BYO… - Bring Your Own **QUÉ**?

Andrés A. Buendía Ucrós
Sensei Sales Engineer - Latin America & Caribbean

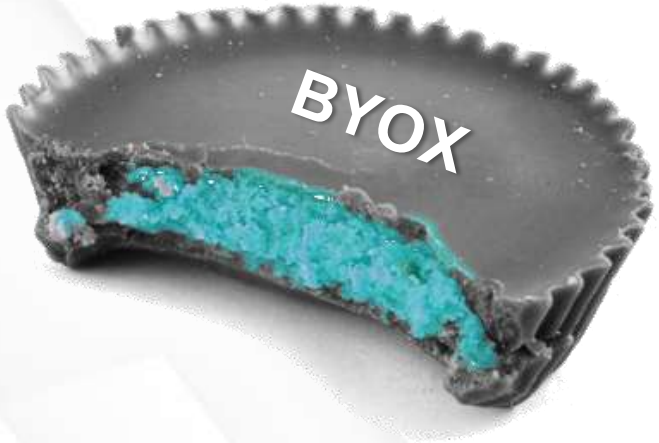
BYO… QUÉ ?

Qué significa BYOX?

BYOD = Bring Your Own Device

BYOA = Bring Your Own Application

BYOD + BYOA = BYOX



BYOD' = Bring Your Own Danger ?

Antes…

Hardware, software y no mucho más.

Ahora…

La tecnología móvil y los medios sociales han cambiado todo.

El cambio empezó en 2.007

El riesgo en la organización aumentó significativamente

Los medios sociales facilitan compartir información confidencial

La Línea Borrosa

El amor de los empleados hacia los dispositivos móviles asegura que estos permanecerán.

Trabajo en cualquier momento y en cualquier parte.

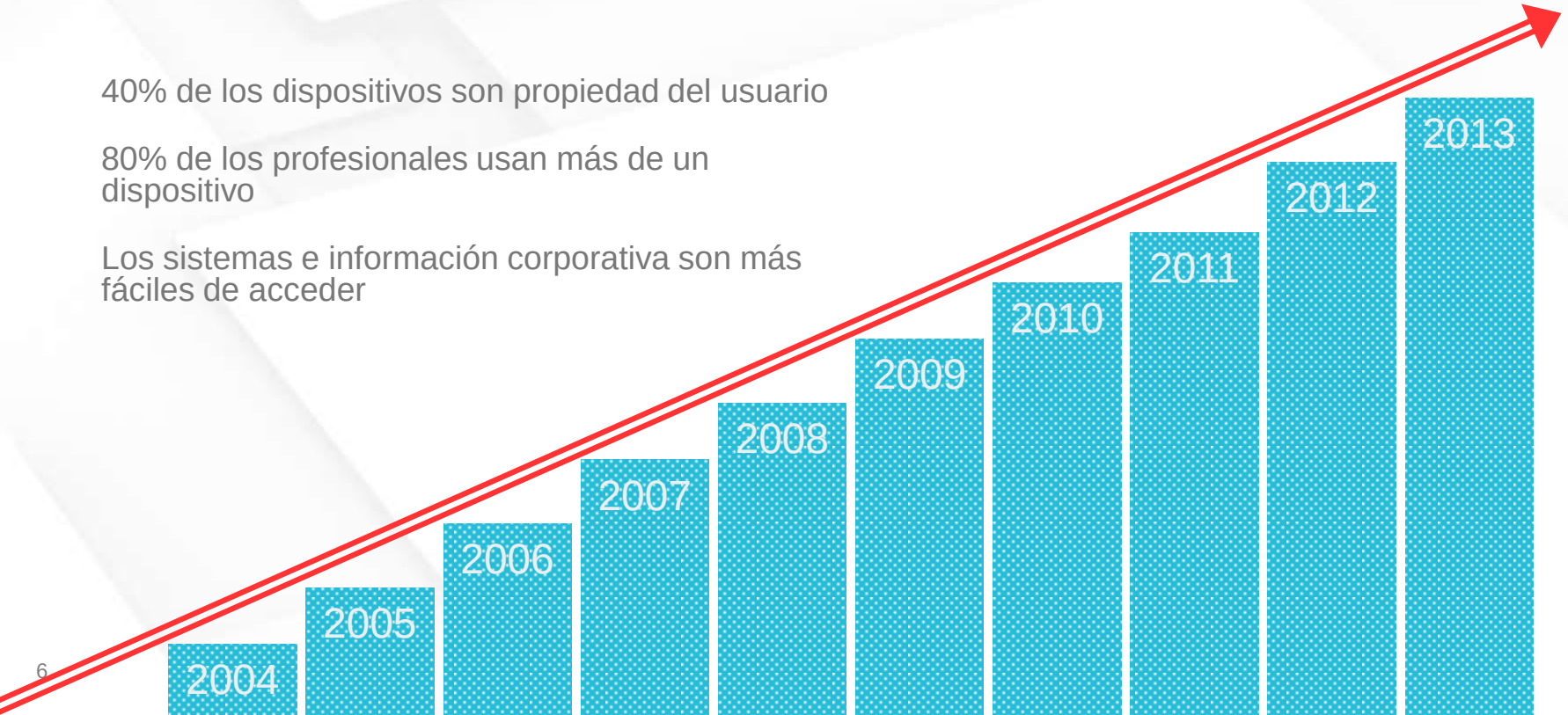
Los beneficios de BYOX superan los riesgos?

