Matias Davila
Etica

1. Identificación y argumentación de mala conducta en la protección de datos

- **Planificación de la auditoría**: La primera irregularidad la encontramos cuando en la planificación, ya que sin un consentimiento formal el auditor recuerda oralmente y vía email de revisar documentos sensibles y la toma de fotografías en las instalaciones. Esto va en contra de las prácticas estándar de protección de datos o normas ISO27001, donde es crucial obtener un consentimiento explícito y documentado para el manejo de información personal y corporativa y te dan acceso a lo que ellos desean.
- **Durante la auditoría**: Durante la auditoria vemos el problema de que el auditor empieza a tomar fotos de la empresa en conjunto a algunos empleados, algunos de los cuales posan para las fotos. Estas acciones no solo vulneran la privacidad de los trabajadores, sino que también incumplen las normativas de protección de datos, al no haber un consentimiento específico para la captura y uso de imágenes personales.
- **Recolección y manejo de datos**: El recolector de datos, que es el auditor, recoge información personal detallada de los empleados, como sus nombres completos y fechas de nacimiento, así como información delicada como contratos, salarios y horarios laborales. No tener las medidas adecuadas para asegurar la confidencialidad y el manejo seguro de estos datos es un descuido grave.
- **Cierre de la auditoría**: Cuando el auditor comparte el documento con anotaciones personales sobre los trabajadores con el jefe de la empresa que está siendo auditada, está poniendo en riesgo aún más la confidencialidad y privacidad de los empleados. Este acto podría llevar a un uso inapropiado de la información confidencial.

2. Propuestas de actuación correcta para salvaguardar la privacidad y protección de datos

- **Planificación de la auditoría**: Para este error era cuestión de conseguir un consentimiento formal en donde se le diera permiso de realizar las actividades.
- **Durante la auditoría**: al igual que en el caso anterior, para este proceso debía conseguir un consentimiento de cada persona y tener en cuenta auditar solo lo necesario.
- **Recolección y manejo de datos**: La información personal debe ser manejada con la mayor confidencialidad posible, asegurando que se almacene de manera segura y limitando el acceso solo a personas autorizadas. Es necesario asegurarse de que los datos se utilicen solo para los propósitos de la auditoría.
- **Cierre de la auditoría**: el auditor debe seguir los protocolos de una auditoria, no puede compartir información a terceros o a personas, los resultados son dirigidos a gerencia o al encargado de seguridad de la información y el es quien maneja las no conformidades oportunidades de mejora con el equipo que asigne.