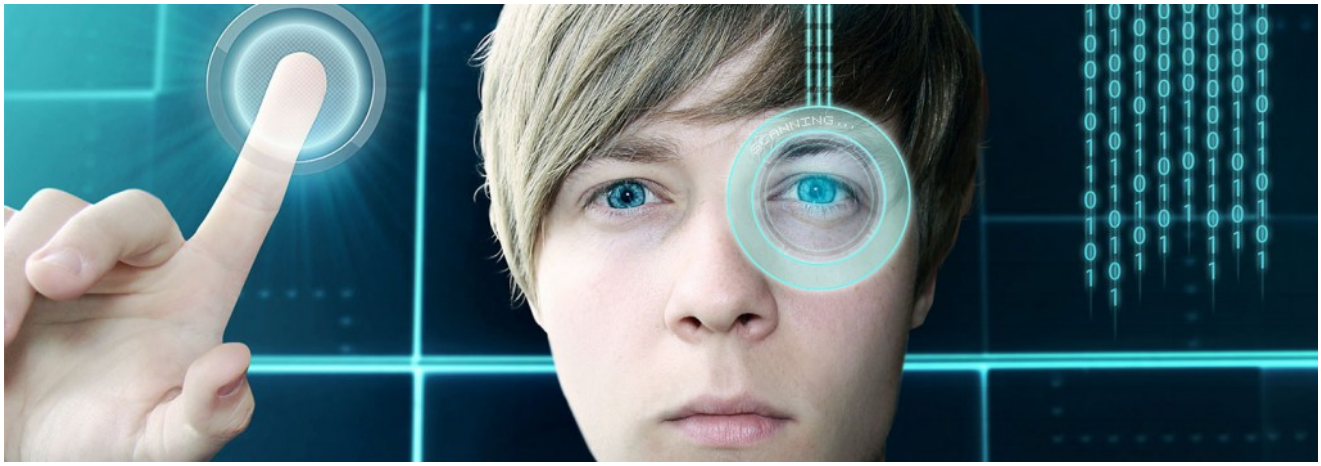
Adentrándonos en la identidad digital (Parte 1)

Hoy en día y cada vez más nuestros archivos, trabajos, investigaciones,… incluso parte de nuestra diversión, se encuentran en medios digitales a los cuales tenemos que acceder. Para ello debemos identificarnos, pero el sistema no puede reconocernos directamente, debemos usar una identidad digital propia, pero… ¿Sabemos cómo es realmente una identidad digital? ¿De qué características se compone? Salgamos de dudas.



La identidad digital es un conjunto de información y recursos proporcionados por un sistema informático a un usuario en particular, mediante los cuales pasar un proceso de identificación digital. En un sentido más amplio que es el conjunto de información disponible en línea y sobre una persona / organización / marca / etc.

Características de la identidad digital

La representación de la identidad digital debe ser mucho más amplia y compleja que la transacción en la que está involucrado. De hecho, el grado de fiabilidad y la cantidad de

información requerida puede variar muy significativamente dependiendo del tipo de transacción.

Una identidad digital se divide en dos partes:

- De quien es (la identidad)
- Las credenciales que uno posee (los atributos de esa identidad)

Las credenciales pueden ser numéricamente y cualitativamente muy variadas y tienen diferentes usos. La identidad digital completa es bastante compleja y tiene implicaciones tanto legales como técnicas. Sin embargo, la identidad digital más fácil consta de un ID (o nombre de usuario) y una palabra de identificación secreta (o contraseña). En este caso, el nombre de usuario es la identidad y la contraseña las credenciales de autenticación. Pero la identidad digital puede ser tan compleja como una identidad humana real.

Autenticación

Cuando en las transacciones se demuestra que la identidad digital presentada es de quién o qué dice ser, hablamos del proceso de autenticación.

La autenticación de un solo factor (el que tiene nombre de usuario y contraseña antes visto), está claro que no es lo más seguro, ya que la contraseña puede ser adivinada por alguien que no sea el usuario real. Por eso, que haya múltiples factores de identificación pueden hacerla más segura, como por

ejemplo: que exista una clave de seguridad física, como puede ser una tarjeta magnética («algo que tienes») y una contraseña («algo que sabes»). Si encima agregamos datos biométricos (como pueden ser: iris, huella digital, impresión de voz, reconocimiento facial, etc.) también añadiríamos otro factor de autenticación basado en «algo que está». Estos 3 factores unidos hacen prácticamente inviable cualquier usurpación de identidad digital, ya que, quien desee acceder, deberá ser igual que tú, tener lo que tú tienes y saber lo que tú sabes.

Autorización o Control de Acceso

Este es el siguiente nivel después de que las identidades digitales sean autenticadas. A menudo se trata de la concesión de la utilización de toda la identidad digital en una transacción, tales como el inicio de sesión de un usuario a un sitio. En otros casos, el control de acceso puede permitir o restringir el acceso a la información privada o permitir el acceso a los productos o servicios por una tarifa.

Continuará…