Más retos de seguridad y menos control.

40% de los dispositivos son propiedad del usuario

80% de los profesionales usan más de un dispositivo

Los sistemas e información corporativa son más fáciles de acceder



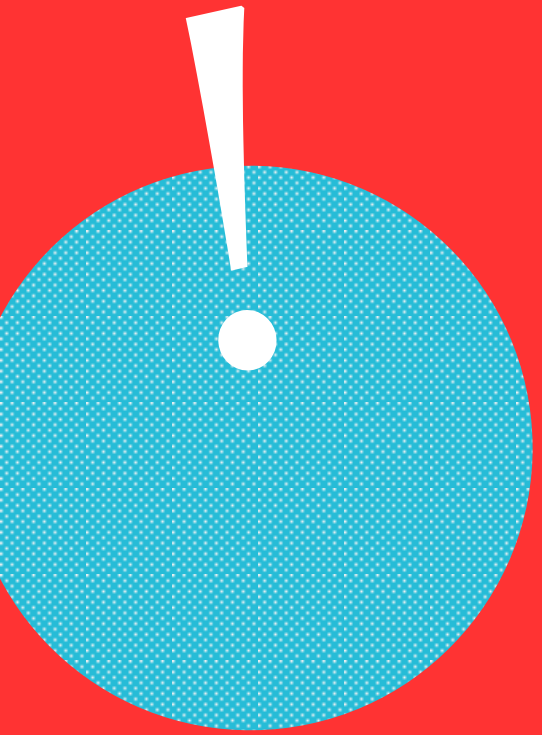
Los beneficios de adoptar una estrategia BYOX

Las ventajas superan las desventajas?

Dispositivos móviles más económicos que los activos de IT

Menor aprovisionamiento y gestión significa menor costo

Aumento de productividad



Retos de BYOX

No se puede proteger lo que no se conoce

Entender y gestionar los riesgos asociados a BYOX.

!

Aplicaciones en la Nube

!

Virus & malware riesgoso

Los dispositivos móviles ofrecen poca protección.

