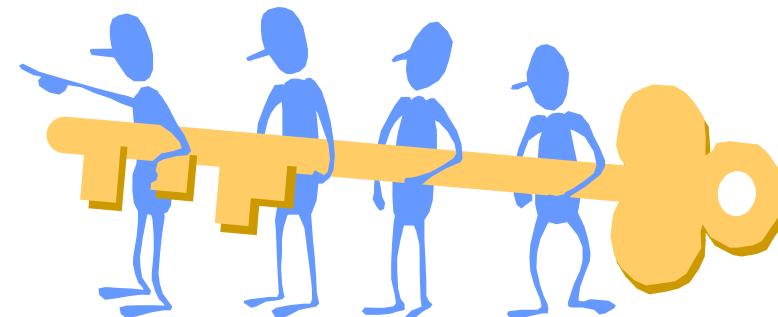
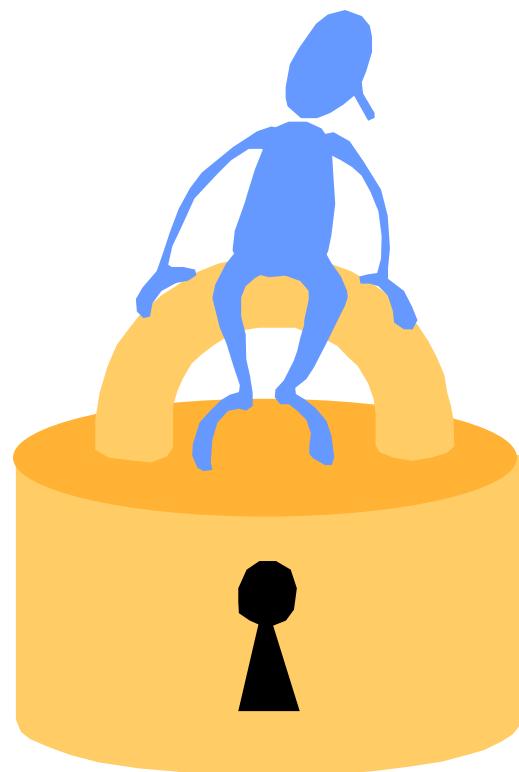


Sistemas de Control de Acceso

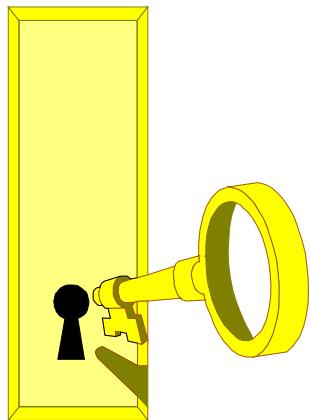
Sesión #6



ABC DEL CONTROL DE ACCESO



AGENDA



- 🔒 ¿Qué es el Control de Acceso?
 - 🔒 Métodos de Identificación
 - 🔒 Beneficios del Control de Acceso
 - 🔒 Componentes del Sistema
 - 🔒 Prestaciones del Sistema
 - 🔒 Análisis de Situaciones
 - 🔒 Tendencias del Mercado
-

¿QUÉ ES EL CONTROL DE ACCESO?

¿QUIEN?



¿DONDE?



¿CUANDO?



- 🔒 Controlamos: Quién va, adónde va, cuándo va
- 🔒 Controlamos la salida y entrada a ciertas áreas de:
 - ➡ Personas, vehículos, y/o activos
- 🔒 Distinguiendo a los que son de los que no son.
- 🔒 La identificación es clave para el control de acceso

MÉTODOS DE IDENTIFICACIÓN

🔒 La identificación es clave para el control de acceso

🔒 Categorías para Identificación :

→ **Algo que la persona trae...**

↳ **Llaves, tarjeta**



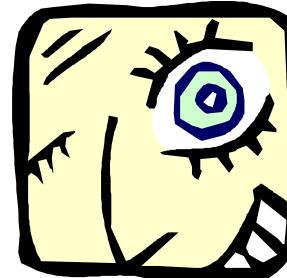
→ **Algo que la persona conoce...**

↳ **Clave, código personal ó una combinación**

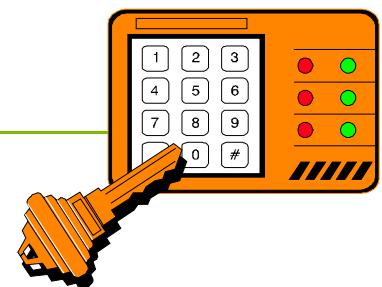


→ **Algo que la persona es...**

↳ **Una característica o atributo**



🔒 Una combinación de cualquiera de las anteriores



BENEFICIOS DEL CONTROL DE ACCESO

🔒 Un ambiente Seguro y controlado

- ↳ Incremento de los niveles de seguridad
- ↳ Archivos y respaldos de eventos
 - 👉 Archivo de entradas y salidas
 - 👉 Administración de riesgos y daños en áreas sensibles.
 - 👉 Respuesta instantánea a alarmas
 - 👉 Reportes

🔒 Reducción de Riesgos (Preventivo)

- ↳ Reducción de pérdidas potenciales
 - ↳ Protección de activos
-



BENEFICIOS DEL CONTROL DE ACCESO

🔒 Reducción de Costos de Seguridad

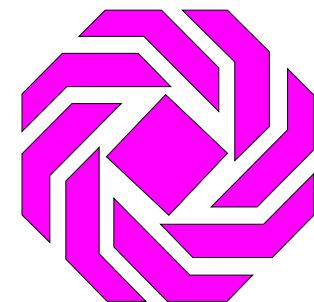
→ El costo total de seguridad se decrementa al:

👉 Disminuir los costos de recursos humanos

⚠ Aumentar la Eficiencia

⚠ Teniendo la información para saber Dónde emplearla y cuánto tiempo

👉 Cerraduras y Llaves (eliminando los cambios de chapas y llaves)



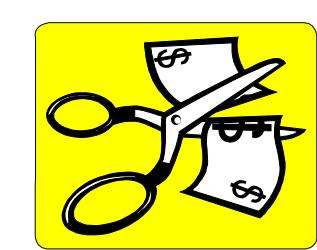
BENEFICIOS DEL CONTROL DE ACCESO

🔒 Oportunidades de Integración

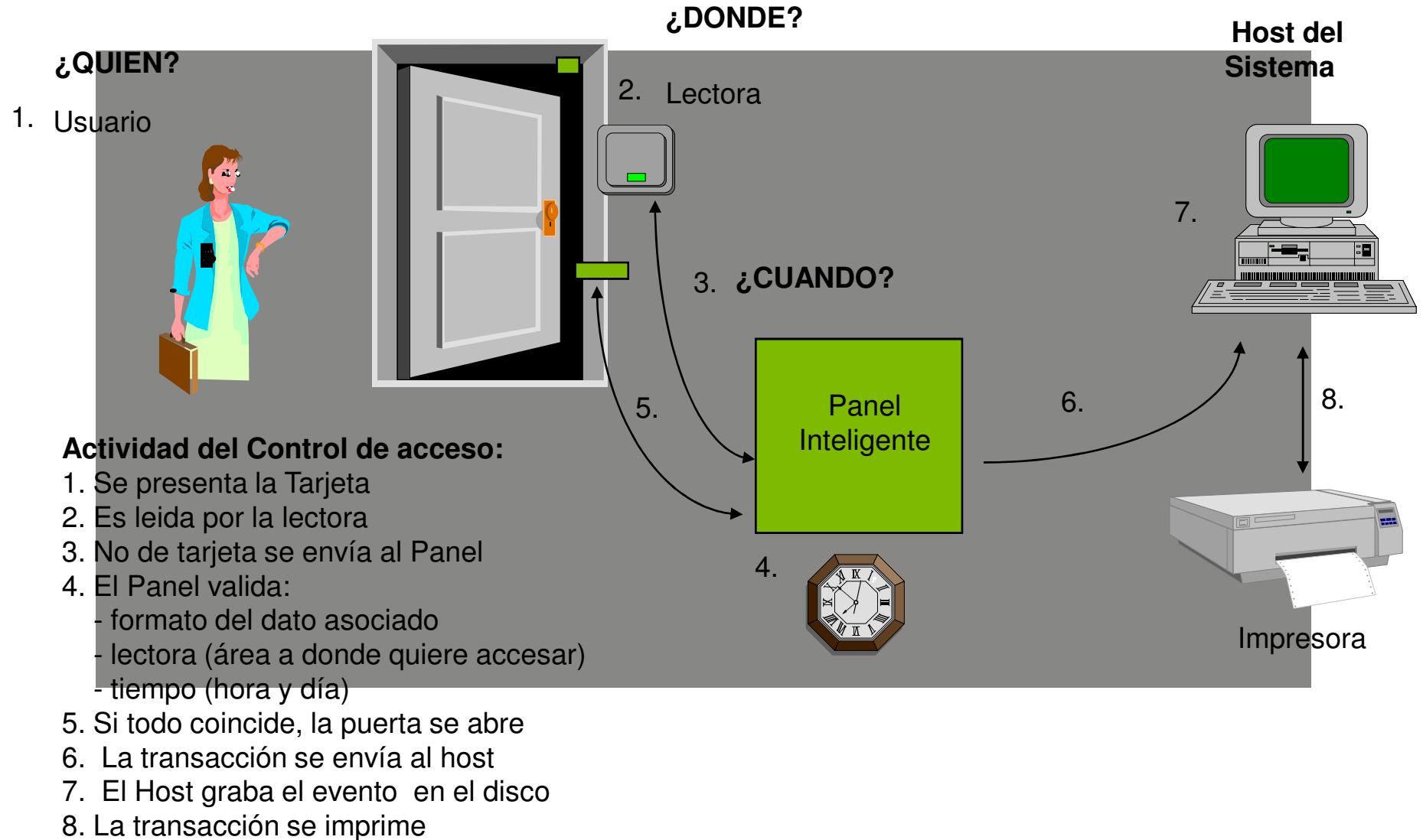
- ↳ Recursos Humanos

- ↳ Tiempo y Asistencia

- ↳ Otros Sistemas de Seguridad



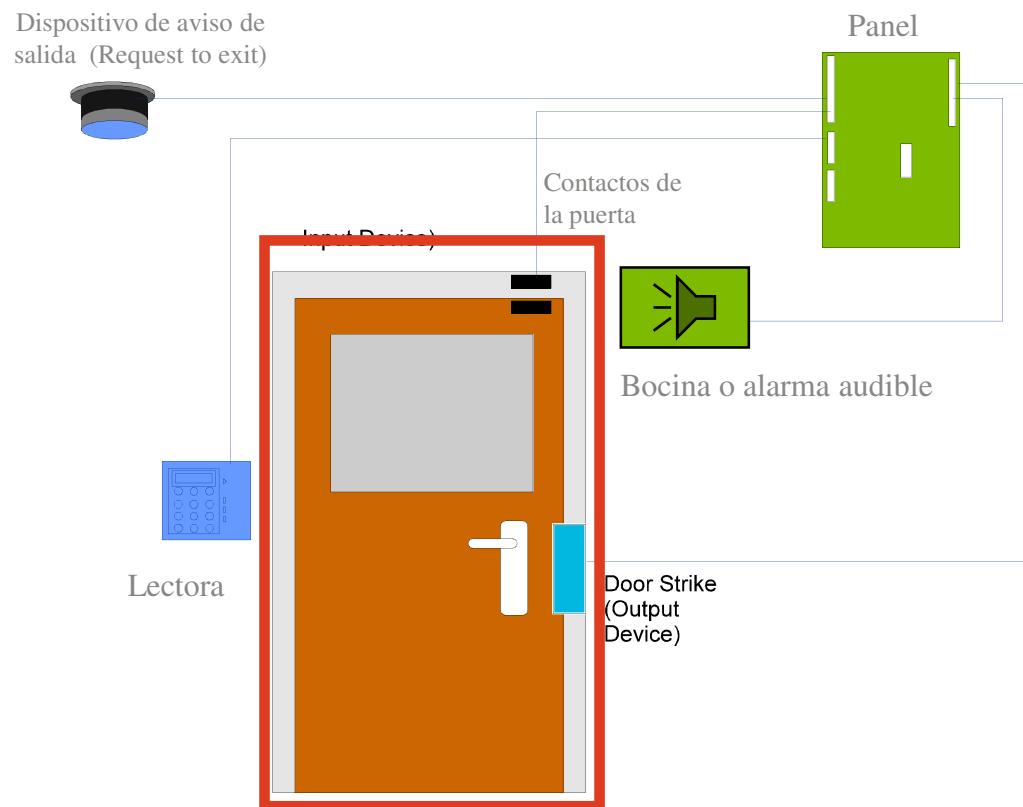
COMPONENTES DEL SISTEMA



Configuración Básica de una Puerta

🔒 CONCEPTO BÁSICO

- 🔒 Lado seguro: es el lado que está dentro del área a la cual se quiere accesar.
- 🔒 Lado no seguro: es el lado desde el cual se solicita el acceso.
- 🔒 Una puerta puede tener ambos lados seguros, especialmente si interesa saber cuántas personas hay en el recinto o controlar la hora de salida del recinto (no solo la de ingreso).



Configuración Básica de una Puerta

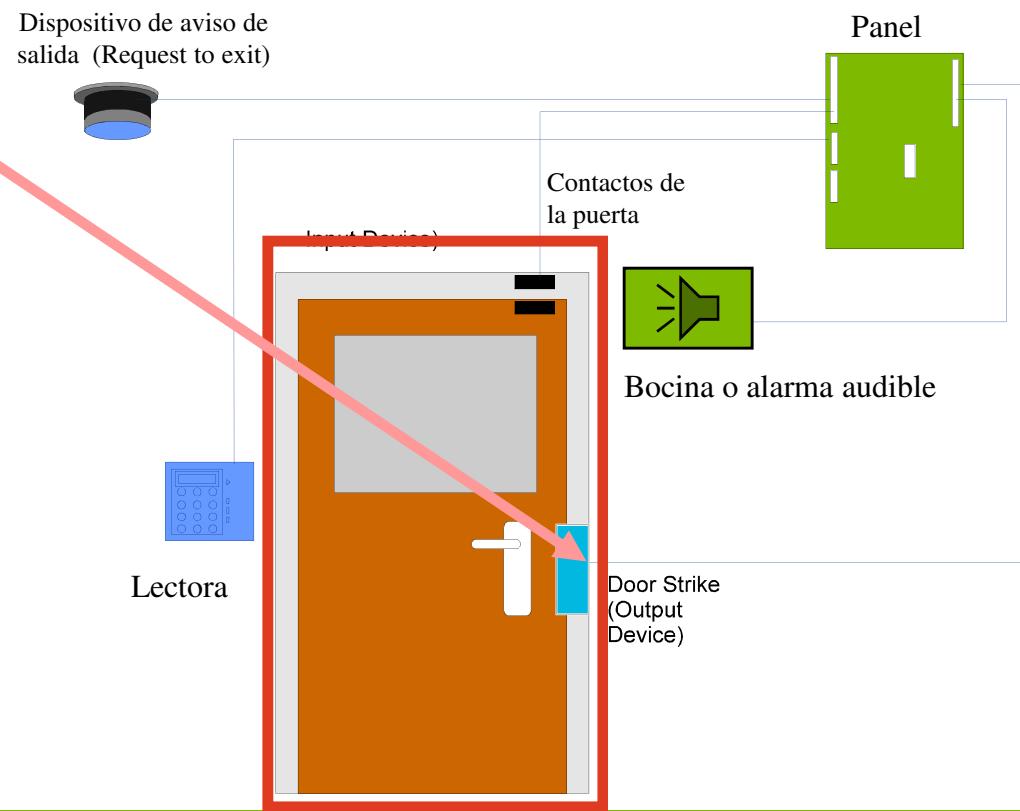
- 🔒 Punto de Control de Acceso
- 🔒 La barrera física a ser controlada para permitir el paso puede ser:
 - ➡ Una puerta, una puerta giratoria, una puerta tipo estadio (trompo), una puerta con apertura por sensor óptico, pluma de estacionamiento, u otro tipo de barrera.



Configuración Básica de una Puerta

🔒 Mecanismo de cerradura:

- ↳ Puede ser una cerradura accionada por un electroimán
- ↳ Puede ser una cerradura electromagnética
- ↳ Puede ser de seguridad en fallas (Fail Safe): se abre cuando ocurre una falla del sistema o de la alimentación
- ↳ O puede ser contra fallas (Fail Secure): Mantiene la cerradura cerrada ante fallas.



Configuración Básica de una Puerta

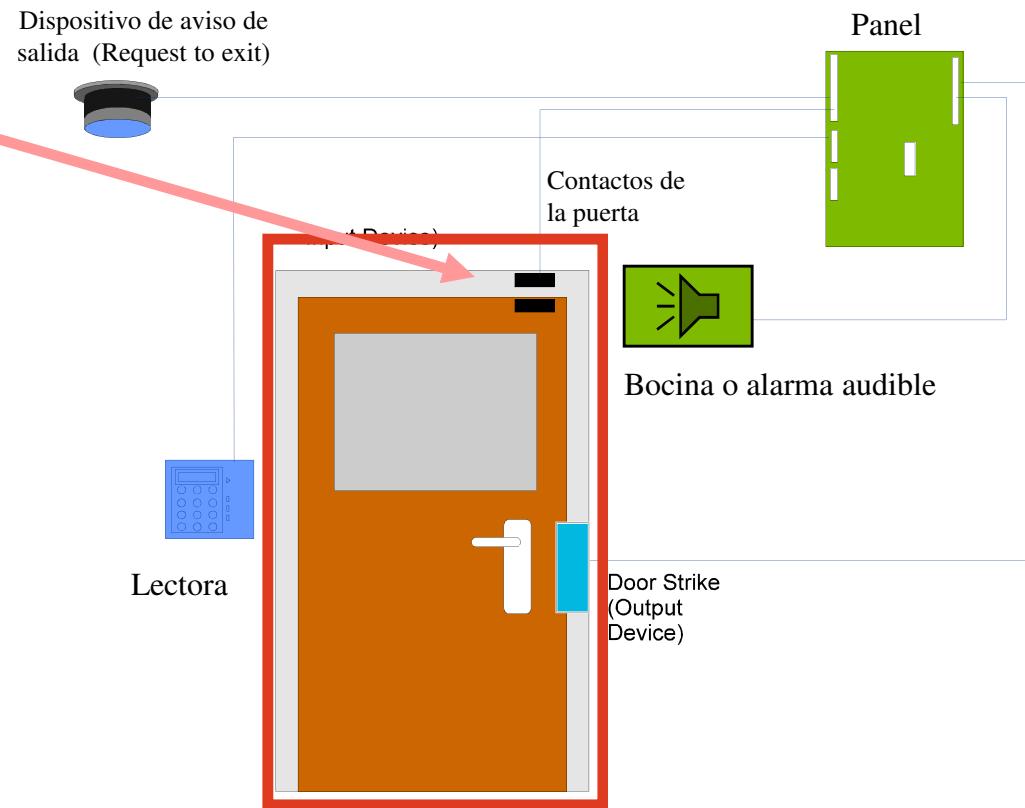
- 🔒 Mecanismo de cerradura:
- 🔒 El más usado es la retención electromagnética:
- 🔒 Puede ser sencilla (puertas de una hoja).
- 🔒 O doble (puertas de dos hojas).
- 🔒 Debe indicarse la fuerza de la retención, típicamente 600 lb, aplicaciones especiales, 1200 lb.



