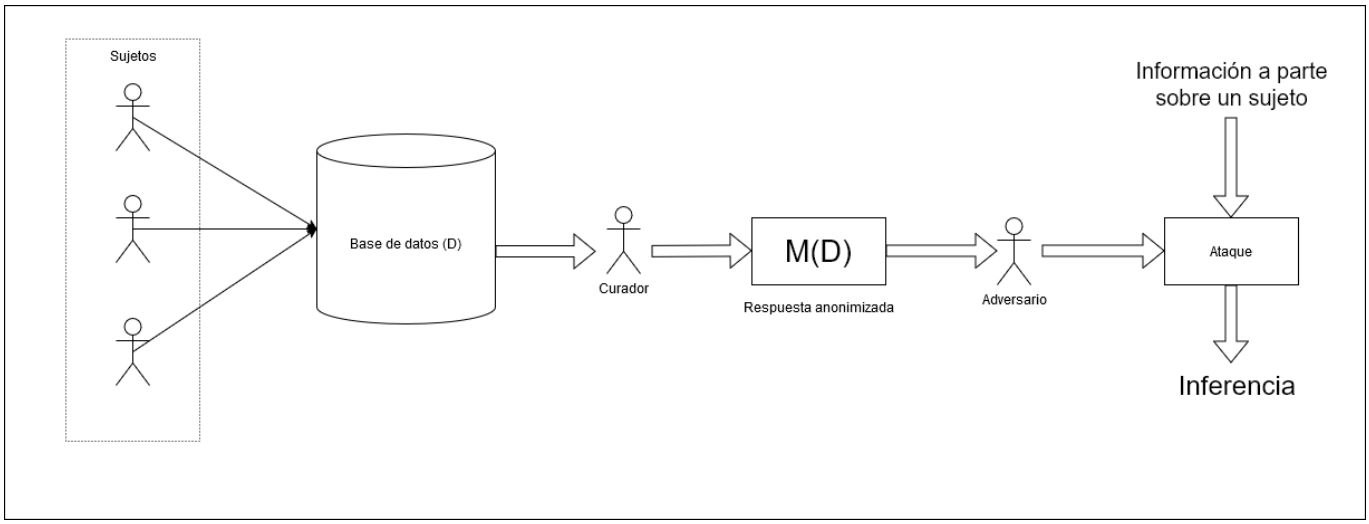
[PAN] Privacidad Diferencial (Resumen)

Caso base

Tenemos un dataset D que contiene datos de usuarios, siendo cada fila los datos de un usuario. El Curador, que es una entidad de confianza para los usuarios, publica algunos datos usando un mecanismo M que da como resultado $R=M(D)$. El adversario trata de realizar inferencias sobre los datos D contenidos en R.

De que protege la privacidad diferencial



La privacidad diferencial protege contra el riesgo del conocimiento de información sobre un sujeto usando inferencia con información obtenida a parte. De esta forma, observando la respuesta R no se puede cambiar lo que el adversario puede saber.

La clave para dificultar a un adversario identificar datos sobre un sujeto es poder crear dos salidas $R=M(D)$ y $R=M(D')$, siendo D y D' dos datasets diferenciados por que el primero contiene al sujeto en cuestión y el segundo no, las cuales no puedan ser distinguibles la una de la otra. Para hacer esto se diseña el mecanismo M, el cual no puede ser deterministico, si no probabilístico.