Nuevas Tendencias en Seguridad Informática

Curso para la obtención del Diploma de Informática Militar

Universidad Rey Juan Carlos

César Cáceres Taladriz (cesar.caceres@urjc.es)
Escuela Técnica Superior de Ingeniería Informática

Contenidos

Universidad Rey Juan Carlos

- Conocer el concepto básico de BYOD e IoT, las amenazas y medidas de seguridad específicas de estos entornos
- Conocer los conceptos básicos de Cloud Computing, las amenazas y medidas de seguridad de estos entornos
- Conocer el concepto de APT. Aprender cómo mitigarlo y prevenirlo
- Conocer los conceptos básicos de las infraestructuras críticas y cómo protegerlas

1. Bring Your Own Device (BYOD)

Universidad Rey Juan Carlos

- ¿Qué es BYOD?
- Ventajas y desventajas de BYOD
- Riesgos en seguridad BYOD
- Contramedidas para BYOD
- Estrategias y políticas en entornos BYOD

Materiales basados principalmente en:

- Cisco Mobility Fundamentals Series BYOD

1. Bring Your Own Device (BYOD)

Universidad Rey Juan Carlos

- Tecnología del usuario vs Tecnología de la empresa
- Desarrollo de:
  - Smartphones
  - Conectividad en el hogar (Internet)
  - Cloud Computing
  - Redes Sociales
- Los empleados quieren utilizar en su entorno laboral aquellas tecnologías (dispositivos, servicios y aplicaciones) que están usando en su entorno personal y con las que dicen poder ser más productivos.

1. Bring Your Own Device (BYOD)

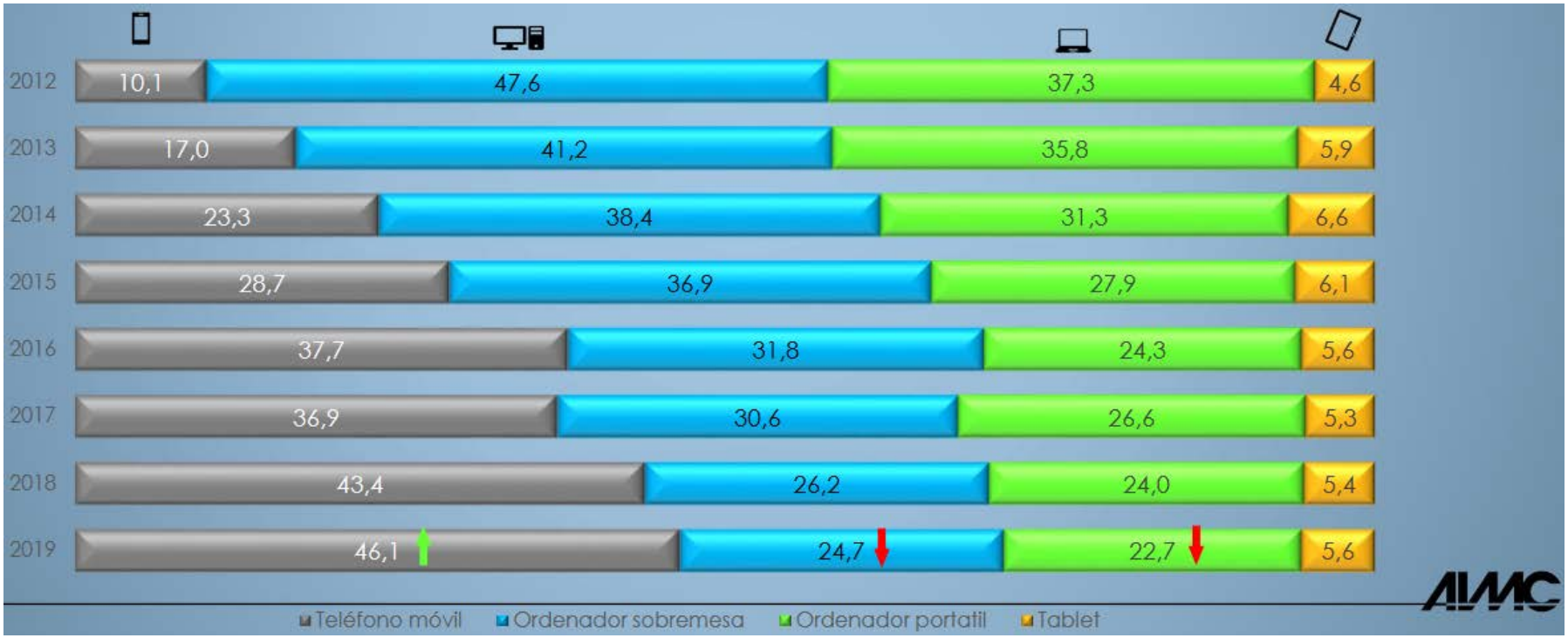
Universidad Rey Juan Carlos

- BYOD (“Bring Your Own Device”)
- BYOA (“Bring Your Own App”)
- BYOC (“Bring Your Own Cloud”)
- BYON (“Bring Your Own Network”)
- BYOT (“Bring Your Own Technology”)
- CYOD (“Choose Your Own Device”)
- POCE (“Personally owned, company enabled”)
- COPE (“Corporate owned, personally enabled”)

1. Bring Your Own Device (BYOD)

- “Mi iPhone me lo llevo al trabajo” (2007)

1. Bring Your Own Device (BYOD)



EGM. Marzo 2020

Algunas estadísticas (Forbes, 2019)

Universidad Rey Juan Carlos

- El mercado BYOD alcanzará los 367 mil millones de dólares en 2022, de los 30 mil millones de 2014 (BetaNews).
- El 61% de los Gen Y y el 50% de los trabajadores 30+ creen que las tecnologías que usan en su vida personal son más efectivas y productivas que las que emplean en su trabajo (Dell)
- El 60% usa el smartphone para el trabajo mientras el 31% lo desearía (Dell)
- Las empresas que utilizan BYOD ahorran 350$ al año por empleado (Cisco)
- Empleando dispositivos móviles para el trabajo ahorra al empleado 58 minutos al día, incrementando su productividad un 34% (Frost & Sullivan)
- El 78.48% de las organizaciones en EEUU han empleado estrategias BYOD en 2018 *(Frost & Sullivan)*

Ventajas del BYOD

Para la empresa

- Facilita la movilidad
- Mayor productividad y eficiencia
- Mejor satisfacción de las necesidades de los empleados
- Reducción de costes
- Facilita el teletrabajo o flexibilidad laboral
- Mejora en la toma de decisiones
- Mejora de los procesos de negocio
- Actualización de los equipos

Para el empleado

- Mayor productividad y eficiencia
- Mayor comodidad y rapidez
- Mejor satisfacción
- Mejor acceso a información corporativa
- Portabilidad
- Equipo posiblemente más moderno
- Reducción de costes de desplazamiento
- Mejor conciliación laboral
- Viajes con un único dispositivo

Desventajas del BYOD

Para la empresa

- Altos costes de implementación y mantenimiento
- Mayor complejidad técnica, administrativa y legislativa
- Mayor riesgo en seguridad y protección de datos
- Posible extravío o hurto
- Necesaria una política clara y transparente
- Incremento del tráfico
- “Islas” de colaboración

Para el empleado

- Instalación de servicios y aplicaciones en su propio dispositivo
- Aceptar cierto control de su equipo
- Separación de vida familiar y laboral
- Distracciones
- Averías
- Compatibilidad

Riesgos en seguridad del BYOD

Universidad Rey Juan Carlos

- Robo, pérdida o daño del dispositivo
- Seguridad desactualizada
- Eliminar controles de seguridad en el sistema operativo
- Conexiones inalámbricas no seguras
- La falta de cifrado en los dispositivo
- Controles de acceso al dispositivo insuficientes o inexistentes
- Instalar aplicaciones no confiables
- Uso del dispositivo por terceros
- Final de la relación laboral del empleado con la empresa

Riesgos en la seguridad física

- El **robo o pérdida** de un portátil, smartphone, tablet, incluso un pendrive, puede provocar graves pérdidas de información, más aún si el dispositivo tiene acceso a la red corporativa.
- Con BYOD, los dispositivos pasan un **tiempo fuera del control físico** de la organización, donde suelen estar más expuestos a este tipo de riesgos.
- No perder de vista la seguridad **dentro de la organización**, al pasar a utilizar **dispositivos portátiles** también son más vulnerables.

Contramedidas en la seguridad física

- Proporcionar aplicaciones que **almacenen la información en servidores propios** y no en el dispositivo, de forma que si el empleado lo pierde o se lo roban, o si el empleado deja de serlo para ir a una empresa de la competencia, pierda el acceso a esos datos.
- Los sistemas de gestión de dispositivos móviles (**Mobile device management (MDM)** systems) pueden localizar los dispositivos de una empresa, incluso bloquearlos o borrarlos de forma remota. Esta solución es compleja de implementar en el caso de BYOD pues la frontera entre la información personal y del trabajo es inexistente en el dispositivo.

Riesgos por malware

- Si el dispositivo de empleado se conecta a la red corporativa hay un riesgo alto de difusión de malware desde el mismo.
- El **email** es una de las vías de entradas de malware y trojanos más habituales, como adjuntos (pdf, Word, vídeo…). A pesar de las medidas de seguridad implementadas en los servidores de email de la compañía, nada impide al usuario acceder a otras cuentas de correo desde su dispositivo.
- Por **Internet** vulnerabilidades como XSS, donde el código malicioso se descarga de la web, o aplicaciones de descarga como BitTorrent, hacen también especialmente vulnerables los equipos personales BYOD que no controla el servicio de informática.
- La conexión de los dispositivos personales a **wifi hotspots** de restaurantes, hoteles, tiendas… incrementa también la posibilidad de ser víctima de un ataque o infección. Incluso hay grupos de hackers especializados en hoteles (Darkhotel).

Contramedidas para malware

- No se puede impedir descargas en dispositivos personales, pero sí que estos accedan a la red corporativa.
- El sistema MDM debería acceder a los dispositivos que gestiona de forma periódica y analizarlos en busca de virus y keyloggers. Si se detecta un malware o si el dispositivo ha sido "rooteado" o "jailbreakeado", este se pone en **cuarentena** hasta su limpieza (con el consentimiento del usuario o incluso haciéndolo él mismo), sin poder acceder a la red corporativa.
- Hay dos formas de garantizar la seguridad frente al malware:
  - Ofrecer a los empleados que usen BYOD una protección gratuita frente a virus y una conexión segura por VPN.
  - **Containerization**: proporcionar aplicaciones a los empleados desde un portal seguro de la empresa. Todos deben acceder a la red corporativa a través de ese portal mediante VPN. El sistema de **gestión de aplicaciones móviles (MAM)** asegura la separación entre las comunicaciones de la empresa y las personales, haciendo que todo el trabajo realizado en el dispositivo resida en el servidor de la empresa, que es monitorizado y controlado.
- Otro sistema que ayuda a la contención es el **gestor de emails en móviles (MEM)**, que asegura el acceso al sistema de correo electrónico de la compañía sobre conexiones cifradas, así como el almacenamiento de los correos en un servidor propio y fuerza el cumplimiento de las políticas sobre emails como la descarga de adjuntos potencialmente peligrosos.

Riesgos en confidencialidad

- Los **riesgos para la seguridad física** comentados, lo son normalmente para la confidencialidad, como por ejemplo el acceso a datos corporativos desde restaurantes u hoteles sin emplear una conexión cifrada (riesgo de MitM) o la pérdida o robo de un equipo no protegido.
- A estos riesgos se añade el de la **visualización de la pantalla del dispositivo** por un tercero, o la **amenaza interna** por parte de empleados descontentos o descuidados que podrían imprimir o copiar ficheros cuando están fuera de la oficina (o incluso dentro de la oficina).

Amenaza interna (Insider Threat)

Los atacantes externos no siempre son la causa de los peores problemas de seguridad. En muchos casos basta con un usuario interno malintencionado, mal formado o simplemente descuidado.