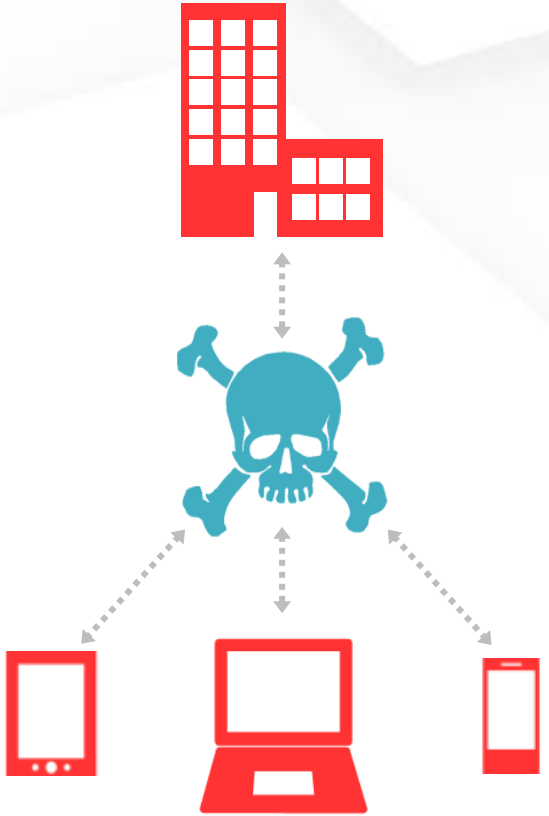
Huéspedes indeseables

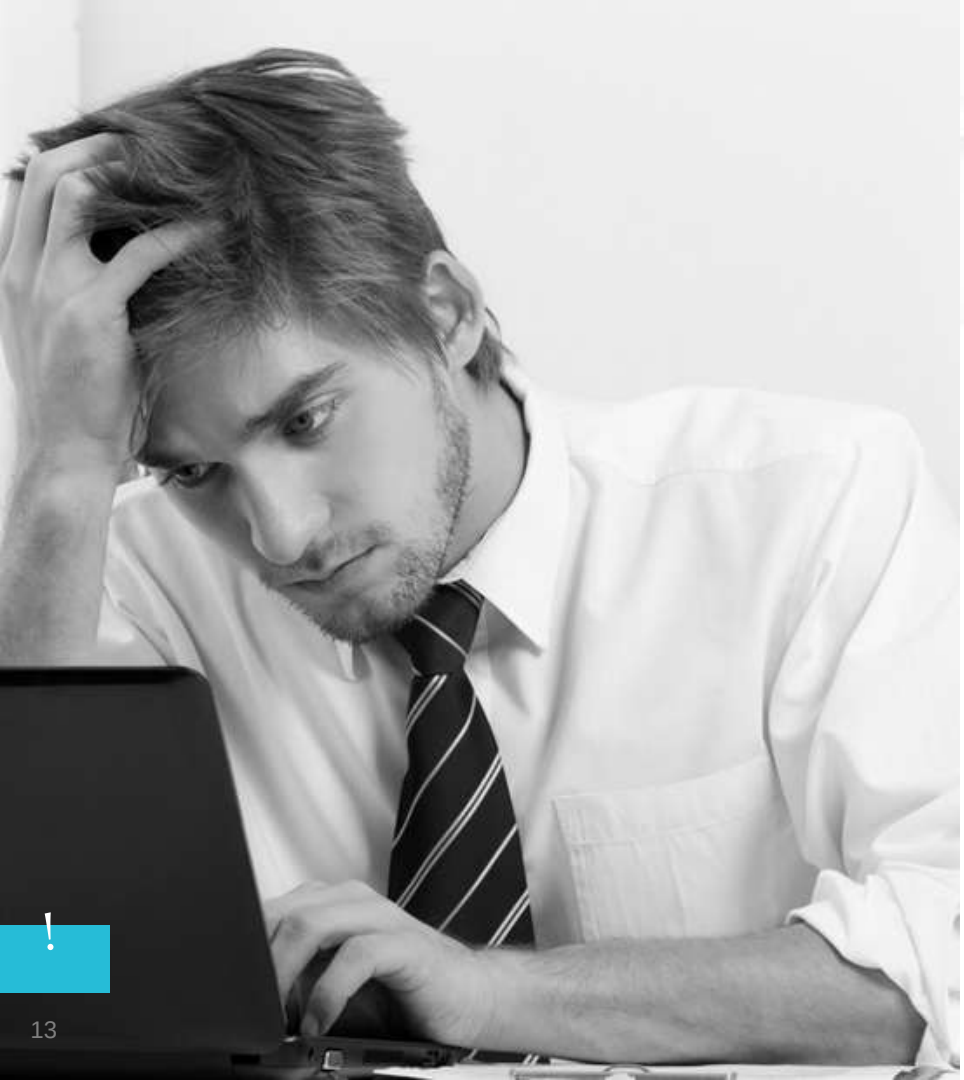
El riesgo de hackers e intrusiones.

