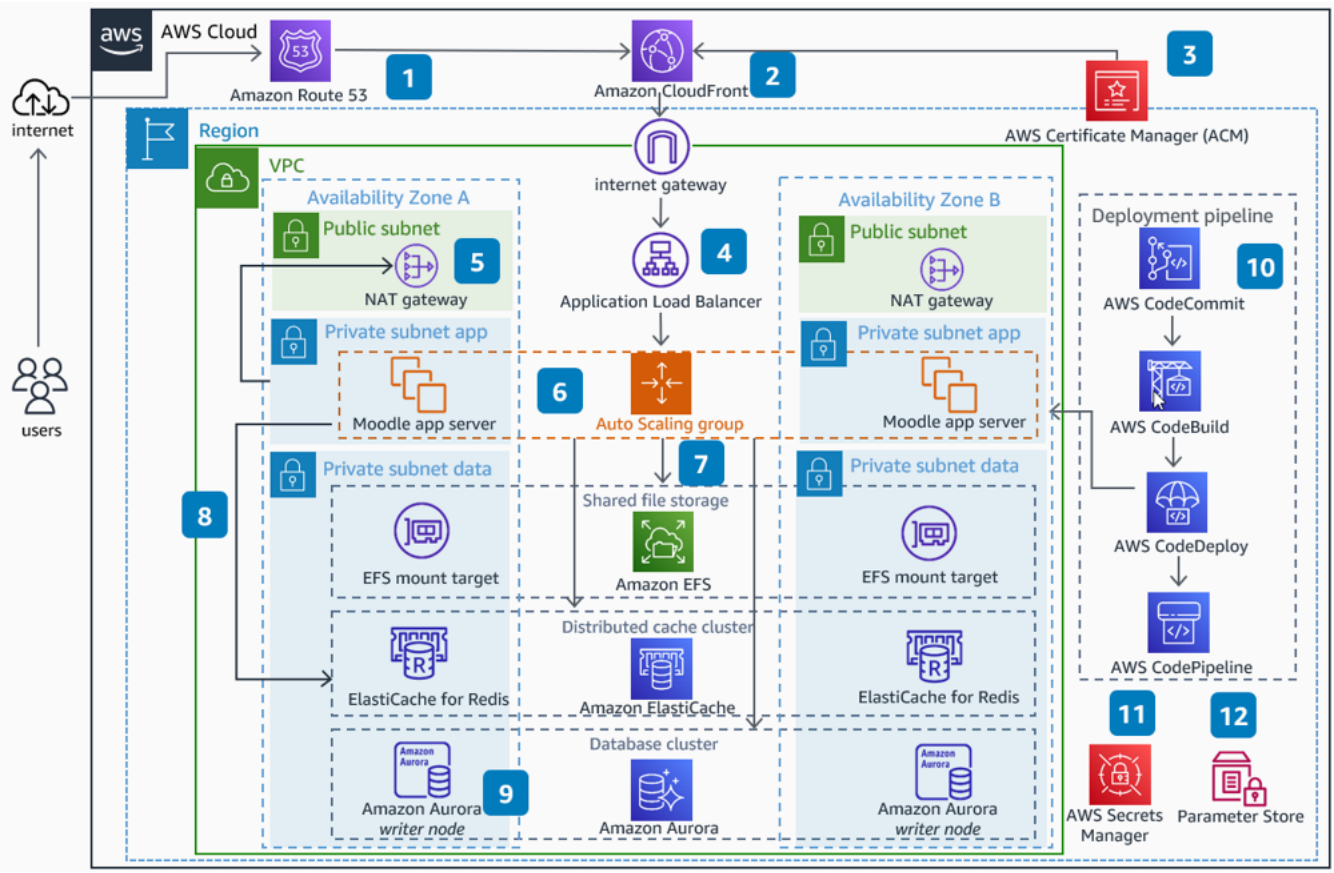

Figura: Arquitectura de referencia de Moodle en AWS (dos AZ con subredes públicas/privadas, balanceador de carga (ALB) al frente, servidores de aplicación Moodle en subredes privadas autoescalables, base de datos en Aurora/RDS multi-AZ, almacenamiento compartido en EFS, CDN con CloudFront, y servicios de soporte como NAT Gateway, Secrets Manager, etc. para una implementación escalable y segura)

- **Amazon VPC (Virtual Private Cloud):** VPC propia que aísla la red de EduTech en la nube. Se configuran subredes públicas (para endpoints externos) y subredes privadas (para servidores internos) en al menos dos AZ. La segmentación de red limita la exposición: las subredes privadas alojan las instancias de aplicación y bases de datos, inaccesibles directamente desde Internet. Se emplean listas de control de acceso de red (ACLs) y Grupos de Seguridad para filtrar el tráfico a nivel de subred e instancia respectivamente, siguiendo el principio de mínimo privilegio en puertos y protocolos.

- **Instancias Amazon EC2 (capa de aplicación Moodle):** Se migrará Moodle a instancias EC2 Linux en subredes privadas (sin IP pública) para reforzar su protección. Un Application Load Balancer (ALB) en la subred pública canaliza el tráfico HTTPS hacia los servidores Moodle en las subredes privadas, permitiendo escalar horizontalmente con Auto Scaling Group según la carga. Las instancias EC2 no exponen puertos de administración al mundo; en su lugar, se usa AWS Systems Manager (SSM) para acceso remoto seguro sin abrir SSH. Cada EC2 tiene un perfil IAM asociado en lugar de credenciales fijas, otorgándole solo los permisos mínimos necesarios (por ejemplo, acceso a leer objetos en S3 si fuera necesario). Los sistemas operativos de las instancias se mantienen parcheados y reforzados (deshabilitando servicios innecesarios, usando AMIs actualizadas) ya que, bajo el modelo de responsabilidad compartida, la configuración del SO y firewalls de instancia son responsabilidad del cliente.

- **Amazon RDS (base de datos gestionada):** La base de datos de Moodle se migra a un servicio RDS (por ejemplo, Amazon Aurora MySQL en configuración Multi-AZ para alta disponibilidad).

RDS facilita la aplicación de parches y respaldos automáticos. Está desplegado en subredes privadas (capa de datos) sin acceso directo desde Internet. Solo los servidores de aplicación en la VPC pueden comunicarse con la base de datos, ya sea mediante su endpoint interno o a través de una peering si se aisla por cuentas. Se habilita el cifrado en reposo de RDS mediante AWS KMS y se forza el cifrado en tránsito (SSL/TLS) para conexiones de la aplicación, protegiendo los datos sensibles de alumnos y profesores tanto en disco como en movimiento. Las políticas de retención de backups se configuran acorde al plan de continuidad (p. ej. copias diarias con retención de 30 días y vault externo en S3).

- **Almacenamiento de archivos (Amazon S3 y EFS):** Los contenidos multimedia de cursos, archivos subidos por usuarios y copias de seguridad de Moodle se almacenarán en servicios de almacenamiento gestionados:
  - **Amazon S3:** para alojar archivos estáticos y backups de Moodle. Se crean buckets S3 privados (con Block Public Access activado) para que ningún objeto sea accesible públicamente por defecto. Solo la aplicación Moodle o administradores con las credenciales adecuadas pueden leer/escribir en ellos. Las políticas de bucket y de IAM restringen el acceso a roles específicos, y se habilita cifrado del lado del servidor (SSE) con claves KMS para proteger los datos en reposo. Un error común es dejar un bucket S3 público por configuración incorrecta; la política de EduTech lo prohíbe explícitamente, ya que si un bucket queda público accidentalmente, es el cliente (EduTech) quien debe mitigarlo, no AWS (ejemplo del modelo de responsabilidad compartida).
  - **Amazon EFS:** dado que Moodle requiere un directorio compartido para archivos de curso (moodledata), se puede optar por un Elastic File System montado en las instancias Moodle. EFS ofrece almacenamiento de red distribuido y cifrado transparente. Se coloca en la misma VPC (accesible solo desde las instancias autorizadas) y facilita escalabilidad y backup centralizado. Si se usa EFS, también se habilita cifrado y LifeCycle Management para migrar datos antiguos a almacenamiento infrecuente, reduciendo superficie de ataque y costo.
- **Entrega de contenido y DNS:** Para mejorar el rendimiento global y la seguridad, se implementa Amazon CloudFront como CDN frente al sitio Moodle. CloudFront almacena en caché contenido estático en edge locations y, combinado con AWS WAF (Web Application Firewall), ayuda a filtrar tráfico malicioso (como intentos de SQLi o XSS en las peticiones) antes de que alcancen la aplicación. El dominio principal (p. ej. moodle.edutechglobal.com) se gestiona con Amazon Route 53, que permite hacer routing al CloudFront/ALB más cercano con baja latencia. Route 53 también puede aplicar DNS Failover para recuperación ante desastres si existiera un sitio de respaldo. Los certificados TLS para el dominio son proporcionados de forma gratuita por AWS Certificate Manager (ACM), asegurando conexiones cifradas (HTTPS) sin costo adicional y con renovación automática.
- **Servicios de gestión y seguridad:** En toda la plataforma se integran servicios transversales de AWS para orquestación y seguridad:
  - **AWS IAM (Identity and Access Management):** Gestiona identidades (usuarios, roles, grupos) y sus permisos. Se definen roles IAM para servicios (EC2, Lambda, etc.) y para usuarios administrativos con privilegios diferenciados. IAM aplica el principio de mínimos privilegios, limitando qué acciones puede realizar cada rol en cada recurso. Por ejemplo, un administrador de bases de datos tiene permisos sobre RDS pero no sobre configuración de VPC; los desarrolladores pueden desplegar en cuentas de desarrollo pero no tocar la de producción, etc. Se habilita MFA obligatorio en cuentas privilegiadas (incluida la cuenta root de AWS) y se considera el uso de AWS SSO (AWS IAM Identity Center) para centralizar la autenticación corporativa.
  - **AWS CloudTrail:** Servicio fundamental de auditoría que registra todas las llamadas a APIs y actividades en la cuenta AWS. CloudTrail se activa en todas las regiones para capturar eventos como inicios de sesión, cambios en configuraciones, acceso a datos, etc. Por defecto retiene 90 días de historial en la consola, y se configura para enviar logs a un bucket S3 central cifrado para almacenamiento a largo plazo y análisis. Gracias a CloudTrail, se puede saber "quién hizo qué, cuándo y desde dónde" en la infraestructura AWS, ya que

registra detalles de cada acción (usuario o rol que la ejecutó, servicio utilizado, parámetros y resultado de la acción). Esto es vital para auditorías de cumplimiento y análisis forense en caso de incidente.