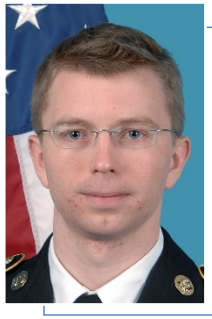
Amenaza interna (Insider Threat)

"Usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos. Lo único que se necesita es una llamada a **un empleado desprevenido** y acceden al sistema sin más. Tienen todo en sus manos".

Kevin Mitnick

Amenaza interna (Insider Threat)

Edward Snowden, consultor tecnológico estadounidense, informante, antiguo empleado de la CIA y de la NSA. En 2013 hizo públicos documentos clasificados como alto secreto sobre varios programas de la NSA, incluyendo los programas de vigilancia masiva PRISM y XKeyscore.



Bradley Manning, exsoldado y analista de inteligencia del ejército de Estados Unidos. En 2010 filtró a Wikileaks miles de documentos clasificados de las guerras de Afganistan e Irak, incluyendo cables diplomáticos de embajadas estadounidenses y el vídeo del ejército conocido como “Collateral murder”.

Hervé Falciani, ingeniero de sistemas italo-francés que trabajó en reforzar la seguridad de la filial suiza del banco HSBC entre 2001 y 2008. En ese periodo logró sustraer información de hasta 130.000 evasores fiscales (“lista Falciani”) y que es utilizada por la justicia de varios países para luchar contra el fraude fiscal.

Amenaza interna (Insider Threat)

Otras veces somos nosotros los que por descuido…

- En junio de 2015 el ejército de los Estados Unidos bombardeó un cuartel general del Estado Islámico que fue localizado gracias a la publicación de un “selfie” de uno de los miembros de dicha organización.
- iknowwhereyourcatlives.com localiza las viviendas de miles de gatos (y por tanto de sus dueños) en el mundo gracias a los metadatos de geolocalización de las fotografías que sus dueños publican en Internet.
- En 2005 se detuvo al asesino en serie de Wichita conocido como BTK que asesinó a 10 personas entre 1974 y 1991. Para su arresto fue fundamental la información recuperada de los metadatos de un documento en Word que estaba en un disquete que el propio asesino envió a una cadena de televisión y que no había borrado de forma segura.

Amenaza interna (Insider Threat)

Casi todos los ciberataques aprovechan en algún momento el factor humano, sobre todo en las primeras fases del ataque para recoger información sobre el objetivo o para lograr acceder o instalar algún malware o troyano. Una vez dentro, el ataque prosigue hasta que es detectado, y normalmente pasan años hasta que esto ocurre.

Contramedidas para confidencialidad

Universidad Rey Juan Carlos

- Muchas estrategias para asegurar los datos son llevadas a cabo por sistemas de **gestión de contenidos móviles (MCM)**, que garantizan el **almacenamiento** de documentos corporativos y datos de trabajo en los **servidores** de la empresa y no en los dispositivos BYOD.
- En caso de permitir la transmisión de esos documentos a los dispositivos, deben ser **sellados** para garantizar la trazabilidad y localizar la fuente de una fuga de datos en caso de que ocurra. Los MCM también pueden bloquear la copia de texto, impresión, envío o captura de estos documentos.
- En cuanto a garantizar la confidencialidad de los datos en tránsito evitando ataques MitM, el uso de conexiones **VPN** es lo más empleado.
- Para evitar la visualización de información en pantallas, el empleo de **salvapantallas** y **bloqueos** de los terminales de forma automática es también recomendado, así como el uso de **filtros** de privacidad para las pantallas de los portátiles.
- El problema de la pérdida o robo se puede mitigar con el bloqueo automático y los métodos de **localización** de dispositivos implementados por los sistemas MDM.
- Los sistemas **MEM** aseguran la protección de los datos de los correos electrónicos y su almacenamiento seguro.

Seguridad perimetral vs Zero-Trust

Cloud

Acceso remoto

Big Data y analítica

SOA

Mobile y BYOD

Resumen: Contramedidas técnicas

Universidad Rey Juan Carlos

- Uso de **conexiones cifradas** a través de redes privadas virtuales o VPN, servicios restringidos y la autenticación de dos factores.
- Uso de **contenedores cifrados**, mediante esos sistemas se crean particiones aisladas y restringidas en el disco duro local, donde se almacenarán los datos relacionados con el trabajo y la empresa y desde donde se establecerá la conexión a la red de la empresa.
- Soluciones de **application streaming** para encapsular aplicaciones y datos corporativos y ofrecerlos en el dispositivo del empleado como si se tratara de un escritorio remoto.
- Uso de **software MDM o de gestión de dispositivos móviles**, que permite la integración y administración central de dispositivos privados en las empresas. Estas interfaces profesionales pueden gestionar datos, instalar actualizaciones y configurar bloqueos para conexiones WLAN no seguras y aplicaciones de proveedores externos desconocidos, todo ello de forma remota. Hay que tener en cuenta que suponen un mayor control por parte del empresario sobre el dispositivo privado.
- **Soluciones sandbox** como los escritorios virtuales o las aplicaciones web, que permiten a los trabajadores acceder de manera remota desde su equipo privado al ordenador de la empresa, de manera que no se almacenan datos confidenciales en dispositivos externos.

Resumen: Contramedidas técnicas

- Uso de programas para **la localización por GPS del dispositivo**, así como la posibilidad de realizar un **borrado remoto**.
- **Cifrado** de los medios de almacenamiento externos (memorias USB, discos duros externos, tarjetas SD…).
- **Actualización** continua de dispositivos, sistemas operativos y aplicaciones instaladas.
- Uso de conexión móvil, **evitando el uso de redes WiFi abiertas** (si es necesario, usar VPN).
- Protección de los dispositivos mediante **mecanismos de acceso robustos**, como contraseñas o mecanismos de control biométricos (como la huella dactilar). Se establecerá un tiempo máximo de inactividad para que el dispositivo se **bloquee automáticamente**.

Resumen: Contramedidas técnicas

Universidad Rey Juan Carlos

- Realizar **copias de seguridad y gestionarlas / almacenarlas de manera segura**.
- Disponer de una **base datos de usuarios y dispositivos**, de manera que se pueda saber en todo momento la relación de dispositivos que acceden a los recursos de la empresa, los usuarios que los manejan y los privilegios de seguridad que tienen.
- Uso de sistemas de **almacenamiento corporativos (no públicos) y en la nube** para intercambiar archivos en lugar de hacerlo de forma "real".
- Tener instalada la **solución anti-malware** corporativa para dispositivos móviles, y si es posible, complementarla con software que permita realizar **white-listing o black-listing** de aplicaciones.
- Instalar sólo las **apps validadas** por la organización o desde su propio market de aplicaciones.

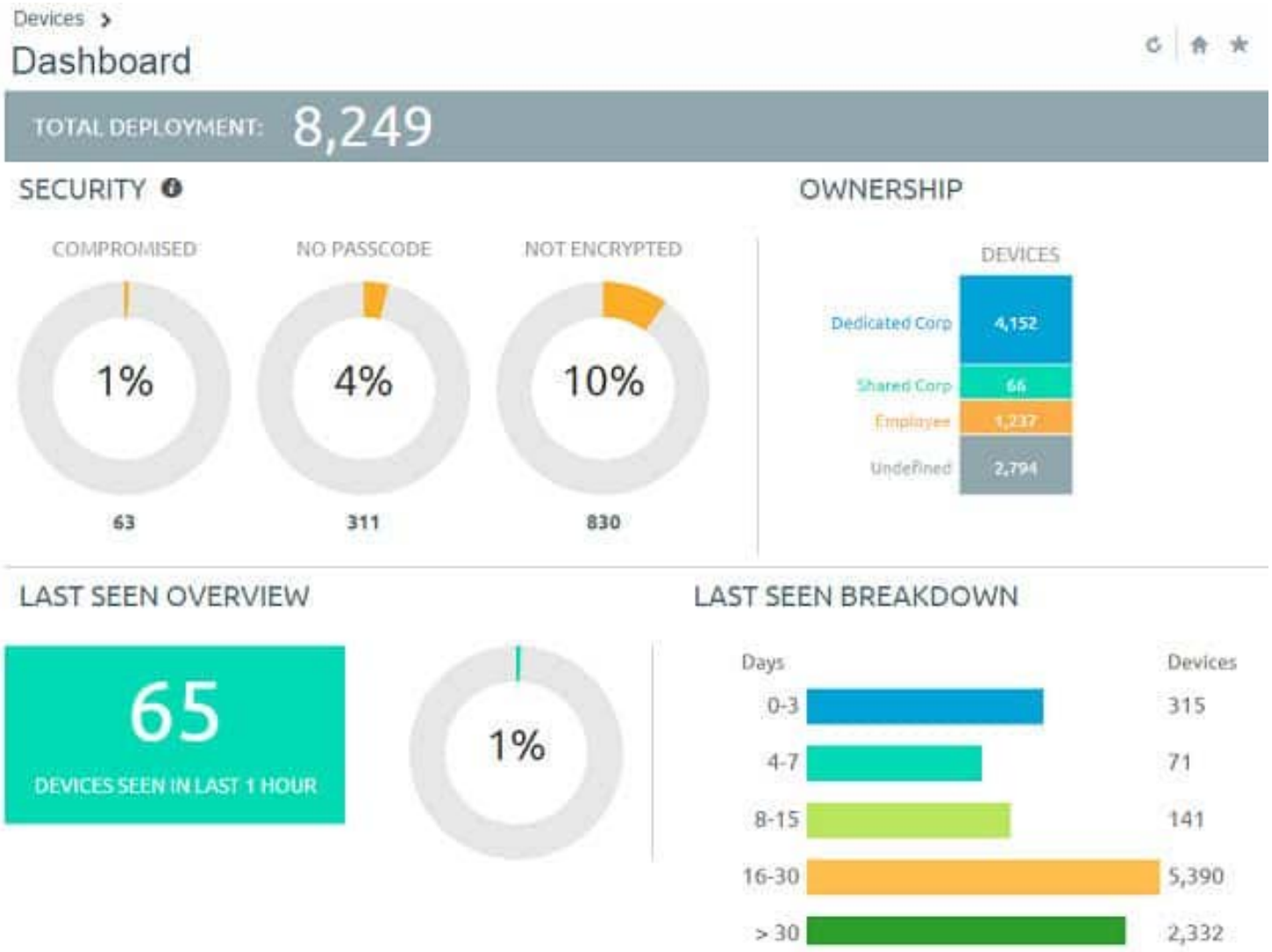
Estrategias y políticas para BYOD

Crear un programa BYOD que permita al equipo de TI:

- La gestión unificada de las políticas: una única plataforma de gestión de políticas que proteja datos, aplicaciones y sistemas, y que reconozca el perfil de usuario. Asimismo debería identificar y gestionar todos los dispositivos móviles que acceden a la red corporativa.
- Proporcionar acceso seguro a la red y servicios corporativos, en función del perfil de usuario y dispositivo usado, y manteniendo la capacidad de red necesaria.
- Proteger los datos independientemente de su ubicación con una seguridad capaz de identificar el contexto.
- Facilitar la transmisión segura de datos entre los dispositivos y la infraestructura de red o cloud.

