

SEGURIDAD DE LOS DATOS CON INNOVADORAS SOLUCIONES INTEGRALES DE SEGURIDAD

CELAES 2019

Miguel Baquero

Regional Sales & Marketing
Manager

Bosch Building Technologies
Centro America, Colombia,
Ecuador y Venezuela

+573153158761

[Miguel. Baquero@co.bosch.com](mailto:Miguel.Baquero@co.bosch.com)



EL ECOSISTEMA UN MUNDO CONECTADO

Tecnología y Tendencia



- ▶ **Personas, Máquinas, Objetos y Sistemas Conectados**



- ▶ **50 billones de “cosas” conectadas en 2020***



- ▶ **Escalabilidad, Acceso Global, *Utility Computing*. Conectado.**



*Cisco IBSG © 2011

© Robert Bosch GmbH 2016. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

EL ECOSISTEMA UN MUNDO CONECTADO

01



96%

of senior business leaders plan to use IoT in the next 3 years.

- Wired

02



30%

of C-level execs believe IoT will unlock new revenue from existing products/services.

- The Economist

03



94%

of businesses have already seen a return on their investments in IoT.

- CMO.com

04



"...IoT will have the biggest impact in **customer service and support**..."

- The Economist

05



The IoT will lead to a

25%

reduction in asset maintenance costs and **35%** reduction in downtime.

- U.S. Department of Energy

06



\$970

will be saved per year per fleet vehicle

- Cisco

07



38%

of businesses believe IoT will have a major impact over the next 3 years.

- The Economist

08



\$41 trillion

will be spent over the next 20 years for infrastructure upgrades.

- Intel

09



IoT could add **\$10-15 TRILLION** to the global GDP.

- OECD

10



Because of the IoT there will be

22x

more data traffic by 2020

- Freescale

11



0.06%

of things that could be connected actually were in 2014.

- Baseline Magazine

12



40%

of all data generated by 2020 will come from connected sensors.

- Frost & Sullivan

Fonte: servicemax.com

EL ECOSISTEMA UN MUNDO CONECTADO



“Vamos a tener que cenar fuera. El refrigerador no está hablando com la estufa.”

SISTEMAS DE SEGURIDAD

Monitorear y proteger personas, propiedad e instituciones

Seguridad electrónica
+
procedimientos adecuados
+
Barreras de protección



- ▶ **Conectados**
Actualmente a la mayoría de los sistemas de seguridad están conectados
- ▶ **IoT & Cloud**
Dispositivos cada vez más conectables y online
- ▶ **Evolución**
 - + Inteligencia
 - + Facilidad
 - + Performance
 - + Multifunciones
 - + Seguro

Pero, será que esos sistemas de seguridad “conectados” son realmente seguros?

MONITOREO DE VIDEO

EVOLUCIÓN DEL MERCADO



**Mas
detalles**



**Número creciente
de Cámaras**
(Mercado global de
cámaras IP CAGR 20% +)



**Necesidades
de evidencia
indiscutible**



**Vídeo y Datos
mas conectados**

EVOLUCIÓN DEL MERCADO

HOY LOS DESAFÍOS REALES SON...



Administra y hacer uso:

