

# Conveniencia vs. Seguridad

## Qué Tan Bien Trabajan los Biométricos?

Puede usted estar absolutamente seguro que un dispositivo biométrico funcionará según lo esperado? Mantendrá confiablemente a "los malos" afuera mientras permite la entrada de manera sencilla a "los buenos"?

Hoy en día la disyuntiva de seguridad versus conveniencia (hacer difícil la entrada a los no autorizados contra permitir el fácil acceso a los autorizados) no representa un problema, dado que la combinación de la identificación biométrica y un código digitado en un teclado ofrece una seguridad virtualmente impenetrable. A continuación explicamos.

Los dispositivos biométricos se pueden ajustar en favor de la seguridad o de la conveniencia del usuario. Comparémoslos con una alarma de auto. Cuando la alarma se programa muy sensible, las probabilidades de que los ladrones le roben es muy baja. Pero el riesgo de que la alarma se active accidentalmente es alto. Reduzca la sensibilidad y el número de "falsas alarmas" también bajará, pero el riesgo de que le roben su auto aumentará.

Los requerimientos de seguridad de una agencia de defensa del gobierno pueden exigir que el dispositivo de la entrada principal se configure para que mantenga afuera a los malos, por ejemplo. Por otro lado, si cientos de empleados deben marcar con un reloj biométrico en una instalación que no necesita una gran seguridad, usted querrá ajustar la sensibilidad de la lectora para que deje entrar a los buenos.

A la gente le gustan las cosas que funcionan. Si el biométrico no le permite un acceso fácil a los empleados, rápidamente crecerá la frustración y podrían no aceptar nunca el dispositivo biométrico. Afortunadamente, esto rara vez ocurre.

### Tasas de Falsa Aceptación

La probabilidad de que un dispositivo biométrico permita entrar a una persona no autorizada se conoce como "Tasa de Falsa Aceptación".

Esta figura debe ser suficientemente baja para que no se convierta en un impedimento para el usuario. Los fabricantes de biométricos proclaman Tasas de Falsa Aceptación de sus equipos que varían entre 0.0001% y 0.1%. Los lectores biométricos de mano en la entrada principal del 60% de las plantas nucleares de EEUU tienen una Tasa de Falsa Aceptación de 0.1%.

Es importante recordar que la única manera que una persona no autorizada puede obtener acceso es si esa persona lo intenta. Por lo tanto, la Tasa de Falsa Aceptación debe multiplicarse por el número de intentos de personas no autorizadas para determinar el número de posibles ocurrencias.

### Tasas de Falso Rechazo

En muchos casos, permitir entrar a los buenos es tan importante como mantener afuera a los malos. La probabilidad que un dispositivo biométrico no reconozca a una persona autorizada se conoce como "Tasa de Falso Rechazo".

Las Tasas de Falso Rechazo para los sistemas biométricos actuales varía entre el 0.00066% y el 1.0%.

## Qué Tan Bien Trabajan los Biométricos?

Puede usted estar absolutamente seguro que un dispositivo biométrico funcionará según lo esperado? Mantendrá confiablemente a "los malos" afuera mientras permite la entrada de manera sencilla a "los buenos"?

Hoy en día la disyuntiva de seguridad versus conveniencia (hacer difícil la entrada a los no autorizados contra permitir el fácil acceso a los autorizados) no representa un problema, dado que la combinación de la identificación biométrica y un código digitado en un teclado ofrece una seguridad virtualmente impenetrable. A continuación explicamos:

Los dispositivos biométricos se pueden ajustar en favor de la seguridad o de la conveniencia del usuario. Comparémoslos con una alarma de auto. Cuando la alarma se programa muy sensible, las probabilidades de que los ladrones le roben es muy baja. Pero el riesgo de que la alarma se active accidentalmente es alto. Reduzca la sensibilidad y el número de "falsas alarmas" también bajará, pero el riesgo de que le roben su auto aumentará.

Los requerimientos de seguridad de una agencia de defensa del gobierno pueden exigir que el dispositivo de la entrada principal se configure para que mantenga afuera a los malos, por ejemplo. Por otro lado, si cientos de empleados deben marcar con un reloj biométrico en una instalación que no necesita una gran seguridad, usted querrá ajustar la sensibilidad de la lectora para que deje entrar a los buenos.

A la gente le gustan las cosas que funcionan. Si el biométrico no le permite un acceso fácil a los empleados, rápidamente crecerá la frustración y podrían no aceptar nunca el dispositivo biométrico. Afortunadamente, esto rara vez ocurre.

### Tasas de Falsa Aceptación

La probabilidad de que un dispositivo biométrico permita entrar a una persona no autorizada se conoce como "Tasa de Falsa Aceptación".

Esta figura debe ser suficientemente baja para que no se convierta en un impedimento para el usuario. Los fabricantes de biométricos proclaman Tasas de Falsa Aceptación de sus equipos que varían entre 0.0001% y 0.1%. Los lectores biométricos de mano en la entrada principal del 60% de las plantas nucleares de EEUU tienen una Tasa de Falsa Aceptación de 0.1%.

Es importante recordar que la única manera que una persona no autorizada puede obtener acceso es si esa persona lo intenta. Por lo tanto, la Tasa de Falsa Aceptación debe multiplicarse por el número de intentos de personas no autorizadas para determinar el número de posibles ocurrencias.

### Tasas de Falso Rechazo

En muchos casos, permitir entrar a los buenos es tan importante como mantener afuera a los malos. La probabilidad que un dispositivo biométrico no reconozca a una persona autorizada se conoce como "Tasa de Falso Rechazo".

Las Tasas de Falso Rechazo para los sistemas biométricos actuales varía entre el 0.00066% y el 1.0%.

## Conclusión

Es Posible Seguridad y Conveniencia a la Vez. Los dispositivos biométricos son extremadamente seguros gracias a la combinación de bajas Tasas de Falsa Aceptación (bajo parámetros de sensibilidad moderada) con códigos de usuario cortos. Al mismo tiempo, los biométricos son