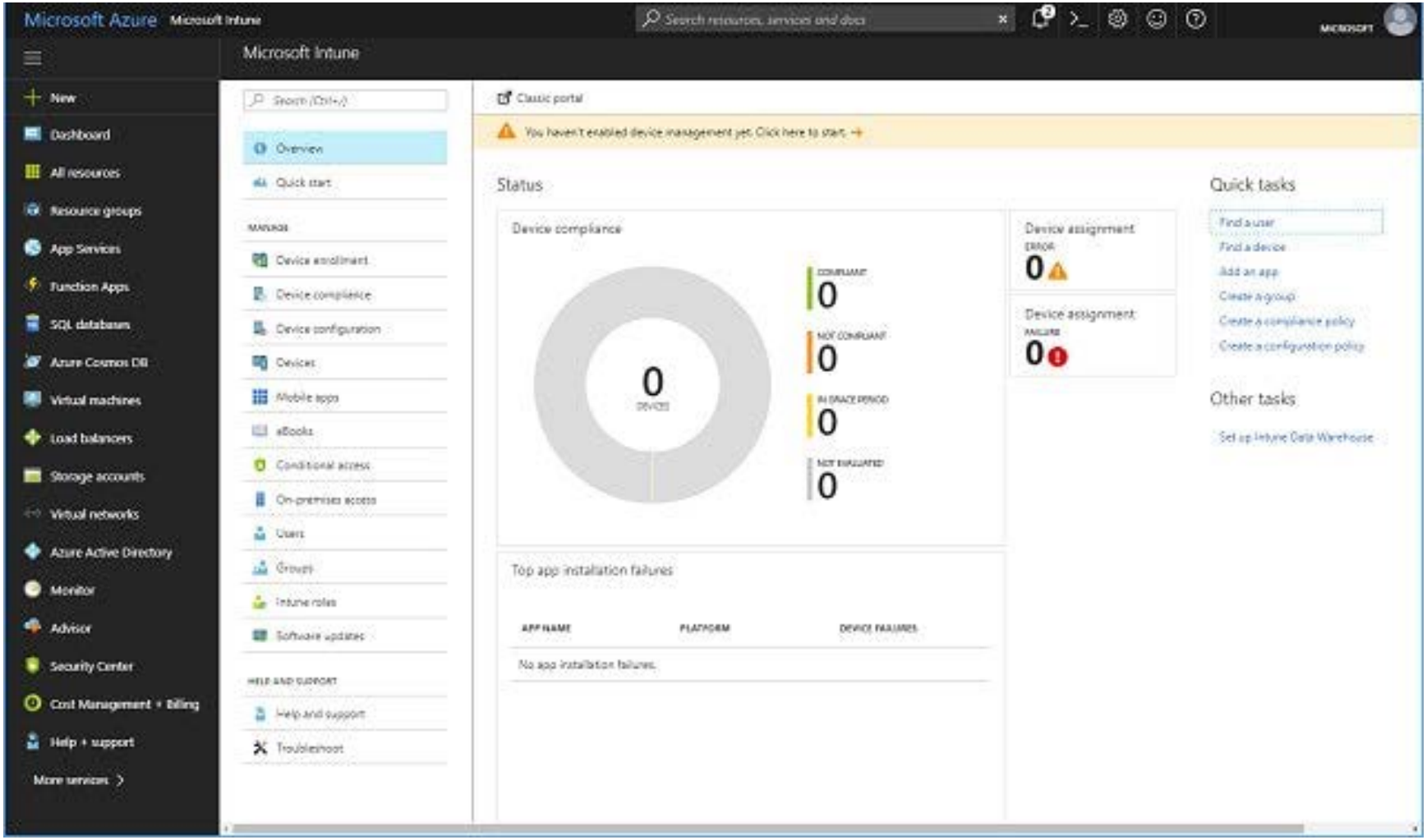
Gestores SW de dispositivos BYOD

Universidad Rey Juan Carlos



Gestores SW de dispositivos BYOD

Universidad Rey Juan Carlos



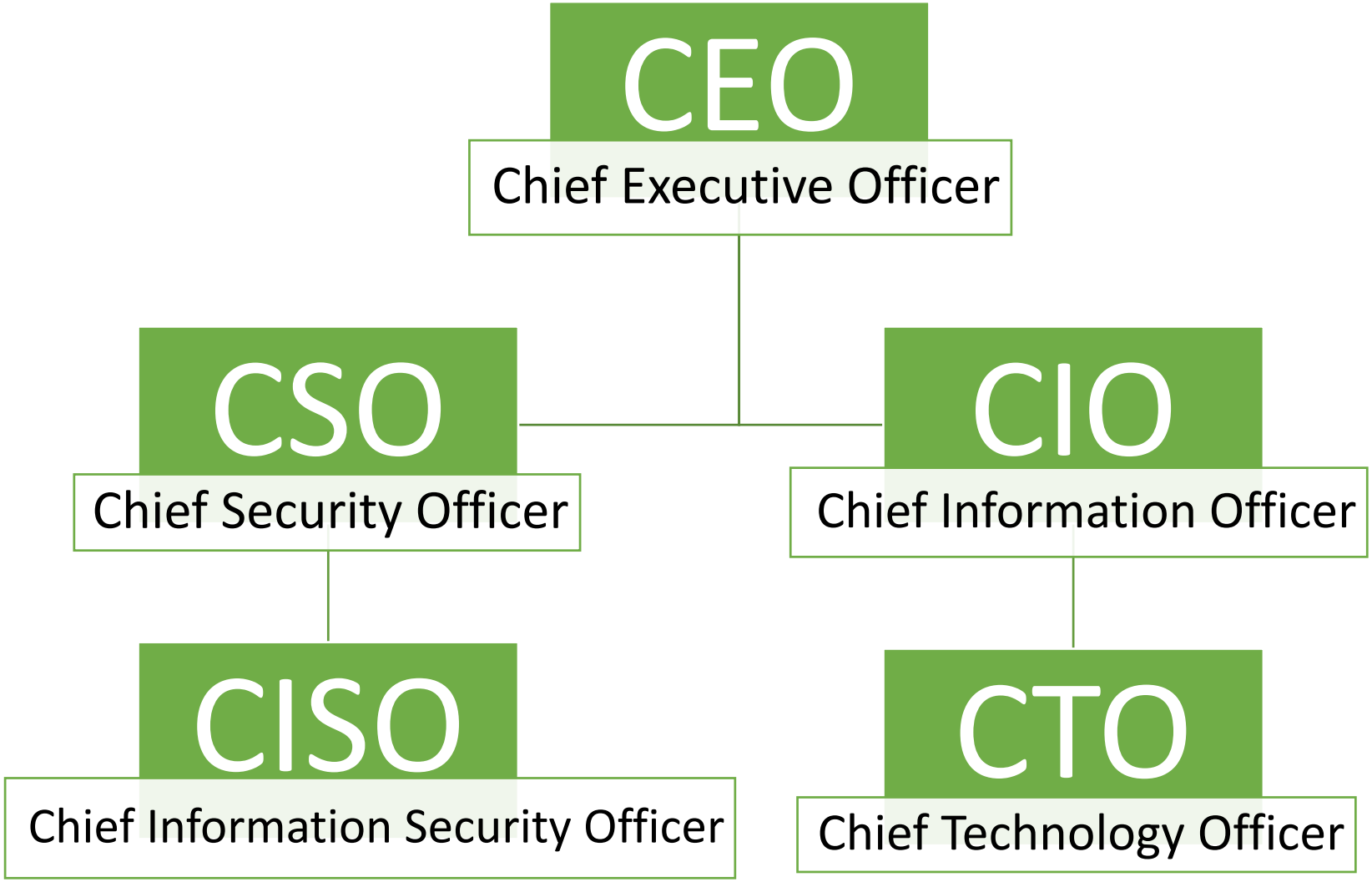
Gestores SW de dispositivos BYOD

Universidad Rey Juan Carlos

Contramedidas políticas en BYOD

- Crear una **normativa clara para regular el uso del BYOD** a la que tendrán acceso todos los empleados. Deberá contener un listado de dispositivos autorizados, condiciones en las que se permite su uso, cómo acceder a la información, las configuraciones de seguridad necesarias para utilizarlos, etc. Incluir una lista con las **aplicaciones permitidas y las prohibidas**. Evitar el uso de dispositivos *rooteados* o que cuenten con un *jailbreak.*
- Implementar una **política de formación y concienciación** para los trabajadores que vayan a hacer uso del BYOD.
- **Evitar ceder el dispositivo** a terceros y mantenerlo siempre bajo custodia.

Responsables en Seguridad Informática




BYOD Is Just the Tip of the Iceberg
BYOD
I need to allow iPads on my network
End User
Tactical
Strategic
I need to help my company develop new mobile business models
I need to ensure workers can be more mobile and more productive
CEO
I need a BYOD strategy that aligns with my VDI and workspace needs
I need to protect intellectual property and confidential data
I need to quickly provide app services to new employees, partners and contractors
CIO
I need to support multiple device types without increasing cost or complexity
I need video and voice on virtual desktops but I can't compromise the experience
Legacy applications don't run natively on new or mobile operating systems
IT
I Need a Workspace Strategy

© Cisco

Responsables en Seguridad Informática

CSO (Chief Security Officer)

Responsable de la seguridad de la organización (seguridad corporativa).

CISO (Chief Information Security Officer)

Director de seguridad de la información. Rol desempeñado a nivel ejecutivo y su función principal es la de alinear la seguridad de la información con los objetivos de negocio, garantizando que la información de la empresa esté protegida adecuadamente.

En organizaciones pequeñas CSO y CISO pueden ser la misma persona, pero el rol del CISO suele estar más centrado en aspectos de seguridad de la información.

Responsables en Seguridad Informática

Una de las responsabilidades del CSO y CISO suele ser definir un **entorno de políticas y procedimientos** que intenten gestionar el factor humano (con gran importancia en la formación y concienciación).

La seguridad por oscuridad no funciona

Tampoco por prohibiciones ni legislación

Deben definirse POLÍTICAS y PROCEDIMIENTOS

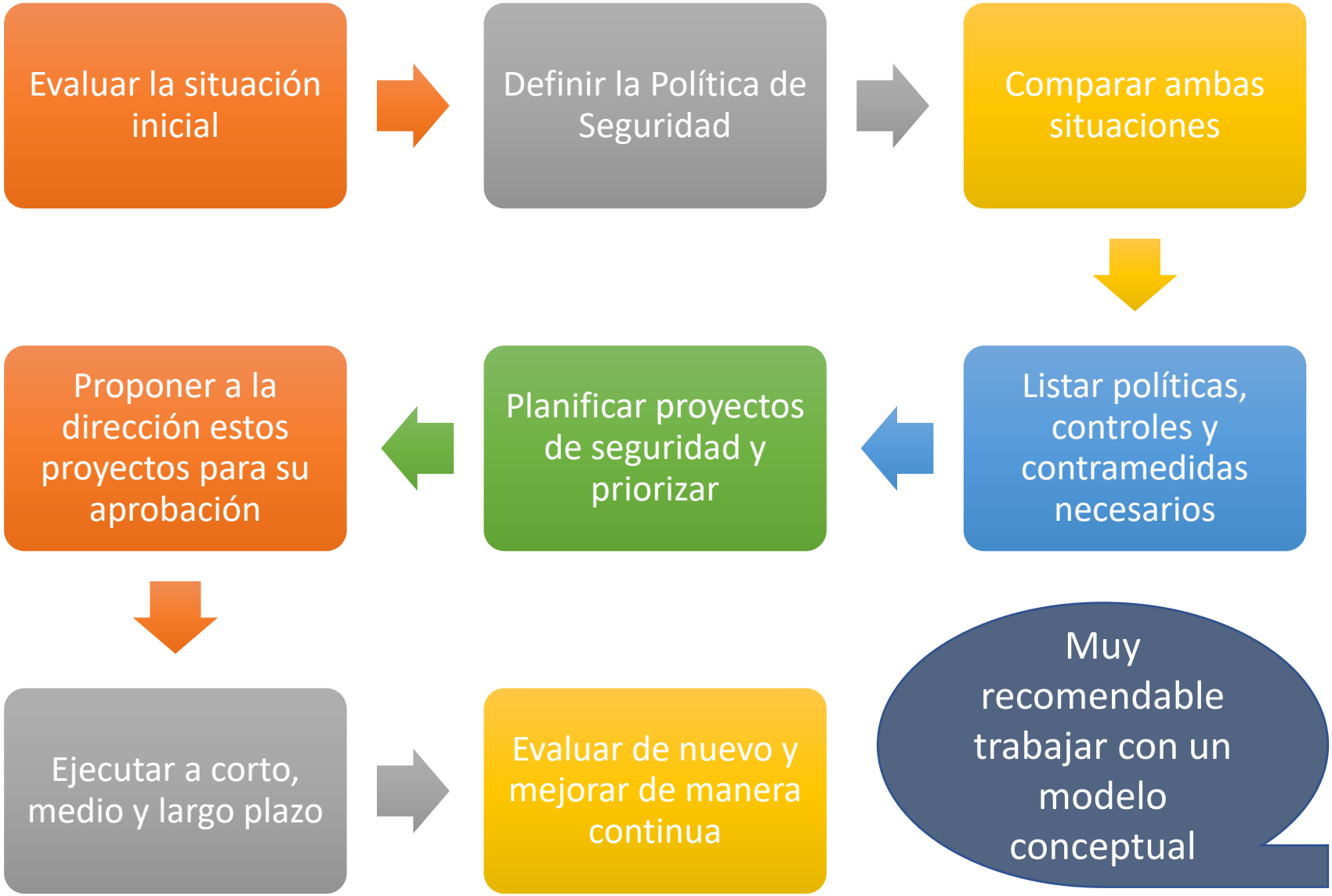
Plan Director de Seguridad

El CISO debe implementar el **Sistema de Gestión de la Seguridad de la Información (SGSI)**, pudiendo seguir estándares como el ISO/IEC 27001:2005.

