PLATAFORMA DE IDENTIDAD OPERACIONAL

UNA SOLA IDENTIDAD FUERTE PARA EL MUNDO FÍSICO + DIGITAL

Biznet Control convierte cada acceso en evidencia digital confiable: presencia validada, biometría local, credenciales inteligentes y autenticación passwordless en un solo modelo de confianza.

1	6	0
IDENTIDAD FUERTE FÍSICA Y DIGITAL	FACTORES: QR·NFC·MRZ FACIAL·PALMA·FIDO2	CONTRASEÑAS EN ACCESOS CRÍTICOS

EL PLANTEAMIENTO

Resumen ejecutivo

Biznet Control evoluciona el control de acceso tradicional hacia una **plataforma de identidad operacional**. Su objetivo ya no es solo abrir una puerta, una barrera o un torniquete: es validar **quién es la persona**, si está físicamente presente, si pertenece al turno y contrato correcto, si tiene autorización vigente y si puede operar también en los sistemas digitales críticos del negocio.

IDEA CENTRAL

Una sola identidad fuerte para el mundo físico y digital: presencia validada, credencial segura, biometría local, trazabilidad operacional y autenticación digital sin contraseñas.

La propuesta une dos dimensiones que históricamente han operado por separado. El terminal BPOINT, las smartcards, NFC, QR dinámico, biometría local, APIs y passkeys/FIDO2 permiten construir un modelo donde el sistema no solo pregunta **"¿tiene clave?"**, sino también **"¿está en el lugar correcto, fue validado de forma fuerte y está autorizado para operar?"**.

DIMENSIÓN A

Acceso físico

Ingreso a recintos, zonas críticas, bodegas, faenas, puertos, salas eléctricas, vehículos, llaves, torniquetes y barreras.

DIMENSIÓN B

Acceso digital

Ingreso a aplicaciones, ERP, CRM, WMS, VPN, plataformas SCADA/MES, firma de eventos y autorización de acciones críticas.

Físico+Digital

Convergencia en un mismo modelo de identidad y de confianza

Passwordless

Autenticación FIDO2 que reduce phishing y robo de claves

Auditable

Cada acción queda trazada a una identidad operacional

POR QUÉ IMPORTA

El problema que resuelve

En muchas organizaciones el mundo físico y el digital están **desconectados**. Una persona entra a planta con una tarjeta, pero accede a sistemas críticos con usuario y contraseña desde otro lugar. El resultado: control de acceso, asistencia, contratistas, ERP y seguridad física operando con **identidades distintas y sin visión unificada**.

Suplantación y préstamo de credenciales	Una tarjeta, PIN o QR **puede ser prestado** si no existe verificación fuerte de identidad asociada a la persona real.
Contraseñas débiles o robadas	El acceso digital sigue expuesto a **phishing, reutilización de claves, filtraciones** y uso indebido de credenciales.
Baja trazabilidad operacional	No siempre se puede **probar** que quien operó un sistema fue la misma persona que ingresó físicamente al recinto.
Riesgo legal por biometría	La biometría **centralizada** aumenta la exposición ante incidentes y las exigencias de protección de datos personales.
Sistemas fragmentados	Acceso, asistencia, contratistas, ERP, apps y seguridad física operan con **identidades separadas** y sin gobierno común.

LA CONSECUENCIA

Sin una identidad unificada, la organización paga el costo en seguridad, cumplimiento y eficiencia operativa — y no puede demostrar lo que ocurrió.

LA VISIÓN

Identidad operacional unificada

Biznet Control propone entender la identidad de una persona como una **identidad operacional**: la combinación de identidad civil o corporativa, credencial física, biometría validada, contexto de presencia, contrato o rol, horario, zona y autorización digital.