Entrar al espacio de trabajo por el dispositivo móvil

Acceso a otros dispositivos e información

Potencial para infecciones ampliadas





Navegadores zombies

Problemas siempre.

Los ataques de Man-in-the-Browser (MitB) aumentan

El malware tradicional se ejecuta cada vez que un dispositivo de cómputo se enciende

Malware de navegador que solamente toma el control de éste

Arriesgar la pérdida de datos

Consecuencias extremas.

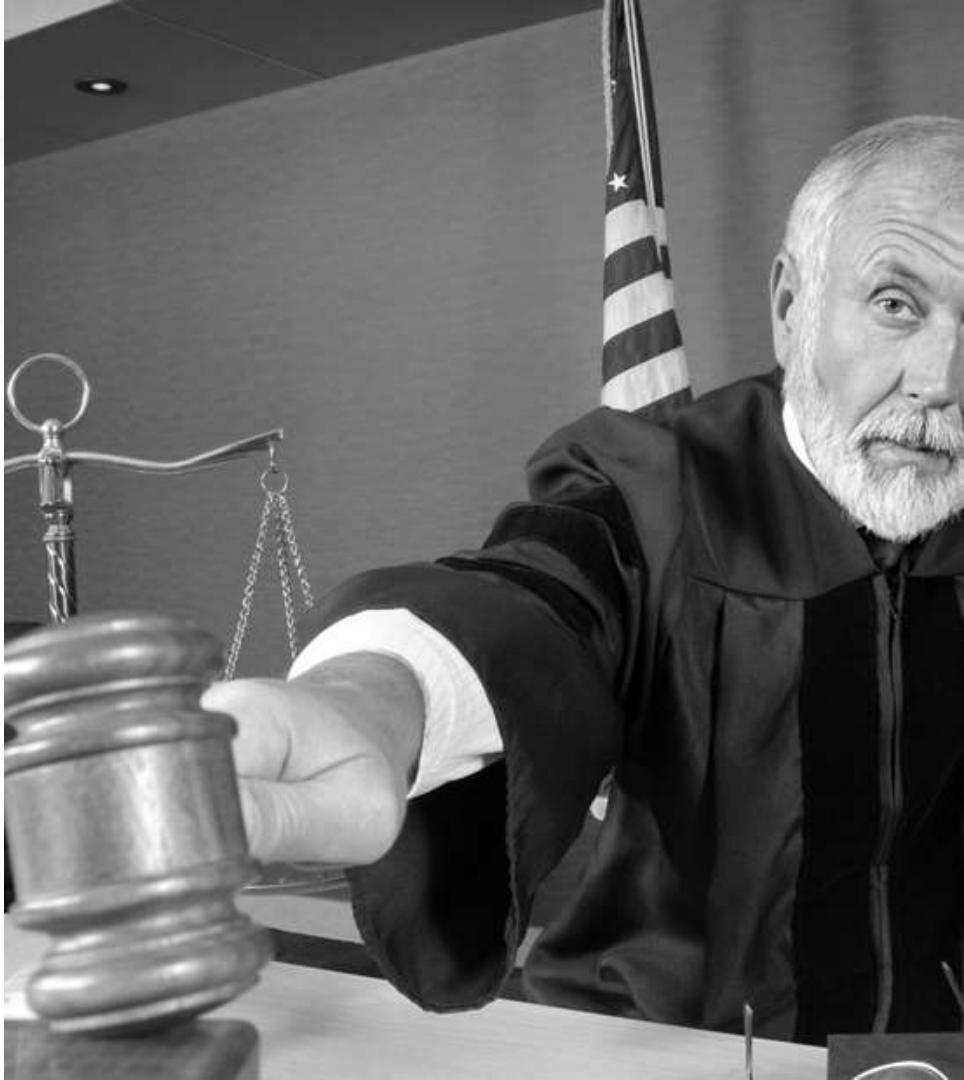
La pérdida de datos acarrea

- Costos legales
- Gastos de divulgación
- Costos de consultoría
- Gastos de remediación

Una fuga de datos genera

- Gastos de análisis de crédito
- Acuerdos legales
- Auditoría de control de información

!