El Plan Director de Seguridad consiste en "la **definición y priorización de** un conjunto de **proyectos** en materia de seguridad de la información dirigido a **reducir los riesgos** a los que está expuesta la organización hasta unos niveles aceptables".

Debe definir las **obligaciones y buenas prácticas** de seguridad que deberán cumplir los trabajadores de la organización así como terceros que colaboran con ésta, es decir, las **políticas de seguridad**.

Plan Director de Seguridad



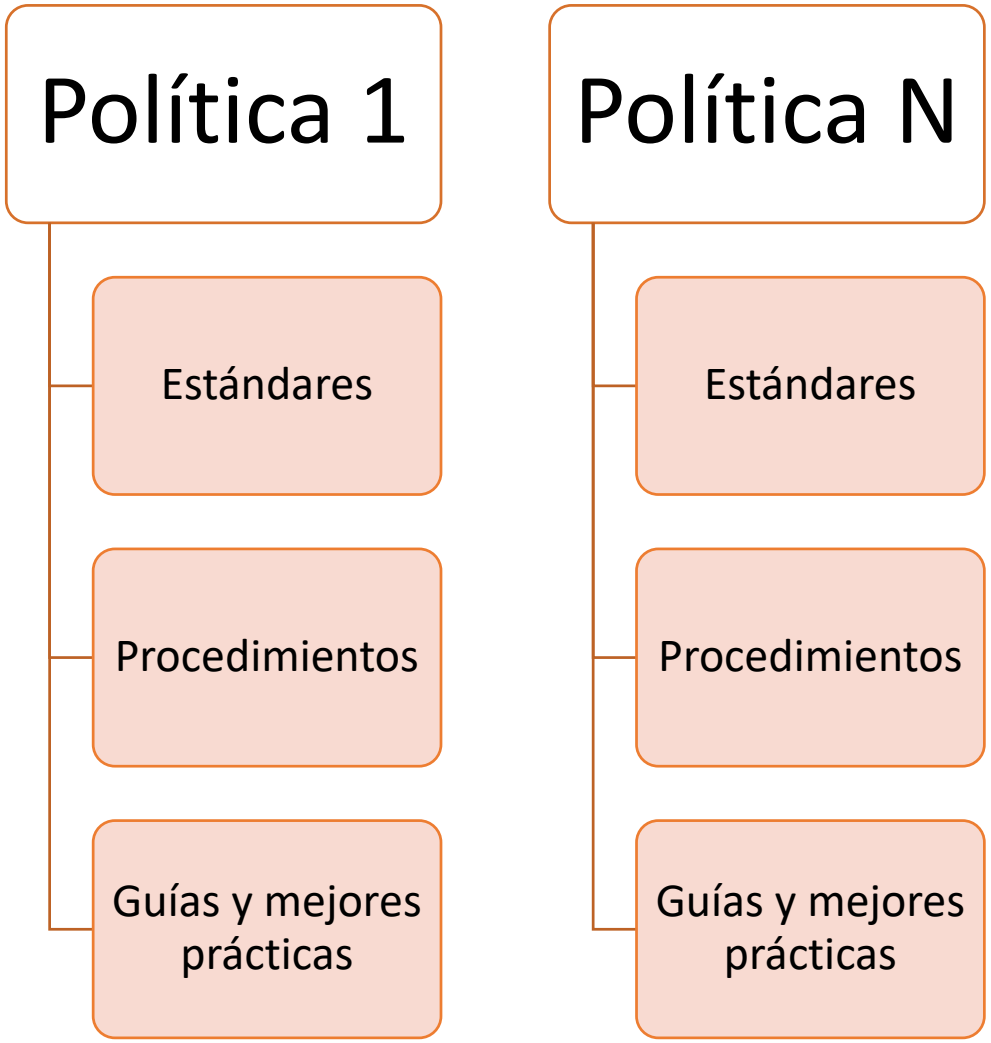
Políticas de Seguridad

Política de Seguridad (RFC 2196): declaración formal de las **reglas** que las personas que tienen acceso a la tecnología e información de una organización deben seguir, con el principal objetivo de **informar** a esos usuarios, empleados y gestores de sus **obligaciones para proteger los activos** de la organización

Políticas de Seguridad

Política: Enunciado corto que se aplica a toda la organización y que proporciona una línea de acción desde la dirección. Suele **definir un conjunto de reglas**.

Deben estar **bien documentadas y bien comunicadas**.



Políticas de Seguridad

- **Estándares**: Traducción de las políticas a detalles concretos de uso de HW y SW.
- **Procedimientos**: Instrucciones concretas acerca de cómo cumplir las políticas teniendo en cuenta los estándares. Suelen definir planes de instalación, testeo, administración, configuración, etc.
- **Guías y mejores prácticas:** Completan a los procedimientos con sugerencias que no son de obligado cumplimiento pero que pueden mejorar el nivel de cumplimiento de objetivos, facilitar el trabajo de administradores y usuarios, etc.

- Ejemplos de Políticas de Seguridad (Sans.org):

Acceptable Use Policy (AUP)

- Define lo que la organización permite y no permite hacer a los empleados con los activos que le pertenecen

Security Awareness Policy

- Especifica cómo se asegura que el personal tiene la conciencia necesaria acerca de SI

Asset Classification Policy

- Define cómo se realiza el inventario y clasificación de los activos de la organización en función de su criticidad para el funcionamiento de la organización

Gestión de políticas BYOD

SOSTENIBILIDAD

Mantenga una experiencia de usuario positiva.
Aunque las preocupaciones por los costes y la seguridad son temas importantes a tratar, la sostenibilidad del programa BYOD dependerá de si se ofrece una experiencia de usuario positiva de manera constante a largo plazo.

SELECCIÓN DE DISPOSITIVOS

Se trata de un concurso de popularidad.
Haga una encuesta entre los empleados para determinar qué dispositivos y plataformas utilizan actualmente y tienen intención de comprar. Cuando se lance el programa, incluya tantos de estos dispositivos como sea posible para maximizar la participación de los empleados.

MARKETING INTERNO

Cree su «marca» informática.
Fomente su programa de BYOD como iniciativa corporativa para apoyar el equilibrio entra la vida profesional y personal gracias a una mayor movilidad y flexibilidad; además, convierta el departamento informático en un aliado de los empleados móviles y modernos.

RESPONSABILIDAD

Proteja a su empresa de acciones legales.
Defina y ponga en práctica políticas y procedimientos claros que protejan a su empresa de las distintas amenazas, desde la pérdida de propiedad intelectual y de datos confidenciales de los clientes, hasta acciones legales, multas y daños a la reputación resultantes la filtración de datos.

DISEÑO Y GOBERNANZA DE APLICACIONES

Exija seguridad sin poner en riesgo la experiencia del usuario.
En un entorno de BYOD, las aplicaciones abarcan datos corporativos confidenciales que pueden quedar comprometidos si, accidentalmente, el dispositivo se pierde o se convierte en el blanco de un ataque móvil. Por lo tanto, su organización querrá contar con suficiente visibilidad y control para proteger las aplicaciones y los datos corporativos sin tener que supervisar la actividad personal de los usuarios en sus propios dispositivos.

EXPERIENCIA Y PRIVACIDAD DEL USUARIO

Establezca la confianza de los empleados.
Una comunicación clara con respecto a la privacidad y la creación de un contrato social entre la empresa y sus empleados que defina claramente la relación del programa BYOD son fundamentales para establecer la confianza de los empleados.

SEGURIDAD DE TIPO CONFIANZA CERO

Mitigue los riesgos de seguridad.
Es absolutamente esencial crear un modelo de confianza que identifique cómo y cuándo un dispositivo está infringiendo el cumplimiento, los pasos para corregir problemas y hasta qué punto estas medidas son aceptables para los usuarios.

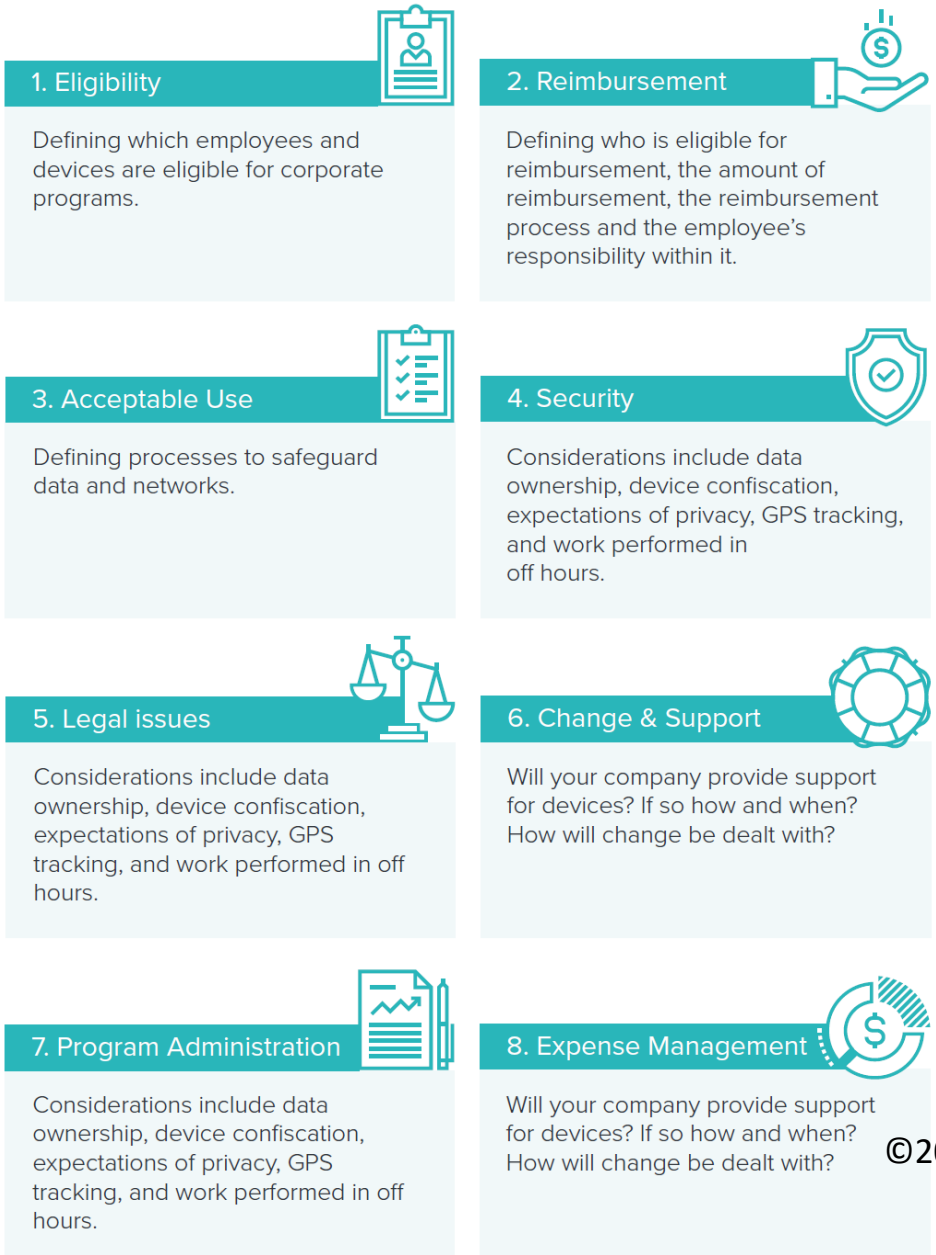
FACTOR ECONÓMICO

Controle los costes de implantar un programa BYOD.
Determine cuál es la mejor forma de estructurar los aspectos financieros de su programa BYOD para que su empresa obtenga el máximo retorno de la inversión.