EL RECORRIDO DE LA CONFIANZA

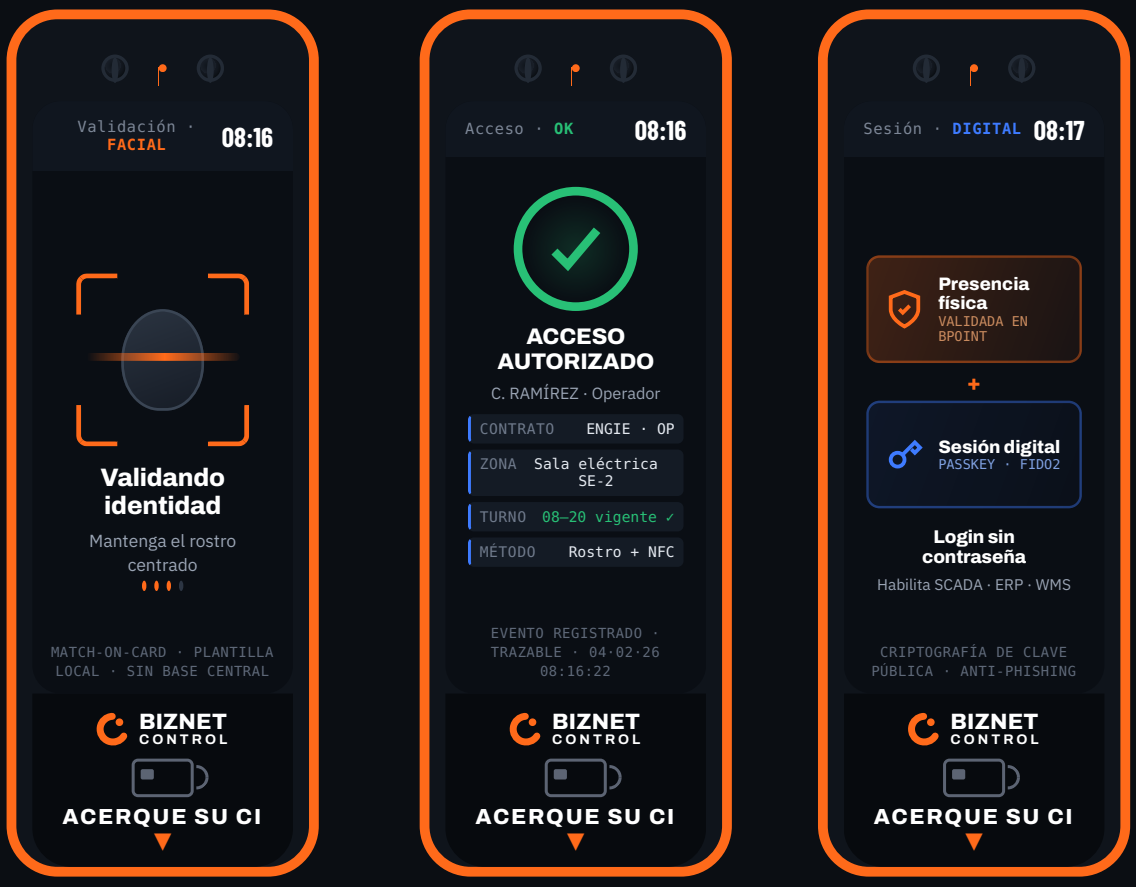
MENSAJE COMERCIAL

No basta con saber si una persona tiene permiso digital. Biznet Control permite saber si esa persona está físicamente presente, fue validada, está dentro de su turno o zona autorizada y puede operar bajo las reglas de la organización.

EL BORDE DE IDENTIDAD

Terminales BPOINT en operación

Los terminales **BPOINT** transforman un evento presencial en evidencia digital confiable. Una misma plataforma, una misma marca — y la pantalla se adapta al flujo que cada punto de control necesita.



A · RECONOCIMIENTO FACIAL B · AUTORIZACIÓN POR CONTEXTO C · LOGIN PASSWORDLESS

LA PLATAFORMA DE BORDE

Capacidades del terminal BPOINT

Los BPOINT actúan como terminales de borde para control de acceso, asistencia, validación de identidad y habilitación operacional. Según la configuración del proyecto, pueden incorporar o integrarse con las siguientes capacidades:

Validación facial
Confirma identidad en accesos, asistencia y zonas controladas.

NFC y documentos de identidad
Lectura de credenciales, tarjetas inteligentes y documentos con chip.

MRZ + NFC
Validación reforzada que comprueba la coherencia del documento.

QR fijo y QR dinámico
Acceso desde credenciales, invitaciones, apps móviles o tokens temporales.

Credenciales DESFire / MDF8K
Tarjetas seguras para control de acceso e identificadores.

Biometría avanzada opcional
Huella, rostro, palma o vena de palma según hardware y caso de uso.

Match-on-card
Validación biométrica local o en tarjeta, sin bases centrales.

Conectividad múltiple
Escenarios con LAN, Wi-Fi y conectividad celular según modelo.

Control de actuadores
Puertas, torniquetes, barreras, cerraduras, relés y periféricos.

