ITIL versión 4

"1. Identificación de activos: Catalogar todos los activos de información (datos, aplicaciones, infraestructura) relacionados con los datos confidenciales. En esta etapa, se recopila información sobre qué datos se manejan, sus ubicaciones y el acceso que tienen distintos roles o usuarios.

2. Evaluación de valor e impacto en el negocio: Evaluar la importancia de cada activo en términos de su valor para el negocio y su impacto si se produce una brecha de seguridad. ITIL promueve un enfoque orientado a los servicios, lo cual significa que se debe considerar cómo la confidencialidad, integridad y disponibilidad de los datos impacta en los servicios finales al cliente.

3. Clasificación por nivel de sensibilidad: Establecer niveles de sensibilidad, como por ejemplo, “Confidencial”, “Restrictivo” o “Público”. Cada activo se clasifica según su nivel de confidencialidad y los riesgos asociados, como la exposición a pérdida o acceso no autorizado. Datos personales, financieros, o propiedad intelectual suelen clasificarse en los niveles más altos de confidencialidad.

4. Análisis de riesgos y controles de seguridad: Evaluar los riesgos asociados a cada activo y definir controles de seguridad específicos. ITIL recomienda emplear estrategias como el análisis de amenazas y vulnerabilidades para determinar los riesgos críticos y aplicar controles como cifrado, autenticación avanzada, monitoreo de accesos y auditorías regulares.

5. Asignación de propietarios y responsables: Asignar un “dueño” de cada activo, quien es responsable de asegurar su protección y monitoreo. La propiedad incluye la supervisión de acceso y la toma de decisiones sobre medidas de seguridad y respuesta ante incidentes.

6. Implementación de políticas de acceso y protección: Basado en la clasificación de cada activo, ITIL sugiere implementar políticas de acceso adecuadas. Esto puede incluir restricciones de acceso físico y digital, así como un enfoque de acceso mínimo necesario, asegurando que solo los usuarios autorizados puedan acceder a información crítica.

7. Monitoreo y revisión continua: Los activos clasificados como críticos deben estar bajo monitoreo constante para identificar posibles vulnerabilidades y actualizar las medidas de protección cuando sea necesario. ITIL también recomienda auditorías periódicas y revisiones de acceso para garantizar que las clasificaciones y políticas se mantengan efectivas y alineadas con los cambios en los riesgos de seguridad."