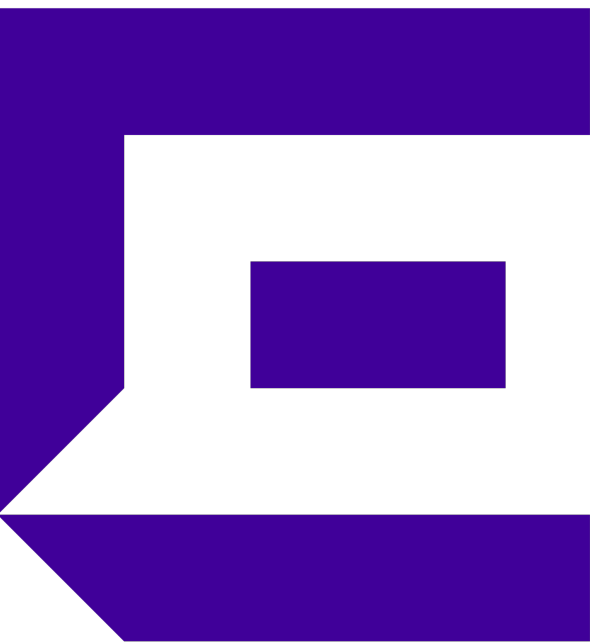




IoT en la Industria de Salud

Name...
Position...
Extreme Networks

Cómo está evolucionando la tecnología para la Salud?

Impulsores de negocio en Servicios de Atención Médica

- Aumento de la seguridad de los pacientes
- Mejora en la satisfacción del paciente
- Aumento de ingresos
- Reducción de costos
- Administración de riesgos & Cumplimiento de normas



Impulsores operativos para Servicios de Atención Médica para Redes

- Registros médicos Electrónicos
- Conectividad de Dispositivos médicos
- BYOD y Comunicaciones de próxima Generación
- Mejora de servicios al paciente
- Flujo de trabajo y Servicios de Localización



Las TI en el Sector de la Salud, requieren Visión

La percepción generalizada, es el motor para el “hospital del futuro”, “el hospital digital” e iniciativas para “habitación inteligente del paciente”.

En esto está en el corazón del sistema de salud en tiempo real.

El HDO CIO tendrá que crear conciencia de la situación e inteligencia en un ambiente rico en dispositivos tecnológicos y nuevas tecnologías aun inmaduras que crean una inteligencia integrada que cruza la brecha entre IT / OT ”.

- Barry Runyon, vicepresidente de investigación en Salud en **Gartner**

Gartner



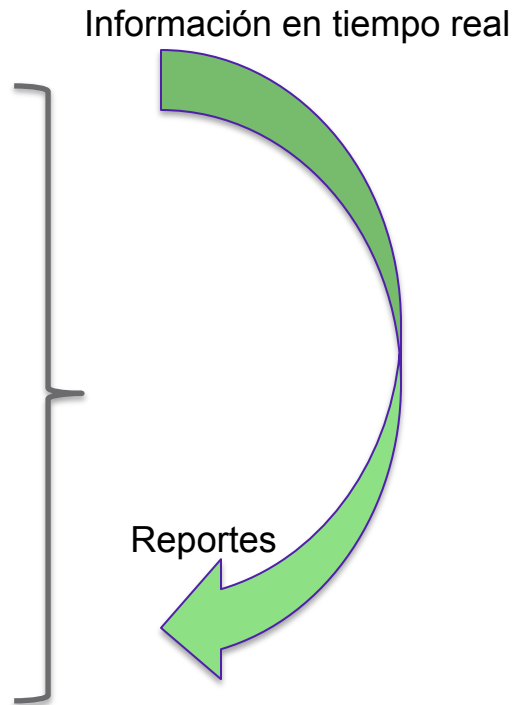


Diseño de un hospital Inteligente Integrado

- Mayor precisión de datos y disponibilidad
 - Registros médicos electrónicos
 - Interconexión de dispositivos médicos compartidos e Integración
 - Vista global del paciente / Unidad
- Rápida difusión de la información y respuestas
 - Datos fisiológicos
 - Administración de alarma para eventos
 - Plataformas de Comunicación Avanzada (tabletas, teléfonos inteligentes, etc.)
 - Ubicación de contenido
- Comprobación y Validación de errores mejorada
 - Identificación y Asociación
 - Ubicación de contenido
 - Información correcta
- Optimización de flujo de trabajo y administración de recursos
- Sistemas de construcción Inteligentes
 - Ambientales
 - Sistemas de seguridad (cámaras, puertas, etc.)