- **Amazon CloudWatch:** Provee monitorización en tiempo real de métricas (CPU, memoria, uso de red, etc.) de los recursos AWS y recolecta logs. Se configuran CloudWatch Alarms para notificar al equipo de TI cuando ocurran eventos fuera de lo normal (p. ej., uso de CPU mayor a 80 por ciento prolongado en un servidor Moodle, que podría indicar carga inusual o un proceso malicioso). CloudWatch Logs centraliza registros de la aplicación Moodle, del sistema operativo y de servicios (por ejemplo, logs de acceso de Apache/Nginx), permitiendo búsquedas y correlaciones. También se pueden definir alarms sobre patrones en logs (ej. múltiples errores de login seguidos pueden indicar fuerza bruta).
- **AWS CloudTrail Insights y Config:** Se habilita CloudTrail Insights para detectar actividad anómala en los patrones de uso de la cuenta (por ejemplo, picos repentinos de llamadas a APIs poco comunes). AWS Config se activa para evaluar continuamente la configuración de los recursos versus reglas de buenas prácticas. Por ejemplo, Config puede alertar si un Security Group abre el puerto 3306 (MySQL) a "0.0.0.0/0" o si un bucket S3 cambia a público, calificándolo de no conforme. Estas herramientas ayudan a identificar desviaciones de la postura de seguridad deseada inmediatamente (parte de las capacidades de detección).

En conjunto, esta infraestructura cloud en AWS proporciona una base sólida y segura para Moodle, aprovechando servicios gestionados y controles de seguridad nativos de AWS. La separación por capas (balanceador público, aplicaciones en subred privada, datos en subred de datos) añade defensa en profundidad. AWS, por su parte, asegura la infraestructura subyacente (datacenters, hardware, hipervisores, redes) – la "seguridad de la nube" –, mientras EduTech Global es responsable de la "seguridad en la nube", es decir, de configurar correctamente sus recursos, proteger sus datos y gestionar los accesos. Esta distinción del modelo de responsabilidad compartida de AWS se ilustra en la siguiente figura.

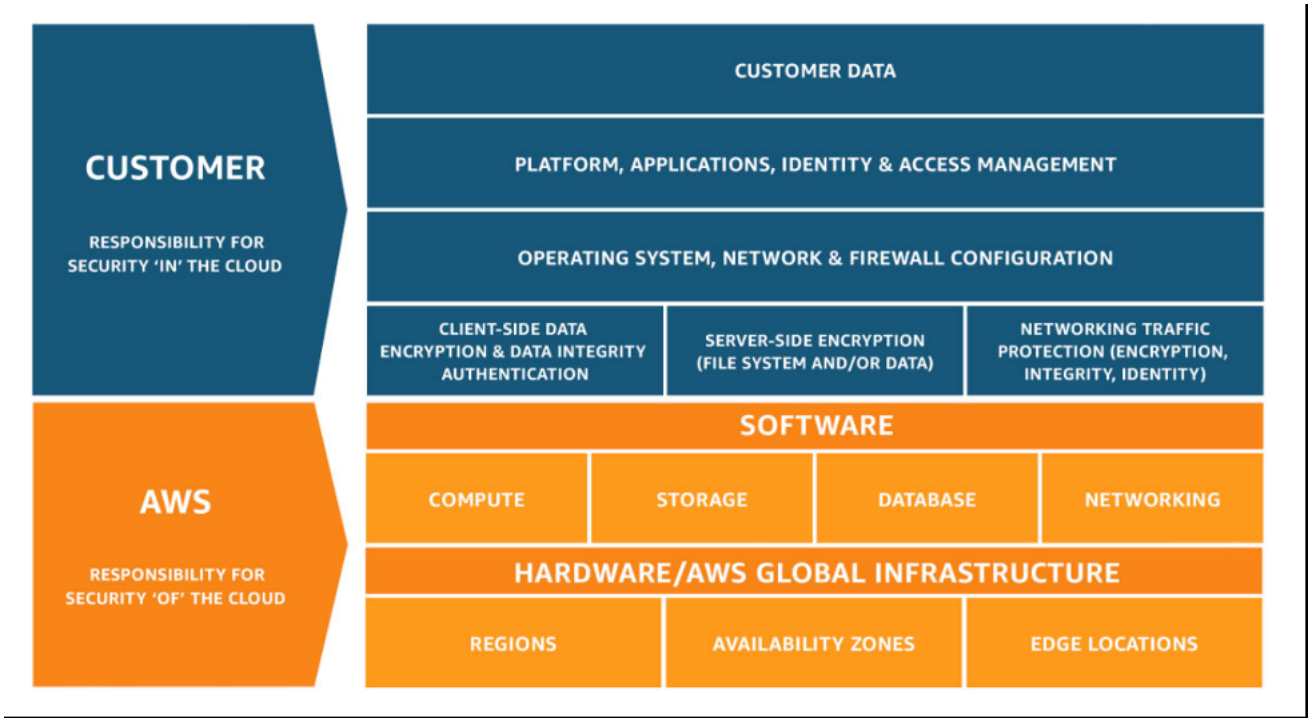

Figura: Modelo de responsabilidad compartida de AWS. AWS (en naranja) se encarga de la seguridad "de" la nube (infraestructura global, regiones, AZ, hardware, software base), mientras que el cliente (en azul) es responsable de la seguridad "en" la nube: sus datos, aplicaciones, sistemas operativos, configuraciones de red, cifrado y gestión de accesos. En resumen, AWS asegura la infraestructura;

EduTech Global debe asegurar lo que construye sobre ella.

3. Principales Retos y Riesgos de Ciberseguridad en entornos Cloud

Migrar a la nube conlleva notables ventajas, pero también presenta retos de ciberseguridad particulares. A continuación, se analizan los principales riesgos para EduTech Global en su nuevo entorno AWS, así como los desafíos a abordar en la estrategia:

- **Configuraciones incorrectas (misconfigurations):** Las malas configuraciones de seguridad en servicios cloud son una de las principales causas de brechas de datos en la nube. Según estudios, las organizaciones citan la configuración incorrecta como la amenaza número uno (68 por ciento) en entornos de nube pública. Un simple error como dejar un bucket S3 con acceso público o una regla amplia en el firewall puede exponer datos sensibles de estudiantes. EduTech debe extremar las validaciones de configuración y aprovechar herramientas (como AWS Config) para evitar este riesgo.
- **Acceso no autorizado y credenciales comprometidas:** El acceso indebido a recursos cloud ocupa un 58 por ciento de las preocupaciones de seguridad. Esto puede ocurrir por credenciales AWS expuestas (p. ej. contraseñas débiles, keys subidas por error a repositorios públicos) o por falta de controles de acceso robustos. Un atacante con credenciales válidas podría escalar privilegios o extraer datos. Es crítico implementar IAM con principio de privilegio mínimo, autenticación multifactor (MFA) en todas las cuentas privilegiadas, y rotación periódica de claves de acceso. También se debe monitorear actividades sospechosas de login (p. ej. inicio de sesión de un administrador desde una ubicación inusual) para detectar posibles secuestros de cuentas.
- **Interfaces e APIs inseguras:** Moodle y otros servicios en la nube exponen APIs o endpoints web que, si no están adecuadamente protegidos, pueden ser vector de ataque (inyecciones SQL, XSS, exploits de API). Un 52 por ciento de organizaciones reconocen las APIs inseguras como gran amenaza. Es esencial aplicar validación de entradas, usar WAF para inspeccionar tráfico HTTP(S) y mantener seguras las claves API (por ejemplo, las credenciales de integraciones de Moodle con otros servicios). AWS proporciona Signature v4 para firmar llamadas API a sus servicios, lo que se debe usar siempre en vez de conexiones sin autenticación. Asimismo, es necesario cifrar todas las comunicaciones (TLS) para evitar intercepción de datos en tránsito.
- **Secuestro de cuentas y movimientos laterales:** El account hijacking es otra preocupación (50 por ciento según encuestas). Un atacante que comprometa la cuenta cloud de EduTech (vía phishing al administrador o explotación de una VM) podría manipular recursos, desplegar malware o realizar cryptojacking. La segmentación de la infraestructura en múltiples cuentas o al menos en VPC separadas para entornos (producción, testing) puede limitar el alcance de un compromiso. AWS Organizations puede ayudar a aislar cuentas con distintos propósitos y aplicar políticas de servicio restringiendo, por ejemplo, que la cuenta de producción no pueda lanzar ciertos recursos fuera del estándar. Además, habilitar Amazon GuardDuty permitirá detectar comportamientos anómalos que podrían indicar uso indebido de la cuenta (como creación masiva de instancias fuera de horario normal, o llamadas API desde regiones no usadas).
- **Pérdida de datos y resiliencia:** En la nube, si bien AWS provee infraestructura redundante, el cliente debe asegurar la protección de sus datos frente a borrados accidentales, fallos lógicos o ataques de ransomware. Se debe contemplar la realización de backups frecuentes de datos críticos (por ejemplo, snapshots de RDS, backups de S3 a ubicaciones separadas), la habilitación de Versioning en buckets S3 para recuperar archivos borrados o modificados maliciosamente, y políticas de retención que cubran escenarios de desastre. Un riesgo adicional es la fuga de datos: sin cifrado adecuado, una intrusión podría exponer información sensible de estudiantes (PII). EduTech debe clasificar sus datos (p. ej. datos personales, calificaciones, contenidos) e

