Row Level Security

Row Level Security (RLS) permite definir una **política de seguridad** para el acceso a los datos de una tabla a nivel registro, basada en un contexto de trabajo. Esta política dinámicamente evaluará los criterios codificados para determinar el filtro en la cláusula WHERE que accederá a los datos del objeto correspondiente.

La política puede ser codificada para evaluar la operación DML realizada: **INSERT, UPDATE, DELETE y/o SELECT**, determinará qué restricción realizará para cada caso (o todos).

Mas información en este documento oficial de Oracle:

<http://docs.oracle.com/cd/B19306_01/network.102/b14266/apdvpoli.htm#i1008538>

o este sitio de la Universidad de Murcia:

<http://www.um.es/atica/oracle-vpd>

¿Cómo lo Usaría?

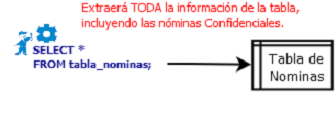
Actualmente veo un GAP en los datos de las nóminas confidenciales. Debido que estos datos se encuentran visible para cualquier personal técnico que tenga acceso a la Base de Datos, pudiendo realizar sentencias SELECT para extracción de registros.

Accidentalmente, un técnico de soporte y/o desarrollo pude ver y/o distribuir la información de esta tabla confidencial.

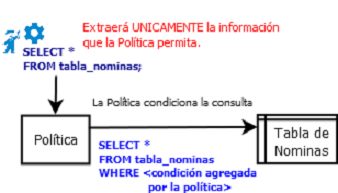
Considero conveniente ocultar los registros para que ningún usuario por accidente pueda ver dicha información. La forma de hacerlo sería usando RLS.

**SITUACIÓN ACTUAL.**

Un colaborador de **Soporte y/o Desarrollo**, ejecuta una consulta directa a la tabla, sin ningún filtro. Esto le devolverá TODOS los registros de la tabla, incluyendo los datos Confidenciales.



Sin embargo, si existiera una Política de seguridad. La política se encargaría de agregar el filtro necesario para evitar que “accidentalmente” una consulta devuelva datos confidenciales



NOTA:

Esta Política afectaría al módulo de FACEL, ya que no podría leer la información Confidencial. FACEL tendría que modificar su código para agregar el seteo antes de realizar su proceso. Este seteo es sencillo.