Configuración Básica de una Puerta

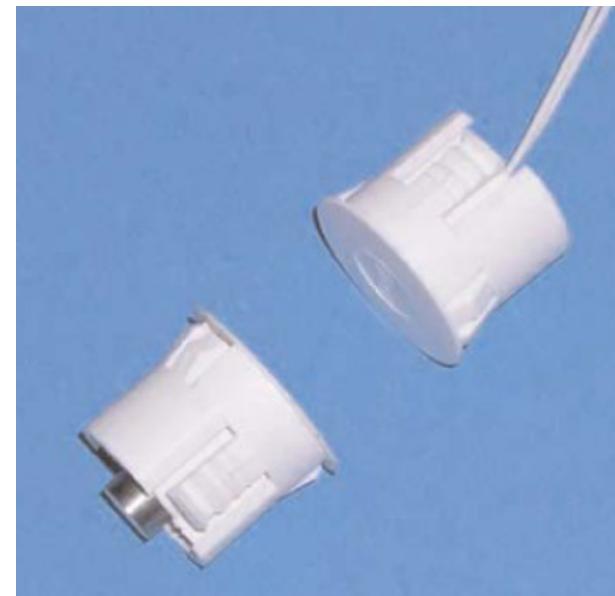
🔒 Contactos de Puerta:

- Un switch magnético que detecta cuando la puerta está abierta o cerrada.
- Se utiliza también para detectar cuando una puerta ha estado demasiado tiempo abierta o su apertura fue forzada.



Configuración Básica de una Puerta

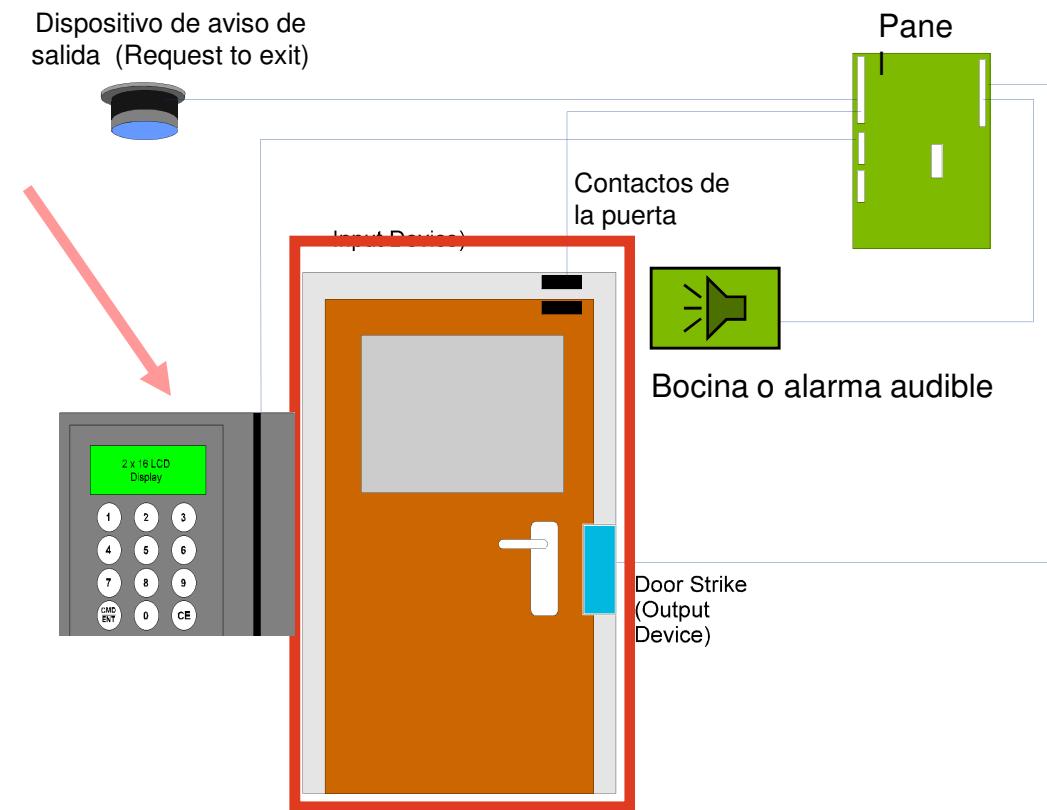
- 🔒 Contactos de Puerta:
 - ↳ Switch NA.
 - ↳ Puede venir incorporado en la retención electromagnética.
 - ↳ Para construcciones nuevas idealmente empotrado.



Configuración Básica de una Puerta

🔒 Dispositivo de solicitud de acceso:

- Típicamente una lectora de tarjetas, pero pudiera ser también un teclado numérico ó un dispositivo biométrico
- Puede dar indicaciones de permiso de acceso o no mediante leds, sonidos o una pantalla alfanumérica.



Configuración Básica de una Puerta

🔒 Dispositivo de pedido de salida (Request to Exit):

- Detecta una solicitud de salida desde la parte segura de la puerta sin el uso de una tarjeta.

- Puede ser pasiva:

- Pulsador

- Ó activa:

- Sensor de presencia.



Configuración Básica de una Puerta

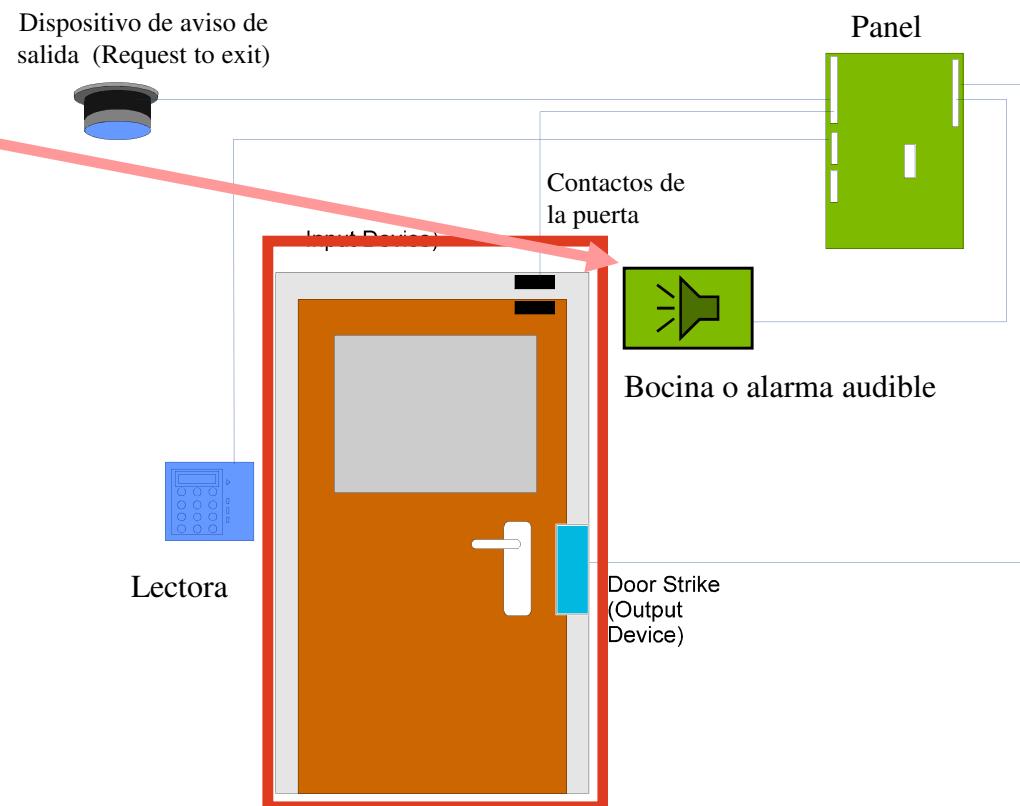
- 🔒 Dispositivo de pedido de salida (Request to Exit):
 - ➡ El más básico es un botón REX.
 - ➡ Puede ser una barra de salida.
 - ➡ O un dispositivo que no requiera contacto (botón o sensor en cielo).



Configuración Básica de una Puerta

🔒 Dispositivo de salida

- Típicamente es un dispositivo sonoro el cual se activa si la puerta se abre mediante un proceso no válido, ó si la puerta se deja abierta demasiado tiempo.



Configuración Básica de una Puerta

🔒 Dispositivo de salida

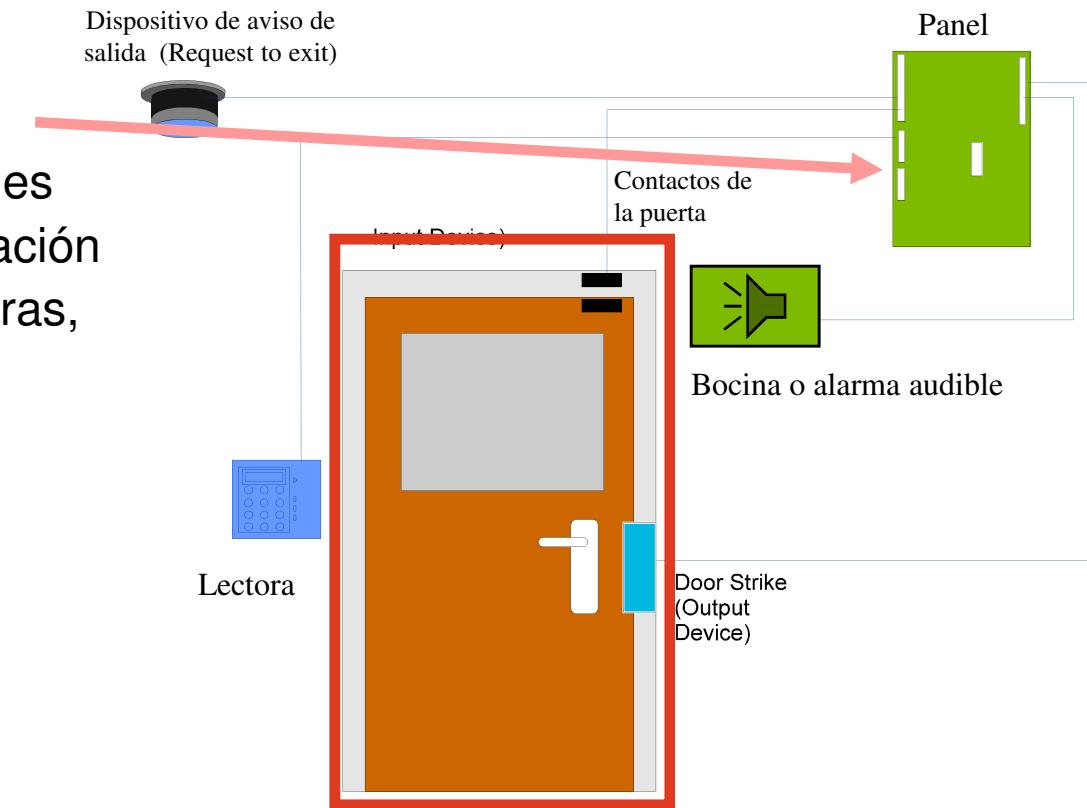
- ↳ Puede ser visual (luz incandescente, led o estroboscópica).
- ↳ O sonoro, por lo general un zumbador.



Configuración Básica de una Puerta

🔒 Panel de control:

- Dispositivo inteligente que es capaz de controlar la operación de hasta 8 puertas (o lectoras, una por cada puerta).



Configuración Básica de una Puerta

🔒 Panel de control:

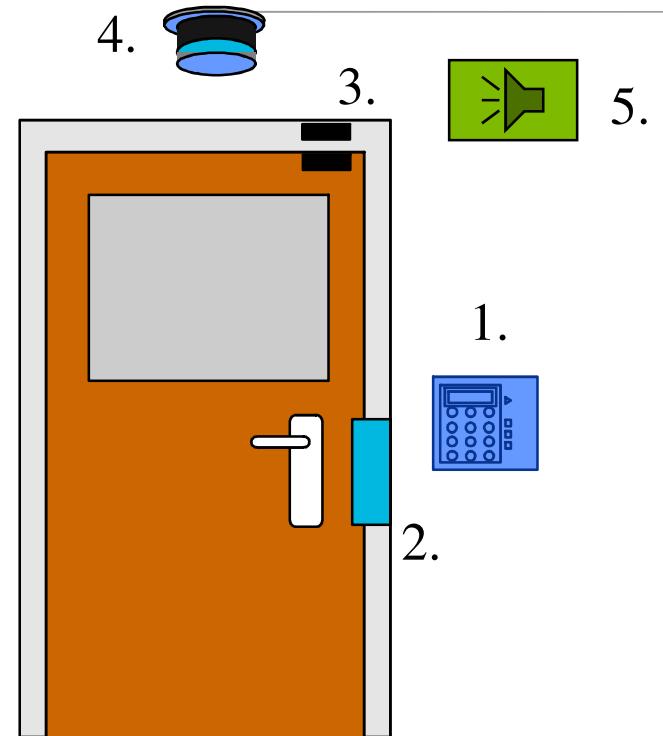
- Puede ser un único panel o varios distribuidos, depende de la cantidad de lectoras y de la topología de red del fabricante.



COMPONENTES EL SISTEMA: RESUMIENDO

🔒 Dispositivos en la puerta:

- ↳ Lectora de tarjetas
- ↳ Mecanismo de cerradura
- ↳ Eléctrica, magnética, etc.
- ↳ Contactos magnéticos en la puerta
 - ⌚ Monitoreo de apertura/cierre de puerta
- ↳ Dispositivo de aviso de salida
 - ⌚ Aviso de apertura desde dentro
 - ⌚ Aviso para suprimir alarma de puerta
- ↳ Salida (alarma audible)
 - ⌚ Indica condición de la alarma
 - ⌚ Local, remota ó ambas



Componentes Clave

1. Lectora
2. Mecanismo de cerradura
3. Contactos Magnéticos
4. Dispositivo de pedido de salida
5. Dispositivo de salida

COMPONENTES DEL SISTEMA

🔒 Instrumentos de Acceso (Tarjeta/Gafete)

↳ Identificación

🔒 Consideraciones Tecnológicas

↳ Aplicación

↳ Estética

↳ Costo



COMPONENTES DEL SISTEMA

🔒 Tarjetas de Acceso (Gafetes)

→ “Llave Electrónica” que identificar al portador

☛ Número de Identificación Codificado



- El número relaciona al portador con la tarjeta dentro del sistema

Código de sitio ó Sucursal

Número Opcional asignado en común a todos los usuarios de un mismo sitio u oficina.

- Este número permite distinguirse de los usuarios de otros sistemas similares.

☛ Nivel variable

- Permite reusar el mismo numero de serie en diferentes tarjetas.

☛ Número de Serie - estampado

- Número visible en la tarjeta para facilitar la identificación

COMPONENTES DEL SISTEMA

🔒 Tecnología de Tarjeta

➡ Código de Barra

☞ Utiliza una serie de líneas de anchura variable

☞ Leída por un scanner óptico

☞ Creado para usarse en infrarrojo para eliminar duplicados

VENTAJAS

Bajo costo

El usuario lo puede codificar

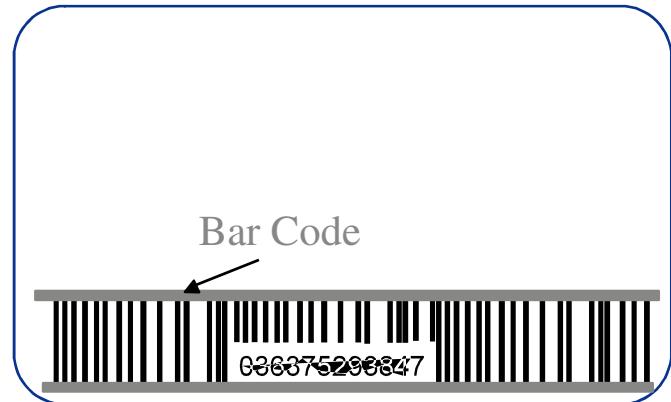
Tecnología Dual

DESVENTAJAS

Fácil de duplicar

El usuario lo puede codificar

Suceptible a errores de lectura por suciedad, etc

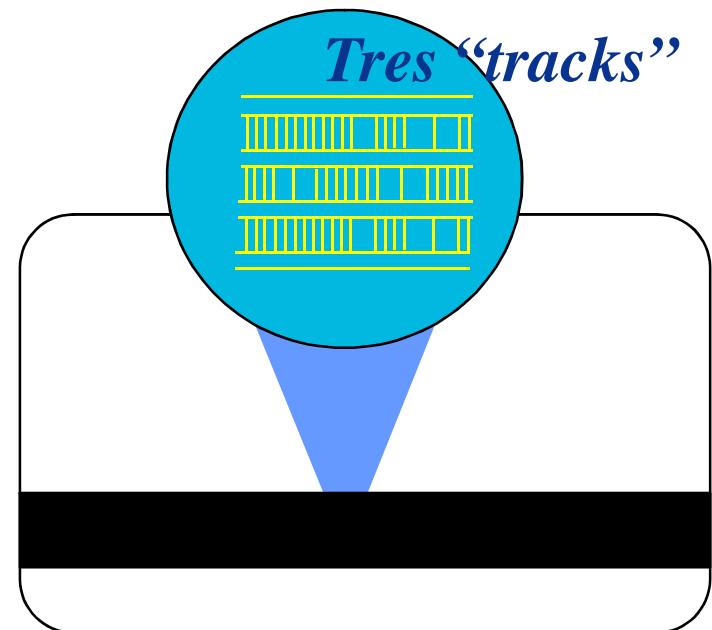


COMPONENTES DEL SISTEMA

🔒 Tecnología de Tarjeta

➡ Tira Magnética

- ☞ Cinta laminada de Oxido Magnético en la tarjeta
- ☞ La información se graba en la cinta magnética
- ☞ Se pueden usar tracks múltiples



VENTAJAS

Bajo costo

El usuario lo puede codificar
Multi-tracks

DESVENTAJAS

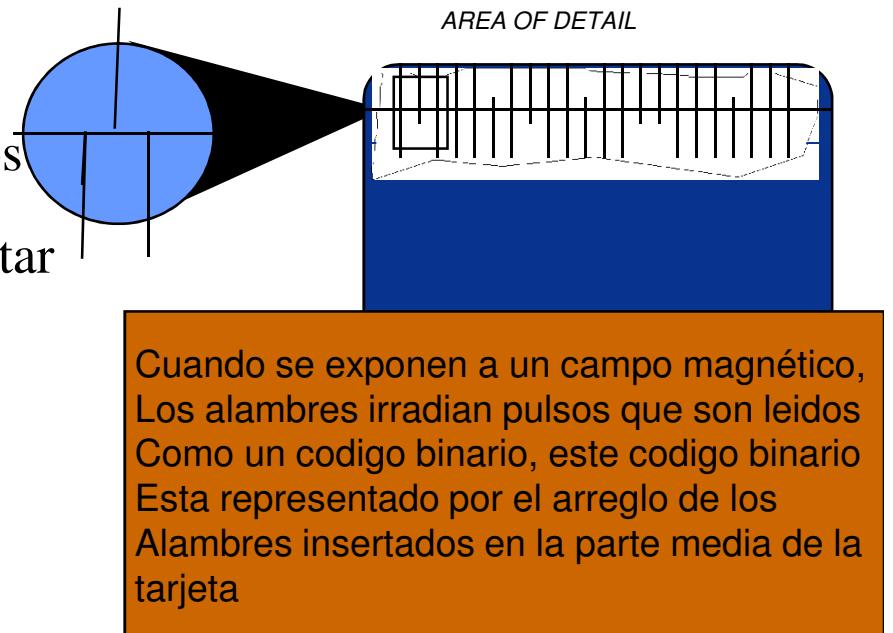
Suceptible a errores de lectura
por suciedad, etc.
El usuario lo puede codificar
Sujetos a alteración

COMPONENTES DEL SISTEMA

🔒 Tecnología de Tarjeta

➡ Wiegand

- ⌚ Alambres ferromagnéticos insertados
- ⌚ Los cuales se arreglan para representar datos
- ⌚ Los datos son leídos al pasar por la cabeza de la lectora
- ⌚ Muchos formatos diferentes



VENTAJAS

- Difícil de duplicar
- Difícil de modificar
- No requiere contacto con lectora

DESVENTAJAS

- No puede ser auto codificado
- Depende de tiempos de envío
- Sus fuentes son Limitadas

COMPONENTES DEL SISTEMA

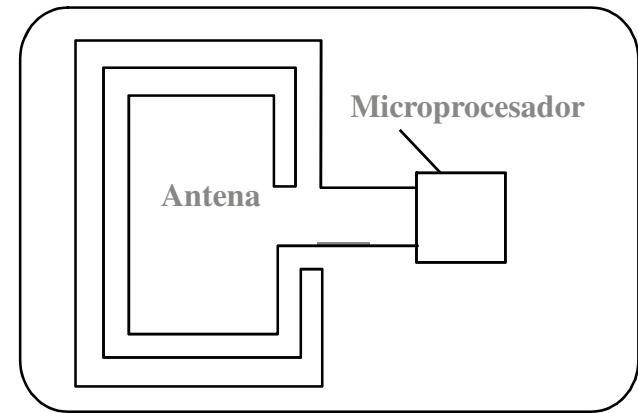
🔒 Tecnología de Tarjeta

➡ Proximidad

⌚ Activa ó Pasiva

⌚ No requiere contacto con lectora

⌚ Cada vez mas popular



VENTAJAS

Muy cercano a manos libres

Imagen de alta tecnología

Estetico

Difícil de duplicar

DESVENTAJAS

Lecturas Accidentales

Interferencia de RF

External magnetic field produced by the reader induces energy into the tuned circuits of the card. Stimulated by this energy, the card then emits various frequencies, each contributing to the overall intelligence of the code.