© MobileIron

Gestores SW de dispositivos BYOD

Universidad Rey Juan Carlos



2. Internet of Things (IoT)

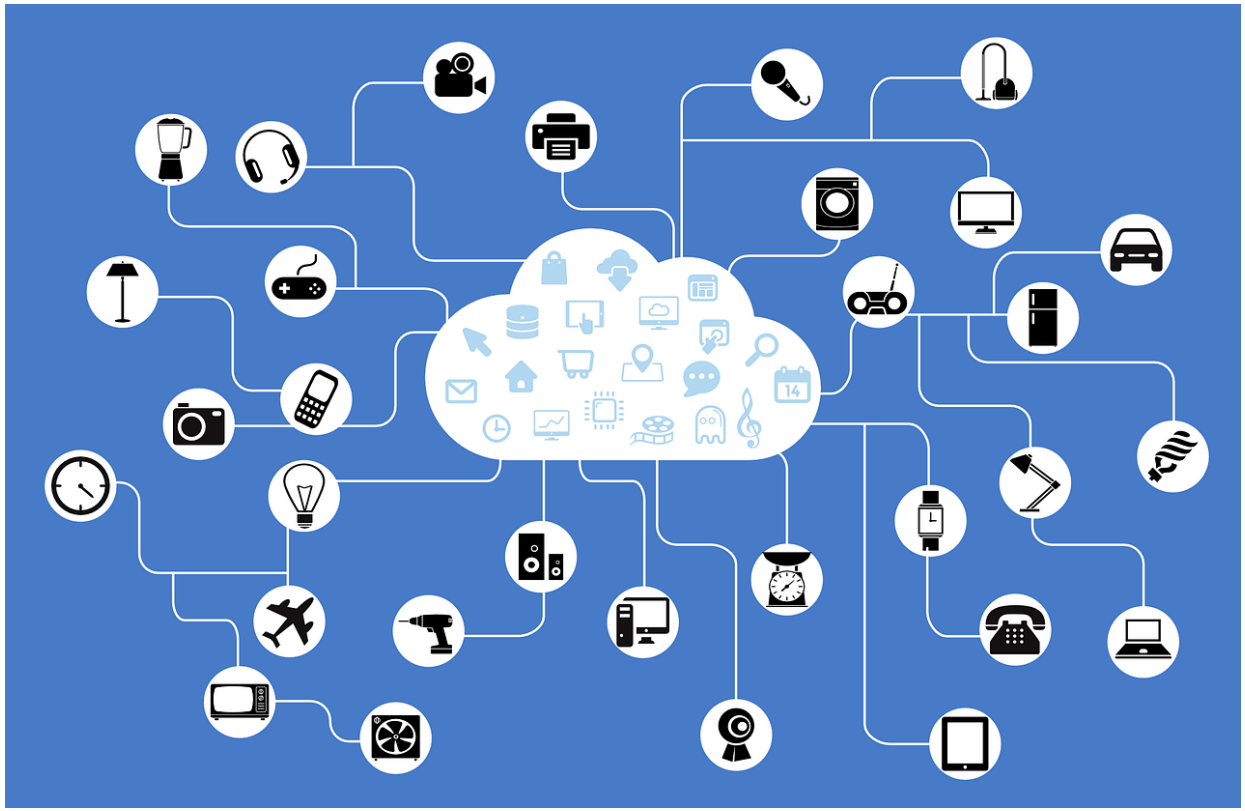
- Introducción a IoT
- Arquitectura y protocolos en IoT
- Seguridad en IoT

Materiales basados principalmente en:

- Cisco Internet of Things Security

Definición de IoT:

- "Concepto que se refiere a una interconexión digital de objetos cotidianos con Internet" (Wikipedia)

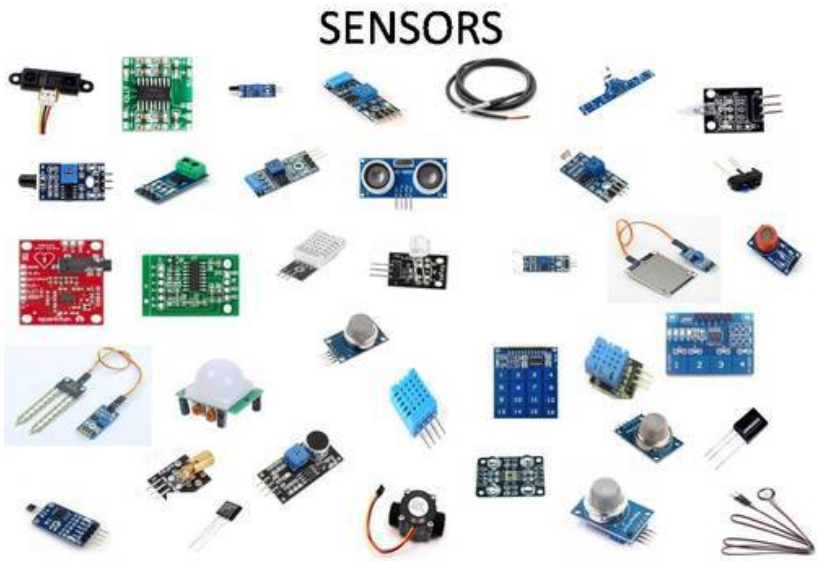


El término IoT va mucho más allá, y engloba **objetos comunes** que hasta ahora no disponían de conectividad. Con esta evolución, algunos elementos como neveras, hornos, lavadoras, coches, relojes, televisores y un largo etcétera disponen ya de conexión a Internet. La conectividad de estos elementos permite, entre otras muchas cosas, controlar el objeto de forma remota a través de otro dispositivo o una aplicación a través de Internet.

- Nikola Tesla, en una entrevista de la revista Colliers en 1926, ya hablaba de la interconexión de todo en lo que él denominó *gran cerebro*.

"Cuando lo inalámbrico esté perfectamente desarrollado, el planeta entero se convertirá en un gran cerebro, que de hecho ya lo es, con todas las cosas siendo partículas de un todo real y rítmico… y los instrumentos que usaremos para ellos serán increíblemente sencillos comparados con nuestros teléfonos actuales. Un hombre podrá llevar uno en su bolsillo"

El concepto de *Internet de las cosas* fue propuesto en 1999, por Kevin Ashton, en el Auto-ID Center del MIT, donde se realizaban investigaciones en el campo de la identificación por radiofrecuencia en red (RFID) y tecnologías de sensores.



Introducción a IoT

- Gartner informa que en 2019 había 14.200 millones de dispositivos IoT conectados y anticipa unos 25.000 millones para 2021.
- IDC data estima que se conectarán unos 152.200 dispositivos IoT cada minuto en 2025 (eso son 80 mil millones de dispositivos conectados al año)
- Fortune Business Insights indica en un informe que el mercado global de IoT, valorado en $190.000 millones en 2018, alcanzará los $1.11 billones en 2026.

- Localización de dispositivos IoT

Beneficios de IoT:

- Eficiencia energética (termostatos inteligentes)
- Dispositivos clínicos de monitorización continua
- Monitorización de actividad física y deportiva
- Conectividad
- Eficiencia
- Facilidad
- Personalización

En IoT se distinguen fundamentalmente tres tipos de dispositivos:

- Los **sensores**, son los que se encargan de medir una o varias magnitudes físicas.
- Los **controladores o *cerebros***, a partir de los valores obtenidos por los sensores, son capaces de interpretar dichos valores y decidir si llevar a cabo o no una acción determinada.
- Los **actuadores**, son aquellos, que mediante acciones mecánicas; eléctricas o químicas, ejecutan la acción del controlador.

IoT y el Big Data

- Los datos son la información que proviene de una variedad de fuentes, como personas, imágenes, texto, sensores, sitios web y dispositivos de tecnología.
- Hay tres características que indican que una organización puede estar haciendo frente a datos masivos:
  - Una gran cantidad de datos que requiere cada vez más espacio de almacenamiento (volumen).
  - Una cantidad de datos que crece exponencialmente rápido (velocidad).
  - Datos que se generan en diferentes formatos (variedad).
- Ejemplos de volúmenes de datos recopilados por los sensores:
  - Un automóvil autónomo puede generar 4000 gigabits (Gb) de datos por día.
  - Un hogar inteligente conectado puede producir 1 gigabyte (GB) de información de la semana.

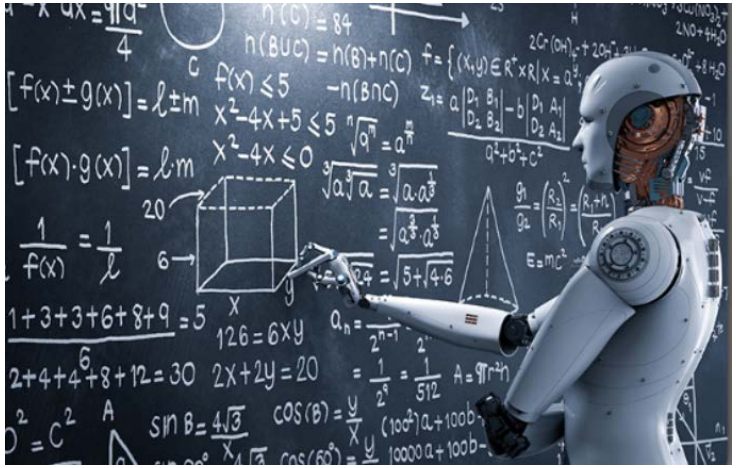
IoT y el Big Data

IoT y la automatización

- La Inteligencia artificial (AI) es la inteligencia que demuestran las máquinas.
  - La AI utiliza agentes inteligentes que pueden percibir el entorno y tomar decisiones.
  - La AI hace referencia a los sistemas que imitan las funciones cognitivas normalmente asociadas a la mente humana, como el aprendizaje y la resolución de problemas.

El **aprendizaje automático (ML)** es un subconjunto de AI que utiliza técnicas estadísticas para otorgar a las computadoras la capacidad para "aprender" de su entorno.

