Pregunta 1:

Se trata de una auditoría de tercera parte, externa e independiente, solicitada por la organización para verificar el cumplimiento tanto del RGPD como de la norma ISO/IEC 27001.

Pregunta 2:

Ha vulnerado los principios de confidencialidad e integridad, al revelar información interna del auditado y actuar con conflicto de intereses al favorecer a un familiar.

Pregunta 3:

No, no puede negarse. El cliente tiene derecho a auditar al encargado del tratamiento para verificar el cumplimiento del contrato y del RGPD. Es una obligación prevista en el art. 28.3.h del RGPD.

Pregunta 4:

El fallo es que Juan Carlos no es el auditor jefe, por tanto no le corresponde asignar funciones. Además, la elaboración del plan de auditoría es responsabilidad del auditor jefe, no de Carmen.

Pregunta 5:

Sobra “equipo auditor”, que pertenece al plan, no al programa. Falta la fecha de realización, criterios de auditoría, objetivos y duración estimada de cada actividad.

Pregunta 6:

Sobra la técnica de mystery shopper, ya que no es propia de la reunión inicial. Falta establecer los requisitos de seguridad durante la auditoría y confirmar la disponibilidad de recursos.ç

Bibliografía

Agencia Española de Protección de Datos (AEPD). (2020). *Guía para la realización de auditorías de protección de datos*. https://www.aepd.es/sites/default/files/2020-03/guia-auditorias-rgpd.pdf

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. ISO.

International Register of Certificated Auditors (IRCA). (2020). *IRCA Auditor Code of Conduct*. https://www.irca.org/resources/code-of-conduct