implementar cifrado tanto en reposo como en tránsito para todos ellos. Servicios como Amazon Macie pueden ayudar a detectar datos sensibles en S3 y posibles accesos no autorizados.

- **Cumplimiento normativo y visibilidad:** En entornos cloud, es fácil perder visibilidad de todos los recursos desplegados (shadow IT) y de cómo se mantienen las configuraciones con el tiempo. Esto dificulta asegurar el cumplimiento de normativas (p. ej. GDPR en datos de alumnos de la UE, estándares ISO/IEC 27001, etc.). Un reto será implementar gobernanza robusta: mantener un inventario actualizado de activos en la nube, monitorear configuraciones con AWS Config, y realizar auditorías periódicas de seguridad. La responsabilidad compartida implica que AWS ofrece certificaciones de sus capas (centros de datos, cumplimiento SOC, etc.), pero EduTech debe encargarse de configurar adecuadamente controles para cumplir sus obligaciones sobre los datos y privacidad. Cualquier brecha por mala configuración no exime a EduTech del cumplimiento, por lo que la estrategia debe incluir revisiones y validaciones continuas.

En resumen, los mayores riesgos en la nube derivan mayormente de fallos de configuración o gestión por parte del cliente, más que de fallos de AWS. EduTech Global debe afrontar estos desafíos adoptando una postura proactiva: comprendiendo el modelo de responsabilidad compartida, fortaleciendo sus controles de IAM, cifrando sus datos, monitorizando agresivamente la actividad e instaurando procedimientos claros de respuesta a incidentes. A continuación, se define una política básica de seguridad cloud y se recomiendan medidas concretas para mitigar estos riesgos.

4. Política Básica de Ciberseguridad en la Nube (Quién, Cuándo, Desde Dónde)

La política de seguridad cloud de EduTech Global establece las normas sobre quién puede acceder a los recursos en AWS, cuándo pueden hacerlo y desde dónde se permiten dichos accesos. Esta política, alineada con la estrategia global, busca garantizar que solo las personas autorizadas accedan a los sistemas adecuados, en momentos apropiados y bajo condiciones controladas. A continuación, se resumen los principios clave de la política:

- **Control de identidades – "Quién" accede:** Se definen claramente los roles y responsabilidades para el acceso a la infraestructura AWS. Solo el personal autorizado puede acceder a recursos sensibles:
  - **Administradores Cloud:** Un equipo reducido de ingenieros de TI/ciberseguridad con privilegios de administrador en la cuenta AWS. Tienen acceso completo para administrar la infraestructura, pero cada uno con su usuario IAM individual (no se comparten cuentas) y con MFA habilitado. No se utiliza la cuenta root de AWS más que para tareas imprescindibles (y está protegida con MFA hardware).
  - **Desarrolladores/DevOps:** Cuentan con accesos limitados según su función. Por ejemplo, el equipo de desarrollo puede desplegar nuevas versiones de la aplicación Moodle usando servicios CI/CD (CodePipeline, etc.) pero no tiene permisos para modificar configuraciones críticas de seguridad o acceder a datos de producción. Se aplican políticas IAM que otorgan a cada rol solo los permisos mínimos necesarios. Cualquier intento de elevación de privilegios o acceso fuera de rol será bloqueado y registrado.
  - **Usuarios finales (profesores/estudiantes):** Estos usuarios no acceden directamente a la infraestructura AWS, sino solo a la aplicación Moodle a través de Internet. Sin embargo, la política establece que sus contraseñas en Moodle deben seguir las directrices de complejidad y que, de ser posible, se integre Moodle con el sistema de identidad central (por ejemplo, SAML SSO) para heredar políticas corporativas. No se crean cuentas de IAM para usuarios finales, limitando IAM solo a administradores y servicios internos.

- **Control temporal – "Cuándo" acceden:** Se implementan restricciones y monitoreo sobre los horarios de acceso a la consola de administración y recursos críticos:

  - Las tareas administrativas rutinarias (actualizaciones, despliegues, cambios de configuración) se realizan en horario laboral estándar o en ventanas de mantenimiento programadas. Esto reduce el ruido en los logs y facilita detectar anomalías fuera de horario.
  - Si se detecta actividad administrativa fuera de las horas permitidas (por ejemplo, un inicio de sesión de administrador a las 3 AM un domingo sin cambio planificado), se generan alertas automáticas (a través de CloudWatch Events/Alarms) para el equipo de seguridad. Este equipo deberá validar si la actividad fue legítima (p. ej. una emergencia) o potencialmente maliciosa.
  - En casos excepcionales de trabajo fuera de horario (como respuesta a un incidente nocturno), la política requiere un registro justificativo del administrador indicando el motivo. Asimismo, se recomienda usar access keys temporales de corta duración o roles con sesión temporal, de modo que los accesos realizados tengan caducidad automática.
  - Las claves de acceso (API keys) que usan los servicios automatizados también se rotan periódicamente y se configuran con duraciones máximas. No se permiten credenciales permanentes sin rotación. Además, se establece un proceso de revisión trimestral de cuentas IAM inactivas para darlas de baja, garantizando que solo acceden quienes realmente lo necesitan en el momento actual.

- **Control de ubicación – "Desde dónde" acceden:** La procedencia de las conexiones a la consola AWS y a los sistemas de administración está restringida para fortalecer la seguridad:

  - Los accesos de administración a AWS (p. ej. vía consola web o AWS CLI) solo se permiten desde redes confiables. En la práctica, esto significa que únicamente desde la red corporativa de EduTech (oficinas centrales, direcciones IP fijas) o mediante VPN segura se puede entrar a la consola. Se aprovechan políticas de IAM con condiciones de IP de origen (aws:SourceIp) para bloquear intentos desde redes no autorizadas. Por ejemplo, si un atacante robara las credenciales de un administrador pero intenta usarlas desde una IP extranjera no aprobada, IAM denegará el acceso.
  - No se permite el acceso de administración desde dispositivos personales no gestionados o desde redes Wi-Fi públicas. Todos los administradores deben conectarse mediante equipos corporativos con las medidas de endpoint security correspondientes (antivirus, disco cifrado, etc.). La política "zero trust" asume que incluso dentro de la red interna, cada petición se valida y autentica.
  - Para el acceso de usuarios finales a la aplicación Moodle, dado que es pública, no se restringe geográficamente de forma estricta (ya que estudiantes/profesores podrían estar en distintos países). Sin embargo, se implementan controles geográficos a nivel de WAF/CloudFront para bloquear regiones desde las cuales no se espera ningún usuario legítimo (mitigando ciertos ataques automatizados provenientes del extranjero). También se podrían imponer retos de CAPTCHA en accesos desde ubicaciones anómalas.
  - Los servicios internos (p. ej., bases de datos, servidores SSH si los hubiera) no se exponen públicamente. Cualquier acceso de mantenimiento a servidores se realiza desde la red interna o a través de un bastion host seguro dentro de la VPC, nunca directamente desde Internet.

Autenticación y sesiones seguras: Complementando el "quién, cuándo, dónde", la política exige el uso de mecanismos de autenticación robustos en todos los accesos:

MFA obligatorio: Ya mencionado para administradores, se extiende esta exigencia a cualquier usuario IAM. Además, se recomienda implementar MFA también en la autenticación de usuarios finales en Moodle (ej. MFA opcional para cuentas de profesores con mayores privilegios en la plataforma educativa).

Contraseñas fuertes y gestión de sesiones: Las contraseñas de cuentas cloud siguen la política corporativa (mínimo 12 caracteres, complejidad alta, rotación periódica cada 90 días para cuentas IAM humanas). En AWS IAM se puede usar AWS Cognito o Identity Center con políticas de contraseña para esto. Las sesiones de consola expiran tras un periodo corto de inactividad (se configura tiempo de sesión reducido para roles sensibles). En Moodle, se configuran políticas de caducidad de sesión y se evita el almacenamiento de credenciales en servidores de aplicaciones (usando IAM roles y AWS Secrets Manager para contraseñas de BD, por ejemplo).