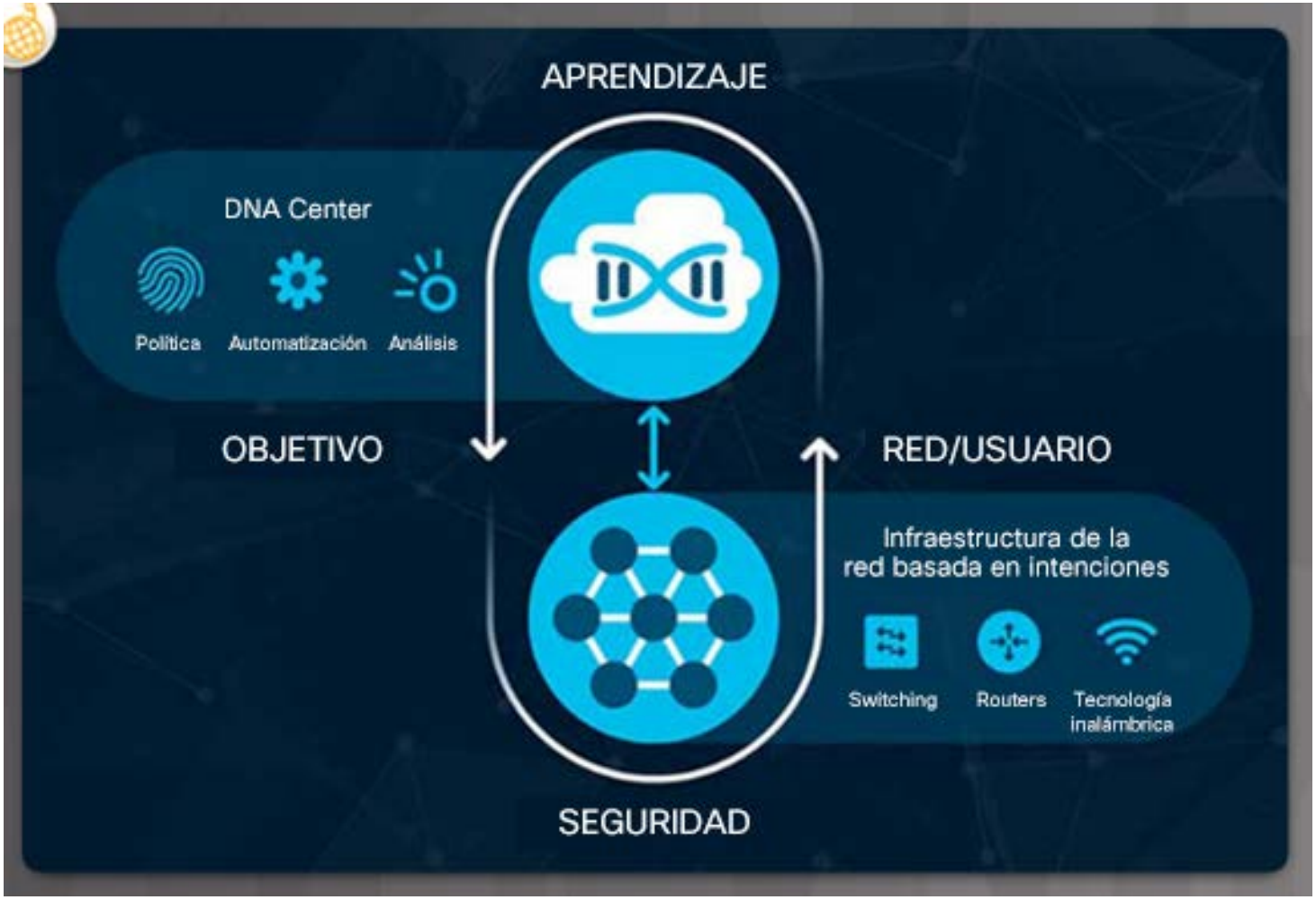
Esto permite que las computadoras mejoren su funcionamiento en una tarea puntual sin que se programe específicamente para esa tarea.



Redes Basadas en la Intención (IBN)

- La industria de TI crea un enfoque sistemático para vincular la administración de infraestructuras con la intención empresarial (IBN).
  - La red empresarial debe integran de manera segura y sin inconvenientes dispositivos de IoT, servicios basados en la nube y oficinas remotas.
  - La red debe proteger estas nuevas iniciativas digitales del panorama de amenazas en constante cambio.
  - La red debe ser lo suficientemente dinámica para adaptarse rápidamente a los cambios de las políticas y los procedimientos de seguridad, los servicios para empresas y las aplicaciones, y las políticas operativas.

Redes Basadas en la Intención (IBN)



IoT y la automatización

- Las redes basadas en la intención aprovechan el poder de la automatización la AI y el ML para controlar la función de una red a fin de lograr un propósito o una intención específica.
  - La red es capaz de traducir la intención en las políticas y, a continuación, usar la automatización para implementar las configuraciones adecuadas necesarias.
- El modelo de redes basadas en la intención consiste en tres elementos clave:
  - **Aseguramiento**: verificación de extremo a extremo del comportamiento de toda la red.
  - **Traducción:** capacidad para aplicar la intención empresarial en la configuración de la red.
  - **Activación**: ocurre después de que se haya especificado la intención y se hayan creado las políticas.

Modelo de redes basado en intenciones

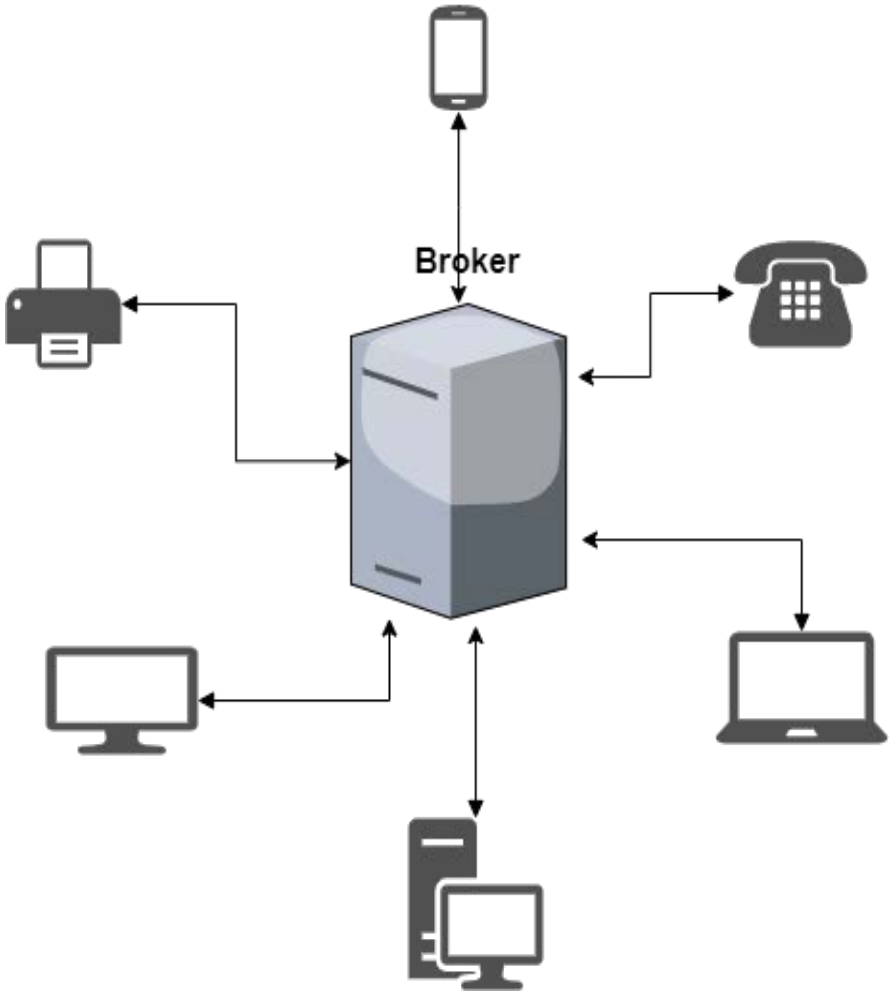
Arquitectura y protocolos en IoT

Los dispositivos IoT se caracterizan por tener **poco almacenamiento**, tener una **capacidad reducida de procesamiento** y utilizar **baterías**. Debido a estas restricciones, la comunicación entre ellos presenta los siguientes retos:

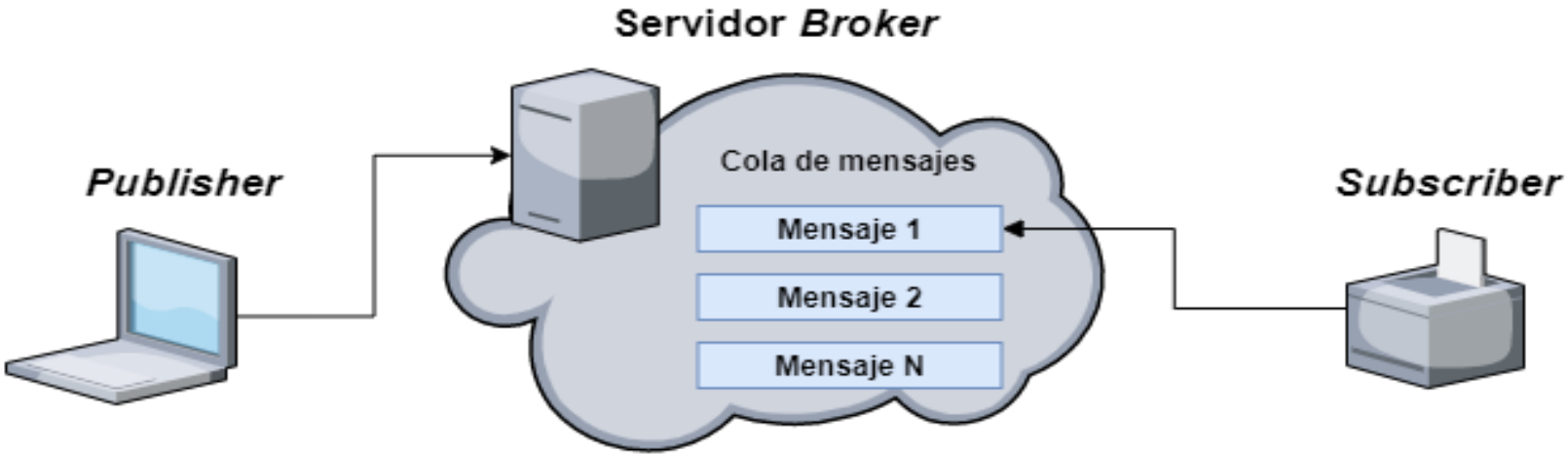
- Direccionamiento e identificación
- Comunicaciones con bajo consumo de energía
- Comunicaciones de alta velocidad y sin pérdidas
- Protocolos eficientes y con bajos requerimientos de memoria
- Movilidad

Arquitectura de red en IoT

- Servidor de notificaciones centralizado: es la arquitectura más utilizada, donde un servidor central (*Broker* o *Router*) se encarga de recibir los mensajes de todos los dispositivos emisores y distribuirlos a los receptores.



- Metodología PubSub (*Publish* / *Subscribe*)
- Metodología RRPC (Router Remote Procedure Calls)
- Metodología híbrida entre las dos anteriores.
- Modelo REST de HTTP



Protocolos en IoT

Capa de enlace:

- IEEE 802.15.1 o Bluetooth
- Bluetooth Low Energy (BLE)
- IEEE 802.15.4
- Radio Frequency Identification (RFID)
- Near Field Communication (NFC)
- IEEE 802.11 (WiFi) y 802.11 Low Power
- Z-Wave
- Especificaciones LPWA (Low Power Wide Area Networks): LoRa, LoRaWan, Sigfox o NWave

Protocolos en IoT

En la capa de aplicación también hacen falta protocolos específicos, pues los dispositivos IoT tienen características especiales, como:

- La cantidad de dispositivos conectados
- Heterogeneidad, es decir, el número y tipo de recursos es variable
- Independencia entre los dispositivos
- Tolerancia a fallos
- Escalabilidad, es decir, que se puedan añadir o eliminar dispositivos sin afectar al rendimiento del sistema
- Interoperabilidad
- Seguridad

Protocolos en IoT (hogar)

- **AllJoyn**. Es un estándar de código abierto, que facilita la comunicación entre dispositivos y aplicaciones, para todo tipo de protocolos de la capa de transporte.
- **HomePlug** y **HomeGrid** son protocolos cuya comunicación se realiza a través de la red eléctrica. Dependiendo del producto adquirido, el tipo de cifrado es diferente, incluso algunos dispositivos transmiten la información sin cifrar.
- **MFi** (*Made For iPhone/iPod/iPad*) es un protocolo de comunicaciones propio de Apple diseñado para interactuar con estos dispositivos. Los dispositivos y elementos de conexión de Apple incorporan un chip mediante el cual verifican que tanto los dispositivos, como los cables de conexión son originales.
- **OCF** (*Open Connectivity Foundation*) es un proyecto de código abierto que ofrece interconectividad con la filosofía *just-works*. Este protocolo pretende garantizar la interoperabilidad de millones de dispositivos, gracias a una implementación de referencia (IoTivity) y un programa de certificación.
- **Thread** (*network protocol*) es una tecnología basada en IPv6 que utiliza cifrado AES. Por ello y por la flexibilidad que ofrece, es un protocolo muy seguro y está preparado para el futuro.