COMPONENTES DEL SISTEMA

🔒 Tecnología de Tarjeta

⬅ Proximidad

☞ Múltiples opciones de presentación:

☞ Tarjeta típica (PVC)

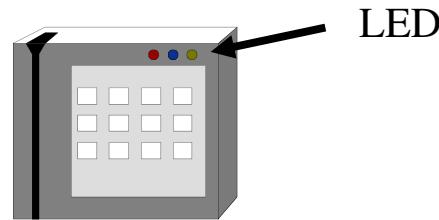
☞ Tags adhesivos para tarjetas existentes: muy útil para no cargar al usuario con dos tarjetas.

☞ Tipo llavero (ver foto) ideal para aplicaciones residenciales.



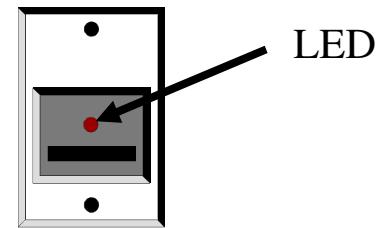
¡EL PROTOCOLO DE COMUNICACIÓN CON EL PANEL ES WEIGAND!

COMPONENTES DEL SISTEMA



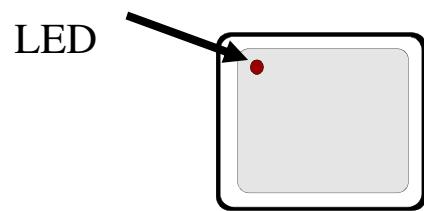
Lectora deslizable

La tarjeta se desliza en la ranura de la lectora para ser leída



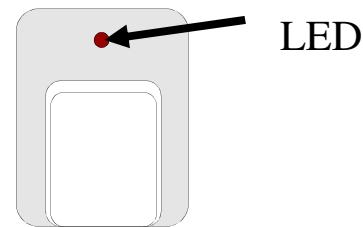
Lectora insertable

La tarjeta se inserta en la ranura de la lectora para ser leída (insertar/sacar)



Lectora de proximidad

La tarjeta es presentada dentro del campo de radiofrecuencia para ser leída

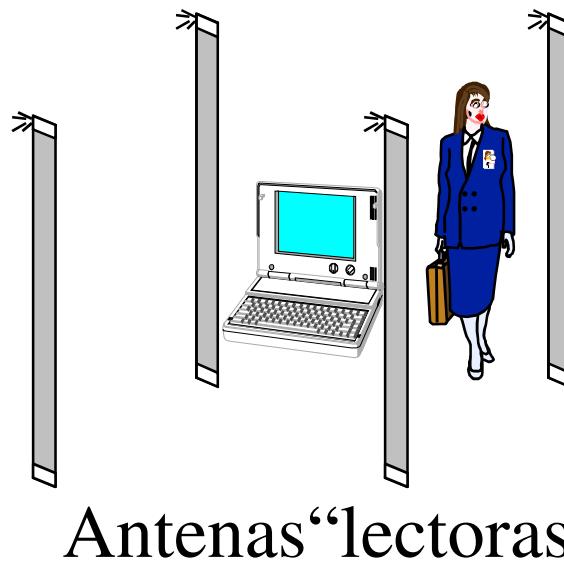


Lectora Wiegand

La tarjeta se pone en contacto con la superficie de la lectora para ser leída

COMPONENTES DEL SISTEMA

¡Los lectores pueden tener varias formas y configuraciones !



COMPONENTES DEL SISTEMA

Lectores biométricos



Huella digital: combina una base de datos local (en el lector) de código de tarjeta vs huella digital.

Luego de verificar transmite al controlador el código del usuario.

Es decir, el controlador no guarda el archivo de las huellas digitales.

Aplicación: laboratorios, tesorería, almacenamiento de materiales peligrosos o confidenciales.

COMPONENTES DEL SISTEMA

Lectores biométricos



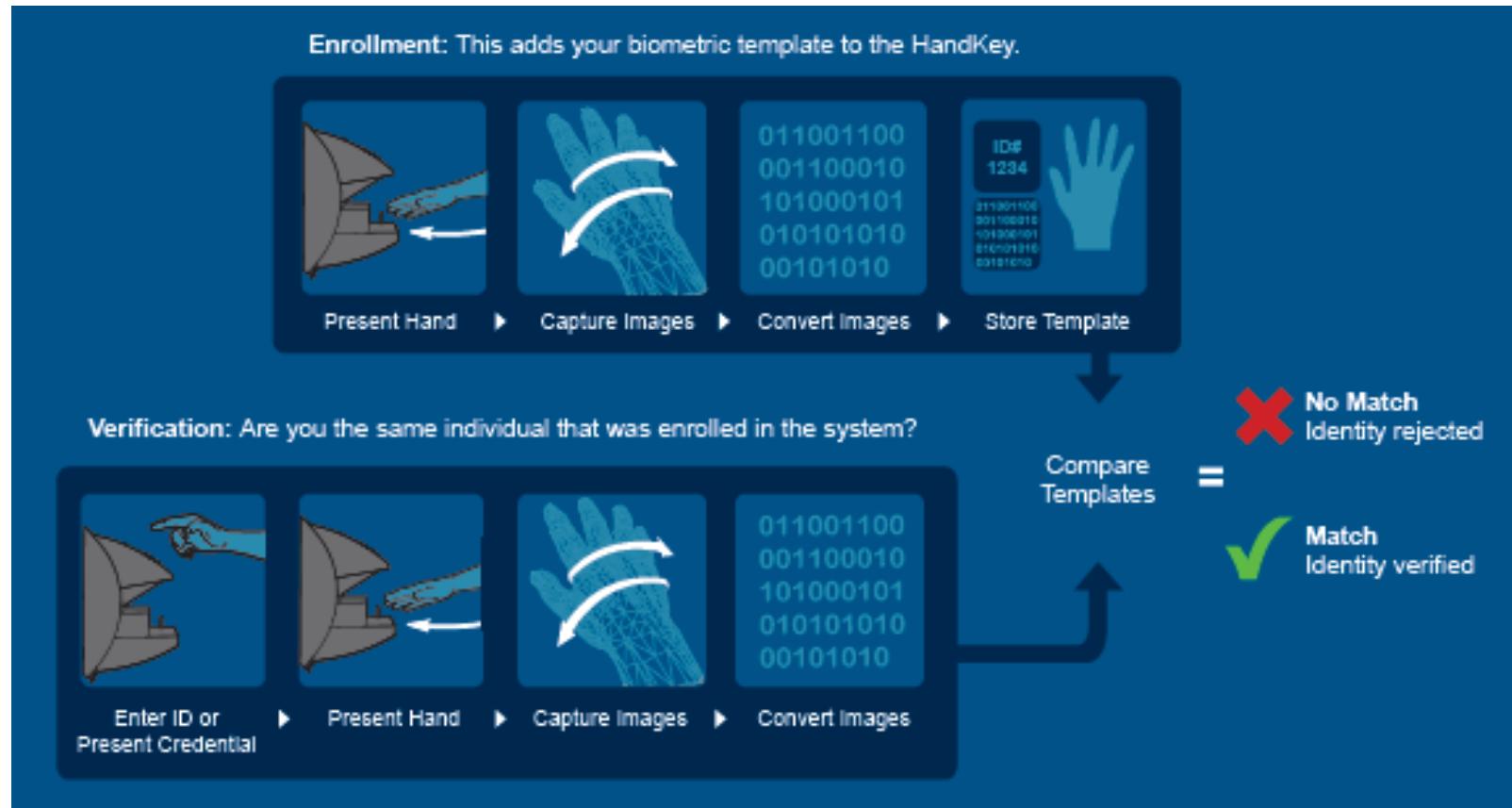
Geometría de la mano: combina una base de datos local (en el lector) de código de tarjeta vs la geometría de la mano.

Mide el tamaño y forma de la mano.

Aplicación: laboratorios, tesorería.

COMPONENTES DEL SISTEMA

Lectores biométricos



COMPONENTES DEL SISTEMA

Lectores biométricos



Geometría de la cara: combina una base de datos local (en el lector) de código de tarjeta vs la geometría de la cara.

Luego de verificar transmite al controlador el código del usuario.

Similar al de huella digital.

Aplicación: laboratorios, tesorería.



COMPONENTES DEL SISTEMA

Lectores biométricos



Iris: combina una base de datos local (en el lector) de código de tarjeta vs el iris del ojo.

El iris es el órgano (de los usados en identificación biométrica) menos susceptible a cambio. La cara, mano o dedo pueden ser afectados por lesiones, edad, etc.

COMPONENTES DEL SISTEMA

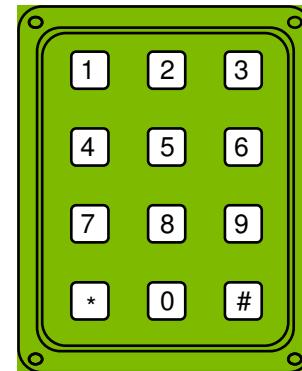
🔒 Dispositivos de Teclado

➡ Número Personal de Identificación

⌚ Único

⌚ Común

➡ Solo numérico o Integrado



Teclado

⌚ VENTAJAS

⌚ Con tarjeta, Alta seguridad

⌚ No se requiere tarjeta

DESVENTAJAS

Sin tarjeta, baja seguridad

Acceso muy lento

COMPONENTES DEL SISTEMA

🔒 Panel Inteligente

↳ Es una computadora

- ↳ Contiene un microprocesador

↳ No tiene disco duro

- ↳ Su almacén de información es su memoria

- ↳ Para almacenamiento permanente cuenta con una computadora externa.

↳ Configuración del Panel

- ↳ Permite la conexión de hasta 16 lectoras

- ↳ Puede recibir Entradas y Salidas múltiples

- ↳ Capacidad de almacenar tarjetas (2K, 10K, 100K)



COMPONENTES DEL SISTEMA

🔒 Panel Inteligente

→ Características físicas:

- Con llavín.
- Tamper switch.
- Con baterías y cargador.
- Recibe y almacena datos desde el host
- Comunicación con el host vía LAN
- Se comunica con las tarjetas de interfase de puertas (donde se conectan los dispositivos de la puerta) por red RS-485 (3 hilos + pantalla).



COMPONENTES DEL SISTEMA

- Toma decisiones de permitir ó negar accesos
 - ☞ Recibe la identificación de la tarjeta desde el lector (un número).
 - ☞ Si permite el acceso, libera la retención.
- Toma decisiones de asociar entradas con salidas
 - ☞ Ejemplo: Negar un acceso puede activar una cámara.
- Transfiere los eventos de lectura y entradas al host



COMPONENTES DEL SISTEMA

🔒 Host o Server del Sistema

➡ Computadora

- ⌚ Disco duro, terminal, teclado, impresora

➡ Software

- ⌚ Sistema Operativo (OS)

- ⌚ Administrador de base de datos

- ⌚ Software de Aplicación (de cada fabricante)



COMPONENTES DEL SISTEMA

↳ Software de Aplicaciones

- ☞ Administra el sistema - perfiles de empleados, actualizaciones, etc.
- ☞ Configuración de Hardware - paneles, lectoras, entradas, etc.
- ☞ Archivos históricos - actividades, reportes, etc.
- ☞ Capacidad de respaldo



Características deseables en el software de control de acceso Sistemas medianos o grandes



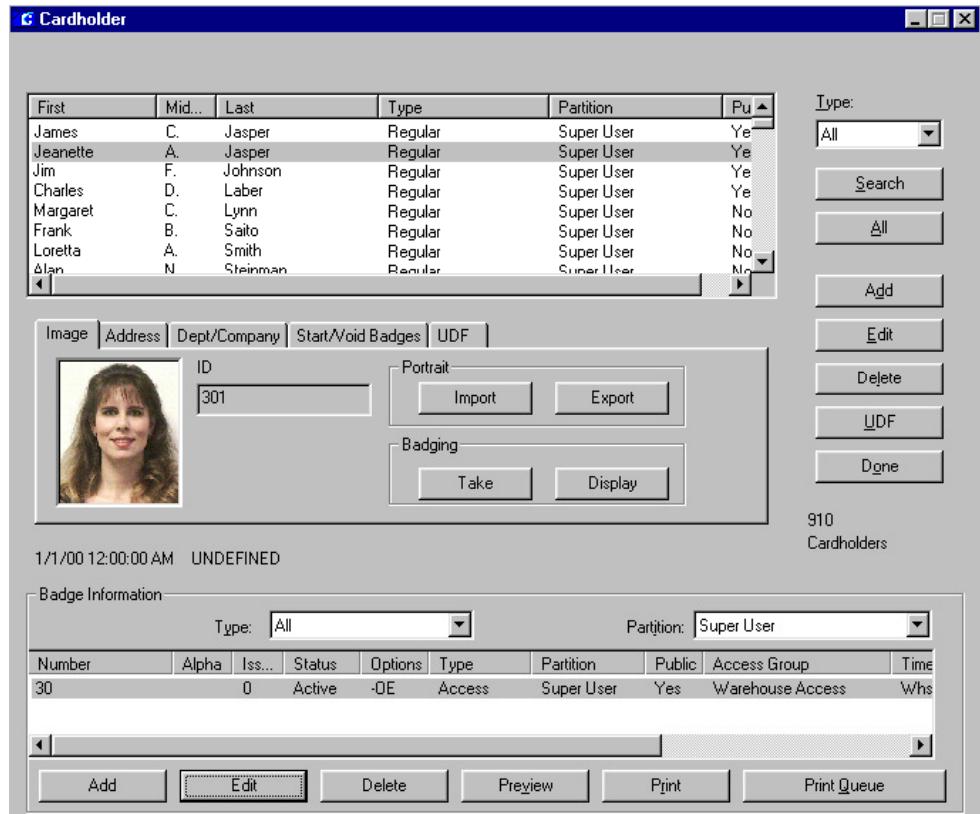
Registro de Tarjetahabientes

Mínimo 5000 tarjetas

128 campos definidos por usuario

Accesos temporales

Machotes de acceso



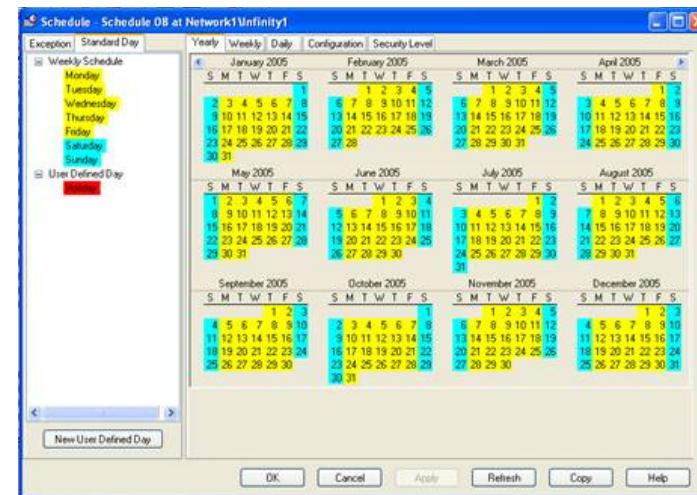
Tarjetahabientes

Zonas de tiempo (horarios) y grupos ilimitados.

Hasta 8 grupos por tarjeta

Soporte de nivel de amenazas
(Threat level support) si se trata de una compañía de USA por ejemplo.

Cumplimiento de ADA

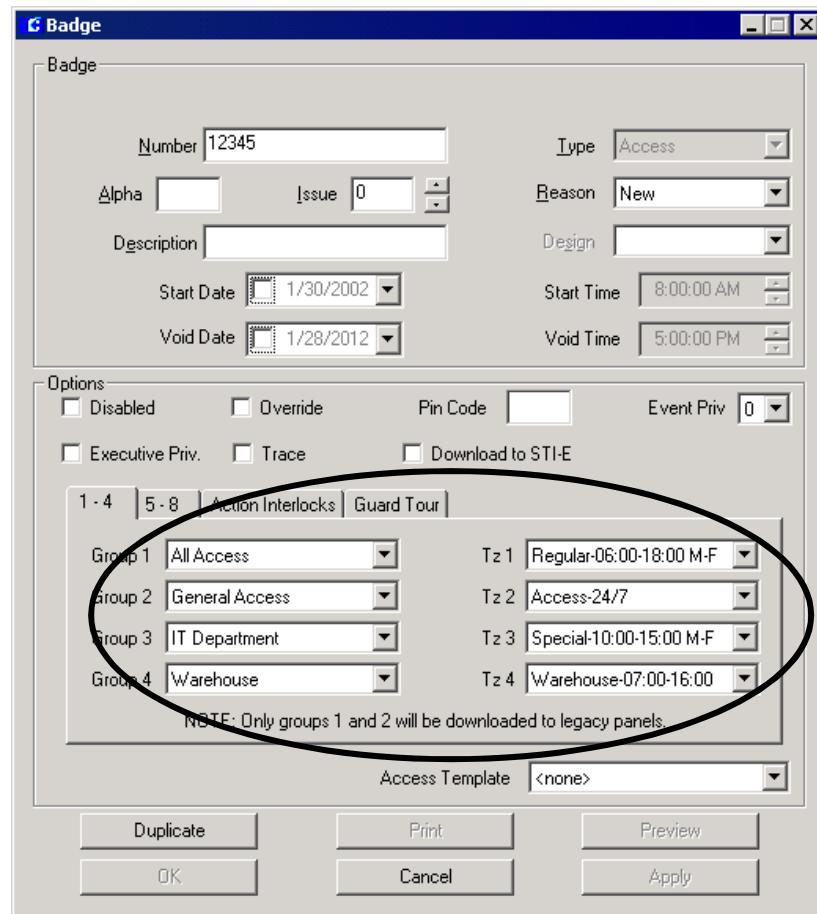


Grupos y horarios

Las zonas de tiempo u horarios se definen previo a la asignación de grupos.