Registro de accesos: La política establece que todas las acciones relevantes deben quedar registradas. AWS CloudTrail ya audita accesos a la infraestructura AWS, y a nivel de Moodle se mantienen logs de autenticación de usuarios. Estos registros serán revisados regularmente según el plan de monitoreo. Cualquier intento fallido repetido de acceso o acceso denegado por políticas se considera evento de interés de seguridad, a investigar.

Segregación de entornos: Aunque no es exactamente "quién/cuándo/dónde", la política incluye que los entornos de producción y desarrollo/pruebas estén separados (idealmente en cuentas AWS distintas o al menos en VPC separadas con controles). Esto garantiza que, por política, ningún desarrollador pruebe cambios directamente en prod y que credenciales de prueba no se usen en entornos reales. También facilita que los accesos "de quién" varíen: los desarrolladores tienen permisos amplios en la cuenta de dev/test pero muy acotados en prod.

En síntesis, la política básica de seguridad cloud de EduTech Global crea un marco de control de accesos riguroso: sólo personal autorizado, en el momento adecuado y desde ubicaciones seguras puede acceder a sistemas críticos. Cualquier excepción requiere aprobación y monitoreo. Esta política, junto con la estrategia técnica, asegura que la migración a AWS mantenga (e incluso eleve) el nivel de seguridad respecto al entorno on-premise.

5. Herramientas y Servicios de Seguridad Recomendados en AWS

Para implementar la estrategia de seguridad, EduTech Global aprovechará diversos servicios nativos de AWS y herramientas de terceros cuando sea necesario. AWS ofrece una amplia gama de servicios de seguridad y cumplimiento que permiten cubrir cada uno de los pilares (IAM, datos, infraestructura, detección/respuesta). A continuación, se detallan las herramientas recomendadas y cómo encajan en la arquitectura segura:

- **Gestión de Identidades y Accesos (IAM):** El servicio central es AWS IAM, con el que se gestionan usuarios, roles y políticas de acceso granulares. Se deben crear políticas IAM personalizadas que restrinjan acciones por rol; por ejemplo, una política para administradores de base de datos que permita rds:* en los recursos de RDS de la cuenta, pero sin tocar S3 o IAM. Igualmente, políticas para desarrolladores que solo les dejen desplegar en determinados recursos (quizá vía CodeDeploy) pero no alterar configuraciones globales. Es recomendable utilizar grupos de IAM para asignar permisos por rol de trabajo en lugar de adjuntar políticas a usuarios individuales, facilitando la administración. AWS IAM también permite establecer condiciones en las políticas (como la restricción de IP de origen ya mencionada en la política). Para mayor seguridad y escalabilidad:
  - **AWS Organizations:** Si EduTech decide manejar múltiples cuentas (prod, dev, sandbox), Organizations permite consolidar la facturación y aplicar Service Control Policies (SCPs) a nivel organizacional. Por ejemplo, una SCP podría prevenir que cualquier cuenta hijo cree recursos fuera de la región aprobada (p. ej. limitar solo a EU-West-1) o que use servicios no aprobados (denegar IAM usuarios fuera del SSO, etc.).

- **AWS SSO / IAM Identity Center:** Facilita la integración con identidades corporativas existentes (via SAML, OAuth) y proporciona gestión centralizada de acceso a múltiples cuentas AWS y aplicaciones. Con Identity Center, EduTech puede federar el inicio de sesión de sus administradores usando, por ejemplo, credenciales de Azure AD o Google Workspace, aplicando políticas de contraseñas y MFA desde ahí.
- **Servicios de directorio:** Si se requiere integración con LDAP/Active Directory para autenticar usuarios (por ejemplo, personal de TI), AWS ofrece AWS Directory Service (AD Connector o Managed AD) para unificar identidades on-premise con la nube.
- **MFA y AWS Config con IAM:** Además de habilitar MFA, AWS Config tiene reglas predefinidas ("root-account-mfa-enabled", "iam-user-mfa-enabled") que EduTech activará para garantizar que ninguna cuenta privilegiada carezca de MFA. Cualquier violación genera una alerta a seguridad. Asimismo, se considerará el uso de AWS CloudTrail eventos con AWS CloudWatch Alarms para detectar usos de la cuenta root y notificar inmediatamente (ya que normalmente no debe usarse).
- **Herramientas externas:** En caso necesario, se podrían evaluar herramientas de Privileged Access Management (PAM) de terceros en AWS Marketplace, aunque IAM junto con las buenas prácticas mencionadas debería cubrir las necesidades.

- **Protección de Datos:** Garantizar la confidencialidad e integridad de los datos educativos es prioritario. AWS provee varias herramientas para proteger datos en reposo, en tránsito y durante su ciclo de vida:

  - **Cifrado con AWS KMS:** El servicio AWS Key Management Service centraliza la gestión de claves de cifrado. Todas las claves (CMKs) para cifrado de S3, EBS, RDS, etc. se manejarán en KMS, permitiendo control granular sobre quién/qué puede usarlas. Por ejemplo, se puede limitar que solo el role de la aplicación Moodle pueda usar la CMK que descifra archivos de curso en S3. Además, KMS provee rotación automática de claves (cada año) y registros de uso de clave (CloudTrail registra cada vez que se usa una clave KMS, útil para auditoría).

- **Encriptación en reposo y en tránsito: Como norma general, todo dato sensible estará cifrado tanto en reposo como en tránsito. Esto implica:**

  - Activar cifrado del lado servidor (SSE) en todos los buckets S3 (con KMS o al menos AES-256 por defecto) y en las bases de datos RDS/EBS subyacentes. Cabe destacar que RDS permite cifrado transparente de la base de datos con KMS al crear la instancia, y cifrado de snapshots.
  - Uso obligatorio de protocolos seguros: HTTPS/TLS para todas las comunicaciones web (apoyado en ACM para certificados) y IPSec/OpenVPN para conexiones VPN. Internamente en la VPC, aunque el tráfico pueda considerarse confiable, también se puede habilitar TLS mutuo para conexiones criticas (por ej. si Moodle se conectase a un microservicio en otra VPC).
  - **Client-side encryption:** En casos extremos, EduTech podría cifrar ciertos datos antes de subirlos a la nube (cifrado del lado cliente) para una capa adicional, aunque gestionarlo añade complejidad. En su lugar, se confiará en KMS y servicios AWS validados.

- **AWS Secrets Manager and Parameter Store:** Para manejar información sensible como contraseñas de la base de datos, claves API de integraciones, etc., se usará Secrets Manager o Parameter Store (parte de AWS Systems Manager). Estas herramientas almacenan secretos de forma cifrada y permiten rotarlos automáticamente. Por ejemplo, la contraseña de la base de datos Moodle puede almacenarse en Secrets Manager; la aplicación Moodle (en EC2) la recupera dinámicamente vía llamadas API autenticadas con su rol IAM, en lugar de tenerla en texto plano en un archivo de configuración. Secrets Manager también puede rotar credenciales (p. ej. contraseñas de RDS) cada X días de forma automática sin interrumpir el servicio.

- **Data Loss Prevention (DLP) y monitoreo de datos sensibles:** AWS ofrece Amazon Macie, un servicio que aplica ML para descubrir y proteger datos sensibles en S3 (como datos personales, identificadores, etc.). Se recomienda habilitar Macie para los buckets con información crítica de estudiantes (por ejemplo, exportaciones de datos, backups) – Macie alertará si detecta, por ejemplo, volúmenes inusuales de datos expuestos o patrones de datos personales sin cifrar. Adicionalmente, se pueden aplicar etiquetas de clasificación a los datos (p. ej. confidencial, interno) y usar AWS Glue Data Catalog junto con Macie para mantener un inventario de dónde residen datos sensibles.

- **Control de versiones y borrado:** En S3 se habilita Versioning para mantener versiones históricas de objetos, lo que protege frente a borrados accidentales o ataques de ransomware (pudiendo restaurar versiones anteriores). También se activa MFA Delete en los buckets más sensibles, requiriendo MFA para borrar versiones o el bucket entero. Esto evita que incluso con credenciales comprometidas se puedan purgar datos sin una autenticación adicional física.

- **Herramientas de backup y archivado:** Además de confiar en snapshots automatizados de RDS, EduTech utilizará AWS Backup, un servicio que orquesta backups centralmente. Con AWS Backup se define una política (Backup Plan) que incluye respaldos regulares de RDS, EFS, volúmenes EBS de servidores, etc., con copia a almacenes de almacenamiento vault cifrados. Se programa la ejecución diaria/nocturna de backups y se prueban restauraciones periódicamente. Para archivos de largo plazo, se considera AWS Glacier o Deep Archive para almacenar históricos de datos (cumpliendo con retención de datos de alumnos, por ejemplo).

- **Protección de datos en dispositivos cliente:** Si bien AWS no cubre esto directamente, la estrategia incluye asegurar que los endpoints (PCs de usuarios, móviles) que acceden a Moodle usen conexiones HTTPS y, en lo posible, implementar cifrado en capa de aplicación para datos especialmente sensibles (por ejemplo, cierto contenido podría requerir descarga cifrada con DRM, etc., aunque esto es más bien consideraciones de la app Moodle misma).