Protocolos en IoT (industria)

- MQTT (Message Queuing Telemetry Transport)
- AMQP (Advanced Message Queuing Protocol)
- WAMP (Web Application Messaging Protocol)
- CoAP (Constrained Application Protocol)
- STOMP (Streaming Text Oriented Messaging Protocol)
- XMPP (Extensible Messaging and Presence Protocol)
- WMQ (WebSphere MQ o IBM MQ)
- DDS (Data Distribution Service)
- OPC UA (Unified Architecture)

Seguridad en IoT

- Los sensores inteligentes en nuestros hogares aumentan la posibilidad de que surjan problemas de seguridad.
- Los sensores pueden proporcionar una manera para que los hackers accedan a nuestra red doméstica y obtengan acceso a cualquier PC y los datos que estén conectados a ella.
- Antes de adquirir sistemas de seguridad en el hogar, es muy importante investigar al desarrollador, y los protocolos de cifrado y seguridad instalados para sus productos.
- Las empresas de IoT no invierten lo suficiente en seguridad.

Seguridad en IoT

Universidad Rey Juan Carlos

Seguridad en IoT

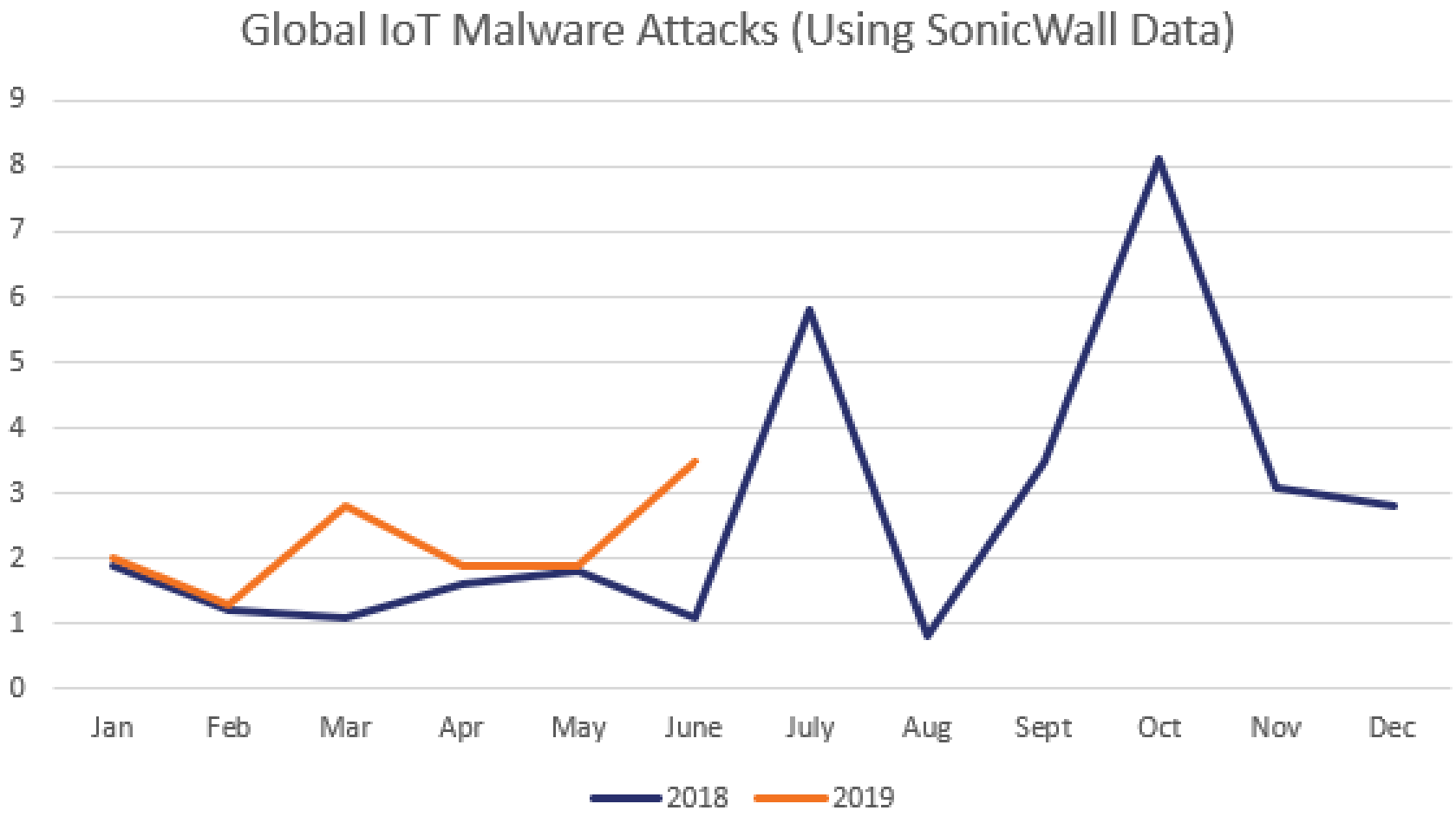
- Dyn is an internet performance management and web application security company founded in 2001 (acquired by Oracle Corporation in 2016) and based in the U.S. It offers products to optimize, control, and monitor online infrastructure.
- On October 21st, Dyn had a series of DDoS attacks targeting systems operated by this DNS provider. The attack affected a large amount of users in North America and Europe. The DDoS attack lasted roughly one day, with spikes coming and going up to **1.2Tbps**. It affected several large businesses and websites with high authority and traffic, such as: Airbnb, Amazon.com, Fox News, HBO, The New York Times, Twitter, Visa and CNN.
- The New World Hackers, Anonymous, and SpainSquad claimed responsibility for the attack, a hacktivist effort to retaliate for Ecuador's rescinding internet access to WikiLeak's founder Julian Assange at their embassy in London where he had asylum. No has confirmed this as the reason.
- Dyn stated that according to risk intelligence firm FlashPoint, this was a botnet coordinated through a large number of IoT-enabled devices, including baby monitors, cameras, and residential gateways that had been infected with *mirai malware*.

Seguridad en IoT

- **Malware GreyEnergy amenaza infraestructuras críticas desde 2015** (17/10/2018)
- **Fuga de información en un casino a través de un termostato IoT** (15/04/2018)
- **Vulnerabilidad en GoAhead podría afectar a miles de dispositivos IoT** (18/12/2017)
- **Cientos de miles de cámaras IP utilizadas para el mayor ataque DDoS** (13/09/2016)

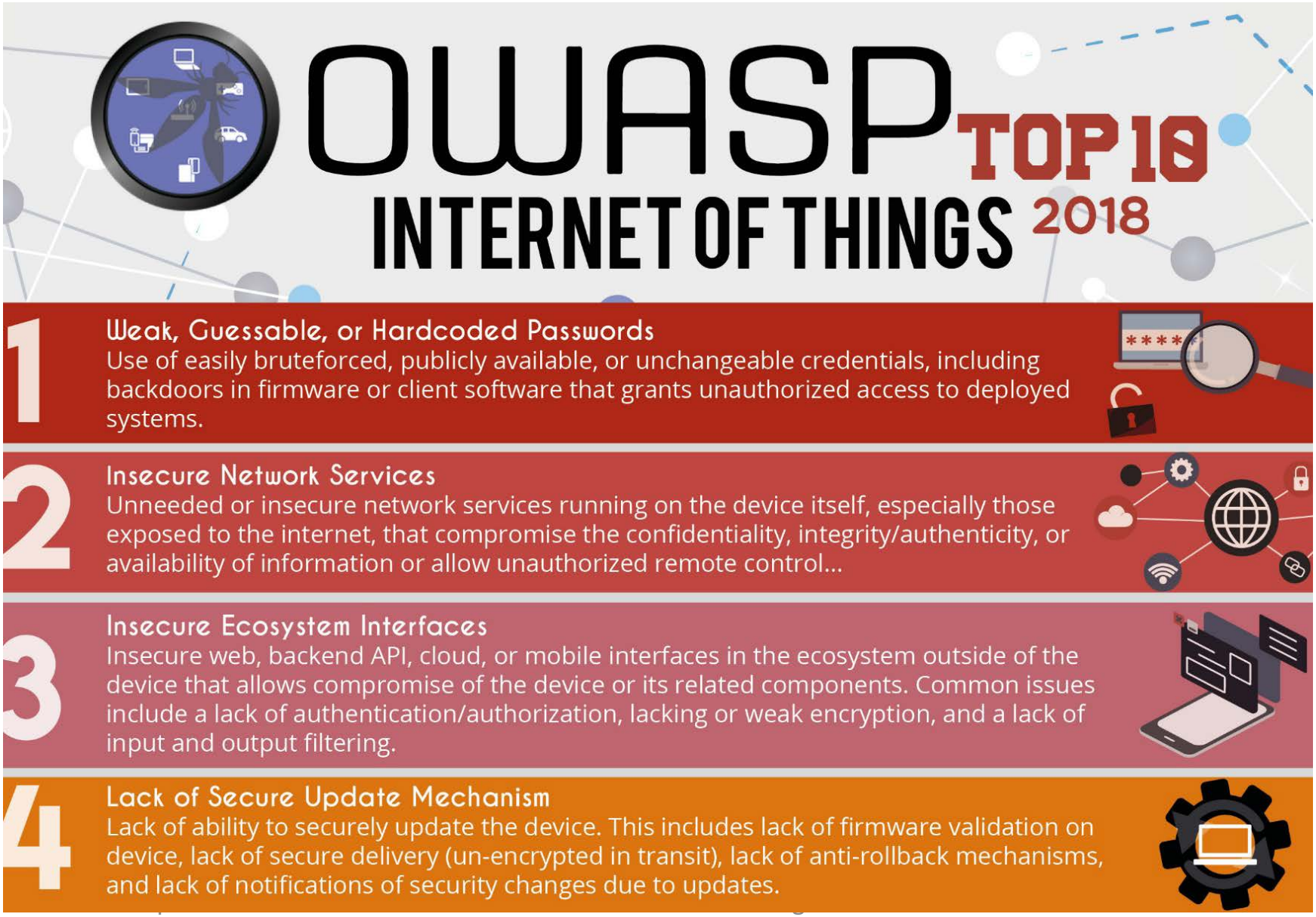
- Aruba HPE afirma que el 84% de las empresas que han adoptado IoT han informado de alguna brecha de seguridad

Seguridad en IoT



Seguridad en IoT

Universidad Rey Juan Carlos



Seguridad en IoT

5 Use of Insecure or Outdated Components
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

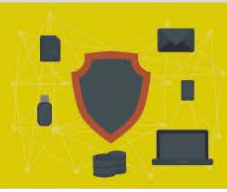
6 Insufficient Privacy Protection
User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

