

Ejercicio 3

Enunciado 1

Una vez completada la tabla anterior, podrás reconocer qué características humanas cumplen con los indicadores que requiere un control de acceso biométrico.

Resolución 1

Para que un control de acceso basado en un sistema biométrico pueda considerarse fiable debe cumplir 4 indicadores: universalidad, unicidad, permanencia y cuantificación. Por lo que viendo la tabla completada en el ejercicio 2, puedo sacar en claro que las características humanas que cumplen con estos cuatro indicadores son: ADN, huella palmar, forma de la nariz, Iris, huella dactilar y la distancia entre pupilas.

Enunciado 2

La siguiente tabla muestra en su parte de arriba grupos de sistemas de control:

- a) Aquellos cuyo soporte es un objeto físico, como tarjetas, llaves mecánicas o electrónicas, etc.
- b) Los que se utilizan introduciendo una contraseña o un PIN.
- c) Los que usan características físicas, fisiológicas o conductuales de las personas.

A la izquierda hay una lista de sucesos o características que cada grupo tendrá o no, desde el punto de vista del usuario (persona que se somete al control de acceso). Marca en la tabla con una X si un grupo de arriba es susceptible o no de los eventos que se relacionan en la parte de la izquierda.

Por ejemplo, una característica biométrica, ¿es algo secreto para otras personas? ¿Es posible una clave? ¿Se puede compartir una tarjeta? ¿Puede ser robada una llave?

Resolución 2

	Objeto físico		Clave conocida		Característica biométrica	
	Sí	No	Sí	No	Sí	No
Pérdida	X			X	X	
Olvido	X		X			X
Robo	X			X	X	
Compartir	X		X			X
Adivinar	X		X			X
Secreto	X		X			X

Bibliografía

Definición:

Cuaderno Seguridad Informática SMR2