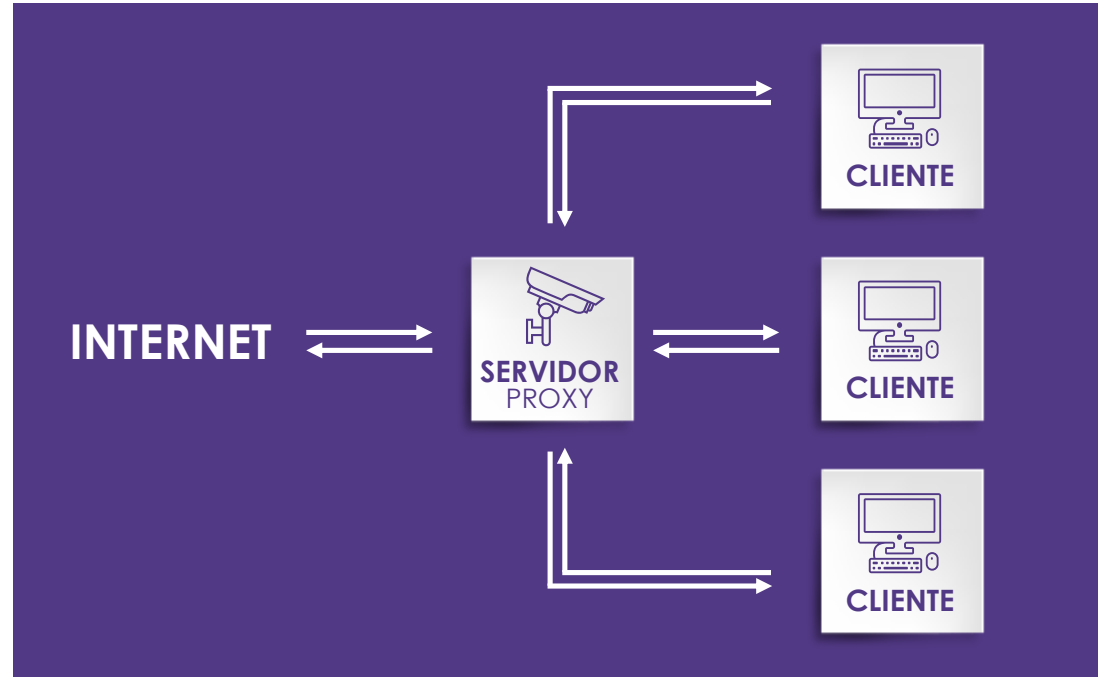
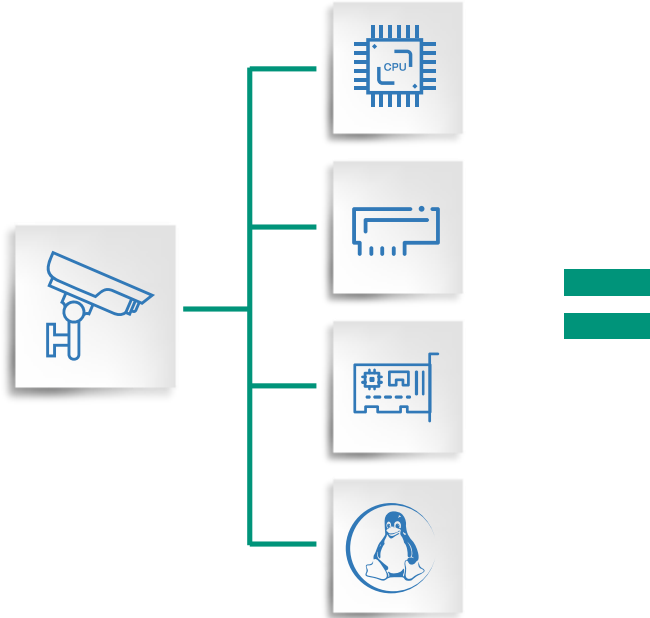
Le los Peta bytes en alto crecimiento de los datos de vídeo capturados



Minimizar:

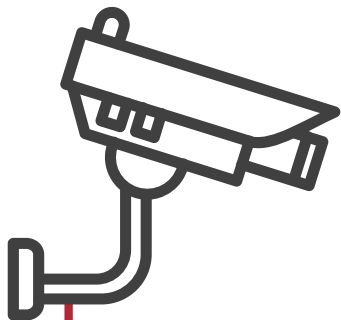
La Vulnerabilidad al cibercrimien

MIRANDO HACIA LA CÁMARA TIENE TODO PARA FUNCIONAR COMO UN SERVIDOR?



ATAcando A LAS CÁMARAS

EXISTEN VIRUS PARA CÁMARAS?



g1.globo.com

ATACANDO LAS CÁMARAS USANDO CÁMARAS PARA PROMOVER UN ATAQUE DDOS...



THE WALL STREET JOURNAL.