Edge computing
Decisiones locales y continuidad ante intermitencia de red.

Protección industrial
Configuraciones resistentes a polvo, humedad o intemperie según modelo.

APIs e integración
Comunicación con ERP, WMS, SCADA, CRM, contratistas y middleware.

TARJETA · BIOMETRÍA · PASSKEY

Tecnologías de credencial

La arquitectura puede incorporar credenciales inteligentes capaces de soportar distintas funciones dentro de una misma tarjeta o dispositivo seguro. Cada función se valida técnicamente por proveedor, certificación y compatibilidad con el flujo.

CONTACTLESS · NFC

MDF8K / DESFire 8K

Capa de acceso físico contactless para puertas, barreras, torniquetes y lectura NFC segura.

ACCESO FÍSICO SEGURO

SECURE OS · APPLETS

JCOP / Java Card

Sistema operativo seguro para ejecutar applets de identidad, certificados, firma o autenticación.

IDENTIDAD PROGRAMABLE

CERTIFICADOS · PKI

PIV / PKI

Credenciales corporativas basadas en certificados para autenticación fuerte, firma y entornos de alta seguridad.

IDENTIDAD DIGITAL CORPORATIVA

PASSWORDLESS · ESTÁNDAR ABIERTO

FIDO2 / Passkeys

Autenticación passwordless mediante criptografía de clave públ que reduce phishing y robo de contraseñas.

ACCESO DIGITAL SIN CONTRASEÑA

PRIVACIDAD POR DISEÑO

MOC — Match-on-card

Comparación biométrica en la tarjeta o contra una credencial protegida, lo que disminuye la exposición de plantillas biométricas en bases centr

PRIVACIDAD BIOMÉTRICA

PUNTO CLAVE DE ARQUITECTURA

Para Biznet Control no es obligatorio que el match-on-card libere directamente el passkey dentro de la tarjeta. Lo importante es que el backend **una dos evidencias**: presencia física validada y autenticación digital fuerte.

Passkeys/FIDO usan credenciales criptográficas asociadas a una cuenta y permiten iniciar sesión sin contraseñas, usando biometría, PIN o patrón como mecanismo de desbloqueo. La FIDO Alliance las define como credenciales FIDO basadas en estándares para autenticación passwordless; Microsoft describe FIDO2 como un estándar abierto basado en criptografía de clave pública.

EL PUENTE

Cómo se conecta lo físico con lo digital

La unión se realiza mediante **eventos confiables, APIs y políticas de autorización**. El ingreso físico genera una evidencia digital; luego la aplicación consulta esa evidencia antes de permitir una operación.

1. **Ingreso al recinto**
   La persona se presenta ante un BPOINT o punto de control.
2. **Validación fuerte**
   Se valida credencial, biometría, documento, QR o una combinación de factores.
3. **Registro operacional**
   Se registra persona, hora, zona, dispositivo, resultado, contrato, turno y reglas aplicadas.
4. **Sesión física vigente**
   El sistema mantiene una condición de presencia: dentro del recinto, zona, turno o con autorización temporal.
5. **Acceso digital**
   La persona entra a una aplicación con passkey/FIDO2, PIV/certificado u otro mecanismo fuerte.
6. **Decisión contextual**
   La app consulta a Biznet Control: presencia, rol, contrato, zona, horario y nivel de validación.
7. **Auditoría**
   Toda acción física y digital queda asociada a una identidad operacional y a un evento trazable.

PANTALLA D · ACCESO TEMPORAL DE CONTRATISTAS

REGLA DE EJEMPLO

Permitir abrir el módulo de operación crítica SI:

- ✓ El usuario autenticó con **passkey/FIDO2**
- ✓ El usuario **ingresó físicamente** al recinto
- ✓ El ingreso fue validado con **biometría o credencial fuerte**
- ✓ El usuario está dentro de **turno vigente**
- ✓ El usuario pertenece al **contrato autorizado**
- ✓ El usuario está en una **zona permitida**
- ✓ No existe **alerta, bloqueo ni excepción** pendiente

DISEÑO DE SOLUCIÓN

Arquitectura de la solución

La arquitectura recomendada separa con claridad los dispositivos de borde, la capa transaccional, el motor de identidad, la integración y las aplicaciones consumidoras.

