Diagnóstico Ejecutivo de Ciberseguridad

Empresa: Coding Giants S.L.

Consultor: Sergio Carretero Otero

Fecha: Julio 2025

Índice

1. Introducción

El presente informe tiene como objetivo diagnosticar el estado actual de la ciberseguridad en Coding Giants S.L., empresa dedicada a la enseñanza online de programación. Para esta evaluación se ha empleado el marco Cloud Controls Matrix versión 4.0 (CCM v4) de la Cloud Security Alliance, complementado con el modelo de madurez COBIT 5.

Dado el alcance limitado del informe y el tamaño de la organización, se ha optado por una muestra representativa de seis controles clave, centrados en áreas críticas como auditoría, identidad, protección de datos, monitoreo, cifrado y gobernanza.

2. Diagnóstico de controles seleccionados

ID Control	Descripción	Estado Actual	Madurez (COBIT 5)	Observación del Experto
A&A-01	Política de auditoría y aseguramiento	No existen políticas ni procedimientos de auditoría ni revisión de accesos.	0 – Inexistente	Definir e implementar una política mínima de revisión de accesos y trazabilidad en servicios cloud.
IAM-01	Gestión de identidades y accesos	Se utilizan cuentas compartidas (usuario Trainer) sin autenticación fuerte.	1 – Inicial	Implementar cuentas individuales por empleado y activar autenticación multifactor (MFA).
DSP-01	Clasificación y protección de datos	Los documentos no están clasificados ni cifrados. No existe política sobre datos sensibles.	1 – Inicial	Definir clasificación mínima de datos y aplicar controles de acceso y cifrado según sensibilidad.
LOG-01	Registro y monitoreo	No hay monitoreo ni registros de actividad en las plataformas utilizadas.	0 – Inexistente	Activar logs en Google Drive y Notion. Establecer revisiones periódicas por parte de TI.
SEF-01	Cifrado en tránsito y almacenamiento	Se depende del cifrado por defecto de los proveedores SaaS, sin verificación técnica.	2 – Gestionado informal	Auditar la configuración de cifrado y documentar el cumplimiento de políticas por parte de Google y Notion.
GOV-01	Gobierno de la seguridad de la información	No se ha asignado un responsable de seguridad ni existe una política marco.	1 – Inicial	Designar un responsable de ciberseguridad, definir una política organizativa y establecer revisiones anuales.

3. Conclusiones ejecutivas

El análisis revela que Coding Giants S.L. presenta un nivel general de madurez bajo (entre 0 y 2) en los controles evaluados. Esto refleja una ausencia de políticas formales,

controles técnicos básicos y funciones de gobernanza de seguridad bien definidas. La dependencia de servicios SaaS como Google Drive y Notion, sin verificación interna ni registros, incrementa el riesgo de exposición de información.

La falta de trazabilidad y gestión adecuada de accesos (uso de cuentas compartidas) supone un riesgo importante, especialmente en un entorno donde se manejan datos de menores y docentes. La carencia de políticas, responsables y mecanismos de revisión periódica indica una cultura reactiva ante la seguridad, donde las acciones dependen más de la urgencia operativa que de una planificación preventiva.

En conjunto, la empresa enfrenta riesgos en materia de cumplimiento normativo (como el RGPD), reputación institucional y continuidad operativa en caso de incidentes de seguridad.

4. Recomendaciones priorizadas

- **Corto plazo (0–3 meses):**
- • Establecer políticas básicas de acceso y control de usuarios en plataformas SaaS.
- • Eliminar cuentas compartidas e implementar autenticación multifactor (MFA).
- • Activar registros de actividad y configurar alertas básicas en Google Workspace y Notion.
- • Nombrar provisionalmente a un responsable de seguridad de la información (aunque sea compartido con otro rol).
- **Medio plazo (3–9 meses):**
- • Redactar y aprobar una política marco de seguridad de la información.
- • Clasificar los datos según su sensibilidad e implementar cifrado cuando corresponda.
- • Formar al personal en buenas prácticas de seguridad y cumplimiento normativo.
- • Establecer un ciclo de revisión y mejora continua para los controles más críticos.

5. Bibliografía

• Cloud Security Alliance (CSA). Cloud Controls Matrix (CCM) v4.0. https://cloudsecurityalliance.org

• ISACA. COBIT 5 Framework. https://www.isaca.org/resources/cobit

• Agencia Española de Protección de Datos (AEPD). https://www.aepd.es/

• Google Workspace Admin Help – Security and Access Controls. https://support.google.com

• Notion Security & Privacy Docs. https://www.notion.so/security