Atualizado 30 de setembro de 2016 às 15:11 ET

Los hackers asumirán el control de las cámaras de seguridad domésticas y los grabadores de vídeo para lanzar uno de los mayores ataques de internet de la historia este mes. Un ataque sin precedentes abrió las preguntas sobre como la Internet lidiará con una gran cantidad de dispositivos conectados y vulnerables que entrarán en operación en los próximos años

VULNERANDO LA CONFIDENCIALIDAD

COSTOS INMENSURABLES

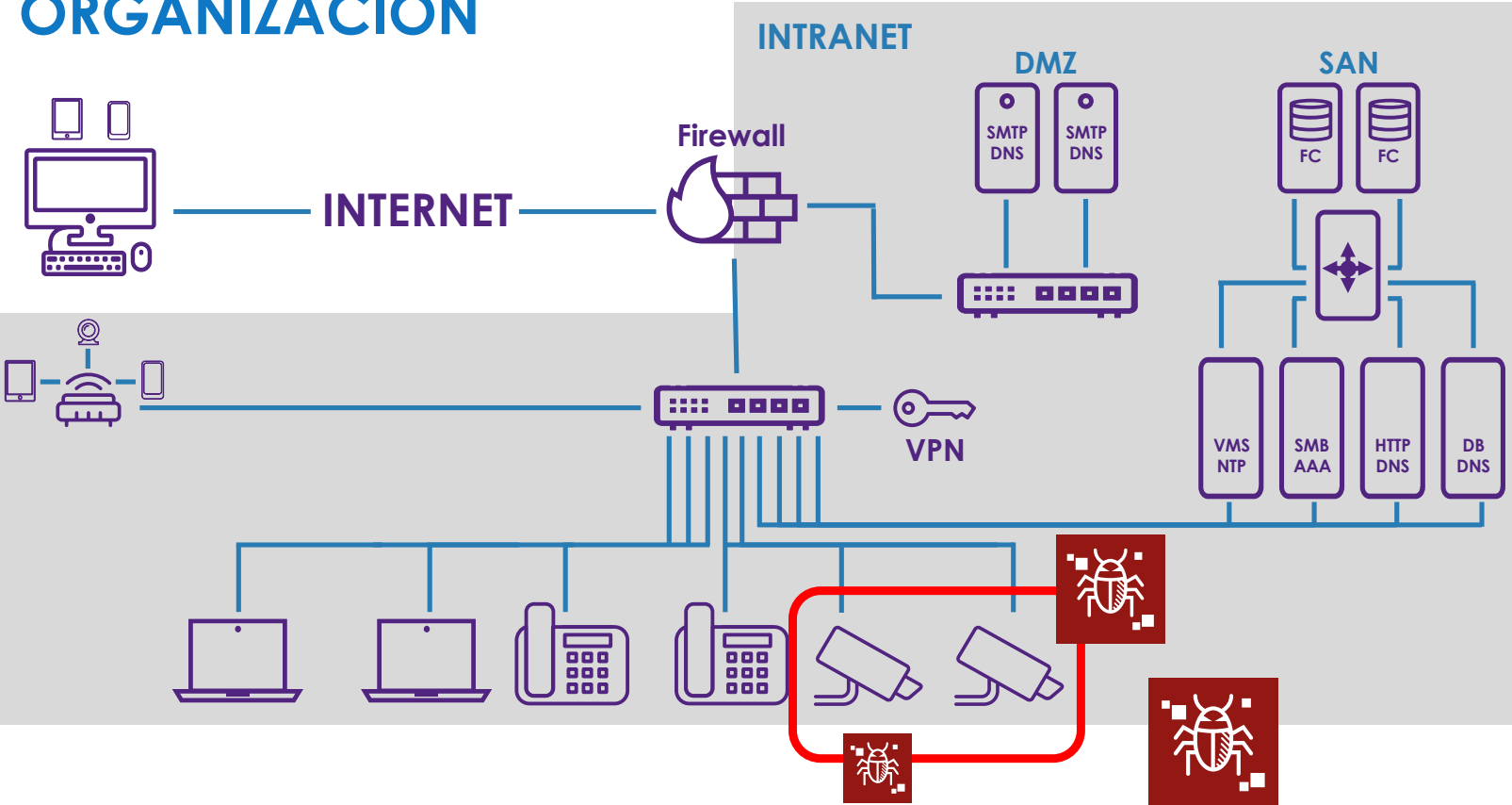
ACUALES SON LAS CONSECUENCIAS DE LA FUGA DE IMAGENES DE VIDEO EN CCTV?