CAPA 01 **Capa física**	BPOINT · Torniquetes · Barreras · Puertas · Cerraduras · Lectores NFC · Cámaras · Sensores · Periféricos
CAPA 02 **Capa de credencial**	Tarjetas DESFire · Smartcards · QR dinámico · Documentos NFC · Biometría local · Credenciales móviles
CAPA 03 · NÚCLEO **Biznet Control**	Registro de eventos · Reglas de acceso · Turnos · Contratos · Perfiles · Zonas · Trazabilidad · Auditoría
CAPA 04 **Identidad digital**	Passkeys / FIDO2 · PIV / PKI · SSO · Directorio corporativo · MFA · Gestión de sesiones
CAPA 05 **Capa de integración**	APIs REST · WebSocket · Colas de eventos · Middleware · WSO2 / bus de integración
CAPA 06 **Aplicaciones**	ERP · CRM · WMS · TMS · SCADA · MES · Apps móviles · Control de llaves

Enfoque "strangler fig" para sistemas heredados

Esta separación permite implementar sin reemplazar todo de una vez: primero se encapsulan los procesos actuales de acceso y autorización, luego se agregan validaciones fuertes y, finalmente, se automatizan las decisiones críticas.

DÓNDE GENERA VALOR

Casos de uso por industria

Biznet Control se adapta a operaciones de alta exigencia donde la presencia física validada y la autorización digital deben converger.

01

Puertos y logística

Validar conductores, contratistas y personal operativo; controlar zonas de regulación de flujo, terminales, patios, bodegas, andenes y retiro de carga.

02

Energía e infraestructura crítica

Controlar ingreso a subestaciones, plantas, salas eléctricas y centros de operación; exigir presencia validada antes de operar sistemas críticos.

03

Minería e industria

Unir acreditación laboral, acceso a faena, habilitación de equipos, control de turnos, seguridad industrial y autorizaciones digitales.

04

Data centers y salas seguras

Doble validación: presencia física con BPOINT y autenticación passwordless para acceder a consolas, racks o sistemas de administración.

05

Flotas, llaves y vehículos

Habilitar entrega de llaves, PIN de arranque o acceso a vehículos solo si la persona está validada y autorizada por turno, contrato y rol.

06

Contratistas y cumplimiento

Asociar identidad, empresa contratista, documentación vigente, inducciones, permisos de trabajo y registro de acceso físico-digital.

PATRÓN COMÚN

En todas las industrias, el valor está en lo mismo: probar quién estuvo, dónde, cuándo y bajo qué autorización — para el mundo físico y el digital.

CUMPLIMIENTO · CHILE

Ley 21.719 de protección de datos

La Ley 21.719 regula la protección y el tratamiento de datos personales y crea la Agencia de Protección de Datos Personales en Chile. La guía oficial de Gobierno Digital indica que fue publicada el **13 de diciembre de 2024** y entrará en vigencia el **1 de diciembre de 2026**, reformando integralmente la Ley 19.628. Los análisis jurídicos destacan que la nueva definición de datos sensibles incorpora expresamente la información biométrica y genética.

Esto es relevante porque el control de acceso trata datos personales: identidad, RUT, empresa, contrato, horarios, ubicación, registros de entrada y salida, logs de uso y, en algunos casos, datos biométricos.

POR QUÉ AHORA

01·DIC 2026

Fecha de entrada en vigencia. El tiempo para diseñar accesos con privacidad por diseño es ahora — no después.

ENFOQUE RECOMENDADO

No vender la solución como "cumplimiento automático" de la ley, sino como una **arquitectura diseñada para facilitar el cumplimiento**: privacidad por diseño, minimización de datos biométricos, trazabilidad, seguridad, finalidad y control de acceso basado en reglas.

Minimización

Usar solo los datos necesarios para validar identidad, presencia y autorización.

Finalidad

Definir claramente para qué se usa cada dato: acceso, asistencia, seguridad o auditoría.

Seguridad

Cifrado, segregación, controles de acceso y auditoría sobre credenciales, plantillas y APIs.

Privacidad por diseño

Preferir match-on-card o validación local para reducir bases biométricas centrales.

Trazabilidad

Evidencia auditable de quién accedió, cuándo, dónde, con qué método y bajo qué autorización.

Gobernanza

Responsables, retención, base de licitud, derechos de titulares y gestión de incidentes.

La biometría deja de ser solo una función de acceso y pasa a ser parte de una arquitectura de confianza: en vez de centralizar plantillas sin necesidad, el modelo valida localmente y registra solo la evidencia de autorización, según la política del cliente y su marco legal aplicable.

