Comparación de los factores de reconocimiento			
Criterios	**Algo que la persona es (dato biométrico)**	**Algo que la persona posee (token o tarjeta de proximidad)**	**Algo que la persona sabe (contraseña o PIN)**
Menor necesidad de secreto	No es necesario que el titular mantenga en secreto u ocultos sus datos biométricos, aunque el responsable deba resguardarlos con las medidas de seguridad óptimas.	Las tarjetas o el token no deben estar al alcance de todos.	Las contraseñas deben ocultarse.
Menor posibilidad de robo	El robo de un dato biométrico y la posibilidad de su uso posterior es más complicado que los otros dos elementos.	El robo del token o tarjetas de proximidad no es poco común ni difícil.	Un descuido del titular puede dar lugar al robo o acceso no autorizado de su contraseña.
Menor posibilidad de pérdida	Al dato biométrico es, en general, permanente y siempre acompaña a la persona.	Las tarjetas y token se pueden perder con facilidad.	El olvido de contraseñas es común.
Fácil registro inicial y posibilidad de renovación	La generación de registros biométricos es más complicada por las distintas fases que conlleva, además que los datos biométricos son limitados.	La facilidad de emitir una tarjeta de proximidad o token es relativamente sencilla comparada con la generación de un registro biométrico.	La facilidad de emitir contraseñas es relativamente sencilla comparada con la generación de un registro biométrico. Además, la capacidad de generar datos biométricos es limitada, mientras que ello no ocurre con las contraseñas.
Fácil proceso de comparación	La comparación de datos biométricos es mucho más complicada, por el procesamiento y capacidades tecnológicas que requiere.	La comparación de tarjetas o token también puede ser sencilla.	La comparación de contraseñas es sencilla.
Mayor comodidad de uso	Como ya se ha dicho, el dato biométrico acompaña a su titular y en general es permanente.	Las tarjetas o token se deben tener a la mano.	Las contraseñas se deben memorizar o gestionar con un programa de administración de contraseñas.
Menor vulnerabilidad a la ingeniería social y ataques técnicos	Si bien los sistemas biométricos pueden ser vulnerados, es más complicado que ello ocurra y que los datos biométricos puedan ser reutilizados, y serán aún más complicado que se pueda vulnerar al propio titular para obtener sus biométricos.	Se puede utilizar ingeniería social o engaño para robar o duplicar una tarjeta o token.	Se puede utilizar ingeniería social, espionaje, engaño o fuerza bruta para obtener de manera ilegítima una contraseña.

Criterios	Algo que la persona es (dato biométrico)	Algo que la persona posee (token o tarjeta de proximidad)	Algo que la persona sabe (contraseña o PIN)
Mayor madurez en medidas de prevención	Las medidas de prevención de los sistemas biométricos no cuentan con el mismo nivel de madurez.	Los ataques a sistemas que utilizan tarjetas o token ocurren desde hace muchos años, por lo que las medidas de prevención presentan un grado de madurez importante.	Los ataques a sistemas que utilizan contraseñas ocurren desde hace muchos años, por lo que las medidas de prevención presentan un grado de madurez importante.
Mejor autenticación de usuarios reales	El dato biométrico, al pertenecer a un individuo en particular, no puede ser compartido ni transferido.	La autenticación de usuarios mediante tarjetas o token depende de hacer estos elementos intransferibles.	La autenticación de usuarios mediante contraseñas depende, en gran medida, de la voluntad de los usuarios de hacer estos elementos únicos.
Menor costo de implementación	Un sistema biométrico puede ser relativamente más costoso que un lector de tarjetas o un sistema de contraseñas, aunque en un análisis más profundo de costo-beneficio pueda resultar ventajoso.	Instaurar un sistema lector de tarjetas puede ser relativamente más barato que la implementación de un sistema biométrico.	Instaurar un sistema de contraseñas puede ser relativamente más barato que la implementación de un sistema biométrico.
Menor costo de mantenimiento	El costo de mantenimiento de un sistema biométrico, una vez que está implementado, puede ser menor al de un sistema de contraseñas o tarjetas, ya que no conlleva gastos de gestión o reposición.	El costo de mantenimiento de un sistema biométrico, una vez que está implementado, puede ser menor al de un sistema de tarjetas, ya que no conlleva gastos de gestión o reposición.	El costo de mantenimiento de un sistema biométrico, una vez que está implementado, puede ser menor al de un sistema de contraseñas ya que no conlleva gastos de gestión.