- **Protección de la Infraestructura:** Aquí se engloban las medidas para endurecer la plataforma cloud a nivel de red, sistemas operativos y aplicaciones, reduciendo la superficie de ataque:

  - **Firewalls de red (Security Groups y NACLs):** Ya mencionado en la arquitectura, se aplican reglas restrictivas. Cada Security Group actúa como firewall stateful en cada instancia: el SG de los servidores Moodle permite únicamente tráfico entrante desde el ALB en puerto 80/443 y desde el SG del bastion (si existe) en puerto 22 (aunque idealmente 0 porque usamos SSM). El SG de la base de datos solo acepta tráfico del SG de las instancias Moodle en puerto 3306. No se permiten rangos abiertos al mundo (0.0.0.0/0) salvo en el ALB que necesita escuchar peticiones web públicas, pero incluso ahí con WAF de por medio. Las Network ACLs, siendo stateless, añaden una capa más para bloquear puertos no usados a nivel subnet (por ejemplo, denegar todo tráfico entrante no origen del ALB hacia la subred privada de app). Estas configuraciones implementan la segmentación de red que aísla la capa de aplicación de la de datos y del resto de la red corporativa.
  - **AWS WAF (Web Application Firewall):** Se implementa frente al ALB o CloudFront para proteger la capa de aplicación web. AWS WAF permite definir reglas para bloquear patrones maliciosos comunes: inyecciones SQL, scripts XSS, exploraciones de directorios, etc. Se puede iniciar con las AWS Managed Rules (conjuntos preconfigurados actualizados regularmente con mitigaciones para CVEs conocidas y tráfico malicioso habitual) y luego personalizar reglas específicas para Moodle (por ejemplo, bloquear accesos al script install.php de Moodle que no debería ser usado en producción, limitar tamaño de ciertos parámetros, etc.). El WAF también ayuda a mitigar intentos de login por fuerza bruta añadiendo rate limiting a la página de login: ej. no más de X intentos por minuto por IP, lo cual se integra con las políticas de Moodle internas.
  - **AWS Shield:** Como la plataforma es pública, existe riesgo de ataques DDoS. AWS Shield Standard está automáticamente habilitado sin costo, brindando protección básica L3/L4 (SYN floods, UDP floods) en las IPs de AWS. Para mayor protección, EduTech puede suscribirse a AWS Shield Advanced (servicio pago) que brinda mitigación ampliada, dashboard

24/7 y integración con el AWS DDoS Response Team. Con Shield Advanced se pueden proteger explícitamente el ALB y CloudFront distributions de Moodle y obtener alertas si se sufre un ataque volumétrico, con posibilidad de crear mitigaciones específicas (como bloquear ciertos patrones de tráfico global).

- **Hardening de instancias y sistemas:** A nivel de servidores EC2, se siguen buenas prácticas de hardening: usar la última versión LTS de sistema operativo soportado, deshabilitar puertos/servicios no necesarios (por ejemplo, si es una AMI genérica, apagar servicios de ejemplo), reforzar configuraciones de Apache/PHP (limitando tamaños de subida, etc.) y aplicar parches de seguridad del SO y Moodle inmediatamente. Para facilitar esto, AWS Systems Manager Patch Manager puede automatizar la instalación de parches en EC2, manteniendo un inventario del estado de cada instancia. Asimismo, se instala un agente de monitoreo de integridad en los servidores (p. ej. AWS Inspector Agent, si corresponde, o herramientas de terceros como Falco/OSSEC) para detectar cambios inesperados en archivos críticos o procesos maliciosos.
- **Amazon Inspector:** Servicio que escanea vulnerabilidades en instancias EC2 y en imágenes de contenedores/ECR. Dado que Moodle se ejecuta en EC2, se habilitará Amazon Inspector para hacer análisis periódicos del sistema en busca de vulnerabilidades de software o configuraciones débiles. Inspector aprovechará la información de Systems Manager (listado de paquetes instalados) y alertará si, por ejemplo, hay un Apache desactualizado con CVE conocida. También puede escanear las imágenes docker si se usara Moodle containerizado en ECS/EKS (en este caso no parece, pero es una posibilidad futura). Los hallazgos de Inspector se integran en AWS Security Hub para dar visibilidad central.
- **AWS Security Hub:** Precisamente, Security Hub se habilita como un panel unificado de seguridad. Agrega hallazgos de varios servicios: GuardDuty, Inspector, Macie, IAM Access Analyzer, etc., y los compara con estándares (AWS Foundational Security Best Practices, CIS AWS Benchmark). Esto permitirá a EduTech ver en un solo dashboard su grado de cumplimiento de mejores prácticas AWS y los incidentes o riesgos detectados. Por ejemplo, Security Hub alertará si detecta a través de GuardDuty una actividad anómala o si mediante Config ve un bucket público, con severidades asignadas. Este servicio será utilizado diariamente por el equipo de seguridad para priorizar acciones.
- **Registro y monitoreo de integridad:** Además de los logs en CloudWatch mencionados, se puede emplear AWS CloudTrail (ya habilitado) no solo para auditoría sino también con Amazon EventBridge (CloudWatch Events) para reaccionar a ciertos eventos. Por ejemplo, al detectarse que alguien deshabilita un log o borra un Security Group, se puede automatizar una respuesta (una Lambda que vuelva a habilitarlo o notifique al instante). La infraestructura se diseñará para ser inmutable en la medida de lo posible (cambios aplicados vía Infrastructure as Code), de forma que cualquier cambio manual sea excepcional y digno de revisión.
- **Pruebas de penetración regulares:** Si bien no es una "herramienta AWS" per se, la política de protección de infraestructura incluye realizar pentests periódicos o bug bounty para la aplicación Moodle desplegada en AWS. AWS permite realizar pruebas de penetración en ciertos servicios (EC2, RDS, CloudFront, etc.) con previo aviso o bajo sus políticas, para identificar vulnerabilidades en la capa aplicativa que las herramientas automatizadas podrían no descubrir.

- **Detección de Amenazas y Respuesta (Monitorización e Inteligencia):** Un pilar crítico es la capacidad de detectar actividades maliciosas e incidentes en tiempo real y responder ágilmente. AWS ofrece servicios inteligentes gestionados para este fin:

  - **Amazon GuardDuty:** Servicio de Threat Detection que analiza de forma continua logs de AWS (CloudTrail, VPC Flow Logs, DNS logs) buscando patrones de ataque o anomalías. EduTech habilitará GuardDuty en su cuenta; al hacerlo, por ejemplo, si un día una instancia EC2 empieza a conectarse a un servidor conocido de botnet o hace minería de criptomonedas, GuardDuty generará un finding (alerta) de severidad alta. Igualmente detecta si una credencial IAM se usa desde una IP inusual o si hay exploraciones de puertos desde nuestra instancia, etc. Estas alertas se enviarán al equipo de seguridad (vía email/SNS) y también

aparecerán en Security Hub. GuardDuty es un servicio "sin agentes" – analiza los flujos y eventos existentes – por lo que es sencillo de mantener.

- **AWS CloudWatch and Alarms:** Más allá de métricas de desempeño, se configura CloudWatch para alarmas de seguridad. Por ejemplo: un alarm que se dispare si hay más de X mensajes de error de autenticación en el log de Moodle en 5 minutos (posible ataque de fuerza bruta). O una alarma si el tráfico saliente de una instancia supera cierto umbral (posible exfiltración de datos). Estas alarmas activarán notificaciones (SNS emails, integración con Slack, etc.) y potencialmente acciones automatizadas (por ej., aislar la instancia de la red colocando un Security Group restrictivo cuando se detecta un comportamiento anómalo).
- **AWS Config y AWS CloudTrail:** Ya descritos, también juegan un rol en detección. AWS Config puede considerarse un sensor de compliance en tiempo real: cualquier cambio de configuración (p. ej. alguien abre un puerto, cambia una policy IAM) queda registrado, evaluado contra reglas, y genera alertas si va contra la baseline. CloudTrail ofrece el histórico de eventos; una práctica recomendada es configurar CloudTrail Lake o enviar los logs a un SIEM externo para correlacionar eventos complejos. No obstante, incluso sin SIEM, AWS ofrece CloudTrail Insights para marcar patrones inusuales de API calls, lo que se aprovechará.
- **Amazon CloudWatch Logs Insights / ELK:** Para investigaciones más profundas, se puede usar CloudWatch Logs Insights (un motor de consulta) para buscar indicios en los logs agregados. Por ejemplo, filtrar en logs de ALB todas las IP que hicieron más de 100 requests por minuto a /login/index.php de Moodle. Si EduTech requiere más capacidades, podría montar un stack ELK (Elasticsearch, Kibana) en AWS para analizar logs, aunque esto conlleva mantenimiento; una alternativa es Amazon OpenSearch Service (servicio gestionado de Elasticsearch) si se necesita análisis avanzado.
- **AWS SNS y AWS Chatbot:** Para asegurar que ninguna alerta crítica pase desapercibida, se integrará Amazon SNS para envío de notificaciones multi-canal (correo al equipo, SMS si es 24/7, etc.). AWS Chatbot también puede usarse para recibir notificaciones de CloudWatch, Security Hub, etc., directamente en canales de Slack o Microsoft Teams del equipo de respuesta, agilizando la visibilidad.
- **AWS Detective:** En caso de incidentes complejos, AWS ofrece Amazon Detective, que puede agregarse posteriormente. Detective toma las alertas de GuardDuty, CloudTrail, etc. y las conecta para facilitar investigaciones (traces de lo que hizo una entidad maliciosa en la cuenta). Si EduTech sufre, por ejemplo, un compromiso de una credencial, Detective ayudaría a mapear todas las acciones realizadas por esa identidad antes y durante el incidente, acelerando el análisis forense.
- **Servicios de terceros (Marketplace):** Adicionalmente, la estrategia considera la posibilidad de incorporar herramientas especializadas si fuese necesario. Por ejemplo, un IDS/IPS de red de terceros en el VPC (aunque con GuardDuty y WAF ya hay bastante cobertura), o soluciones EDR en las instancias EC2 (AWS colabora con partners como CrowdStrike, etc.). Cualquier solución añadida debe integrarse con los flujos de alertas ya establecidos.

