

TECNOLOGÍA · 14 PÁGINAS

Credenciales Móviles vs Key Fobs — Comparativa de Seguridad

Comparativa lado a lado de seguridad y operación de credenciales móviles vs key fobs físicos. Incluye análisis de ciclo de vida de la credencial y costo total a 5 años.

14 páginas · Incluye hoja de costos imprimible · PDF

Por Qué el Tipo de Credencial Importa Más que el Lector

Cuando las propiedades evalúan control de acceso, la mayor parte de la conversación se centra en el hardware de la puerta — el panel, el lector, el motor del portón. La credencial misma, lo que un residente realmente lleva o usa para demostrar que pertenece ahí, tiende a tratarse como algo secundario. Eso está al revés. La credencial es donde realmente viven la mayoría de las brechas de seguridad del mundo real y el costo operativo continuo.

Los key fobs físicos y las credenciales móviles no son solo dos formatos distintos para la misma idea — se comportan de forma diferente exactamente en las condiciones que más importan: qué pasa cuando se pierde uno, qué tan fácil es duplicarlo, qué tan rápido se puede revocar el acceso, y cuánto cuesta realmente administrarlo a lo largo de los años, no solo en la instalación inicial.

QUÉ CUBRE ESTA GUÍA

Una mirada factual y lado a lado de cómo funciona realmente cada tipo de credencial, dónde cada una es genuinamente más vulnerable, cómo se ve administrar cada una durante toda la estadía de un residente, y una hoja de trabajo imprimible para comparar tu costo real a 5 años para cualquiera de los dos enfoques.

Cómo Funcionan Realmente los Key Fobs Físicos

La mayoría de los key fobs y tarjetas de proximidad usan RFID (identificación por radiofrecuencia) — un pequeño chip dentro del fob transmite un número de identificación a un lector cuando se acerca lo suficiente. El lector pasa ese número al panel de control de acceso, que lo verifica contra una lista de credenciales autorizadas y desbloquea la puerta si coincide.

No Todos los Fobs Son Igual de Seguros

Existe una diferencia importante entre las tarjetas de proximidad antiguas de baja frecuencia (125kHz) — ampliamente usadas desde los años 90 — y las tarjetas inteligentes más nuevas y cifradas (13.56MHz, como HID iCLASS Seos o similares). Los fobs de baja frecuencia transmiten un número estático y sin cifrar, lo cual es precisamente lo que los hace vulnerables a la clonación con dispositivos económicos y ampliamente disponibles. Las tarjetas inteligentes cifradas usan autenticación criptográfica entre la tarjeta y el lector, lo cual es considerablemente más difícil de duplicar — pero cuestan más por credencial y requieren lectores compatibles.

LA PREGUNTA PRÁCTICA

Antes de comparar fobs con credenciales móviles, vale la pena saber qué tipo de fob usa realmente tu propiedad. Los sistemas de proximidad de baja frecuencia heredados y las tarjetas inteligentes cifradas modernas tienen perfiles de riesgo muy distintos — pregúntale a tu proveedor actual cuál está instalado.

Cómo Funcionan Realmente las Credenciales Móviles

Una credencial móvil es una llave digital emitida al smartphone de un residente a través de una app, en lugar de un objeto físico. Dependiendo de la plataforma, el teléfono se comunica con el lector por Bluetooth, NFC, o un código QR, y la credencial misma está protegida por claves criptográficas únicas para la cuenta de ese residente, vinculadas a su dispositivo específico.

Qué la Hace Diferente de "Solo una App"

El modelo de seguridad no es simplemente "la app tiene una llave" — está en capas. El acceso típicamente requiere que el residente tenga una sesión autenticada (a menudo protegida por el propio bloqueo de pantalla del teléfono, PIN, o biometría), una credencial válida y no vencida emitida por la plataforma en la nube de la propiedad, y en la mayoría de los sistemas, un intercambio criptográfico entre el teléfono y el lector que resiste la interceptación simple o la repetición, a diferencia de un número RFID estático.

Debido a que la credencial se emite y administra centralmente en la nube, puede cambiarse, expirar, o revocarse en el instante en que un administrador de propiedad hace ese cambio — no hay ningún objeto físico que recuperar o reemitir.