Zonas típicas:

- 24/7 (dueño, Gerentes).
- Oficina: 7 am a 6 pm.
- Turnos (manufactura, call centers).



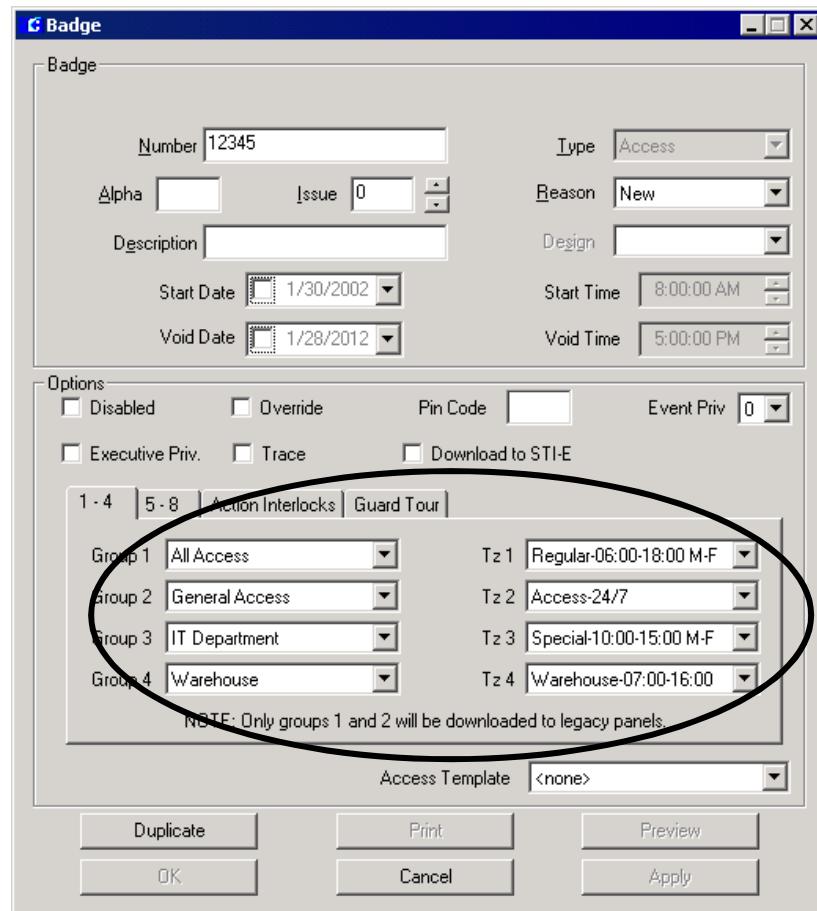
Grupos y horarios

Luego se juntan las puertas en grupos de acceso.

Se da acceso a la puerta principal, así como a las que lleven a su departamento y otras comunes (por ejemplo comedor, sala de capacitación).

Generalmente por departamento:

- Puertas-Financiero.
- Puertas-Ventas.
- Puertas-Servicio.
- Puertas-Todo: para Gerentes por ejemplo

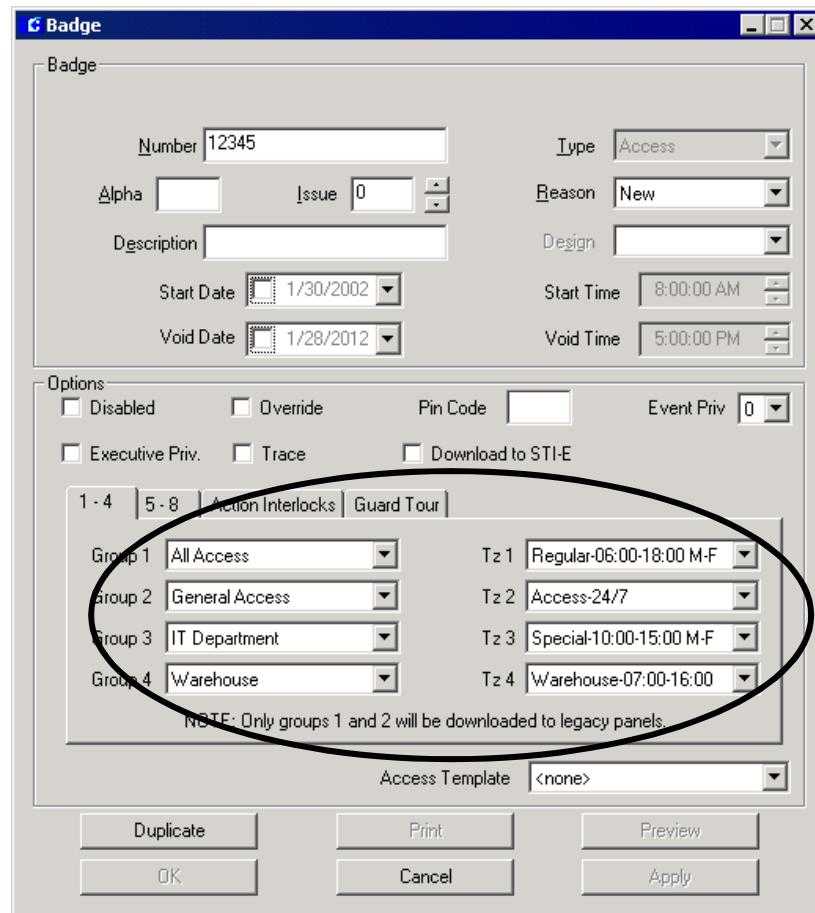


Grupos y horarios

Finalmente se crean los grupos de usuarios.

Por lo general por departamento:

- Financiero: se le asignan Puertas-Financiero y Oficina (horario).
- Gerentes: se le asignan Puertas-todas y 24/7 (horario).
- Mantenimiento: se le asignan Puertas-todas y Oficina (horario).
- Las combinaciones son infinitas.



Perfiles

- 🔒 Tarjetas/Credenciales de Acceso

➡ Tipos y Estados

- 👤 Personal Permanente
- 👤 Proveedor
- 👤 Visitantes/Invitados

- 🔒 Fechas de Expiración
- 🔒 Datos del Ultimo Acceso
- 🔒 Asignación de Accesos
- 🔒 Campos definidos para el Usuario

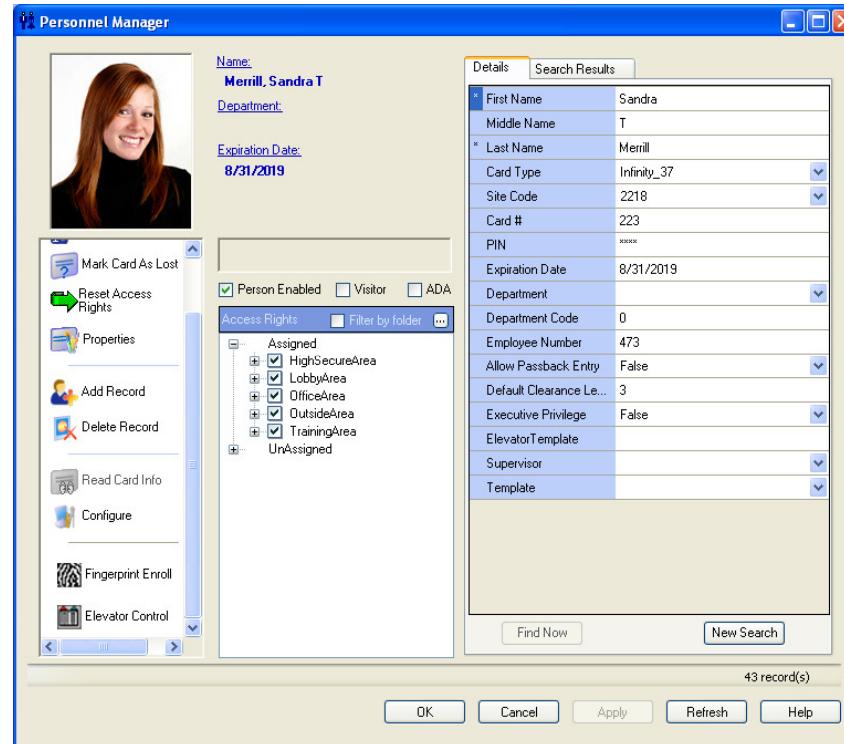


Video Imaging

Generalmente un módulo adicional (opcional) al software de control de acceso.

Al crear un tarjetahabiente y su gafete se le asigna un grupo de usuarios.

Diseños ilimitados.



Video Imaging



🔒 Imagen del Usuario

➡ Captura, Almacenamiento, y visualización

🔒 Diseños de identificaciones

🔒 Impresión de gafetes y codificación (Opcional)



Manejo de Alarmas



- Monitoreo en tiempo real
- Gráficos dinámicos.
- Módulos de integración a CCTV y BMS
opcionales.

Manejo de Alarmas

- ⌚ Sistema de Monitoreo de Eventos
- ⌚ Visualización / Anuncio
- ⌚ Rutina de Alarmas
 - ⌚ A cierta hora del Día
- ⌚ Asignación de Prioridades
- ⌚ Reconocimiento
 - ⌚ Respuesta del Operador
- ⌚ Alarmas Gráficas



Reporte de alarmas e incidentes

Texto de instrucciones

Histórico

Códigos de respuesta

Alarm Response

Description:	Forced Door BIOCENTRICS_READER	Condition:	Alarm	
Instruction				
DISPATCH SECURITY PERSONNEL TO LOCATION REQUEST REPORT LOG REPORT				
History				
Action Date/Time	Alarm Status	User Name	Alarm State	Date/Time
1/29/2002 10:33:33 AM	Responding	Cardkey	Alarm	1/29/2002 10:33:17 AM
1/29/2002 10:33:17 AM	Pending		Alarm	1/29/2002 10:33:17 AM
1/29/2002 10:23:03 AM	Responding	Cardkey	Secure	1/29/2002 10:18:00 AM
1/29/2002 10:18:21 AM	Acknowledged	Administrator	Secure	1/29/2002 10:18:00 AM

Response

Predefined Alarm Response Text:

Text:

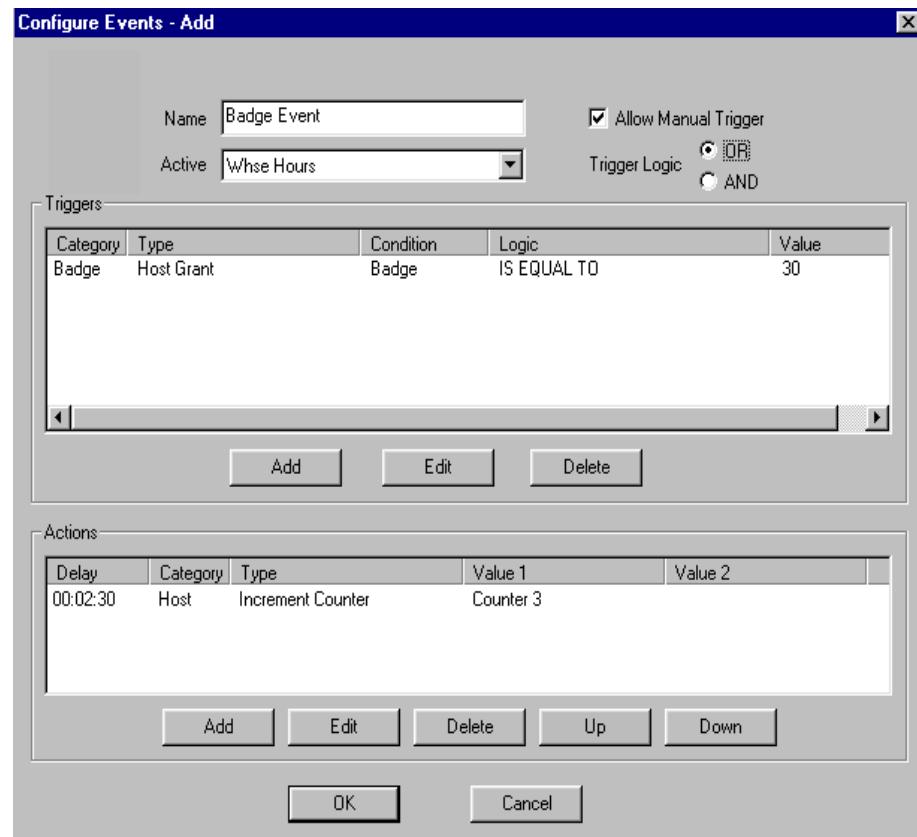
Date/Time	Response Text
1/29/2002 10:33:46 AM	DOOR PROPPED BY MAINTENANCE

Acciones y Disparadores de Eventos

Programados con lógica

Contadores hacia arriba y
abajo

Accionados automáticamente

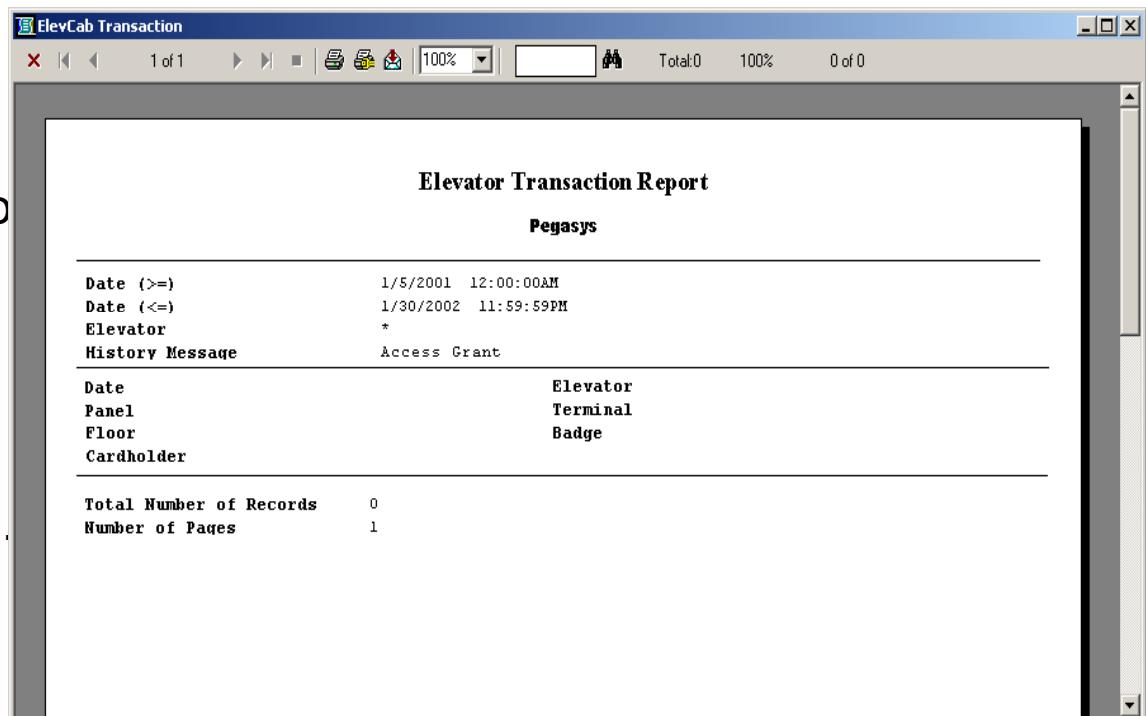


Control de elevadores

128 pisos por controlador

Rastreo de pisos

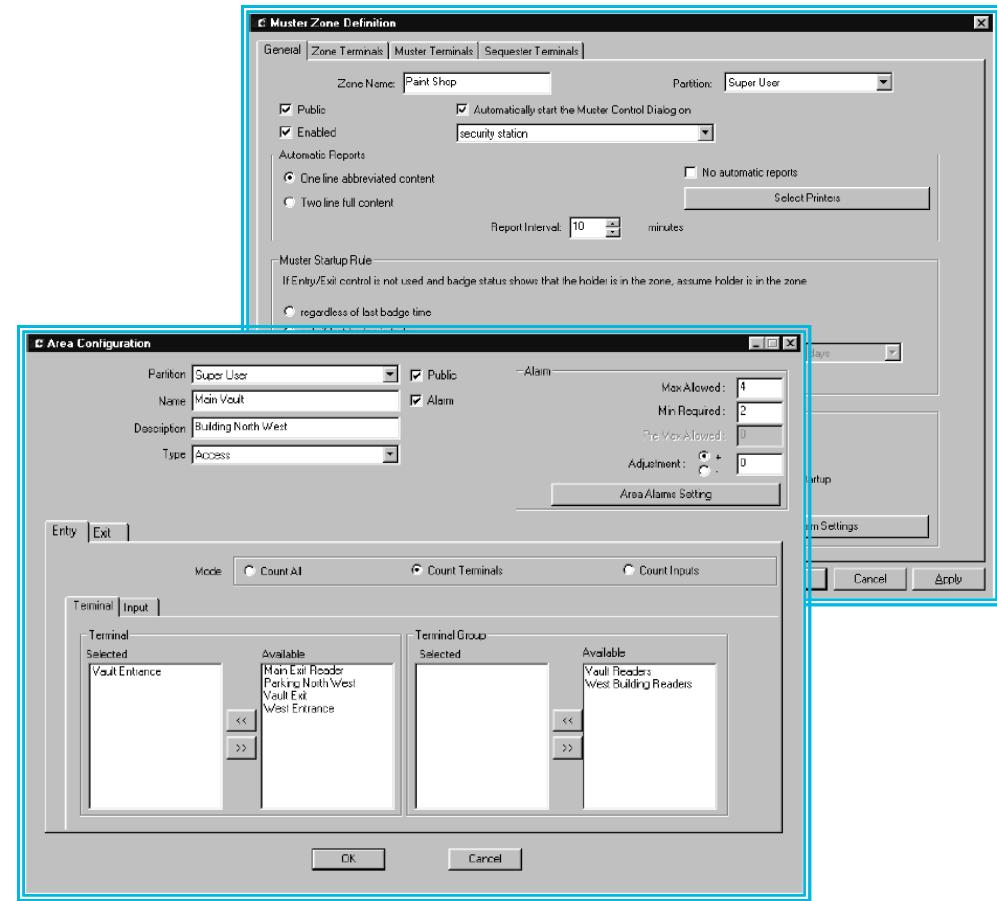
Determinar la necesidad de esa interfase y el grado de integración (los elevadores pueden pedirse de fábrica con lectoras de proximidad para integrarla al sistema).



Manejo de áreas y “Mustering”

Monitorea áreas altamente sensibles.

Mustering: rastrear el personal en emergencias. Se instala una lectora en un punto de reunión de manera que se puede saber si todos salieron.



