

Figura 2.1: Tarjetas de Banda Magnética

crea una polarización magnética en la zona de influencia de la cabeza, afectando a esa parte de la banda.

El proceso de lectura es inverso al de grabación. Se basa en la propiedad que tienen las diferencias de polarización en inducir una corriente en una bobina. De esta manera, al hacer pasar una banda por la cabeza de lectura (que tiene otra bobina para la lectura) con una velocidad constante, se inducen pulsos de corriente en uno u otro sentido, lo que indicará "1" o "0".

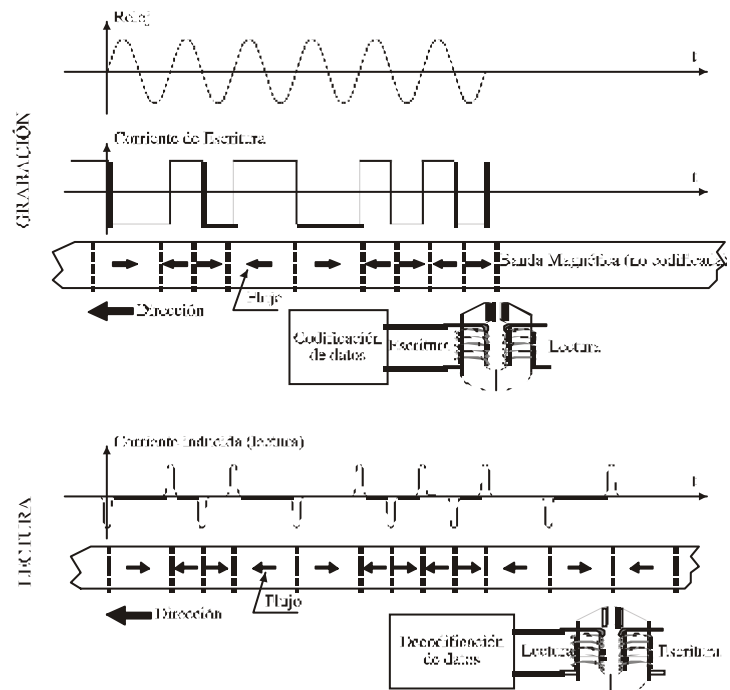


Figura 2.2: Grabación y lectura en una Banda Magnética

Ambos procesos están basados en los mecanismos de grabación y lectura presentes en las cintas magnéticas de música o vídeo. Podemos observar un gráfico de todo el sistema en la figura 2.2.

Por último, aclarar que las Tarjetas de Banda Magnética poseen tres pistas dentro de la banda magnética.

Datos almacenados en la banda magnética.

La banda magnética posee tres pistas da datos en las que podemos almacenar información.

La pista normalmente utilizada en cajeros es la dos, donde escribimos los datos del usuario. También en la pista uno se graban datos del usuarios preparados para su uso en los Datáfonos. La pista tres es utilizada en modo propietario, es decir, cada esquema almacena datos que se utilizan en la transacción y parametrizarla (online, offline, ...). También se almacena en estas pistas un residuo del PIN, este residuo será el que nos permita validar el PIN en operaciones offline.

Seguridad en la banda magnética.

En un entorno de Banda Magnética implementamos la seguridad en varios frentes:

PIN: En operaciones que requieran la presentación del PIN, tenemos varias posibilidades, en operaciones Online el PIN lo valida el Host, en operaciones Offline el pin lo valida el terminal sirviéndose del residuo almacenado en la tarjeta. Este residuo se calcula con algoritmo que tiene como entradas el PIN y una clave, el resultado de este calculo se almacena en la tarjeta. La seguridad de este mecanismo estriba en el desconocimiento del algoritmo y la clave.

CVV: También tenemos en la banda almacenado una firma que nos protege contra la clonación de tarjetas. Con los datos: nombre, número de tarjeta y fecha de caducidad y usando una clave calculamos una firma. Si alguien nos roba los datos de la tarjeta por ejemplo en Internet nunca podrá clonarla porque no puede calcular esta firma.

Firma: La medida tradicional sigue siendo la firma del recibo. Esta firma nos autentifica y garantiza el no repudio.

La copia o clonación de tarjetas si alguien es capaz de leer todos los datos de la banda magnética queda protegida solamente por la presentación del PIN por parte del usuario a la hora de autorizar la transacción, por la presentación del DNI o por la firma del correspondiente justificante.