COBIT

"1. Identificación de datos sensibles: Identificar y catalogar los datos que contienen información sensible o confidencial, como datos personales, financieros o de salud, y su nivel de sensibilidad en relación con la privacidad.

2. Evaluación de impacto: Evaluar el impacto potencial que tendría el acceso no autorizado, la alteración o la pérdida de los datos sobre la privacidad y confidencialidad, afectando tanto a la organización como a las personas involucradas.

3. Cumplimiento normativo: Revisar regulaciones y normativas (como GDPR, CCPA, LGPD) que afecten a los datos en cuestión y determinar si los activos deben ser clasificados como críticos en función de su cumplimiento.

4. Acceso y control: Determinar qué usuarios y roles deben tener acceso a los datos y qué niveles de control son necesarios para garantizar que solo las personas autorizadas puedan ver o modificar los activos de información.

5. Criterios de confidencialidad: Analizar los niveles de confidencialidad requeridos, aplicando una clasificación basada en quién puede ver la información y si esta requiere medidas de seguridad específicas.

6. Mecanismos de seguridad: Evaluar los mecanismos de protección existentes, como encriptación, autenticación y auditoría, para asegurar que los activos clasificados cuenten con la seguridad adecuada.

7. Propiedad y responsabilidad: Asignar responsabilidades claras sobre los datos y definir los roles encargados de la protección y clasificación de cada activo de información, garantizando que la responsabilidad esté formalmente documentada.

8. Ciclo de vida del dato: Evaluar en qué etapa del ciclo de vida (creación, almacenamiento, procesamiento, eliminación) se encuentran los datos y determinar si requieren protección adicional en cada fase.

9. Riesgo de exposición: Considerar el riesgo de exposición de los activos ante posibles amenazas externas e internas, especialmente si estos activos contienen datos privados de clientes o empleados.

10. Valor estratégico y reputacional: Analizar si la pérdida o filtración de los activos podría dañar la reputación de la organización o comprometer su posición competitiva, dando prioridad a aquellos activos que representan un valor estratégico importante.

11. Plan de recuperación y continuidad: Evaluar si los activos deben ser clasificados como críticos en base a la necesidad de un plan de recuperación en caso de incidentes que comprometan la confidencialidad y privacidad.

12. Revisión y actualización periódica: Implementar un proceso regular de revisión y actualización de la clasificación de los activos para reflejar cambios en el entorno normativo, de negocio o de riesgo.

"