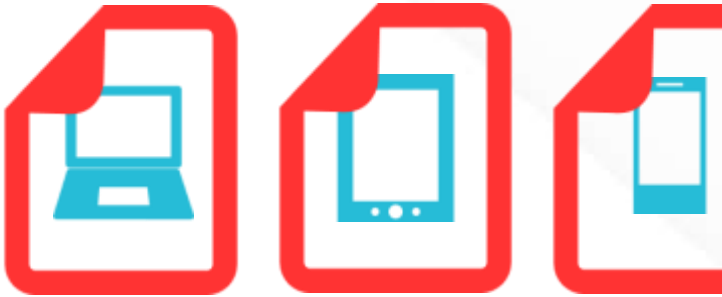
Ejecución de políticas

IT es desafiado por espacios de trabajo BYOX.

Crear políticas para cada dispositivo es complejo

Pérdida de control

Soluciones inmaduras para este tipo de plataforma



Errores en BYOX

Errores de BYOX

1. No saber qué dispositivos y aplicaciones se utilizan.

No conocer lo que los empleados hacen en la red se contrapone a una planeación exitosa

Errores de BYOX

2. No saber cómo trabajan las estrategias de los medios sociales con las políticas de BYOX.

Empleados que acceden a redes y aplicaciones sociales
no necesariamente están perdiendo el tiempo

Errores de BYOX

3. Gestión débil de contraseñas.

Las contraseñas generadas por los usuarios son por lo general débiles y pueden comprometer los sistemas de IT

Estrategias BYOX

Política = Simplicidad

El foco en la política es el primer paso.

Determinar qué dispositivos pueden acceder a la red

Determinar qué dispositivos se soportarán

Separar el trabajo de la diversión

Asegurarse que los empleados entiendan las reglas y los riesgos.

La vida personal y el trabajo se deben mantener separadas

Para tener acceso a la red, los empleados deben aceptar las políticas de uso

IT debe monitorear la actividad

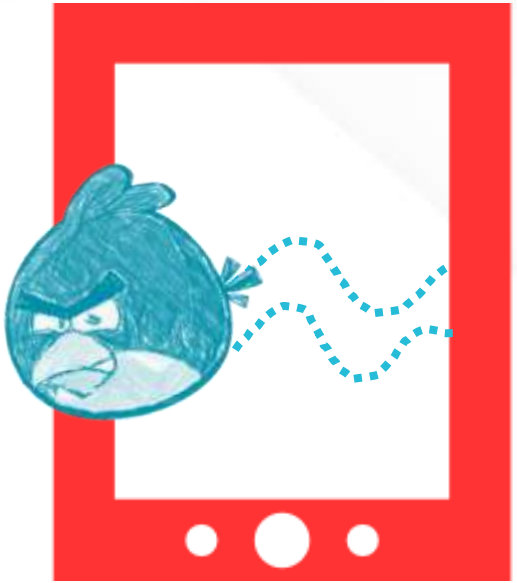
Controles más allá del dispositivo móvil

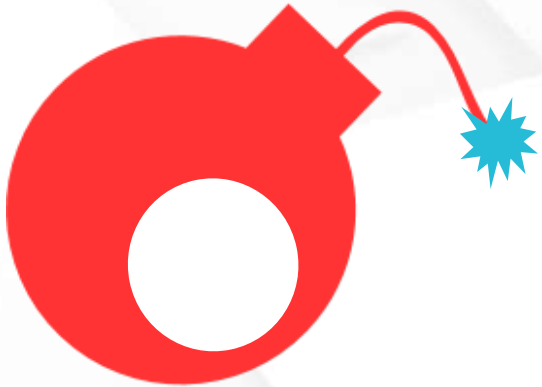
No se debe ignorar las aplicaciones.

Estrategias de control de aplicaciones hacen que las pol;iticas de BYOX sean más seguras

Decidir qué aplicaciones son aceptables y cuáles no

Segmentar la red para protección adicional





Considerarar riesgos adicionales

Esenciales las mejores prácticas y la aplicación de políticas

La organización está sujeta a controles tipo HIPAA o PCI DSS?