Anti pass-back y Anti tailgate

- 🔒 Control de la Secuencia Entrada/Salida

- 🔒 Zonas Múltiples

- ↳ Local

- ↳ Global

- 🔒 Opciones de Reset

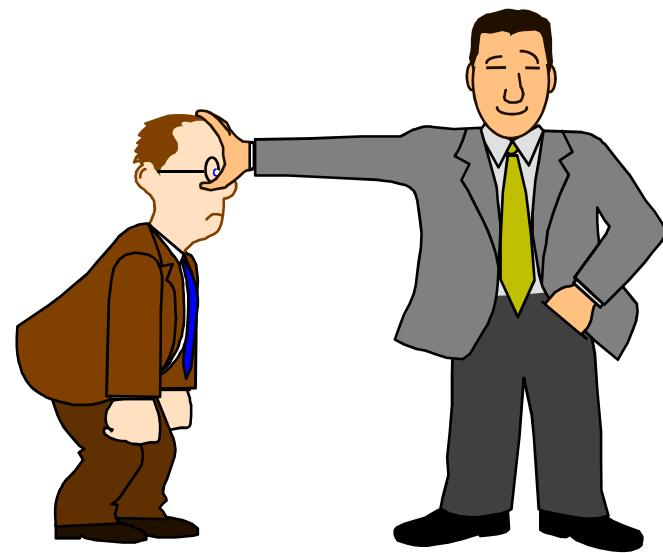
- ↳ Uno ó Todos las tarjetas

- ↳ Todas las zonas

- 🔒 Excepciones de Usuario

- 🔒 Passback: por tiempo o con doble lectora.

- 🔒 Tailgate: con doble lectora.

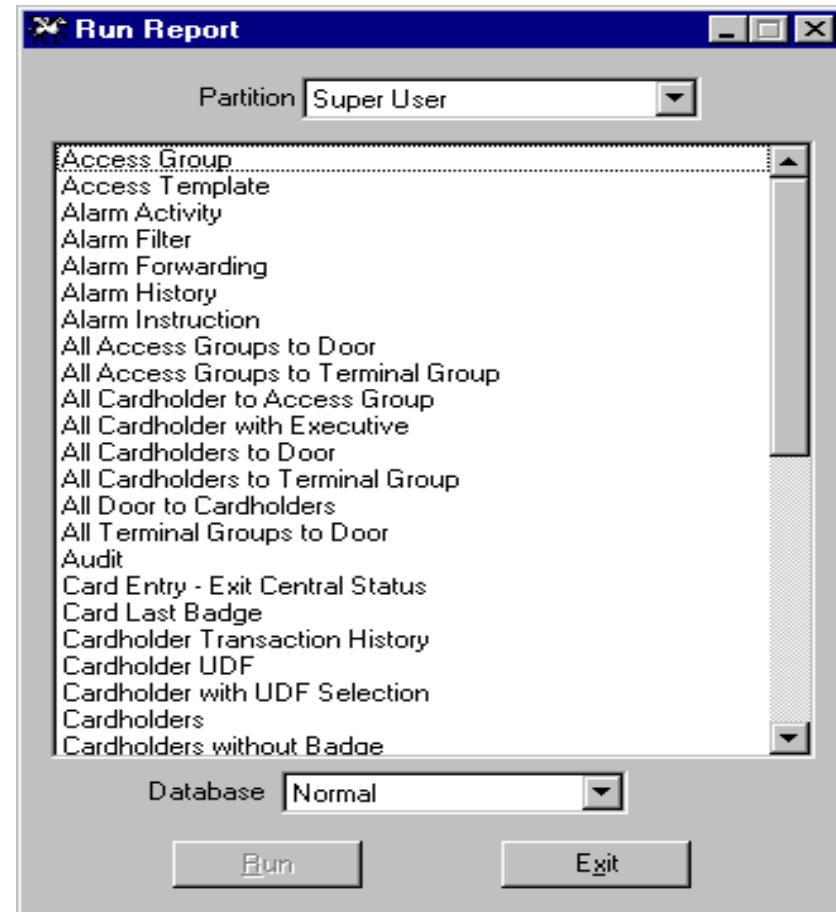


Manejo de reportes

Al menos 40 reportes predefinidos.

Opción de software para crear reportes nuevos personalizados (Crystal Reports usualmente)

- ↳ Listado de tarjetas
- ↳ Listado de Accesos
- ↳ Violaciones de Accesos
- ↳ Actividades de las Alarmas
- ↳ Actividades de los Operadores



Operadores del Sistema

- 🔒 Identificación de los Operadores

- ↳ Personal de Seguridad

- ↳ Administradores de áreas

- ↳ Recepcionistas

- ↳ Asignación de Claves

- ↳ Niveles de Privilegio

- ↳ Trabajos/Funciones

- ↳ Restricciones/Ver/Editar

- ↳ Clave del Operador y en que Fecha/hora intervino

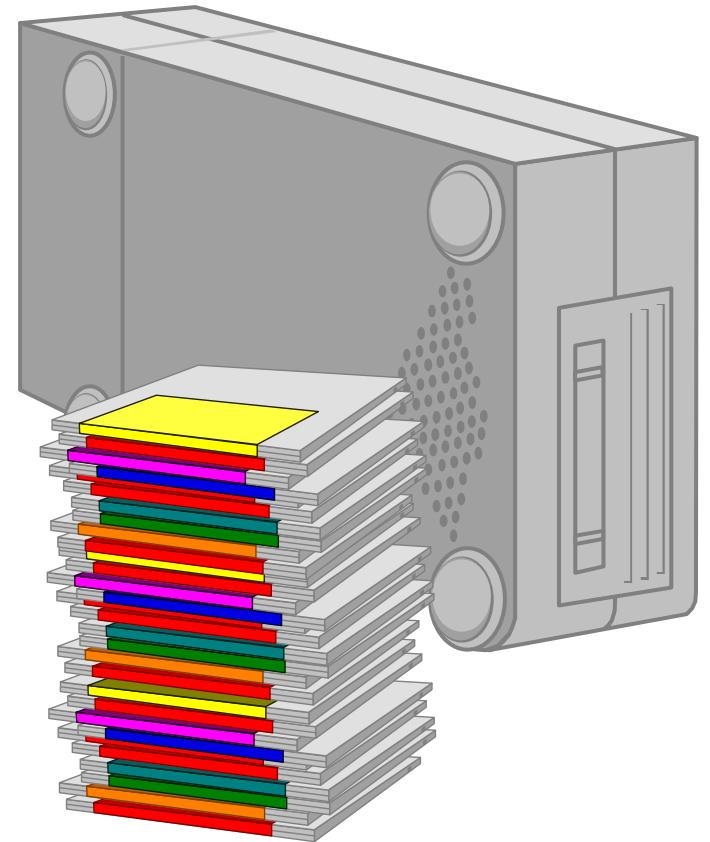


Respaldos

🔒 Software de Aplicación

↳ Archivos de Datos

↳ Almacenamiento de Archivos



FIN DE SESIÓN #6



Sistemas de Control de Acceso

Sesión #7



Cableado de los sistemas de Control de Acceso



Recordemos los principales componentes en campo

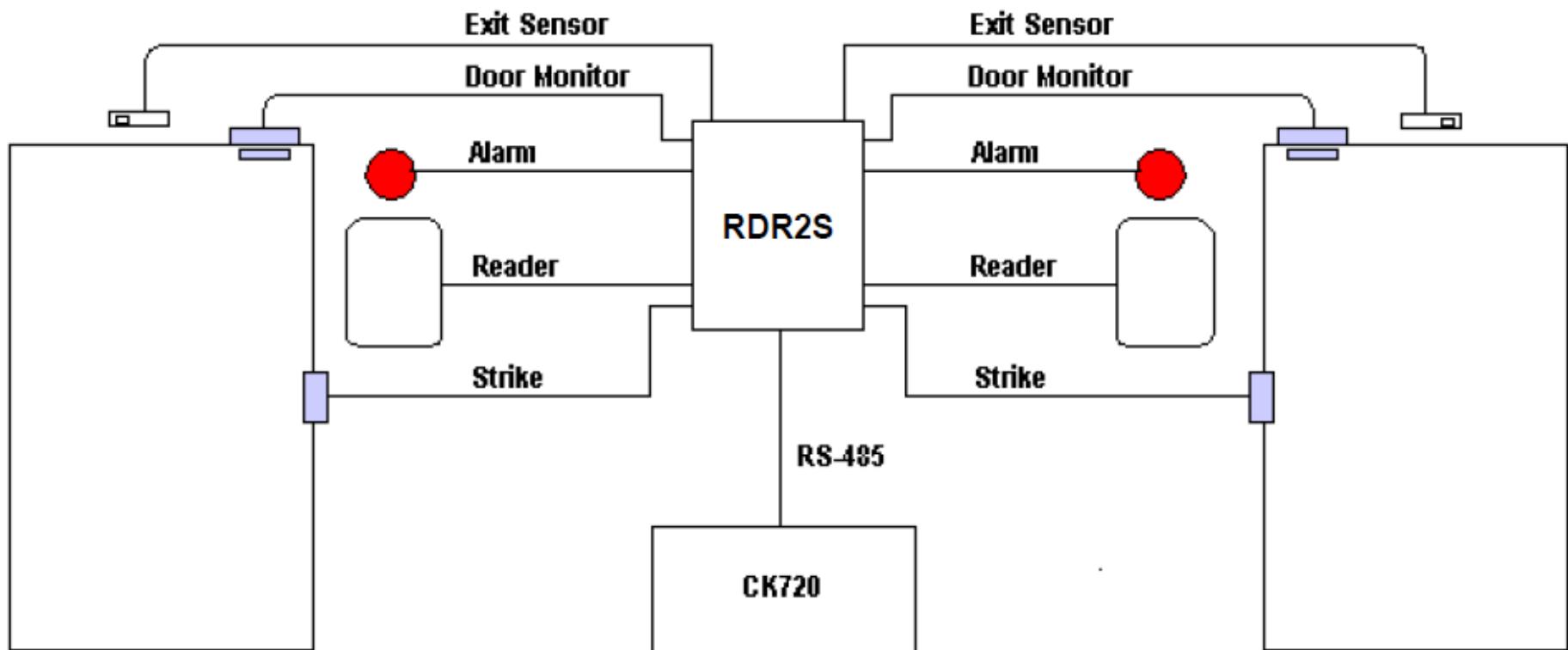
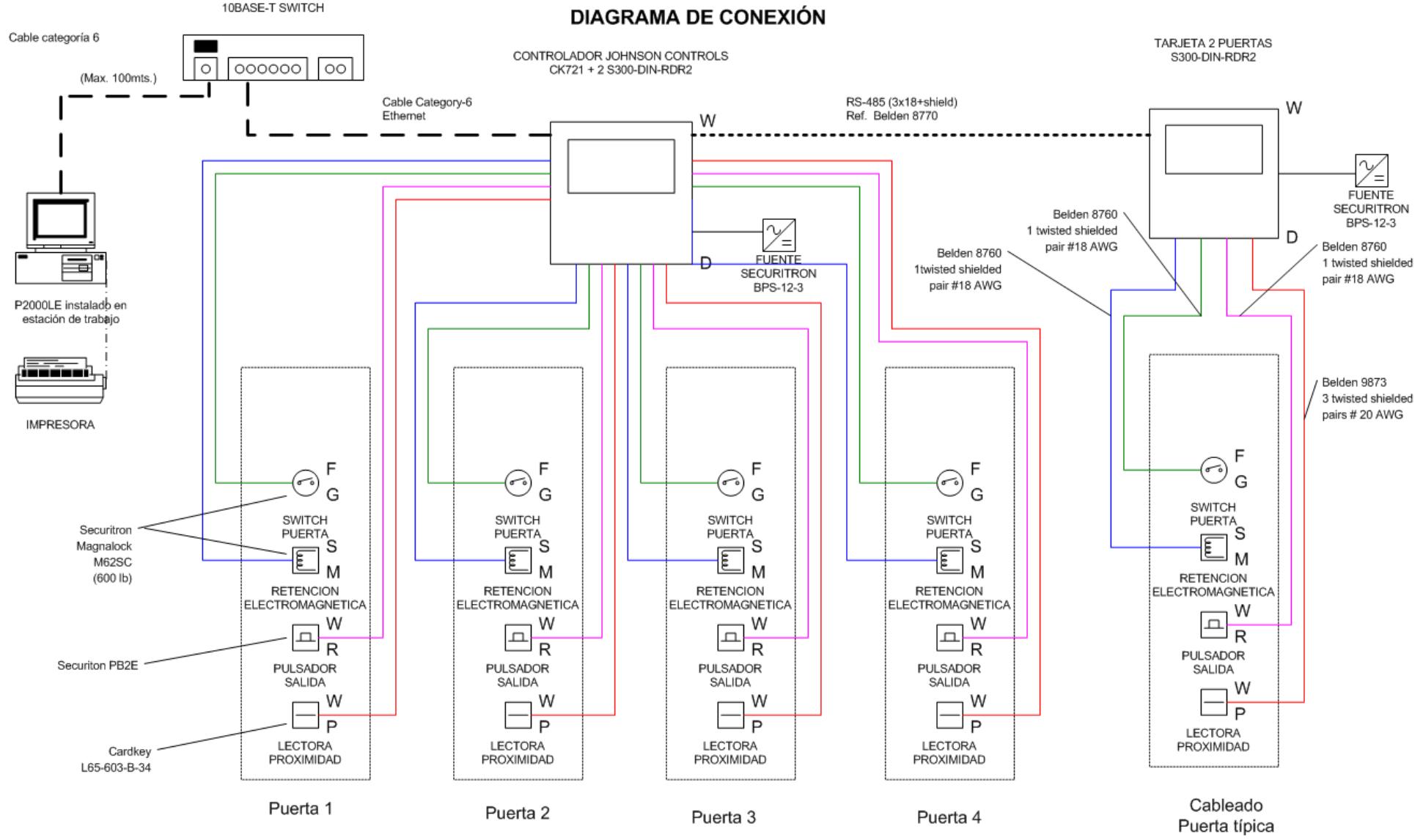
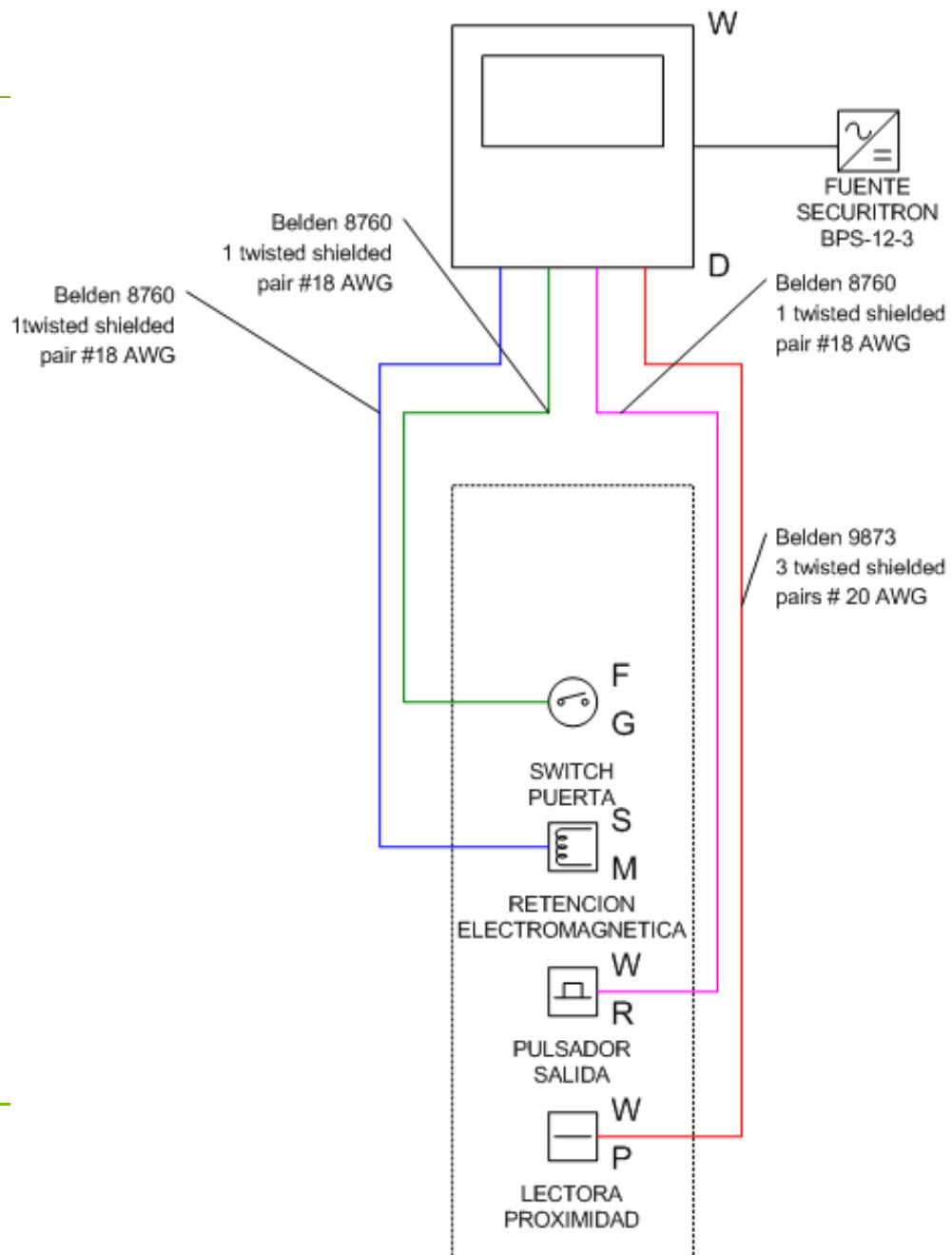