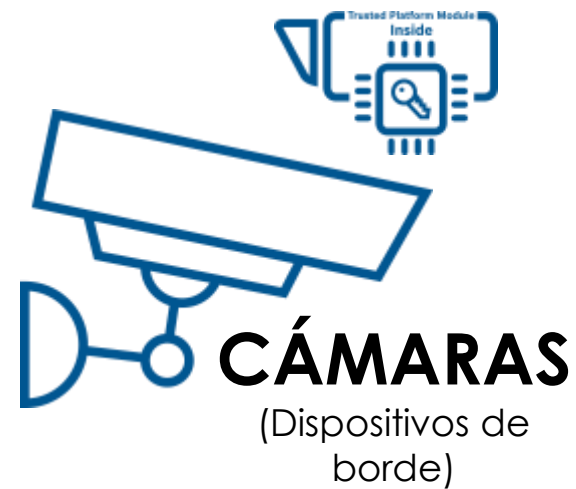
Tal vez se acuerde de la Copa mundo de Rugby de 2011 de Nueva Zelanda, de cierto jugador del equipo Ingles (casado con miembro de la familia real) que se escapaba de la concentración del equipo que fueron capturadas en CCTV y fueron publicadas

El gabinete del comisario de información del Reino unido tiene el poder de multar empresas y organizaciones con hasta **500.000** libras por violación de los datos.