Todas estas herramientas combinadas proporcionan una arquitectura de seguridad en capas. Como resume un blog: AWS ofrece soluciones para IAM (usuarios y roles), KMS (cifrado), Config (monitoreo de configuraciones) y GuardDuty (detección de amenazas) para ayudar al cliente a gestionar su parte de la seguridad. La clave es configurarlas adecuadamente y asegurarse de que generen acciones: de nada sirve CloudTrail registrando eventos si nadie los revisa. Por ello, a continuación se describe brevemente cómo EduTech implementó algunas de estas medidas en un entorno de prueba y cómo se gestionará la monitorización continua y respuesta a incidentes.

6. Implementación de Medidas de Seguridad (Reto opcional en AWS)

(Nota: Esta sección describe una implementación práctica opcional realizada en una cuenta gratuita de AWS para validar parte de la estrategia. Incluye las configuraciones efectuadas, las evidencias obtenidas y las limitaciones encontradas al usar la capa gratuita.)

Para demostrar la eficacia de la estrategia, se procedió a configurar un entorno AWS de prueba, aplicando medidas de seguridad clave hasta donde las limitaciones de la cuenta gratuita lo permitieron. A continuación, se enumeran las principales acciones realizadas y observaciones:

- **Configuración de IAM y MFA:** Se creó un usuario IAM administrativo de prueba (AdminEduTech) sin privilegios de root, al cual se le asignó una política IAM custom restringida (basada en PowerUser, sin permiso sobre Billing ni cambio de políticas IAM críticas). Inmediatamente se habilitó MFA virtual (app Authenticator) para este usuario y se verificó su funcionamiento. Evidencia: Al intentar login sin el código MFA, el acceso fue denegado. También se probó añadir una condición de IP de origen en la policy: se simuló un intento de login desde una IP no permitida (usando TOR browser, por ejemplo) y CloudTrail registró el evento de inicio de sesión fallido por restricción de condición, confirmando que la política funciona.
- **Roles IAM y mínimos privilegios:** Se definió un rol IAM llamado MoodleEC2Role pensado para asignar a instancias EC2 de la aplicación. Este rol tiene una política que le permite únicamente leer de un bucket S3 específico (edutech-moodle-data) y escribir logs en CloudWatch. Se lanzó una instancia EC2 t2.micro en free tier, con Amazon Linux 2, y se le adjuntó el rol MoodleEC2Role. En pruebas dentro de la instancia, se confirmó que podía obtener objetos del bucket S3 designado mediante AWS CLI, pero no enumerar ni acceder a ningún otro recurso (e.g., al intentar listar contenido de otro bucket, la solicitud fue denegada con error 403 Access Denied, evidenciando el principio de mínimo privilegio).
- **Buckets S3 privados y bloqueo público:** Se creó el bucket S3 edutech-moodle-data para almacenar archivos de Moodle. Durante la creación, se mantuvieron habilitadas las opciones de "Block Public Access" para el bucket. Luego, se subió un archivo de muestra prueba.txt con datos ficticios. Como prueba, se intentó acceder públicamente al objeto vía URL sin credenciales: el resultado fue un error 403 Forbidden, lo cual confirma que el bucket no permite acceso público. En la consola S3, la sección de Permissions mostraba claramente "Bucket and objects not public" (bucket y objetos no públicos) como estado. Adicionalmente, se añadió una etiqueta al bucket indicando su nivel de sensibilidad ("confidencial"), pensando en futuras integraciones con Macie para clasificar contenido. La evidencia de la configuración se capturó en capturas de pantalla de la consola S3 que muestran el indicador de bloqueo público activo y el intento de acceso fallido.
- **CloudTrail y CloudWatch Logs:** Se habilitó CloudTrail en la cuenta (free tier incluye trail para management events). Se configuró para enviar los logs a un bucket S3 edutech-cloudtrail-logs. Se validó generando actividad: por ejemplo, realizando una acción sencilla como listar instancias EC2. Luego, en la consola de CloudTrail ¿Event History, apareció el evento DescribeInstances con detalles de quién (el usuario AdminEduTech) y cuándo. Esta es evidencia de que CloudTrail está registrando correctamente. Asimismo, se habilitó CloudWatch Logs en la instancia EC2 instalando el agente de CloudWatch. Se configuró para enviar el syslog de Linux y los logs de Apache (simulando que Moodle estuviera sirviendo tráfico) hacia CloudWatch. Tras generar unas peticiones, se verificó en CloudWatch Logs Insights que las entradas aparecían. Por ejemplo, se pudo consultar cuántas veces la IP 203.0.113.5 accedió al recurso /login/index.php en los últimos 10 minutos. Esto demuestra la capacidad de auditoría en tiempo real.
- **AWS Config (reglas de seguridad):** En la región us-east-1, se activó AWS Config y se añadió una regla gestionada "s3-bucket-public-read-prohibited" para asegurarse de que ningún bucket permita lectura pública. Como prueba, se cambió intencionalmente la policy del bucket de logs (no crítico) para permitir acceso público de lectura. En cuestión de minutos, AWS Config marcó

la regla como No conforme para ese bucket y generó un hallazgo visible en la consola (evidencia: captura de pantalla de la regla violada con el bucket listado). Esto confirmó el valor de Config para detectar configuraciones inseguras. (Después, se revirtió la policy del bucket a privada). Otras reglas habilitadas incluyeron "iam-user-mfa-enabled" (para verificar que todos los usuarios IAM humanos tengan MFA). Al crear un usuario de prueba sin MFA, la regla saltó a No conforme, lo cual fue otra evidencia tangible.

- **GuardDuty y CloudWatch Alarms:** Se habilitó Amazon GuardDuty (que ofrece 30 días de prueba gratuita). Dado lo breve de la prueba, no surgieron hallazgos reales de amenaza, por lo que para evidenciar su funcionamiento se utilizó una técnica de simulación que AWS proporciona: ejecutar un script de AWS GuardDuty Tester que genera findings simulados (como si se detectara un puerto sospechoso o malware en la red). Al correr el simulador, en la consola de GuardDuty aparecieron los findings con severidades variadas (simulando por ejemplo "Recon:EC2/PortProbe" y "Trojan:EC2/DNSDataExfiltration"). Estas entradas, marcadas claramente como pruebas, demostraron la capacidad de GuardDuty para ingresar alertas. Se configuró una alerta de CloudWatch que monitoriza el stream de findings de GuardDuty (via EventBridge) y envía una notificación por email al equipo cuando haya alguna de severidad Alta. Al ejecutar el simulador de nuevo con un finding de alta severidad, se recibió efectivamente el correo de alerta (evidencia: captura del email de SNS alertando del hallazgo de GuardDuty).
- **CloudWatch alarmas de performance/anomalías:** También se creó una alarma sencilla en CloudWatch: un alarm que se activa si la CPU de la instancia EC2 supera 80 por ciento por 5 minutos consecutivos. Dado que en free tier la instancia es pequeña, para probar la alarma se ejecutó una carga intensiva (stress test) en la instancia elevando la CPU. La alarma entró en estado ALARM y envió una notificación por SNS. Esto comprueba que ante un uso anómalo de recursos (posible indicador de compromiso), el equipo sería notificado. Otra alarma configurada fue a nivel de facturación (Billing Alarm) para alertar si los gastos mensuales excedían 0 euros (útil en free tier para detectar cargos accidentales), la cual se probó forzando un gasto mínimo (activando un servicio fuera de la capa gratuita) y fue disparada.

Limitaciones encontradas: La cuenta gratuita de AWS impone ciertas restricciones que se observaron durante la implementación:

- **Recursos limitados:** Solo se pudo ejecutar una instancia EC2 de baja capacidad (t2.micro) simultáneamente sin costo. Esto limita probar un clúster autoescalable multi-AZ. Del mismo modo, servicios como RDS solo permiten instancias pequeñas en free tier (db.t2.micro) y no en multi-AZ a menos que se asuman costos. Por ello, no se pudo simular completamente la arquitectura redundante (se probó con una sola AZ).
- **Períodos de prueba en servicios de seguridad:** Servicios como GuardDuty, Macie, Inspector, etc., ofrecen periodos de prueba (30 días). Pasado ese tiempo, continuar usándolos generaría costos. Durante la práctica, solo GuardDuty e Inspector se habilitaron brevemente. Macie no se probó debido a que requiere habilitarlo globalmente y potencialmente clasificar datos (actividad que podría generar costo tras el análisis inicial). Sin embargo, se revisó su consola en modo trial para ver cómo reportaría un hallazgo (sin incurrir en gastos significativos).
- **AWS WAF y Shield Advanced:** Estas soluciones no tienen free tier. No se pudo implementar AWS WAF en la práctica porque requiere asociarlo a un distribuidor (ALB/CloudFront) y tiene un costo por regla/solicitud. En su lugar, se configuró una pequeña regla de prueba en el ALB mediante la funcionalidad básica de ALB (una regla que bloqueaba una IP específica) para simular control de acceso. Shield Advanced tampoco se activó por ser un servicio enterprise de pago.
- **Herramientas externas:** No se pudo integrar soluciones de terceros (p.e. un agente antivirus en EC2) por simplicidad, pero se asume que en producción EduTech podría instalar software adicional en las instancias (por ejemplo, ClamAV para escanear archivos subidos a Moodle).