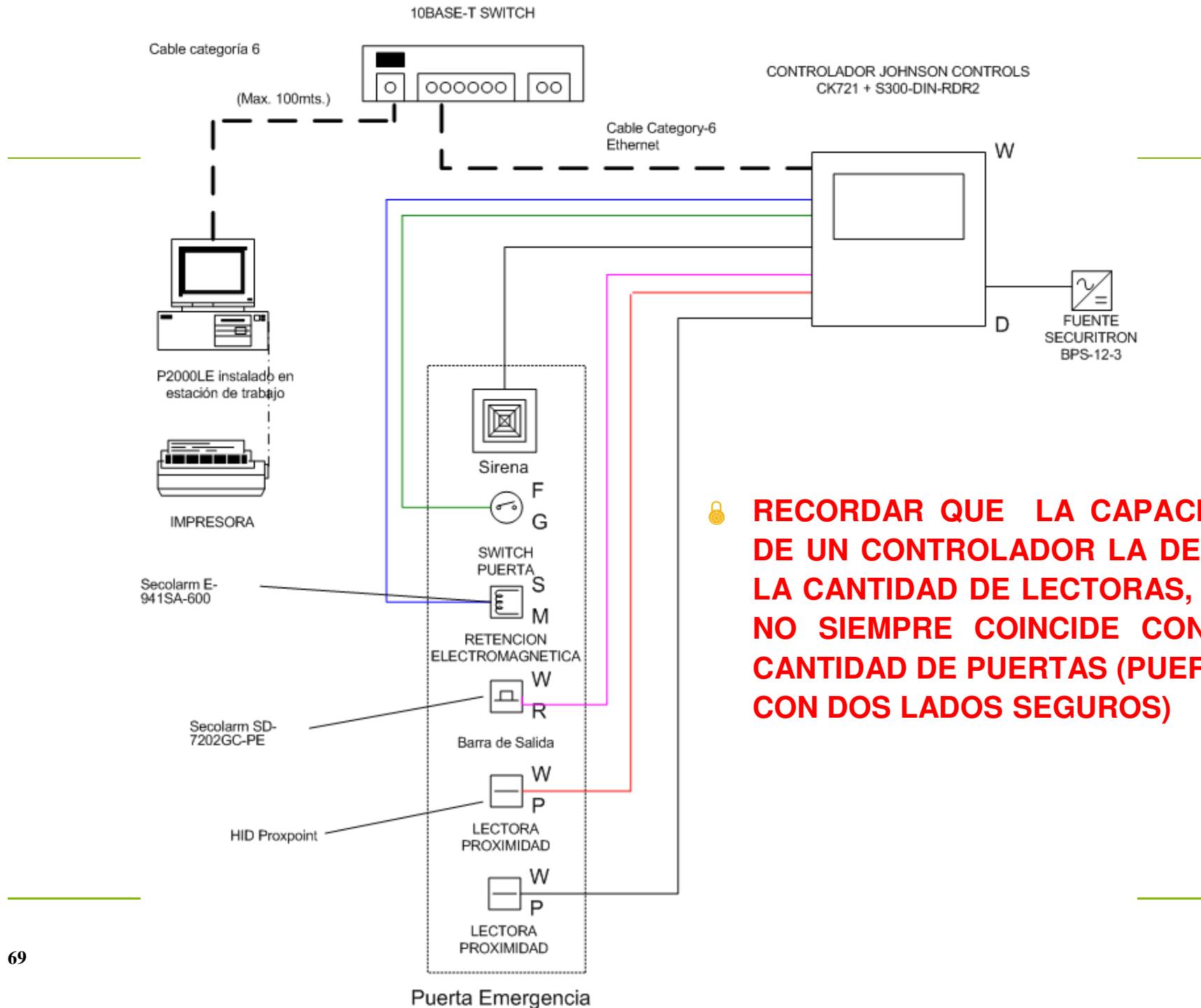
Figure 4: RDR2S Sample Configuration

DIAGRAMA DE CONEXIÓN



TARJETA 2 PUERTAS
S300-DIN-RDR2





CABLEADO EN CONTROL DE ACCESO

Connection	Description	Recommended Cable	Maximum Length
CK721 CPU Panel to Hub (internal or external)	10/100Base-T Ethernet	Listed, Category-5, unshielded, 24 AWG, solid, 2- or 4-pair type.	354 ft (100m) between segments.
Local User Interface (COM1, COM2)	RS232	Listed, Category-5, shielded, 24 AWG, solid, 4-pair type.	25 ft shield terminated at the entrance to the enclosure where termination points are provided.
CK721 Panel to Expansion Enclosure	RS-485	Listed, 18 AWG, 3-conductor, shielded.	4000 ft (1219m) max. Any expansion enclosure connected to a single CK721 CPU panel must be within 4000 ft.
Binary Output	General purpose relay	Belden 8760, 1 twisted, shielded pair, 18 AWG.	500 ft. (152m).
Binary Input (2 provided)	General purpose input	Belden 8761, 1 twisted, shielded pair, 22 AWG.	500 ft. (152m).
Note: Length depends on power requirements of the door strike. Voltage to the strike cannot be reduced more than 10% over the 18 AWG wire.			
Reader	Reader	Belden 8446, 6 conductor shielded, 22 AWG	Approx. 250 ft. (76m). Refer to individual reader specification. Approx. 500 ft. (152m). Refer to individual reader specification.

Tips de cableado y configuración al diseñar

- 🔒 El cable que debe ser obligatorio en cumplimiento siempre debe ser el de la lectora (comunicación).
- 🔒 El resto de dispositivos en la puerta pueden ser sustituidos por opciones más convencionales (TFF por ejemplo) si hay requerimientos de reducción de costos.
- 🔒 Los cables pueden viajar con cableado de comunicación o de otros sistemas de control (regido por NEC).

Tips de cableado y configuración al diseñar

- 🔒 Especificar un mínimo de grupos de puertas, zonas horarias y usuarios que el contratista debe dejar configurados (de manera que luego el usuario final se haga cargo).
- 🔒 Consultar al usuario final si desea aplicaciones especiales tales como:
 - 🔒 Interacción con otros sistemas.
 - 🔒 Aplicaciones especiales para productividad como reportes o interfase con sistema de Time & Attendance o Guardtour (por lo general son módulos adicionales).
 - 🔒 Emergencias: en un caso por ejemplo puede asignarse una tarjeta para que al pasarla por CUALQUIER lectora libere todas las puertas (un temblor por ejemplo que no puede ser fácilmente detectado por otro sistema, a diferencia de un incendio).

**PROCESO DE DISEÑO
DE SISTEMAS DE
CONTROL DE ACCESO**

Diseño de Sistemas de Control de Acceso Resumido

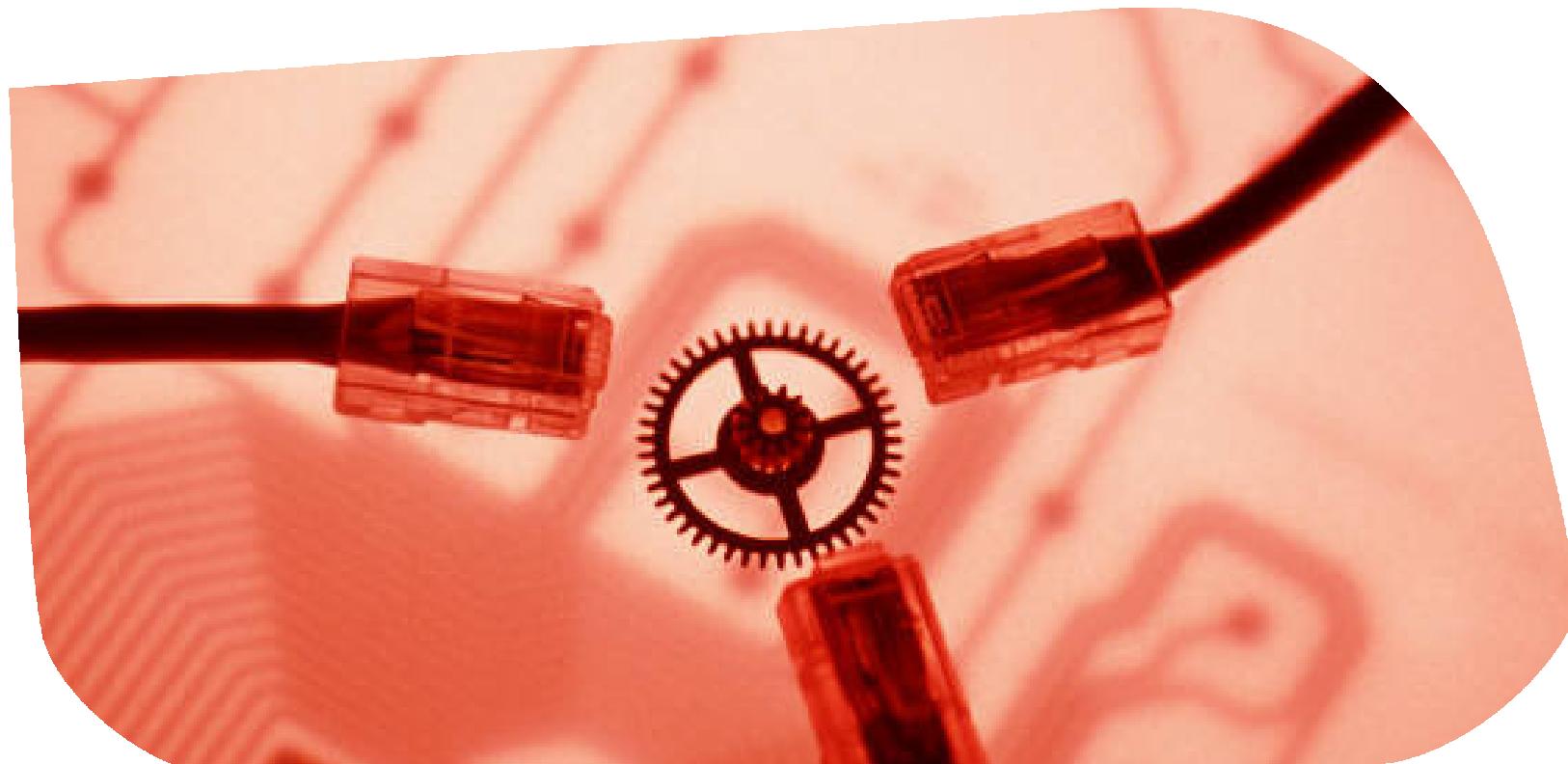
¿Dónde empiezo?

- Defina los tipos de puerta qué hay en el proyecto, lo que depende de:
 1. Cantidad de hojas (1 o 2), lo que afecta tipo de retención.
 2. Cantidad de lectoras (1 o 2).
 3. Tipo de lectora (proximidad medio o largo alcance, biométrica y tipo).
 4. Tipo de dispositivo de salida (botón REX, PIR).
 5. Si tiene o no salida de aviso local y tipo (sonoro o visual).
 - Dibuje el diagrama típico de cada puerta incluyendo tipos de cable.
-

Diseño de Sistemas de Control de Acceso Resumido

- Etiquete las puertas en el plano de planta física; enumerándolas y asignando el tipo de puerta respectivo.
- Determine las zonas en que se concentran las puertas para definir la cantidad y distribución de módulos de lectoras (2 lectoras por módulo, puede haber varios módulos juntos).
- Defina la cantidad de controladores, de acuerdo con la cantidad de lectoras que soporta el modelo.
- Dibuje el unifilar considerando los tipos de cableado de comunicación: RS-485 entre controlador y módulos, y Ethernet entre controladores y estaciones de trabajo o server.
- Determine si se requieren módulos de entradas y salidas adicionales a los de lectoras (pueden ser de 8 o 16 I/Os) y su interconexión con otros sistemas (incendio, BMS, CCTV).
- *Diseñe el sistema*

INTEGRACIÓN CON OTROS SISTEMAS



La integración es el “**arte**” de reunir la suma de todas las partes en un sistema unificado.

Control de Acceso

Videovigilancia

Detección de Intrusión

Detección de Incendio

Foto Imagen



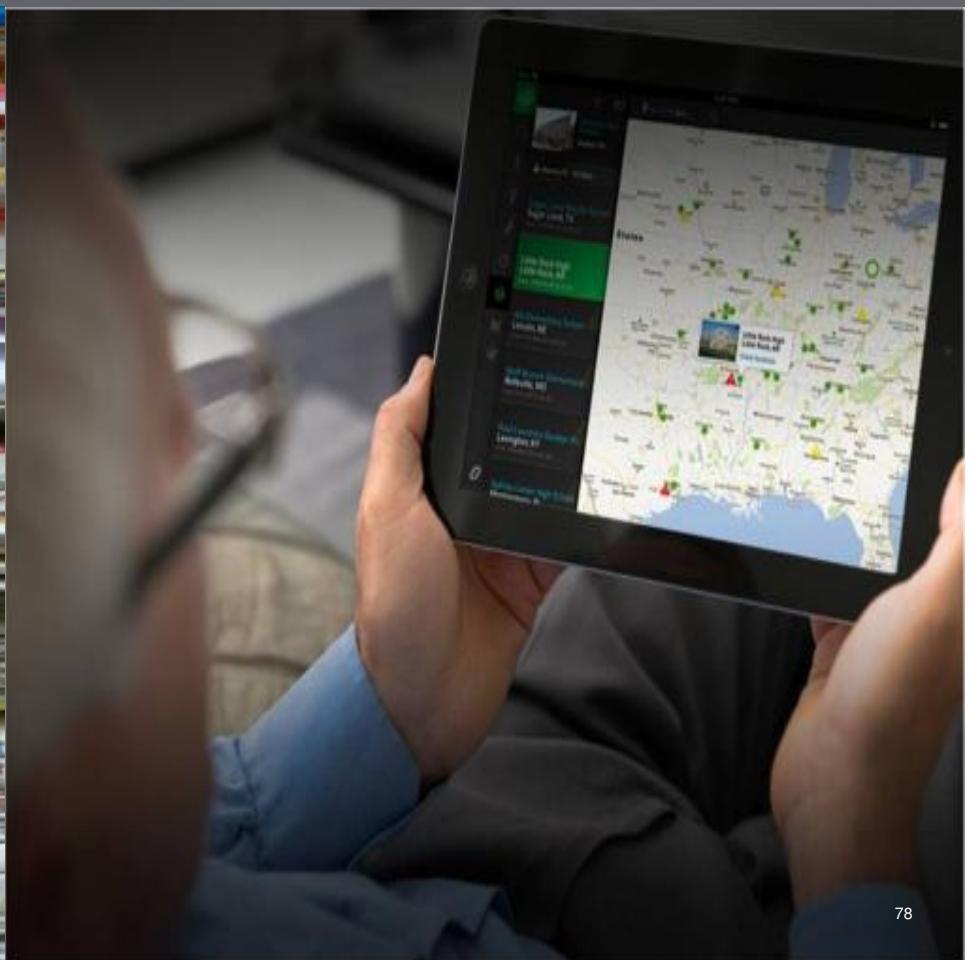
Control de aire acondicionado e iluminación

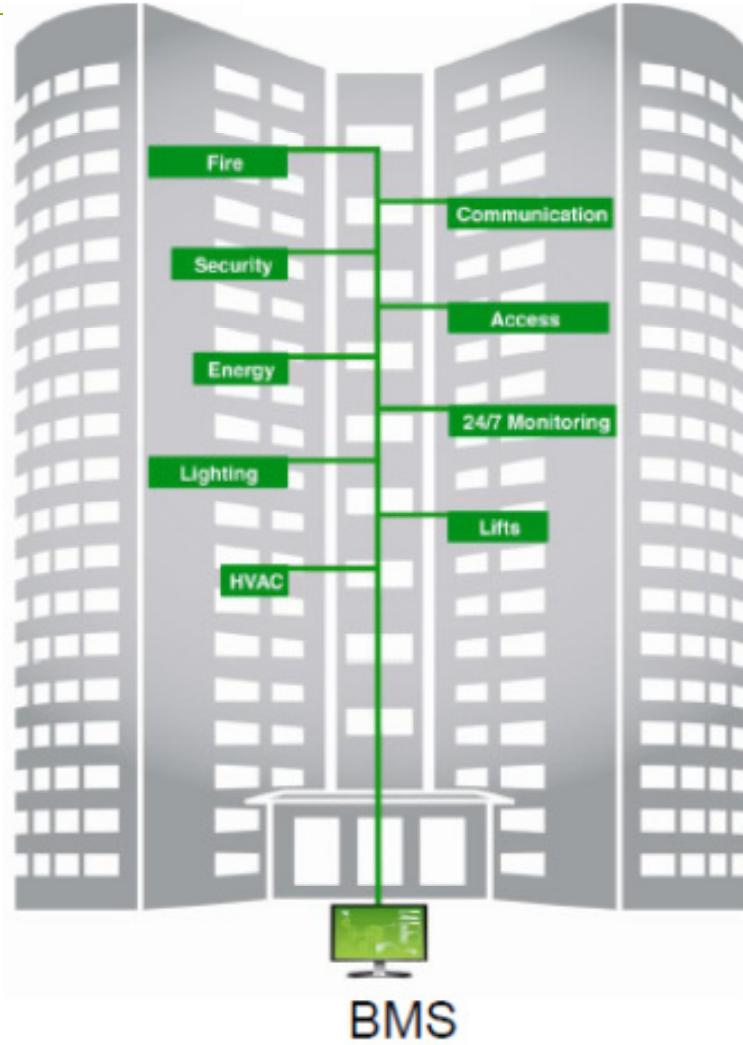
Otros

Analógico



Digital





La idea de integración – Sistema de Administración de Edificio BMS

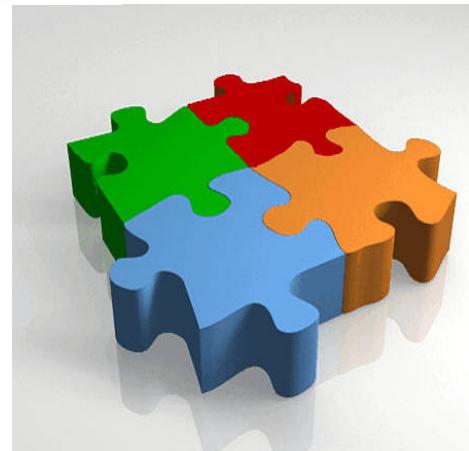
Interactúa con el usuario



Informa al Administrador

Altamente programable

```
buttonGrp -edit -en false -select 3 $radioButtons;
"onCommand" radioButtonGrp -edit -en true -select 1 $radioButtons;
"offCommand" radioButtonGrp -edit -en false $radioButtons;
"button -e -en true butASD; button -e -en false butB";
"onCommand2
"button -e -en false butASD; button -e -en true butB";
"button -e -en false butASD; button -e -en true butB";
$delme[] = 'listRelatives -p $sourceCV';
$delme[] = 'listRelatives -p $delme[0]';
$delme[] = 'listRelatives -p $delme[0]';
```

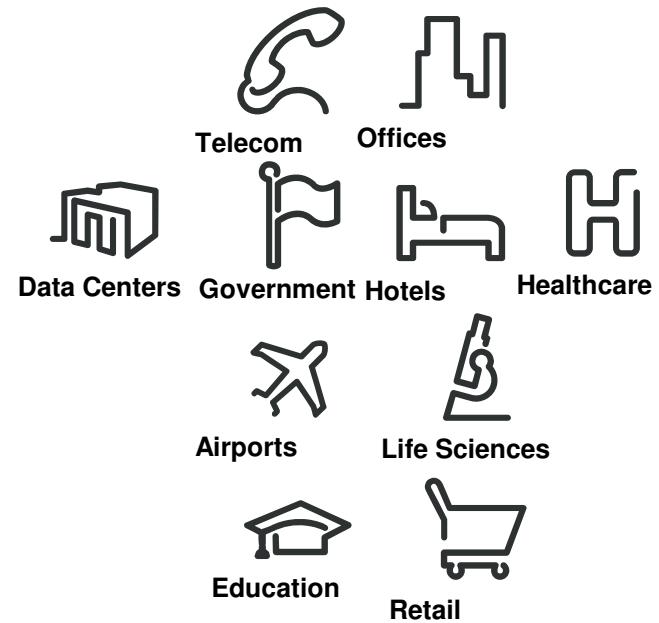


Normaliza y administra datos = INFORMACIÓN



Interactúa con distintos protocolos

Sistemas que se pueden integrar



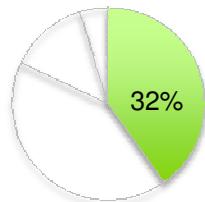
Segments

Niveles de Integración



Los procesos del usuario determinan la integración

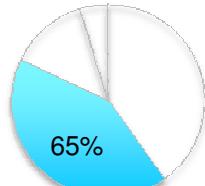
Nivel 0



Típicamente hay responsabilidad fragmentada por la seguridad en la organización. Las grandes organizaciones pueden tener varios sistemas nivel 0. Los procesos de seguridad son caóticos, ad hoc, y el éxito en la gestión depende de quién lo maneje y no del sistema en sí.