DIAGRAMA DE UNA RED BÁSICA ORGANIZACIÓN

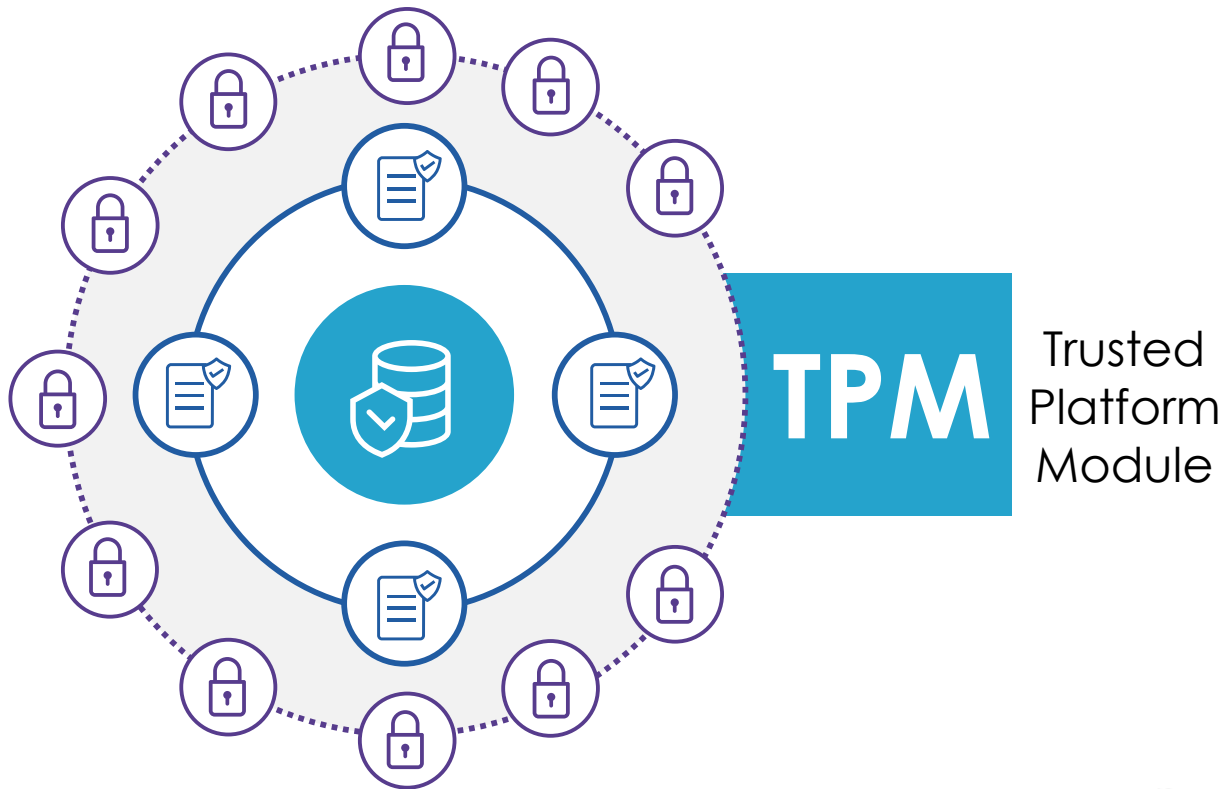


MANTENGA LOS DATOS DE VÍDEO SEGUROS COMO PROTEGEMOS NUESTRAS CÁMARAS



MANTENIENDO SU SECRETO

ALMACENAMIENTO DE CONTRASEÑAS Y CERTIFICADOS



MANTENER LOS DATOS DE VÍDEO SEGUROS

4 PASOS DE BOSCH CONSIDERANDO LA INFRAESTRUCTURA COMPLETA



1: Crear confianza



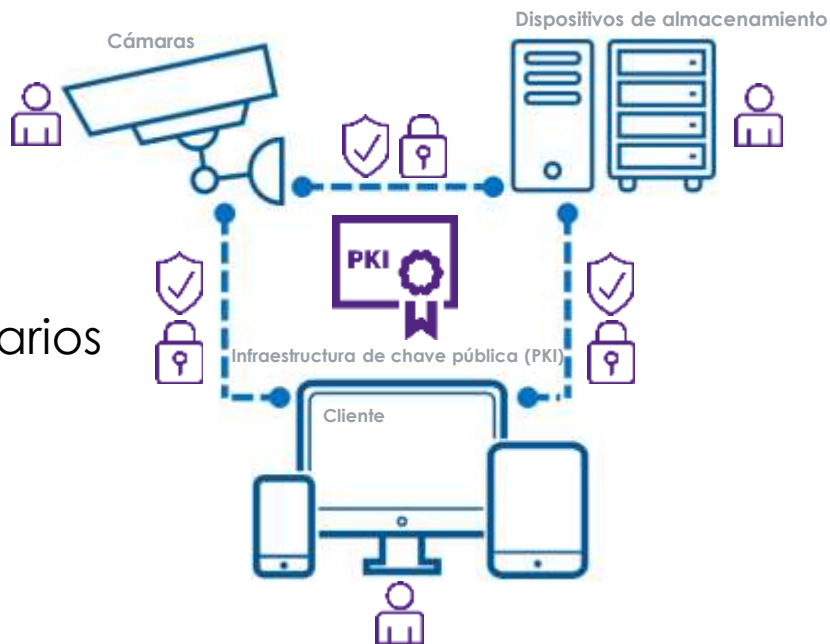
2: Proteger los datos



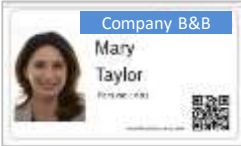
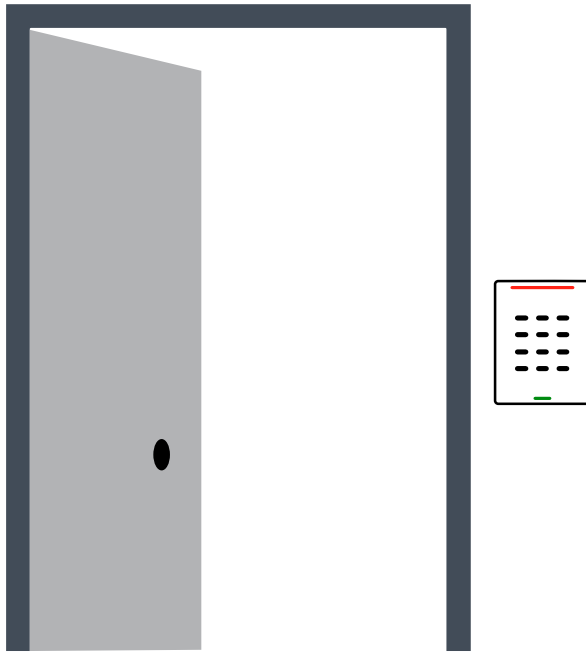
3: Administrar el Acceso a Usuarios



4: Atender los patrones de IT



CONTROL DE ACCESO REALMENTE SEGURO?