Análisis y uso de datos

- **Datos Clínicos**
 - Parámetros Psicológicos
 - Ordenes del médico
 - Información del laboratorio
 - Información radiológica
- **Administración de alarmas → alarmas y alertas**
- **Localización de contenido en tiempo real**
 - Flujo de Trabajo
- **Disponibilidad de recursos**
 - Equipos y suministros
 - Personal
- **Cuidado del Medio Ambiente**
 - Temperatura
 - Humedad
 - Protección contra Incendios
- **Información Administrativa / Administración**
 - Inteligencia de Negocio



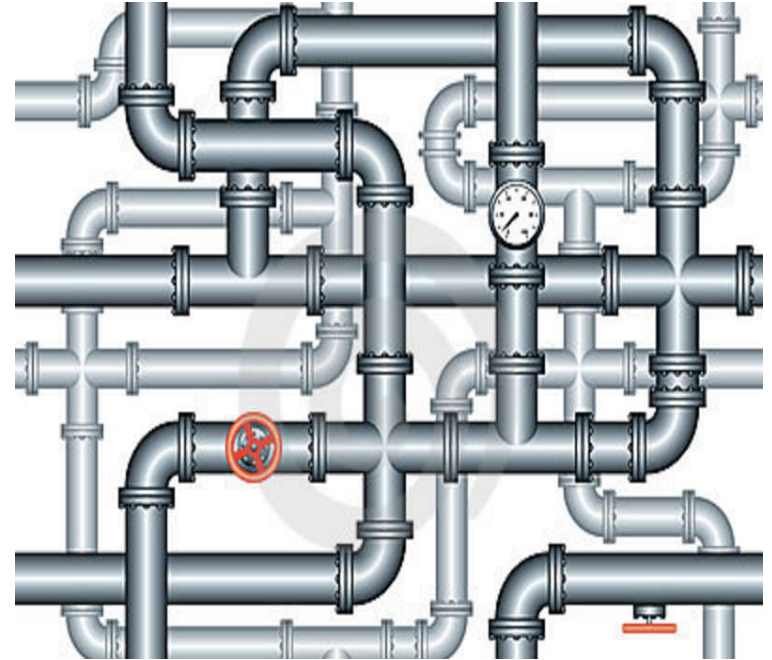


-

Retos y preocupaciones sobre IoT

Los dispositivos conectados requieren Estrategia

- El líder se centra en aplicaciones no en la infraestructura
- Todo el mundo asume que Wireless funcionará
- Los requerimientos del hospital de la red con cable e inalámbrica son complejos
- Servicio a menudo inconexo entre la aplicación independiente y la propiedad de la red
- Falta de visibilidad y de las mediciones del rendimiento crean retos
- Experiencias de usuario de baja calidad retardo en la adopción, aumento de tickets de problemas, reducción del rendimiento de la inversión



La Red es Fundamental en la Tecnología de Hospitales

"No hay que subestimar los requerimientos de infraestructura de red necesarios para un nuevo EMR"

Richard Royale, UnitingCare Health (HIMSS AsiaPac 2015)

Primer hospital certificado de Australia, Information Management System Society (HIMSS) Etapa 6

- Prescripción electrónica asistida (PEA)
- Sistema de apoyo de decisiones clínicas
- Loop cerrado de Administración de Medicamentos
- Integración PACS



Los Dispositivos médicos requieren Control Inteligente

- Los dispositivos médicos se están alejando de las bandas ISM dedicadas y redes.
- La entrega está a menudo inconexa entre TI y grupos clínicos o Ingeniería Biomédica.
- La falta de visibilidad de la ubicación del dispositivo, el uso y comportamiento es un reto para TI.
- La Seguridad en el mundo de los dispositivos médicos IoT es una preocupación fundamental para la seguridad del paciente.