Fragmentado
-Acceso
-Video
-Incendio
-Intrusión

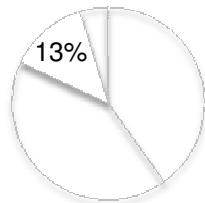
Nivel 1



Estas integraciones se dan por una obvia conclusión como verificar una condición de alarma (métricas acordadas). Muchos sistemas proveen alguna integración de este nivel, típicamente entre Intrusión o Acceso con Vídeovigilancia.

Administrado
-Mejor desempeño
-Vídeo ligado a eventos
-Reporte de incidentes

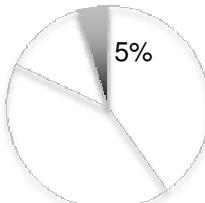
Nivel 2



Estas compañías han formalizado sus requerimientos de seguridad en el negocio. Los requerimientos indican qué sistemas se integran a la red de datos. Los procesos serán aplicados y verificados contra las acciones de operadores.

Definidos
-Reglas del negocio
-Interface de usuario consistente
-Administración según flujo de trabajo

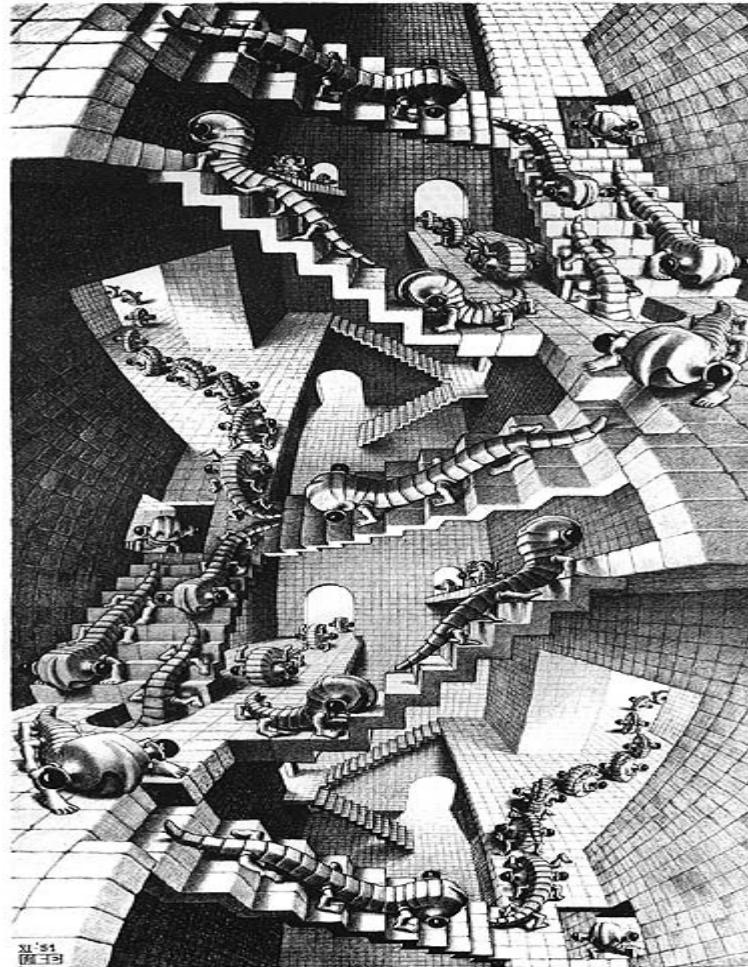
Nivel 3



Estas compañías requieren el máximo nivel posible de integración. De hecho miden el desempeño de sus sistemas de seguridad y administración continuamente para buscar mejoras en la eficiencia y ahorro en costos. Se añaden nuevos sistemas para complementar la infraestructura existente.

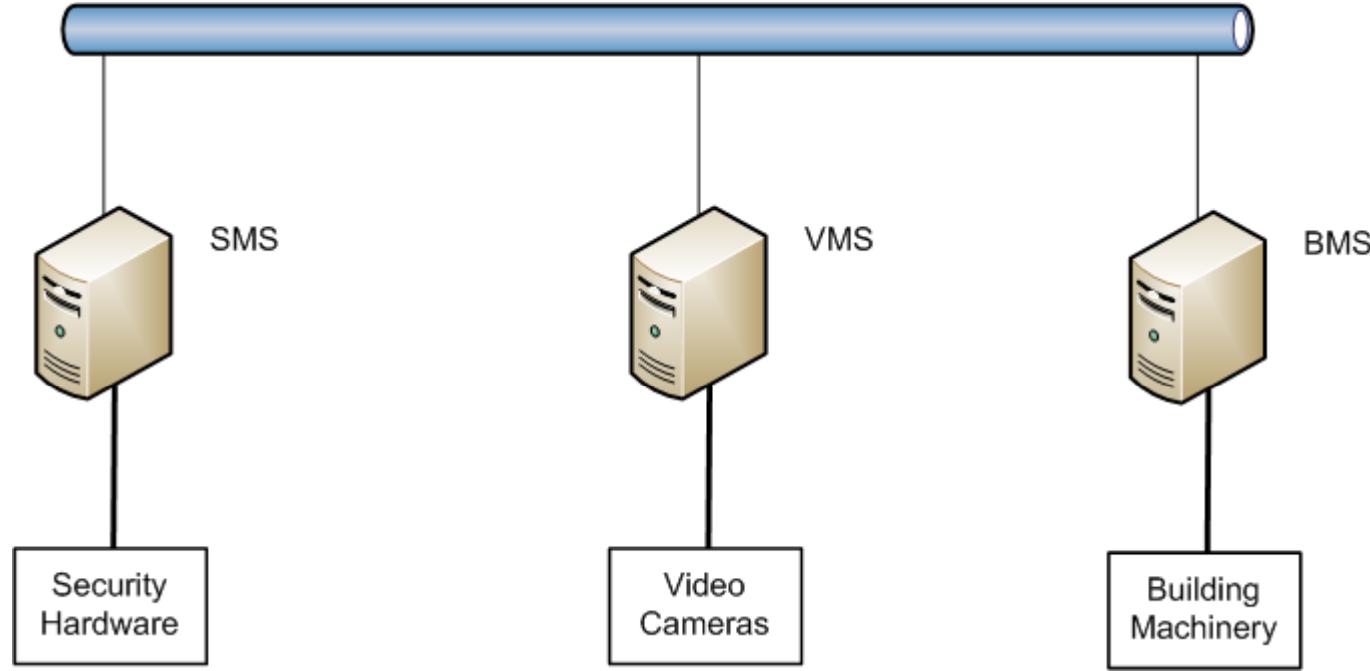
Cuantitativo
-Credenciales Globales
-Administración del Cumplimiento
-Información contra demanda

Implementación técnica



Arquitectura nivel 0

Aunque se conectan a la misma red de datos, no comparten información ni interactúan



El hardware local opera independientemente, las decisiones y el control se ejecutan en un “silo”

Niveles 0-1: Entradas y salidas (I/O) básicas

¿Qué?

- Provee una interfase básica Sí/No

¿Cómo?

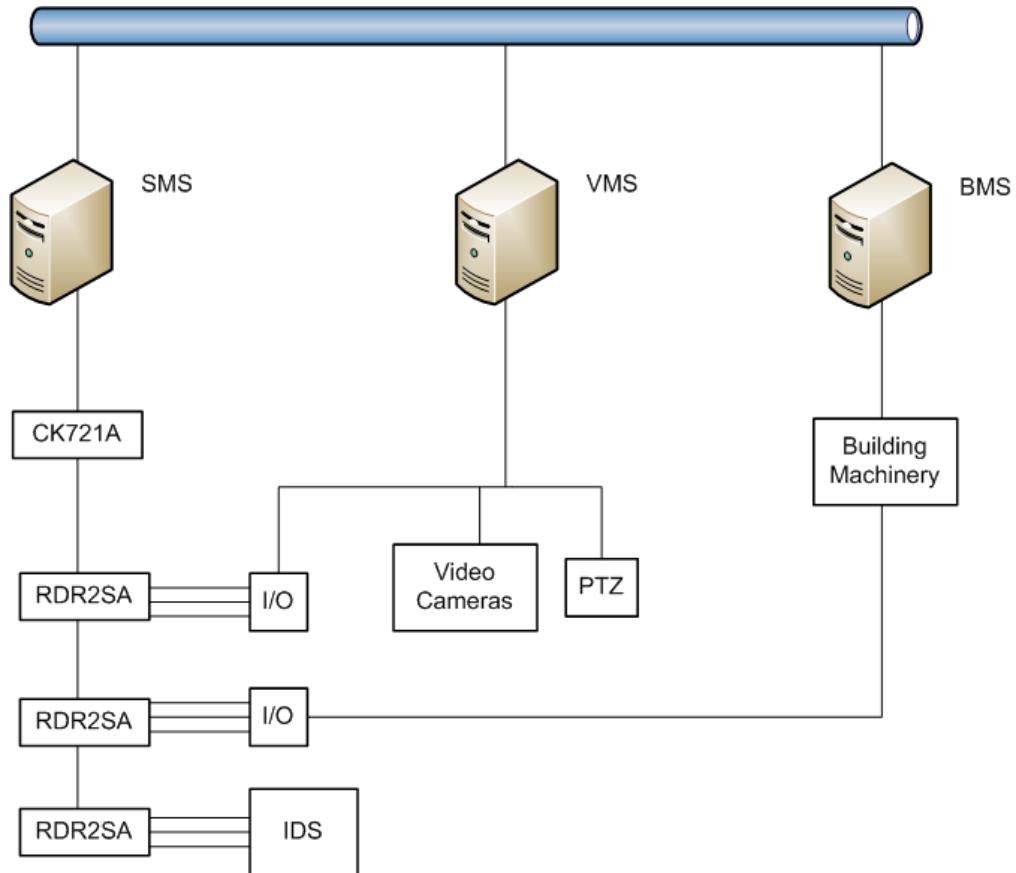
- Convierte interruptores en puntos de control
- Provee salidas binarias basado en status

¿Por qué?

- Los sistemas requieren una acción para responder
- El costo es un tema muy sensible

Arquitectura Nivel 1

Aunque están en una misma red, la comunicación es vía contactos secos (libres de potencial)

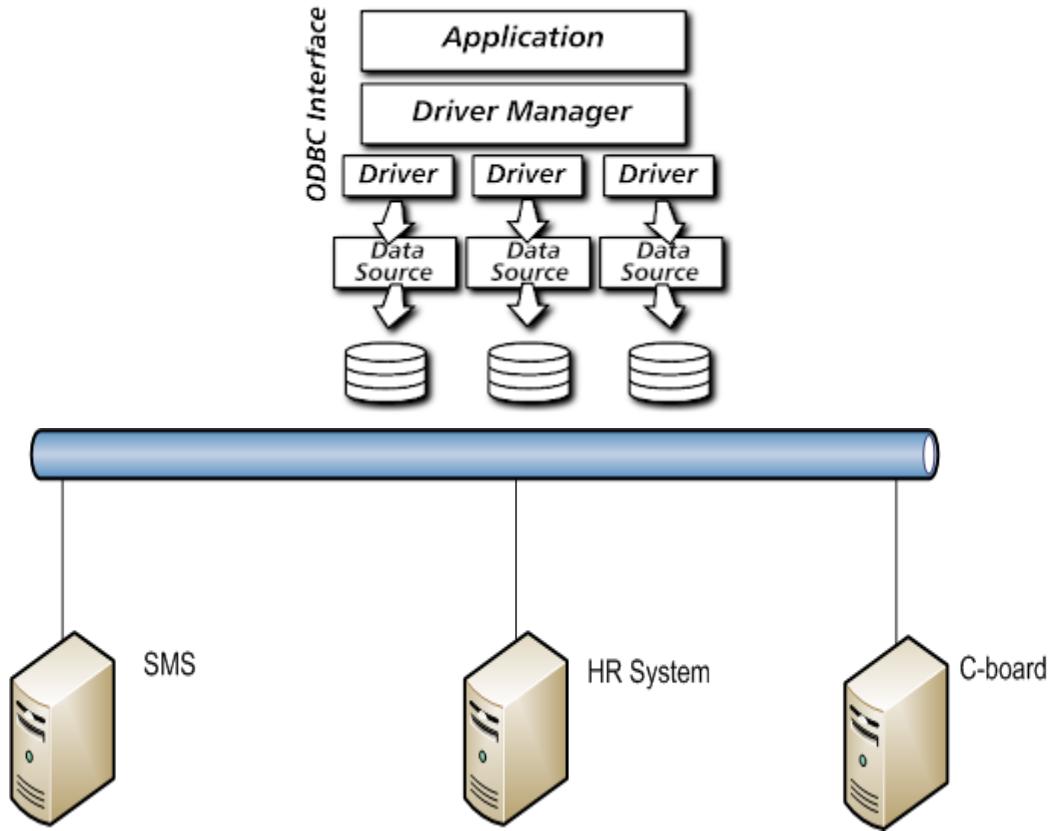


Aplicaciones típicas:

- Con un módulo de entradas y salidas en acceso se leen salidas de módulos de relé de incendio asociados a distintas zonas de incendio para liberar las puertas respectivas.
- Una salida de control de acceso se conecta a una entrada de la matriz de vídeo para generar una acción específica (macro) como mover X cámara a Y posición y grabar o desplegarla en la pantalla principal.

Arquitectura Nivel 2: Administración de identidades

Usa la red para crear conexiones ODBC



Un sistema debe ser la fuente autoritaria (casi siempre el de acceso trae módulos para interesar al resto)

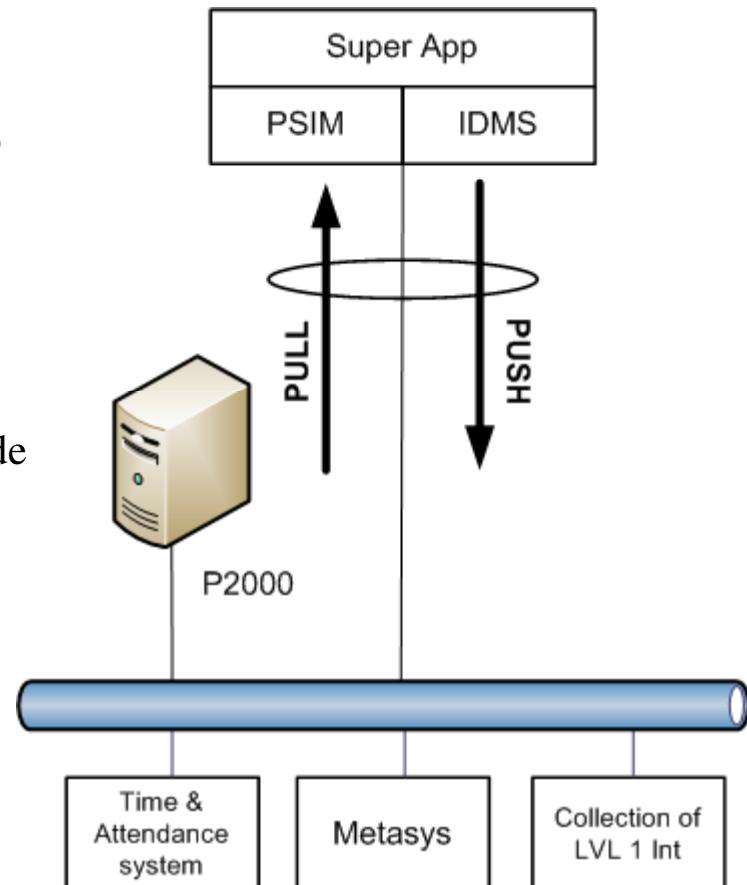
Niveles 2-3 Protocolos propietarios

Usa la red, aunque puede ser un protocolo serial

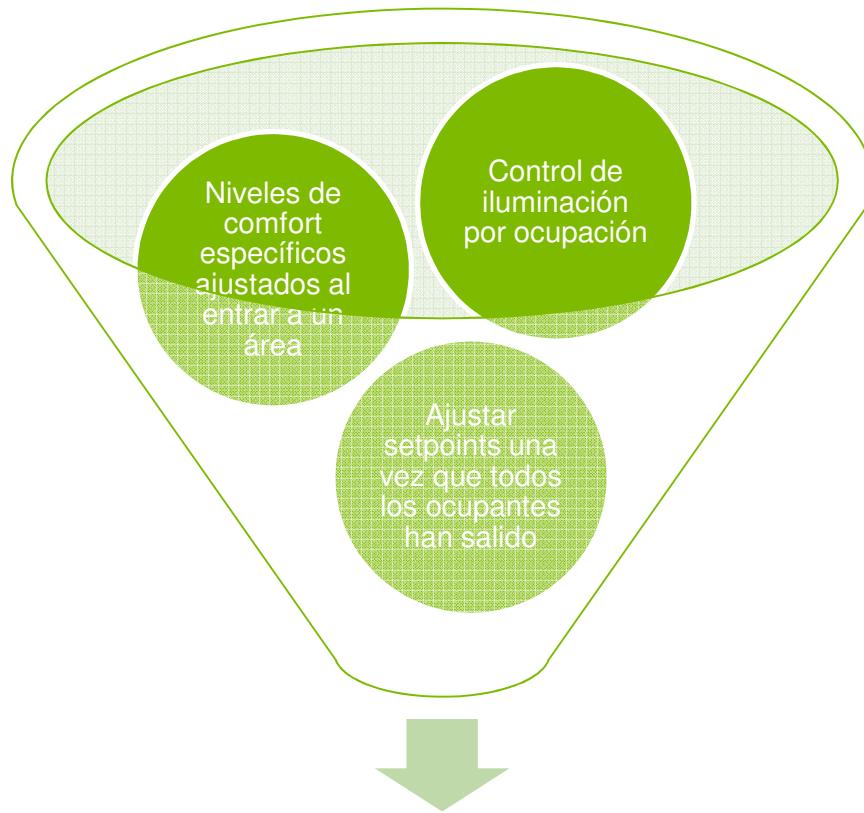
El sistema de acceso puede actuar como un hub entre sistemas aprovechando su capacidad de protocolos.

Aplicaciones típicas:

- Equipar el panel de incendio con una tarjeta de comunicación Bacnet, de manera que el sistema de automatización pueda ver todos los puntos monitoreados y tomar decisiones con base en eso (estrategias de control de humo).
- Enlazar el sistema de acceso con el de automatización de modo que cuando ingrese el gerente por la aguja de parqueo de inmediato se acondicione su oficina (luz-temperatura-música) para que al llegar esté preparada totalmente.