- **Experiencia de usuario free tier:** Algunas tareas debieron realizarse manualmente debido a la escala reducida. Por ejemplo, para evidenciar la rotación de claves KMS, se simuló cifrar y descifrar datos con una CMK pero no se esperó un año a la rotación automática. Igualmente, la generación de suficiente tráfico malicioso real para probar detecciones no era viable, por lo que se dependió de simuladores.

A pesar de las limitaciones, la implementación en la cuenta gratuita permitió validar aspectos fundamentales de la estrategia: IAM con MFA y restricciones de IP funcionando, S3 privado con bloqueo público, logs de CloudTrail y CloudWatch confirmando trazabilidad, Config detectando desviaciones de configuración, GuardDuty listo para alertar de amenazas, y alarmas básicas de CloudWatch activas. Todo esto proporciona confianza en que, al escalar a un entorno de producción completo, las mismas medidas (extendidas adecuadamente) protegerán la infraestructura de EduTech Global.

7. Monitorización, Respuesta ante Incidentes y Mejores Prácticas

La seguridad en la nube no termina con la implementación de controles; requiere una monitorización continua y la capacidad de responder eficazmente a incidentes. EduTech Global adoptará un enfoque proactivo, apoyado en las herramientas mencionadas, para mantener vigilancia 24/7 sobre su entorno AWS y un plan estructurado de respuesta. Además, incorporará mejores prácticas y procesos de mejora continua. Esta sección describe cómo se llevará a cabo la monitorización, el plan de respuesta ante incidentes y las prácticas recomendadas a seguir.

Monitorización continua: Mediante la combinación de CloudTrail, CloudWatch, GuardDuty, Config, etc., el equipo de seguridad dispone de visibilidad casi total de la actividad en la nube:

- Todos los logs de auditoría (CloudTrail), de servicio (ELB, RDS) y de la aplicación Moodle (a través de CloudWatch Logs) se recopilan y almacenan centralizadamente. Se define una política de retención: por ejemplo, logs críticos de seguridad se retienen al menos 1 año en S3/Glacier para posibles análisis forenses.
- Se establecen revisiones diarias de los paneles de Security Hub y GuardDuty. Cada mañana, un analista de seguridad verifica si hay nuevos hallazgos de alta severidad. También se configuran alertas inmediatas (vía SNS/Email/Slack) para eventos críticos, de modo que no se espere hasta la revisión diaria en caso de algo urgente (p. ej. se detectó una clave AWS expuesta públicamente – GuardDuty puede detectar esto – se actúa de inmediato).
- **Reuniones semanales de revisión de seguridad:** El equipo de TI se reunirá al menos una vez por semana para repasar el estado de seguridad en AWS: revisar métricas, tendencias de incidentes (fallidos de login, intentos de escaneo detectados), estado de parches, cumplimiento de políticas (informes de Config) y planificar acciones preventivas (como endurecer alguna configuración si se observó actividad sospechosa constante).
- **Pruebas de los sistemas de monitoreo:** Periódicamente se harán simulacros para comprobar que las alertas funcionan y el equipo responde en tiempos adecuados. Por ejemplo, un ejercicio trimestral podría ser simular un comportamiento de insider malicioso (lanzando manualmente una instancia fuera de política) y verificar que Config/GuardDuty lo señalan y que el equipo sigue el proceso de respuesta correctamente.
- **Integración con SIEM corporativo:** Si EduTech tiene un SOC o SIEM on-premise, se considerará integrar los logs de AWS a esa plataforma para correlacionar con eventos de toda la empresa. AWS ofrece integraciones o se puede hacer streaming de CloudTrail/GuardDuty events hacia sistemas como Splunk, QRadar, etc. De momento, se usará Security Hub como pseudo-SIEM cloud.

Respuesta ante incidentes: EduTech Global dispone de un Plan de Respuesta a Incidentes adaptado al entorno cloud, basado en las mejores prácticas (p. ej. NIST 800-61) y en el plan que ya tenía on-premise, ahora actualizado. El plan define un equipo de respuesta (CSIRT) con roles (coordinador, analistas técnicos, comunicaciones, legal, etc. como ya se había establecido en la organización) y sigue las siguientes fases estructuradas:

1. **Detección y Análisis:** La fase inicial consiste en identificar rápidamente que está ocurriendo un incidente y evaluarlo. En la nube, esto se logra a través de las alertas de las herramientas mencionadas y también de reportes de usuarios. Por ejemplo, un pico inusual de tráfico detectado por CloudWatch o un hallazgo de GuardDuty constituyen disparadores. El equipo de seguridad valida la alerta, reuniendo evidencias: logs de CloudTrail, métricas, etc., para determinar la naturaleza y alcance del problema (p. ej., ¿es un ataque DDoS, una intrusión en una instancia, una credencial comprometida?). La rapidez es clave: se utilizan dashboards y consultas predefinidas para el análisis inicial. (En el plan anterior on-premise se usaban sistemas ELK para correlación; ahora se apoya en AWS Security Hub y servicios cloud equivalentes). Si un usuario final o administrador reporta comportamiento extraño (ej. la aplicación Moodle está mostrando contenido erróneo), eso también inicia esta fase.

2. **Contención:** Una vez identificado un incidente, el primer objetivo es frenar su avance y limitar el daño. En AWS, existen capacidades muy ágiles para contención:

   - **Aislamiento de instancias afectadas:** Si se sospecha que una instancia EC2 fue comprometida (ej. indicios de malware), se aislará inmediatamente sacándola del grupo de autoescalado (para que deje de recibir tráfico) y aplicándole un Security Group aislado que bloquee todo el tráfico excepto el del equipo de respuesta. AWS SSM también permite aislar instancias. Esto confina la amenaza y permite análisis offline.
   - **Bloqueo de accesos y credenciales:** Si el incidente es una fuga de credenciales (por ej. una API key expuesta), la credencial comprometida se desactiva o rota enseguida. Si un usuario malicioso obtuvo acceso a una cuenta, se le revocan los permisos o se suspende la cuenta IAM involucrada. En AWS se puede usar IAM Access Analyzer para buscar accesos no autorizados y en casos extremos AWS puede, a solicitud, bloquear temporalmente la cuenta entera si se cree que fue secuestrada.
   - **Filtrado de tráfico malicioso:** En caso de ataque externo (DDoS, exploit), se implementan reglas de contención en la capa perimetral. Por ejemplo, usando AWS WAF se bloquean IPs o patrones específicos del ataque en curso. Si es un DDoS masivo, se coordina con AWS Shield (el equipo de Shield Advanced si está contratado) para absorción del tráfico.
   - **Contención en servicios gestionados:** Si el incidente involucra un servicio alto nivel (por ejemplo, un bucket S3 con datos expuestos), la acción de contención es sencilla: cerrar el acceso público del bucket o incluso habilitar S3 Block Public Access a nivel de cuenta para garantizar que nada sea público mientras se investiga. Si fuese una base de datos comprometida, se podría congelar su acceso (ej. quitarle la accesibilidad pública si la tuviera, o pausar la instancia Aurora) para impedir más filtraciones.
   - Todas estas acciones de contención se realizan siguiendo runbooks predefinidos para no improvisar en caliente. Se prioriza mantener la continuidad de la plataforma educativa siempre que sea seguro; por ejemplo, aislar uno de los servidores de Moodle pero mantener otro sirviendo si es intacto, mostrando quizás un mensaje de "modo mantenimiento parcial" a los usuarios.

3. **Erradicación:** Tras contener, se elimina la amenaza de raíz. Según el incidente, esto incluye:

   - **Remoción de malware/puerta trasera:** Si en la fase de análisis forense de la instancia aislada se halla malware, se elimina o, más comúnmente en nube, se reemplaza la instancia por una nueva limpia. De hecho, AWS fomenta tratar los servidores como efímeros: lo más rápido es desplegar una instancia nueva desde la AMI de oro parcheada y desechar la comprometida (tras recoger evidencias). Así se asegura erradicar cualquier residuo.