Si se pierde un dispositivo, se puede eliminar la información?

Los empleados saben que el acceso de su dispositivo móvil está restringido?

BYOX & WatchGuard

WatchGuard

Gestión de BYOX con WatchGuard

Servicios de seguridad fáciles de usar para los administradores IT.

WatchGuard hace que la administración de BYOX sea sencilla al utilizar herramientas y productos fáciles de utilizar. Los Administradores pueden aplicar políticas desde pequeños negocios hasta grandes organizaciones

Control de la red y las aplicaciones

Los productos WatchGuard dan control de cómo se utilizan los dispositivos.

Rápida y fácil configuración de segmentos de red

Mantener el cumplimiento y la alta seguridad

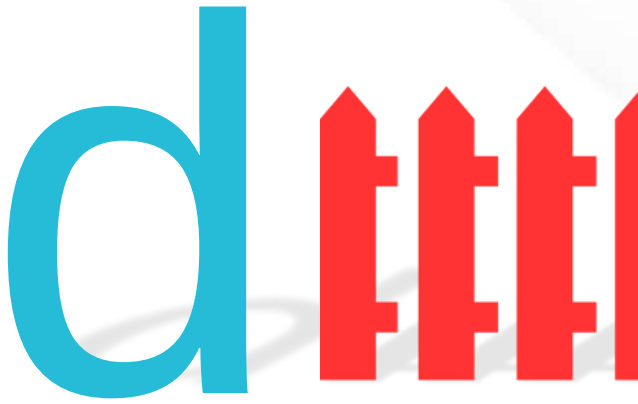
Monitoreo de más de 1.800 tipos de aplicaciones

Control de Aplicaciones

Protección de malware móvil en los dispositivos conectados.

El perímetro de la red es la primera línea de defensa.

WatchGuard utiliza la mejor tecnología en su clase para asegurar que los dispositivos conectados a la red tengan protección de antivirus.



Solución de navegación segura

WebBlocker de WatchGuard
Protege a los usuarios de los entornos hostiles.

Reside en el gateway

Agnóstico al dispositivo (Win, Mac, UX, Droid, iOS)

Configuración sencilla

Proteger la información corporativa

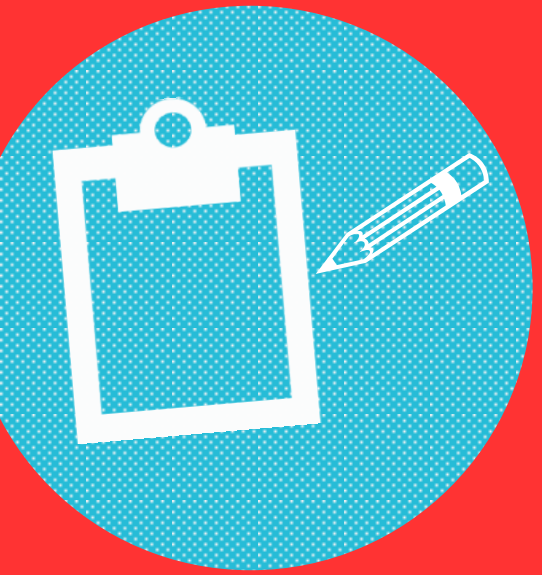
Limitar el acceso usando VPN.

Para protección de alto nivel, limitar el acceso a dispositivos que soporten conectividad VPN y requerir una conexión segura

Qué está conectado?
Qué se está usando?

WatchGuard señala los puntos potenciales de problemas

Logs y reportes son de las herramientas con mayor valor para apalancar una estrategia BYOX. Ayudan a proteger los recursos y las áreas de interés



Resumen

BYOX llegó para quedarse

Tendencia importante que cambia la IT.

Crecimiento en tamaño y alcance

Presenta nuevos retos y oportunidades

Una estrategia BYOX es esencial para la seguridad de la información

Gracias

Andrés A. Buendía Ucrós

Sensei Sales Engineer - Latin America & Caribbean