Lado a Lado: Dónde Es Vulnerable Cada Credencial

Factor de Riesgo	Key Fob Físico	Credencial Móvil
Riesgo de clonación	Alto para fobs de baja frecuencia; bajo para tarjetas inteligentes cifradas	Bajo — credenciales criptográficas vinculadas al dispositivo resisten la duplicación simple
Ventana de exposición ante pérdida	Activa hasta que se reporta físicamente y se desactiva manualmente	Puede revocarse instantánea y remotamente, en el momento en que se reporta
Préstamo o uso compartido no autorizado	Fácil — un fob físico puede prestarse a cualquiera sin ningún registro	Más difícil — vinculada a la cuenta autenticada y dispositivo de un individuo
Robo de la credencial misma	Utilizable de inmediato por quien la tenga	Típicamente requiere el propio bloqueo del teléfono (PIN/biometría) para activarse
Registro de auditoría de uso	Limitado a "se usó este número de fob" sin verificación de identidad	Vinculado a una cuenta autenticada, con mayor confianza de identidad
Vulnerabilidad si la plataforma misma es comprometida	Menor — sin dependencia de red para la credencial en sí	Depende de las prácticas de seguridad en la nube del proveedor

Las credenciales móviles superan en la mayoría de los riesgos cotidianos, pero introducen una nueva dependencia: la seguridad de la plataforma en la nube y app del proveedor. Pregunta directamente a cualquier proveedor sobre sus prácticas de seguridad de datos y cifrado — consulta la Sección 4 de nuestra Plantilla de RFP para los requisitos específicos a verificar.

Administrar un Key Fob, Desde la Mudanza hasta la Salida

1. **Pedido e inventario.** Los fobs deben comprarse y mantenerse en existencia antes de necesitarse — un faltante el día de mudanza crea un problema operativo real.
2. **Programación.** Cada fob debe programarse o registrarse manualmente en el sistema de acceso por parte del personal.
3. **Distribución.** Un miembro del personal entrega el fob al residente en persona, típicamente requiriendo una firma o confirmación.
4. **Seguimiento continuo.** La propiedad debe mantener un registro de qué número de fob pertenece a qué residente — una hoja de cálculo o sistema que debe mantenerse preciso con el tiempo.
5. **Evento de pérdida.** Cuando se pierde un fob, alguien debe reportarlo, el personal debe desactivar la credencial anterior, y debe emitirse un nuevo fob — a menudo con una tarifa de reemplazo.
6. **Salida.** El personal debe recuperar físicamente el fob, o desactivarlo si no se devuelve, y actualizar los registros correspondientemente.

Cada uno de estos seis pasos requiere tiempo del personal y es un punto donde el registro puede desincronizarse de la realidad — un residente que se mudó con un fob activo y no recuperado es una brecha común y a menudo invisible.

Administrar una Credencial Móvil, Desde la Mudanza hasta la Salida

1. **Invitación.** El personal envía una invitación digital al correo o número de teléfono del residente — no se requiere inventario físico.
2. **Activación de autoservicio.** El residente descarga la app (o abre una credencial basada en web) y activa su propio acceso, típicamente en minutos, sin visita del personal.
3. **No se necesita seguimiento manual.** El propio sistema mantiene el registro de quién tiene qué credencial — no hay una hoja de cálculo separada que mantener sincronizada.
4. **Evento de pérdida.** Si se pierde o roba un teléfono, el residente o el personal revoca el acceso instantáneamente desde la app o el panel — sin hardware de reemplazo, sin recuperación física.
5. **Salida.** El personal desactiva la credencial de forma remota en el momento en que termina el contrato de arrendamiento — no se requiere coordinación para recuperar nada físicamente.

El ciclo de vida es más corto y elimina los dos pasos con mayor probabilidad de fallar en un sistema físico: la precisión del seguimiento manual y la recuperación física en la salida.

Comparación de Ciclo de Vida de un Vistazo

Etapas del Ciclo de Vida	Key Fob	Credencial Móvil
Emisión inicial	Requiere inventario físico y programación del personal	Invitación digital, activación de autoservicio
Tiempo de personal por emisión	Moderado — requiere entrega en persona	Mínimo — invitación automatizada
Precisión de seguimiento con el tiempo	Manual, propenso a desviarse	El sistema de registro es automático
Tiempo de respuesta ante una credencial perdida	Depende de cuándo se reporta y la disponibilidad del personal	Instantáneo, el residente o el personal pueden revocar de inmediato
Proceso de salida	Requiere recuperación física o desactivación manual	Desactivación remota, sin coordinación necesaria

DÓNDE SE REFLEJA ESTO EN TU PRESUPUESTO

Cada etapa donde un fob requiere tiempo de personal o coordinación física es un costo laboral recurrente que una credencial móvil elimina en gran parte. Las siguientes tres páginas te guían para cuantificar esa diferencia para tu propiedad específica.

Metodología y Supuestos

Para comparar justamente ambos enfoques durante un período de 5 años, esta hoja de trabajo considera los costos que son fáciles de pasar por alto en una simple comparación de precio por unidad: reemplazo por pérdida, tiempo de personal, y reemisión por rotación de residentes.