- **Aplicación de parches y correcciones:** Si la intrusión explotó una vulnerabilidad (p. ej. un plugin de Moodle vulnerable), se parchea inmediatamente en todos los sistemas similares. Esto podría implicar actualizar el código de la aplicación, la configuración (cerrar el vector) y usar Infrastructure as Code para que el parche se incluya en futuras instancias.
- **Revocación y recreación de credenciales:** Todas las credenciales potencialmente expuestas se regeneran. Por ejemplo, si se sospecha que un atacante accedió a la base de datos, se cambiarán las contraseñas de ésta y las claves API asociadas, y se invalidarán tokens de usuarios si aplicase. AWS Secrets Manager facilita la rotación de secretos para este fin.
- **Limpieza de recursos no autorizados:** En algunos incidentes, un atacante podría crear recursos (ej. instancias para minado, snapshots de datos). La erradicación incluye revisar la cuenta AWS en busca de recursos inesperados y eliminarlos. Herramientas como GuardDuty pueden indicar si hay instancias sospechosas corriendo (EC2 bajo control de botnet).
- **Fortalecimiento post-incidente:** Se cierran brechas configurativas descubiertas: si fue un bucket abierto, se implementan cambios para que no vuelva a ocurrir (como políticas SCP que impidan hacer buckets públicos). Esta parte se superpone con la fase de lecciones aprendidas, pero algunas mejoras se aplican de inmediato para prevenir reinfección durante el incidente.

4. **Recuperación:** Una vez eliminada la amenaza, se procede a restaurar los sistemas y servicios a la normalidad. En AWS esto puede ser rápido gracias a la elasticidad:

   - **Restaurar datos desde backups** si hubo pérdida o corrupción. Por ejemplo, si una base de datos fue dañada, se lanza una nueva instancia RDS desde el snapshot más reciente y se verifica su integridad. O si un bucket S3 fue limpiado por un atacante, se restauran las versiones previas de objetos (Versioning) o desde backups externos.
   - **Re-deploy de infraestructura:** En caso de que servidores completos fueran comprometidos, se puede reconstruir la capa de aplicación desplegando la infraestructura como código (CloudFormation/Terraform) para asegurar que todo vuelve a estado conocido. Esto minimiza errores de configuración manual al recuperarse. Si se cuenta con AMIs seguras o contenedores de Moodle, simplemente se reinicia el servicio con esas imágenes.
   - **Reincorporación controlada al servicio:** Se va levantando la plataforma gradualmente, monitoreando de cerca que el incidente no resurge. Por ejemplo, tras recuperar la base de datos y servidores, se reabre el acceso a usuarios progresivamente, manteniendo un modo de monitoreo intensivo. CloudWatch se usará para vigilar que los patrones de uso vuelvan a la normalidad. Si se hizo cambios (parches, nuevas reglas WAF), se observa su efecto en performance y seguridad.
   - **Comunicación:** En esta fase, también es importante la comunicación a usuarios y partes interesadas de que el servicio se ha restaurado. Siguiendo el plan, el equipo de comunicaciones de EduTech emitiría notificaciones (por ejemplo, "La plataforma Moodle estuvo en mantenimiento debido a un incidente de seguridad, ya está operativa. No se ha comprometido información personal" – si aplica). La transparencia gestionada es clave, más aún en contexto educativo donde la confianza es importante.

5. **Lecciones Aprendidas:** Luego de la resolución, el equipo realiza una revisión post-mortem del incidente:

   - Se documenta todo el timeline de lo ocurrido, cómo se detectó, qué falló o qué funcionó en la respuesta. Este informe incluirá métricas (tiempo de detección, tiempo de contención, impacto medido).
   - **Análisis de causa raíz:** Más allá de detenerlo, se busca entender profundamente la causa original. Por ejemplo, ¿El ataque fue posible por un error humano, una puerta trasera en un plugin, una mala configuración? Identificar esto permite acciones preventivas a futuro (como mejorar procesos de revisión de configuraciones o capacitación).
   - **Mejoras al plan y controles:** Se actualiza la estrategia/política según lo aprendido. Si hubo demoras en la detección, quizás ajustar umbrales de alarmas; si una comunicación

interna falló, mejorar el protocolo; si un tipo de ataque no estaba en el radar, añadirlo a las consideraciones. Por ejemplo, si el incidente fue phishing a un desarrollador que filtró credenciales, se refuerza la formación anti-phishing y quizá se implementa AWS IAM Access Analyzer para detectar políticas que podrían llevar a exposición involuntaria de datos.

- Se reúne al equipo involucrado y a la gerencia para presentar las lecciones. Esto cierra el ciclo de retroalimentación, asegurando una mejora continua de la postura de ciberseguridad.

Mejores Prácticas adicionales: Más allá de los puntos anteriores, EduTech Global incorpora en su estrategia en AWS un conjunto de mejores prácticas generales de ciberseguridad:

- **Principio de mínima superficie de ataque:** Desplegar solo los servicios necesarios, deshabilitar y cerrar puertos, protocolos y cuentas no usados. Por ejemplo, si no se usan IPv6 en la VPC, bloquearlo; si no se necesita FTP, no abrirlo, etc. Mientras menos puntos de entrada, menor riesgo.
- **Actualizaciones frecuentes y gestión de parches:** A nivel cloud, aprovechar la automatización. Se programa la aplicación automática de parches críticos del sistema operativo usando Systems Manager Maintenance Windows, fuera de horas punta. Moodle y sus plugins deben mantenerse en su última versión estable; idealmente se suscribe a listas de seguridad de Moodle para enterarse de parches y aplicarlos rápidamente.
- **Infrastructure as Code and Automatización:** Toda la infraestructura (VPC, subnets, SG, instancias, etc.) se define en código (CloudFormation/Terraform). Esto no solo acelera despliegues sino que asegura que los entornos son reproducibles y evita errores manuales de configuración. Además, permite hacer reviews de los cambios de infraestructura (código versionado) igual que se revisa código de aplicación, detectando posibles fallos antes de aplicar. La automatización también se extiende a respuesta: se pueden implementar AWS SSM Automation runbooks que, con un click, realicen acciones de contención que de otra forma tomarían varios pasos manuales.
- **Principio de privilegio mínimo y separación de funciones:** Ya cubierto en IAM pero se enfatiza: nunca dar más permisos de los necesarios. Realizar auditorías de permisos periódicas, usando por ejemplo IAM Access Analyzer (que identifica si alguna policy otorga acceso demasiado amplio, incluso a terceros) y revocar accesos sobrantes. Separar tareas: quienes desarrollan no administran la nube, y viceversa, para reducir riesgo interno.
- **Plan de Continuidad de Negocio (BCP):** Complementario a la ciberseguridad, EduTech mantiene un plan de contingencia para desastres. Gracias a la nube, se puede aprovechar la multi-región: por ejemplo, tener backups críticos replicados en otra región AWS (ej. en caso de caída total de eu-west-1, contar con posibilidad de restaurar Moodle en us-east-1). Se definen RPO/RTO claros (p.ej. máximo 1 hora de datos perdidos, 4 horas para recuperar la plataforma). Se prueban estos escenarios de DR (disaster recovery drills) al menos una vez al año.
- **Cumplimiento y gobierno:** Asegurar que el uso de AWS cumpla con GDPR y leyes educativas. Esto implica configurar regiones adecuadas (datos de estudiantes europeos residiendo en AWS EU), firmar acuerdos de procesamiento de datos con AWS (AWS GDPR DPA), y habilitar características de conformidad (como Encryption y CloudTrail obligatorios). AWS proporciona certificaciones pero EduTech debe preparar documentación de cómo su configuración es conforme (aquí AWS Config y Security Hub con el estándar CIS AWS ayudan, mostrando porcentaje de cumplimiento de controles).
- **Capacitación del personal:** La migración a la nube trae también una evolución en habilidades. EduTech invertirá en formación continua de su equipo de TI en temas de AWS Security. Esto incluye entrenamientos oficiales (AWS Security Essentials, cert. AWS Security Specialty) y simulaciones de incidentes en la nube. Asimismo, se hacen campañas para toda la empresa sobre higiene digital: aunque los usuarios finales no toquen AWS directamente, siguen siendo vector (phishing, contraseñas).

- **Revisiones de arquitectura:** Por último, se aprovecharán recursos como el AWS Well-Architected Framework – Security Pillar reviews, posiblemente con ayuda de partners, para auditar periódicamente la arquitectura y detectar desviaciones de las mejores prácticas de AWS. Estas revisiones ofrecen recomendaciones que se incorporarán para mantener la estrategia actualizada.

8. Conclusión

Con esta estrategia de ciberseguridad en la nube, EduTech Global adapta sus controles al entorno AWS, asegurando que la confidencialidad, integridad y disponibilidad de su plataforma educativa permanezcan sólidas tras la migración.

La combinación de una arquitectura cloud segura, políticas claras de acceso, herramientas de seguridad de AWS (IAM, KMS, CloudTrail, Config, GuardDuty, etc.), y un equipo preparado para monitorizar y responder a incidentes, proporciona una defensa en profundidad. Si bien la nube introduce nuevos retos, también brinda oportunidades de mejorar la postura de seguridad gracias a la automatización y a la variedad de servicios especializados.

Al centrarse en los cuatro pilares – identidad, datos, infraestructura y detección/respuesta – EduTech Global puede avanzar en su transformación digital de forma segura, protegiendo la experiencia de aprendizaje de miles de usuarios en línea. Como reza el enfoque de AWS: "mover rápido y mantenerse seguro" es posible con la estrategia adecuada, y EduTech está comprometida con ese objetivo en su viaje a la nube. Referencias: Todas las fuentes consultadas (documentación de AWS, blogs de seguridad y contenidos del curso) se listan a continuación para respaldar las mejores prácticas y afirmaciones realizadas en el informe.

Referencias