Leer
(())



Escribir
(())



ACCESO
CONCEDIDO

CONTROL DE ACCESO

CRENCIALES

Identificación



Credencial

Utilice tarjetas con datos protegidos por criptografía

- **Tecnologías 125KHz no son protegidas** y los datos almacenados en las tarjetas son fácilmente copiados y clonados fácilmente
- **Mifare DESFire EV1 e iClass SE/Seos** aumenta el nivel de seguridad. Soportan autenticación mutua de llave diversificada. Los datos transmitidos son protegidos por criptografía (ex: AES)
- La autenticación multifactor aumenta el nivel de seguridad
 - Ex: **Biometría + tarjeta + PIN**
- La Video verificación puede servir como una validación adicional

CONTROL DE ACCESO

COMUNICACIÓN ENTRE EL LECTOR Y CONTROLADORA

Interfaz



Lector

Wiegand/
RS-485



Decisión

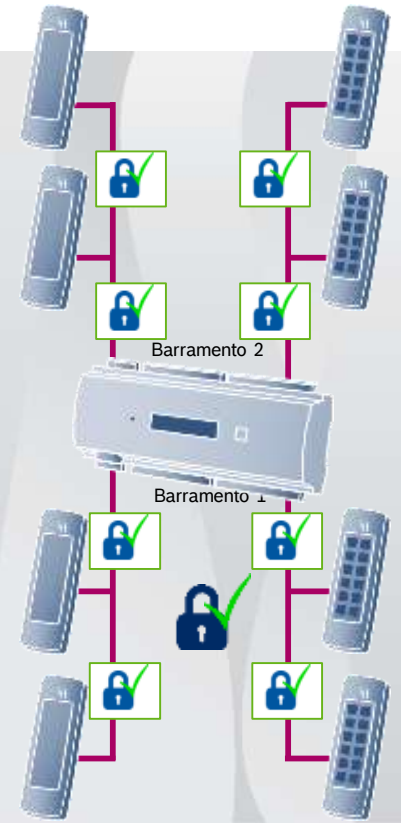


Controlador

- Las dos tecnologías más usadas:
 - 1) Interfaz **Wiegand - Protocolo Wiegand**
 - 2) Interfaz **RS485 - Open Supervised Device Protocol (OSDP)**
- La mayoría de los sistemas instalados mundialmente (cerca del 80%) utilizan Wiegand
- Wiegand es un protocolo/interfaz que no utiliza comunicación criptografía (google **“Como hackear una interface Wiegand”**)

Como todos los datos del titular de una tarjeta, es esencial mantener una comunicación segura

- Creado en 2008 y adoptado como patrón por la Security Industry Association (SIA) en 2012
- Protocolo para comunicación **bidireccional** seguro entre dispositivos de sistemas de control de acceso físico
- Mejora la **interoperabilidad** entre productos control de acceso y seguridad
- **OSDPv2 soporte criptografía avanzada AES-128 bits**





BOSCH

Invented for life



Support

Product Security

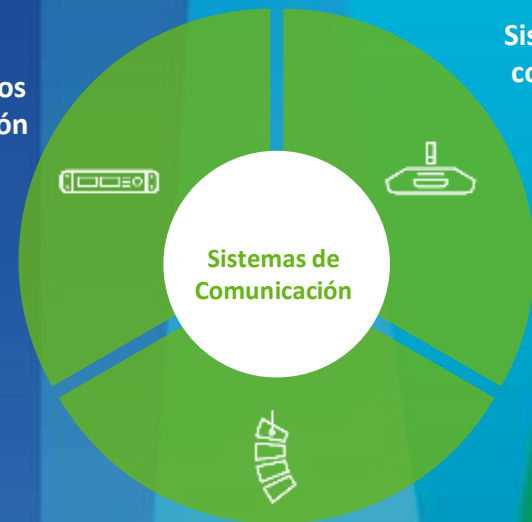


“...es una parte esencial de la promesa de calidad de Bosch que nuestros productos sean seguros...”

PORTAFOLIO DE SOLUCIONES BOSCH



Sistemas Críticos de Comunicación



BOSCH

Invented for life

Nuestra gama de cámaras inteligentes

Donde la inteligencia
se une al rendimiento



Soluciones Analítica de Video

16 Analíticas embebidas – 8 Simultaneas



“La mayor brecha de seguridad se genera cuando creemos, sin desconfiar, que estamos totalmente seguros”

GRACIAS

Miguel Baquero

Regional Sales & Marketing
Manager

Bosch Building Technologies
Centro America, Colombia,
Ecuador y Venezuela

+573153158761

Miguel. Baquero@co.bosch.com

