Asignatura: Auditoría informática
Carrera: Ingeniería de Software
Docente: Harry Carpio S.
Estudiante: Dennis Quiguire & Jonathan Caiza

Preguntas:

PREGUNTA 1.- Para cada uno de los riesgos descritos en el punto dos de la sección anterior (2. Aspectos y riesgos identificados sujetos a auditoría), identifique y explique dos revisiones de auditoría que se deben definir en la fase de planificación de la auditoría informática

ASPECTO	RIESGO	AUDITORIA
Seguridad del código fuente y Propiedad Intelectual	Fuga de Código (Filtraciones antes del lanzamiento)	1. Verificación de políticas de control de versiones (Branch protection, pull requests) 2. Auditoria de accesos a repositorios con revisión de logs de GitHub y la rotación de credenciales
Seguridad en Infraestructura Multiplayer	Ataques DDoS y exploits en servidores	1. Revisión de configuración de firewalls como WAF y balanceadores de carga en AWS/GCP 2. Evaluación de mecanismos anti-cheats y pruebas de penetración en servidores multiplayer
Protección de datos de Usuarios	Sanciones por mal manejo de datos personales	1. Revisión de cumplimientos de normativas como GDPR/CCPA en el manejo de datos de usuarios 2. Evaluación de cifrado de datos en transito y en reposo como los HHTPS y cifrado de base de datos
Gestión de Activos Digitales (Artes y diseños)	Perdida o robo de arte no publicado	1. Auditoria de respaldo y versionamientos de archivos en

		servidores de arte digital 2. Control de acceso a carpetas compartidas y permisos sobre software como Figma o Adobe
Desarrollo de Seguros (SSDLC)	Vulnerabilidades como inyección SQL	1. Revisión del ciclo de desarrollo seguro como análisis estático , dinámico de código 2. Verificación del uso de librerías y actualizaciones como por ejemplo el escaneo de vulnerabilidades, dependa Bot
Monetización y Anti-Fraude	Fraude en micro transacciones	1. Análisis de patrones de transacciones anómalas en la base de datos de pagos 2. Revisión de integración con pasarelas de pago y políticas antifraude implementadas
Cumplimiento con Plataformas	Rechazo de certificación por TRC/XR	1. Validación de cumplimiento de checklist de Sony, Microsoft y Nintendo 2. Auditoria de pruebas internas previas a la entrega para certificación

Asignatura: Auditoría informática
Carrera: Ingeniería de Software
Docente: Harry Carpio S.
Estudiante: Dennis Quiguire & Jonathan Caiza

PREGUNTA 2.- Suponga que ha finalizado la auditoría planteada, identifique y describa dos hallazgos críticos y dos hallazgos importantes que requieran de un seguimiento y corrección post-auditoría.

HALLAZGOS CRITICOS	HALLAZGOS IMPORTANTES
Se detecto acceso sin restricciones a repositorios de código fuente por parte de excolaboradores	No se cuenta con una política documentada de desarrollo seguro
No se están cifrando datos sensibles de los usuarios en la base de datos como nombres, correos, métodos de pago entre otros datos muy delicados	Las copias de seguridad de arte digital no se están realizando de forma periódica ni automatizada

PREGUNTA 3.- Realice dos recomendaciones post-auditoría.

- ✓ Implementar una política de gestión de accesos con revisión trimestral y eliminación automática de accesos invalidas
- ✓ Establecer un proceso formal de desarrollo seguro que incluya capacitación continua y pruebas de vulnerabilidad y realización de revisiones de código sistemáticas

PREGUNTA 4.- Mencione y explique tres beneficios de la auditoría realizada.

1. **Identificaron de riesgos ocultos:**

   La auditoría permitió descubrir vulnerabilidad criticas que ponía en riesgo los activos de la empresa

2. **Mejora en la protección de datos:**

   Al implementar cifrado y controles de acceso esto reducirá el riesgo de filtraciones y sanciones legales

3. **Cumplimiento normativo y de plataforma:**

   Esto Ayudara a asegurar que los productos puedan ser certificados por consolas y que se cumpla con las regulaciones de datos