Ahora, una preocupación de los reguladores



U.S. Department of Health & Human Services

FDA U.S. Food and Drug Administration
Protecting and Promoting *Your* Health

A to Z Index | Follow FDA | FDA Voice Blog

SEARCH

Most Popular Searches

Home Food Drugs **Medical Devices** Radiation-Emitting Products Vaccines, Blood & Biologics Animal & Veterinary Cosmetics Tobacco Products

Medical Devices

Home Medical Devices Medical Device Safety Safety Communications

Medical Device Safety

- Safety Communications
- Information About Heparin
- Medical Device Safety Archive
- Tubing and Luer Misconnections: Preventing Dangerous Medical Errors**

FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks

Date Issued: June 13, 2013

Audience: Medical device manufacturers, hospitals, medical device user facilities, health care IT and procurements staff; and biomedical engineers

Issue: Cybersecurity for medical devices and hospital networks

Purpose: The FDA is recommending that medical device manufacturers and health care facilities take steps to assure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack, which could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks.

Summary of Problem and Scope: Many medical devices contain configurable embedded computer systems that can be vulnerable to cybersecurity breaches. In addition, as medical devices are increasingly interconnected, via the Internet, hospital networks, other medical device, and smartphones, there is an increased risk of cybersecurity breaches, which could affect how a medical device operates.

¿Cómo deberían abordarlo los hospitales?

Para centros de salud, las recomendaciones de la FDA de Estados Unidos incluyen:

- La restricción del acceso no autorizado a redes y dispositivos médicos, y el seguimiento de la actividad de red, por si acaso
- Esfuerzos de actualización de antivirus y firewall, así como los parches de seguridad
- Creación y evaluación de estrategias para mantener la funcionalidad durante los eventos adversos

El Reto Continúa



Safety

Home > Safety > MedWatch The FDA Safety Information and Adverse Event Reporting Program > Safety Information > Safety Alerts for Human Medical Products

Safety Alerts for Human Medical Products

[2015 Safety Alerts for Human Medical Products](#)

[2014 Safety Alerts for Human Medical Products](#)

[2013 Safety Alerts for Human Medical Products](#)

[2012 Safety Alerts for Human Medical Products](#)

Symbiq Infusion System by Hospira: FDA Safety Communication - Cybersecurity Vulnerabilities

[f SHARE](#) [t TWEET](#) [in LINKEDIN](#) [p PIN IT](#) [e EMAIL](#) [p PRINT](#)

[Posted 07/31/2015]

AUDIENCE: Risk Manager, Oncology, Nursing

ISSUE: The FDA, the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and Hospira are aware of cybersecurity vulnerabilities associated with the Symbiq Infusion System. FDA strongly encourages health care facilities transition to alternative infusion systems, and discontinue use of these pumps.



Nuevas Directrices de Regulación

Symbiq Infusion System de Hospira:

- Asegura que los puertos no utilizados están cerrados, incluyendo Puerto 20 / FTP y el puerto 23 / TELNET.
- Supervisa y registra todo el tráfico de red de intentar alcanzar el producto afectado a través del puerto 20 / FTP, puerto 23 / Telnet y el puerto 8443.
- Contacta con el soporte técnico de Hospira para cambiar la contraseña predeterminada que se utiliza para tener acceso a puerto 8443 o cerrar.



Quien está en el asiento del conductor?

- La tecnología está siendo implementada en todos los departamentos del hospital con o sin TI.
- La sombra no está en las sombras.
- Hay varios proveedores tratando de hacer el mismo trabajo.
- La ingeniería biomédica y clínica se están moviendo hacia TI.
- TI debe ponerse al frente de los departamentos de forma proactiva y organizar la estrategia.



IoT Esta aquí

- BYOD, CYOD, AYOD – Toda persona tiene dispositivos de grado de consumo.
- Cada departamento tiene algo que puede ir en WiFi.
- No todos los dispositivos combinan bien juntos.
- No todos los dispositivos son buenos en Wi-Fi.
- Alguien tiene que estar a cargo de los dispositivos.
- ¿Cómo va a hacer que se cumplan las exigencias de la red?

Un Futuro Enfocado en Wireless

- Más dispositivos son inalámbricos que de cable.
- El Diseño y Apoyo son críticos.
- Se requieren Ingenieros con entrenamiento de RF.
- Rogue access points, hot spots, y los atascos suceden.



Una base segura para la Salud Inteligente

- Wireless omnipresente
- Automatización de Control de Acceso a la Red
- Entrega de aplicaciones en base a políticas
- Análisis de uso basado en la red
- Seguridad de la Información y Administración de Eventos





Thank You

WWW.EXTREMENETWORKS.COM