Para Key Fobs, Necesitarás

- ✓ Costo por fob (típicamente \$3–\$15 dependiendo de si es un fob básico de baja frecuencia o una credencial inteligente cifrada)
- ✓ Número de residentes / unidades que requieren una credencial
- ✓ Tasa anual estimada de pérdida/reemplazo (muchas propiedades ven entre 10–20% de sus fobs reemplazados anualmente por pérdida, daño, o no devolución en la salida)
- ✓ Tiempo de personal por evento de emisión o reemplazo, y el costo por hora asociado

Para Credenciales Móviles, Necesitarás

- ✓ Si la credencialización móvil está incluida en la suscripción de software de tu plataforma o se factura por separado por credencial
- ✓ Tiempo de personal por emisión (típicamente mínimo, ya que la activación es de autoservicio)

Hoja de Trabajo Imprimible

Key Fob — Costo de Emisión Inicial

Número de unidades: _____ × Costo por fob: \$ _____ = \$ _____

Key Fob — Costo Anual de Reemplazo

Número de unidades: _____ × Tasa anual de pérdida: _____ % × Costo por fob: \$ _____ =
\$ _____ /año

× 5 años = \$ _____

Key Fob — Costo de Tiempo de Personal

Eventos de emisión/reemplazo por año: _____ × Horas por evento: _____ × Salario por hora:
\$ _____ = \$ _____ /año

× 5 años = \$ _____

COSTO TOTAL DE KEY FOB A 5 AÑOS = \$ _____

Hoja de Trabajo, Continuación

Credencial Móvil — Costo de Software

Si está incluido en la suscripción de tu plataforma, usa \$0 aquí y bázate en el costo mensual de tu plataforma. Si se factura por credencial:

Número de unidades: _____ × Costo anual por credencial: \$ _____ × 5 años = \$ _____

Credencial Móvil — Costo de Tiempo de Personal

Eventos de emisión por año: _____ × Horas por evento: _____ × Salario por hora: \$ _____ =
\$ _____ /año

× 5 años = \$ _____

COSTO TOTAL DE CREDENCIAL MÓVIL A 5 AÑOS = \$ _____

Costo Total de Key Fob a 5 Años (de la página 10): \$ _____

Costo Total de Credencial Móvil a 5 Años (de arriba): \$ _____

Ahorro Estimado a 5 Años = \$ _____

Vulnerabilidades Comunes que Vale la Pena Conocer

- ✓ **Los dispositivos de clonación de fobs son económicos y ampliamente disponibles en línea** para tarjetas de proximidad de baja frecuencia — este es un riesgo documentado y real para sistemas de fobs heredados, no teórico.
- ✓ **Los fobs se prestan de manera informal** — un residente que presta su fob a un familiar, paseador de perros, o contratista crea acceso sin rastro que el sistema no tiene forma de detectar.
- ✓ **La recuperación en la salida es inconsistente.** Las propiedades con alta rotación frecuentemente tienen una población de fobs activos "huérfanos" de residentes que nunca los devolvieron.
- ✓ **Las credenciales móviles trasladan el riesgo a la seguridad del teléfono** — un residente sin bloqueo de pantalla o PIN en su teléfono reduce el beneficio práctico de seguridad, así que la higiene a nivel de dispositivo importa.
- ✓ **La seguridad de la credencial móvil es tan fuerte como la implementación del proveedor** — pregunta directamente sobre los estándares de cifrado y si las credenciales están vinculadas al dispositivo o son transferibles, según la Sección 4 de nuestra Plantilla de RFP.

Qué Buscar, y Puntos Clave

- ✓ Confirma si tus fobs actuales son de baja frecuencia (mayor riesgo de clonación) o credenciales inteligentes cifradas, antes de asumir que tu sistema actual es seguro.
- ✓ Las credenciales móviles generalmente superan a los fobs en velocidad de revocación, resistencia a la clonación, y calidad del registro de auditoría — pero su seguridad depende de la implementación en la nube y app del proveedor.
- ✓ El costo de ciclo de vida de los key fobs está impulsado por la tasa de pérdida/reemplazo y el tiempo de personal, no solo el precio por unidad — ambos suelen subestimarse.
- ✓ Ejecuta la hoja de trabajo a 5 años de esta guía con los números reales de tu propiedad antes de asumir que un enfoque es más económico que el otro.
- ✓ Un enfoque híbrido — credenciales móviles para la mayoría de los residentes, fobs físicos disponibles para quienes los prefieran — es común y razonable, siempre que ambos tipos de credencial se rastreen y revoquen desde la misma plataforma.

VIVO CONTROL

Credenciales Móviles, Administradas Desde una Sola Plataforma

Vivo Control emite y revoca el acceso de residentes al instante desde la nube — sin inventario de fobs, sin seguimiento manual, y sin coordinación necesaria en la salida.

Reserva una Demo Gratis →

www.vivocontrol.com/es/demo/ · hello@vivocontrol.com · Esta guía tiene fines informativos generales y no constituye asesoría de ingeniería de seguridad para tu propiedad específica.