**Escenario de Seguridad**

**1. ¿Qué debe hacer 4Geeks Academy para evitar la exposición de los datos de sus usuarios?**

Para evitar la exposición de los datos de estudiantes, egresados y socios, \*\*4Geeks Academy\*\* debe implementar las siguientes medidas de seguridad:

* Cifrado de Datos: Los datos tanto en tránsito (durante la comunicación) como en reposo (almacenados) deben estar cifrados utilizando estándares robustos como AES-256 para el almacenamiento y TLS 1.2 o 1.3 para la transmisión. Esto asegurará que la información esté protegida incluso si es interceptada.
* Control de Acceso Basado en Roles (RBAC): Implementar un modelo de control de acceso basado en roles, en el que solo los empleados autorizados puedan acceder a los datos sensibles según su función. Los estudiantes y egresados deberían tener acceso solo a su propia información.
* Autenticación Multifactor (MFA): Implementar un sistema de autenticación multifactor para asegurar que solo los usuarios autorizados puedan acceder a sus cuentas o a sistemas internos.
* Auditoría y Monitoreo: Configurar un sistema de monitoreo continuo y auditoría de registros para detectar cualquier actividad inusual o intento de acceso no autorizado.
* Protección contra amenazas: Implementar tecnologías de protección como firewalls, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), y herramientas de prevención de pérdida de datos (DLP).
* Actualización y Parches: Asegurarse de que todos los sistemas, aplicaciones y plataformas utilizadas estén actualizados y con los parches de seguridad más recientes para evitar vulnerabilidades.
* Backup Regular: Crear copias de seguridad regulares y automáticas de los datos, almacenándolas en ubicaciones seguras y separadas del entorno principal.

**2. ¿Qué es lo peor que podría pasar y por qué es tan importante mantener la privacidad de los datos?**

Lo peor que podría pasar es una fuga masiva de datos de estudiantes, egresados y socios, lo cual puede tener varias consecuencias graves:

* Pérdida de Confianza: La confianza de los estudiantes y las empresas asociadas se vería gravemente afectada, lo que podría provocar una disminución significativa en las inscripciones y asociaciones.
* Daño a la Reputación: Un incidente de fuga de datos generaría una mala reputación a nivel global, lo que podría afectar la imagen de la academia y sus operaciones comerciales.
* Sanciones Legales: Dependiendo de las regulaciones locales (como GDPR, CCPA u otras leyes de protección de datos), 4Geeks Academy podría enfrentarse a multas y sanciones significativas si no cumple con las normativas de privacidad y seguridad de datos.
* Explotación de Datos: Los datos expuestos podrían ser utilizados para robo de identidad, fraude, y phishing, lo que pondría en riesgo a estudiantes, egresados y empresas.

Mantener la privacidad de los datos es crucial para evitar estos riesgos y mantener la confianza de los usuarios en la plataforma.

**3. ¿Quién debería gestionar los datos de los estudiantes, egresados y socios?**

* Equipo de TI/Ciberseguridad: El equipo de tecnología y ciberseguridad debe ser responsable de implementar las políticas y controles técnicos necesarios para proteger los datos.
* Oficial de Seguridad de la Información (CISO): Si la organización tiene una estructura más compleja, el CISO (Chief Information Security Officer) sería responsable de supervisar la seguridad de la información a nivel organizacional.
* Responsables de Cumplimiento y Privacidad: También debe haber responsables que se encarguen de asegurar el cumplimiento de normativas como GDPR, CCPA, o las que apliquen, gestionando las políticas de tratamiento de datos personales.
* Gestión Descentralizada con Supervisión Centralizada: Los datos pueden ser gestionados de manera segmentada, pero es importante que haya un sistema de supervisión centralizada para asegurar que se sigan las políticas de seguridad.

**4. ¿Qué tratamiento de seguridad deberían recibir los datos?**

Los datos deben recibir tratamiento específico en función de su sensibilidad. Aquí se puede clasificar de la siguiente manera:

* Datos Públicos: Datos no sensibles que no requieren tratamiento de seguridad especial (e.g., perfiles de egresados accesibles en el sitio público).
* Datos Personales Sensibles: Información como nombres, correos electrónicos, datos de pagos, etc., deben ser cifrados y solo accesibles mediante autenticación segura.
* Datos Críticos: Información de naturaleza muy sensible, como datos financieros o detalles personales altamente sensibles, deben tener controles adicionales como cifrado robusto, acceso limitado y almacenamiento en entornos altamente seguros.

**5. Plan de Recuperación de Datos y Plan de Prevención de Fugas**

Plan de Recuperación de Datos:

1. Copia de Seguridad Automática: Implementar backups automáticos diarios de todos los datos clave. Utilizar una política de almacenamiento en la nube segura y con redundancia geográfica para proteger la disponibilidad.

2. Pruebas Regulares de Recuperación: Realizar simulaciones y pruebas de recuperación de datos regularmente para asegurar que, en caso de un incidente, la recuperación sea rápida y efectiva.

3. Plan de Respuesta a Incidentes: Definir claramente el proceso de respuesta a incidentes, con personal asignado para identificar la causa de una fuga o pérdida de datos y activar protocolos de contención.

4. Plan de Comunicación de Incidentes: Tener un protocolo para notificar a los estudiantes, egresados y empresas afectadas en caso de un incidente, cumpliendo con los requisitos legales y normativos.

**Plan de Prevención de Fugas:**

1. Implementación de Soluciones DLP (Data Loss Prevention): Las herramientas de DLP permiten detectar y prevenir la fuga de datos mediante la monitorización del tráfico y el control de dispositivos externos (e.g., USB, almacenamiento en la nube).

2. Formación en Seguridad: Capacitar regularmente al personal y a los usuarios sobre buenas prácticas de seguridad, incluyendo la gestión de contraseñas, phishing y manejo de datos sensibles.

3. Mantenimiento de Políticas de Seguridad: Implementar políticas de manejo de datos, acceso, y uso de dispositivos móviles, que deban ser cumplidas por todo el personal de 4Geeks Academy.

4. Seguridad en la Nube: Dado que muchos datos pueden estar alojados en la nube, asegurar que los proveedores de servicios en la nube sigan normas estrictas de seguridad como ISO 27001.