POR QUÉ BIZNET CONTROL

Diferenciadores

01 **Identidad operacional unificada**
Integra acceso físico, asistencia, seguridad y autorización digital en una misma lógica.

02 **Evolución sin ruptura**
Permite pasar de tarjetas o QR tradicionales a credenciales inteligentes, biometría local y passkeys.

03 **Menos contraseñas, menos riesgo**
Incorpora autenticación passwordless para las aplicaciones críticas.

04 **Presencia antes de permiso**
Valida la presencia física antes de autorizar acciones digitales sensibles.

05 **Integra lo que ya existe**
Se conecta con sistemas actuales mediante APIs, middleware y eventos.

06 **Privacidad por diseño**
Facilita estrategias de minimización en escenarios con biometría.

07 **Implementación gradual**
No exige reemplazar todos los sistemas existentes desde el primer día.

08 **Trazabilidad demostrable**
Cada evento físico y digital queda asociado a una identidad auditable.

ANTES

Control de acceso tradicional: tarjetas prestables, claves robables, sistemas fragmentados y baja trazabilidad.

→

DESPUÉS

Identidad operacional unificada: física, digital, biométrica, criptográfica y auditable — en un solo modelo de confianza.

CÓMO SE DESPLIEGA

Plan de implementación sugerido

Un recorrido por fases que reduce riesgo: cada etapa entrega un resultado medible antes de avanzar a la siguiente.

FASE 01
Diagnóstico de identidad operacional

Levantamiento de recintos, zonas, flujos físicos, sistemas digitales, perfiles, riesgos, reglas y datos tratados.

RESULTADO
Mapa de riesgos y reglas

FASE 02
Piloto BPOINT

Instalación controlada en uno o dos puntos críticos con credencial, biometría o QR, registro de eventos y dashboard.

RESULTADO
Piloto operativo medible

FASE 03
Integración digital

Conexión con app, ERP, WMS, directorio o middleware para consultar presencia física antes de autorizar operaciones.

RESULTADO
APIs y decisión contextual

FASE 04
Passkey / FIDO2 y credencial inteligente

Autenticación passwordless y evaluación de smartcards con FIDO2, PIV, DESFire y match-on-card.

RESULTADO
Login físico-digital convergente

FASE 05
Escalamiento y gobierno

Políticas, retención de datos, auditoría, continuidad operacional, métricas y despliegue por zonas o sitios.

RESULTADO
Modelo escalable y auditable

FILOSOFÍA DE DESPLIEGUE

Empezar pequeño, probar con datos reales y escalar con gobierno. Cada fase es una victoria operativa, no una promesa.

CIERRE

Conclusión

Biznet Control se posiciona como una **plataforma de identidad operacional** para organizaciones que requieren mayor seguridad, trazabilidad y control en ambientes físicos y digitales. La oportunidad no está solo en abrir puertas: está en unir presencia física, autorización por contexto y autenticación digital fuerte en un mismo modelo de confianza.

FRASE DE POSICIONAMIENTO

Biznet Control permite pasar del control de acceso tradicional a una identidad operacional unificada: física, digital, biométrica, criptográfica y auditable.

SIGUIENTE PASO

Agendemos un diagnóstico de identidad operacional

1 · Diagnóstico
Levantamiento de recintos, flujos y reglas de su operación.

2 · Piloto BPOINT
Demostración medible en uno o dos puntos críticos.

3 · Hoja de ruta
Plan de escalamiento físico-digital a la medida.

REFERENCIAS

Biblioteca del Congreso Nacional de Chile — Ley 21.719, protección y tratamiento de datos personales. bcn.cl/leychile

Gobierno Digital de Chile — Guía práctica de implementación de la nueva Ley de Datos Personales. wikiguias.digital.gob.cl

FIDO Alliance — Passkeys: autenticación passwordless. fidoalliance.org/passkeys

Microsoft Security — What is FIDO2: estándar abierto basado en criptografía de clave pública. microsoft.com

Gestión y Tendencias — Análisis de la Ley 21.719 y datos sensibles biométricos y genéticos.

BIZNET
IT · CONTROL

Biznet IT — Tecnologías de Información Ltda.
www.biznet.cl
Identidad operacional físico-digital

DOCUMENTO
Ejecutivo técnico-comercial · 19·05·2026