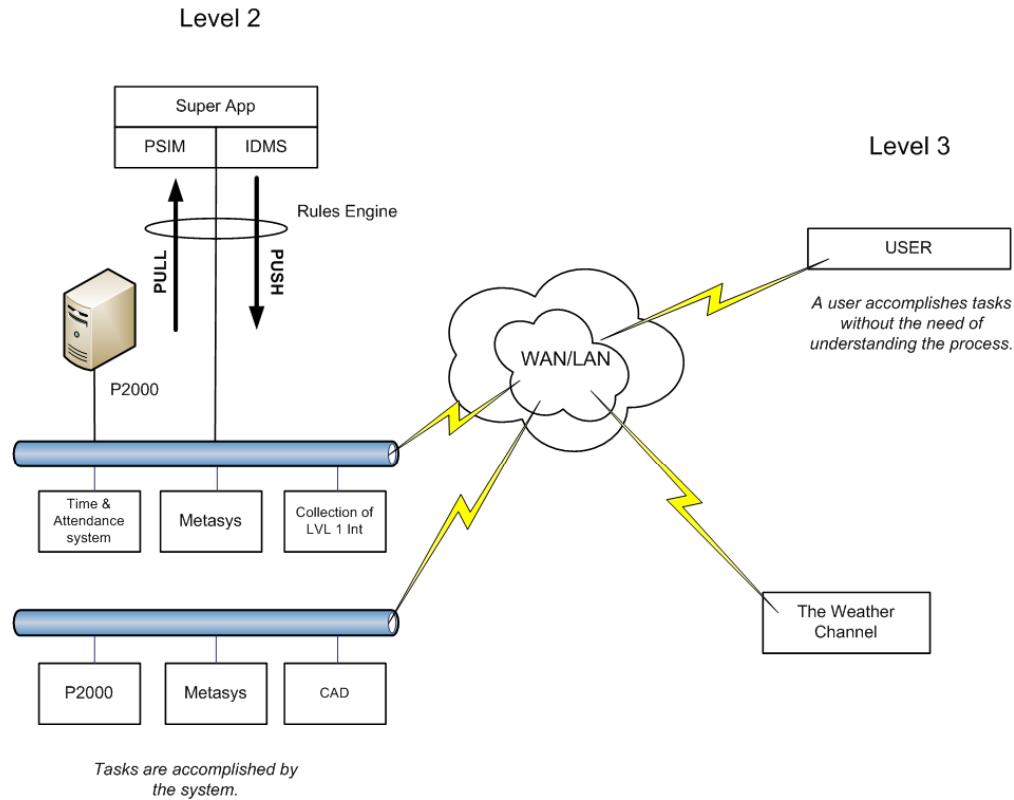


Posibilidades de Integración



Resultado: Ahorro de energía,
mayor eficiencia operativa

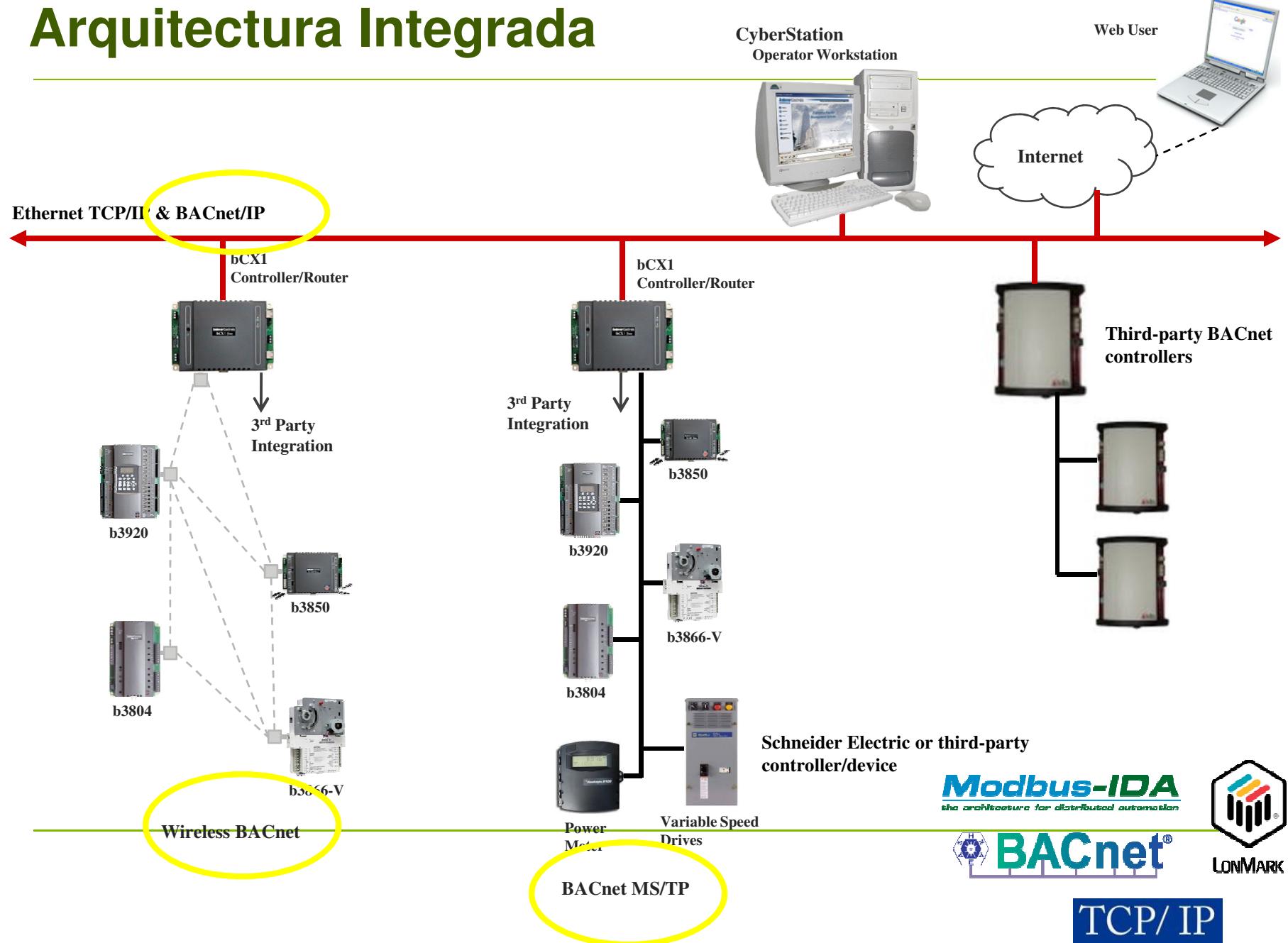
Nivel 3



- Enlazado con sistemas externos.
- El IMN indica que estará inusualmente caliente en la región donde está la empresa
- El BAS tiene apagado el aire según su horario
- El SCA sabe que debe cerrar las puertas de atrás y adelante (si están abiertas genera alarmas)
- El usuario es notificado vía mobile app, que el status en la región es anormal, pero no crítico, e incluye información de vídeo para mostrar
- El usuario hace un rápido chequeo y nota que eso ha pasado 12 veces este año.
- Modifica las reglas para identificar y prevenir problemas similares.

La información por demanda determina las decisiones a este nivel

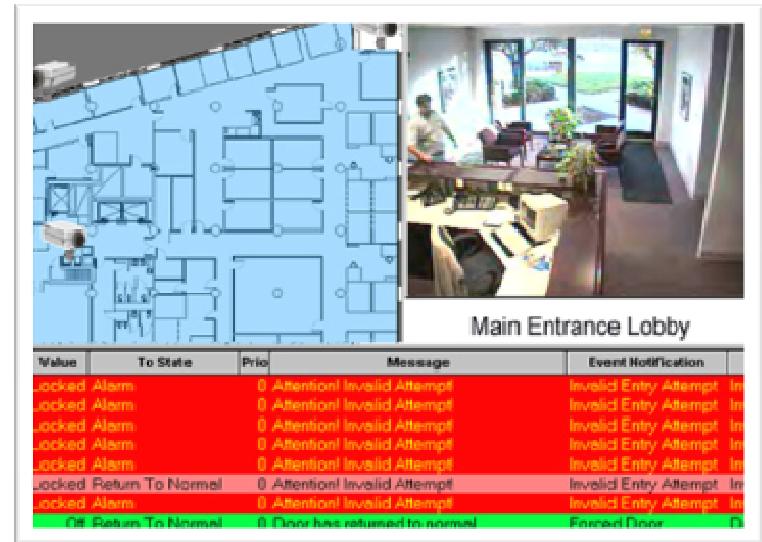
Arquitectura Integrada



EL PODER DE UNA INTEGRACIÓN REAL (nivel 2 o 3)

Con un solo click o rutina automática

- Estrategia de Alarmas coordinada.
- Despliegue de vídeo automático según alarma o evento.
- Abrir/Cerrar puertas.
- Presurización.
- Iluminación de emergencia.
- Electricidad de emergencia.
- Grabación de vídeo.
- Evacuación y manejo de humo.
- Mustering
- Encendido/Apagado de HVAC.



TENDENCIAS FUTURO INMEDIATO

- Las necesidades del negocio (ahorro operativo o regulaciones legales) moldearán la tendencia a integración y crecimiento

Tecnología

- Aplicaciones móviles e integración a la nube
- Dispositivos IP crecen enormemente
 - Inteligencia distribuida
- La analítica en vídeo ha bajado su ritmo de demanda (sigue cara) pero aún puede ser un factor importante
- Big Data.
- La Nube.

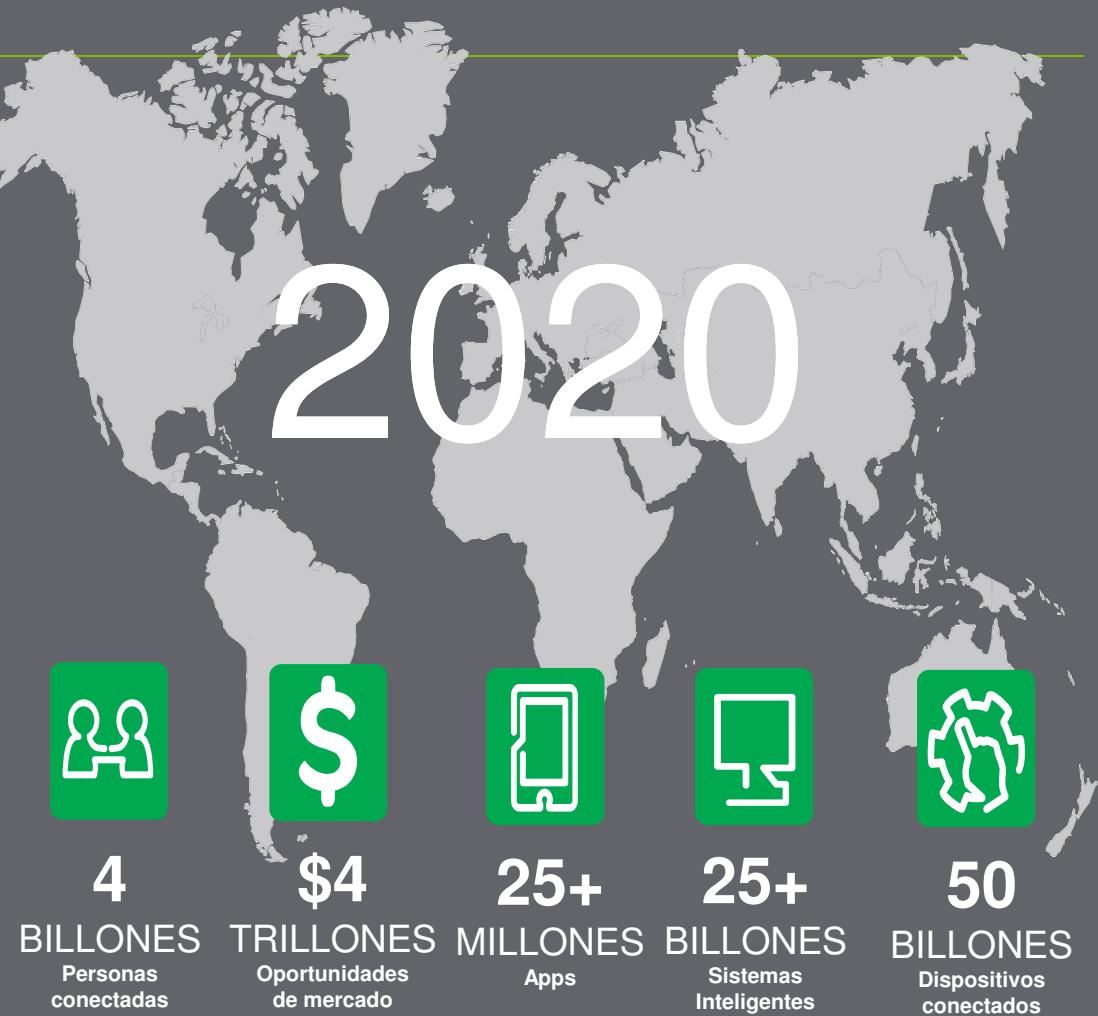


La información y los datos están creciendo exponencialmente.

“Entre los albores de la civilización y el año 2003 más de 5 exabytes de información fue creada.

Hoy en día esta misma información se crea cada 2 días”

(Eric Schmidt – former Google CEO)



Pensemos un momento

La convergencia de las tecnologías de información (IT) y las operacionales (OT) trae ventajas claras tangibles a las empresas

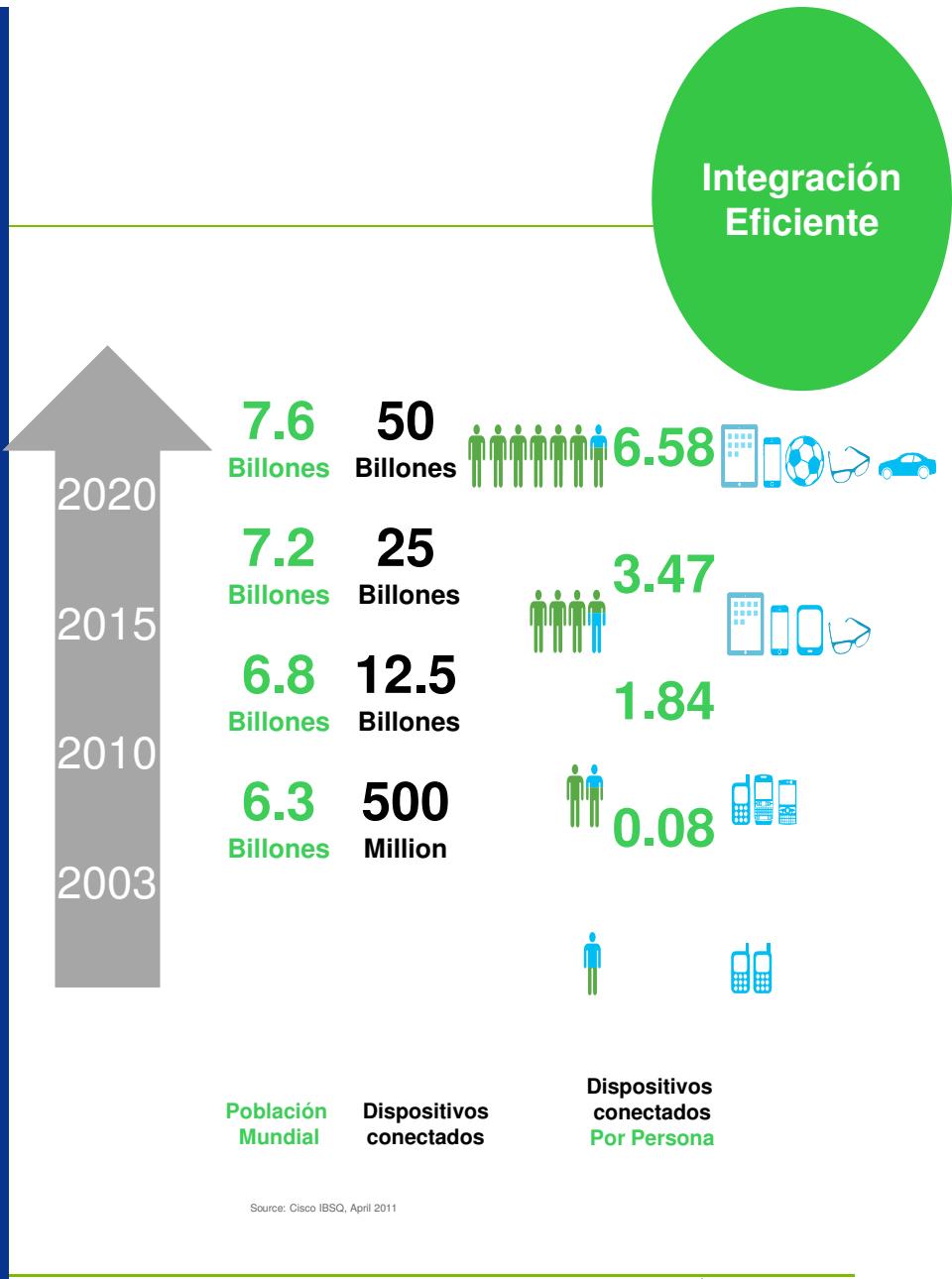
IT-OT está creando oportunidades estratégicas para nuevas eficiencias através de la empresa y nuevas metodologías de contratación.

Muchas organizaciones están equilibrando sus facilidades OT y las inversiones en IT.

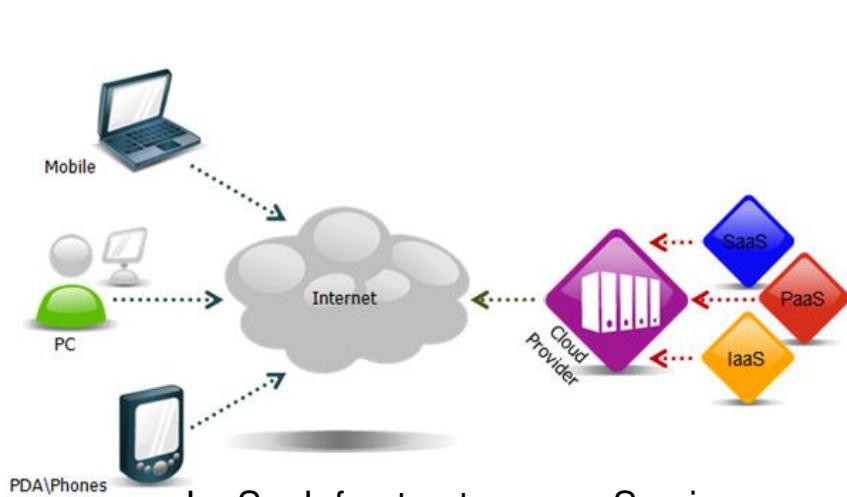
"La integración de las tecnologías de la información (IT) y las operacionales (OT) proporciona una vista única de la gestión de la información empresarial, como un elemento fundamental para construir ambientes de trabajo de alto desempeño, donde cada persona, sensor, instrumento o cualquier otro dispositivo utilizado, tiene la información requerida en el formato correcto y en el momento indicado con el propósito de tomar la mejor decisión."

Gartner (Julio 2011). IT and Operational Technology Alignment Innovation Key Initiative Overview

Integración
Eficiente



Capacidades futuras



“...El cómputo basado en internet, donde recursos compartidos, software e información se provee a las computadoras y otros dispositivos contra demanda, como la electricidad y el gas” Wikipedia

IaaS – Infrastructure as a Service

- Las compañías (IT y Operaciones) accesan la infraestructura cuando la ocupan.
- Pagan por la capacidad usada.
- Ejemplos: Amazon, IBM, Rackspace

SaaS - Software as a Service

- Se accesa el software en la web con un ID y password
- Las actualizaciones y nuevas características se dan continuamente sin interrumpir a los clientes
- Ejemplos: salesforce.com, Google Mail, OnStar

PaaS – Platform as a Service

- Los desarrolladores accesan la plataforma para desarrollar y ejecutar aplicaciones
- Usualmente se compra con un software developers kit
- Ejemplos: Microsoft Azure, GoogleApps, force.com

Preguntas



FIN DE SESIÓN #7