7 Insecure Data Transfer and Storage
Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

8 Lack of Device Management
Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.

9 Insecure Default Settings
Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

10 Lack of Physical Hardening
Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.




IoT
Security Foundation


WE'RE
CONNECTED

Modelo de referencia IoT

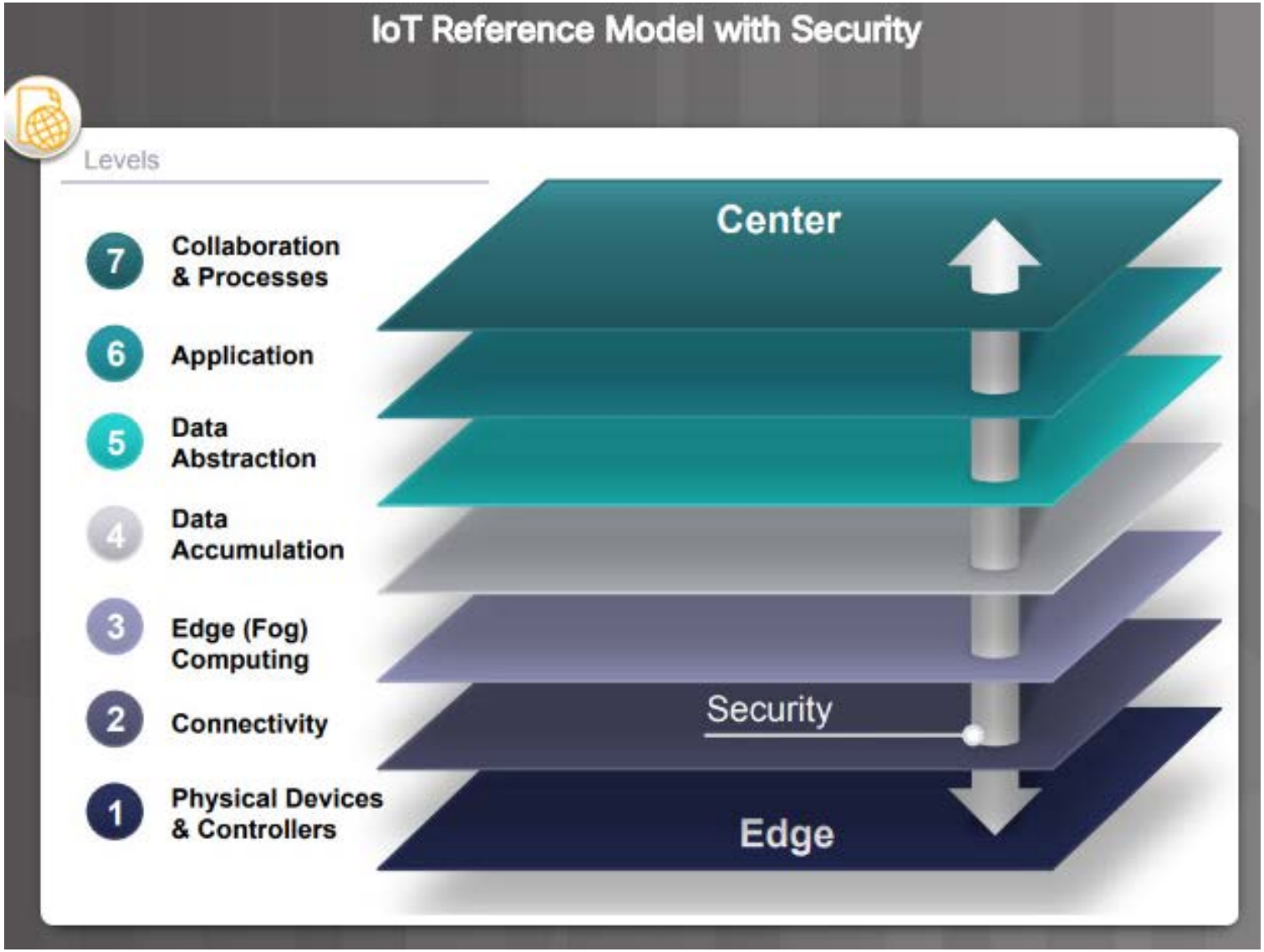
Universidad Rey Juan Carlos

IoT Reference Model

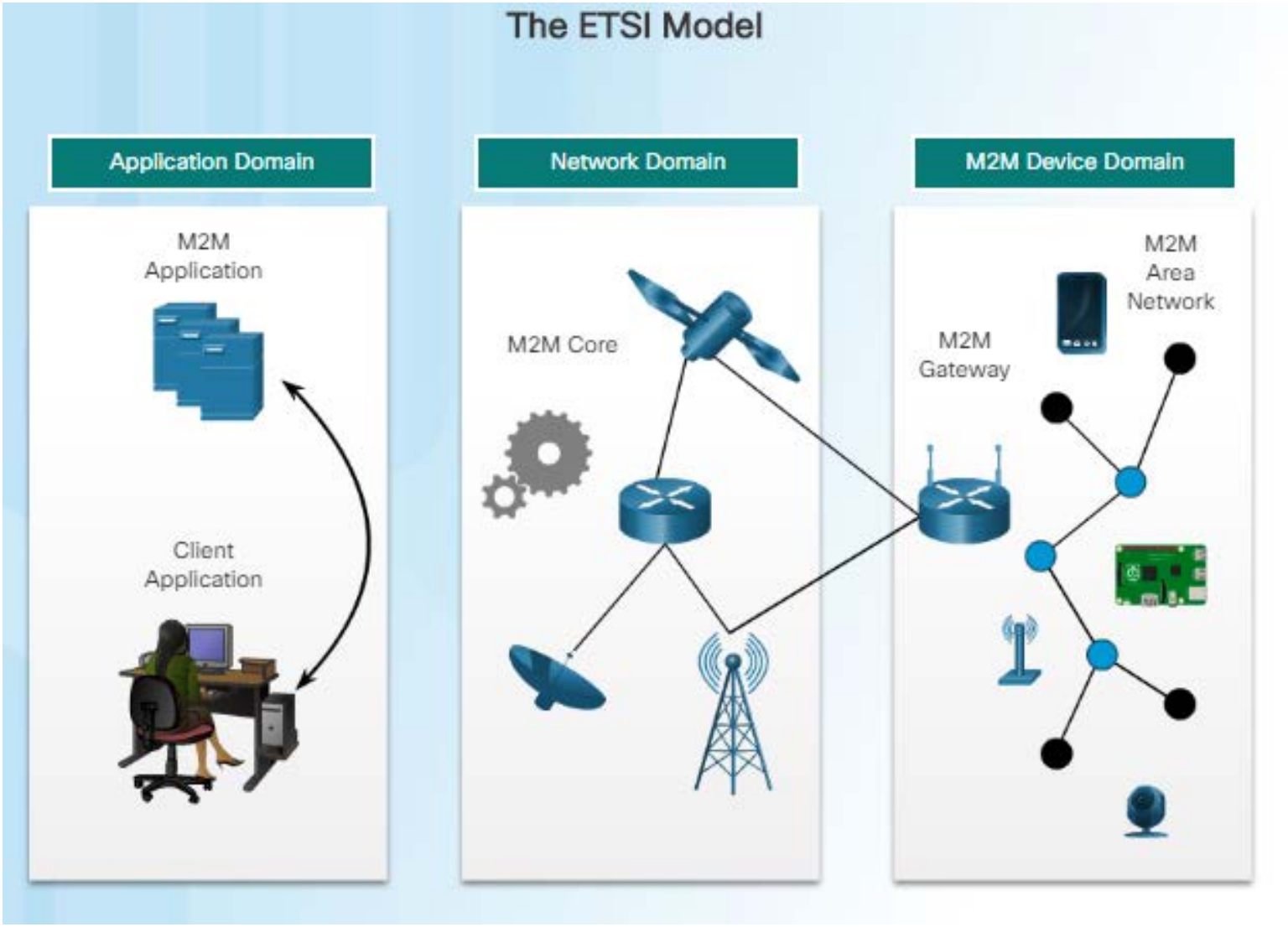
Level		Description
7	Collaboration & Processes (Involving people and business processes)	Transcends multiple applications to include the communication and collaboration required between people and business processes.
6	Application (Reporting, analytics, control)	Information interpretation based on the nature of the device data and business needs.
5	Data Abstraction (Aggregation and access)	Focused on rendering the data and its storage in ways to enable application development.
4	Data Accumulation (Storage)	Data in motion is converted to data at rest. The data is also transformed so that it can be consumed by upper levels.
3	Edge (Fog) Computing (Data element analysis and transformation)	Converts data into information that is suitable for storage and higher level processing.
2	Connectivity (Communication and processing units)	Responsible for reliable and timely data transmission between devices and the network, across networks, and between the network and data processing in Level 3.
1	Physical Devices & Controllers (The "Things" of IoT)	Includes a wide range of endpoint devices that send and receive information.

Seguridad en Modelo de referencia IoT

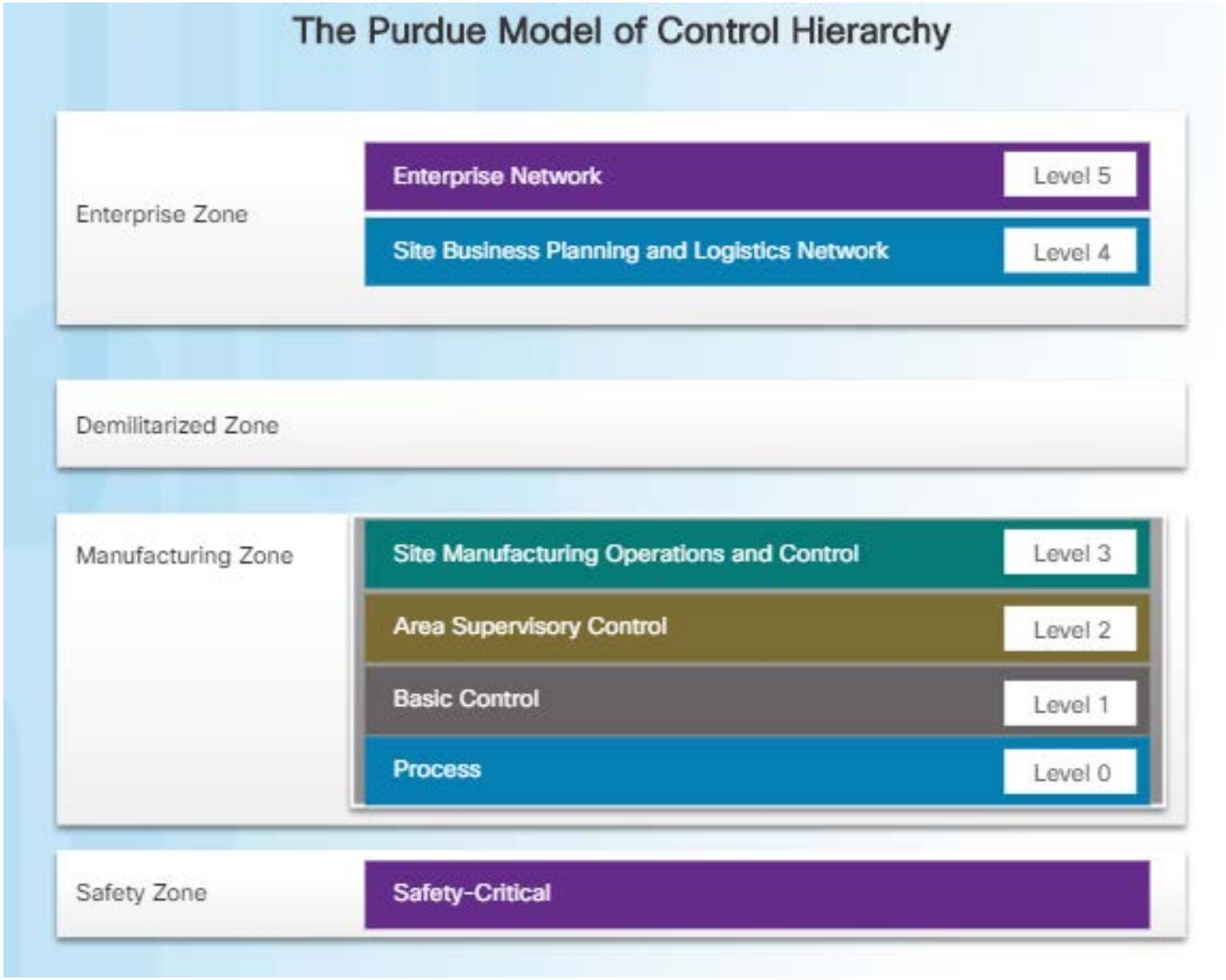
Universidad Rey Juan Carlos



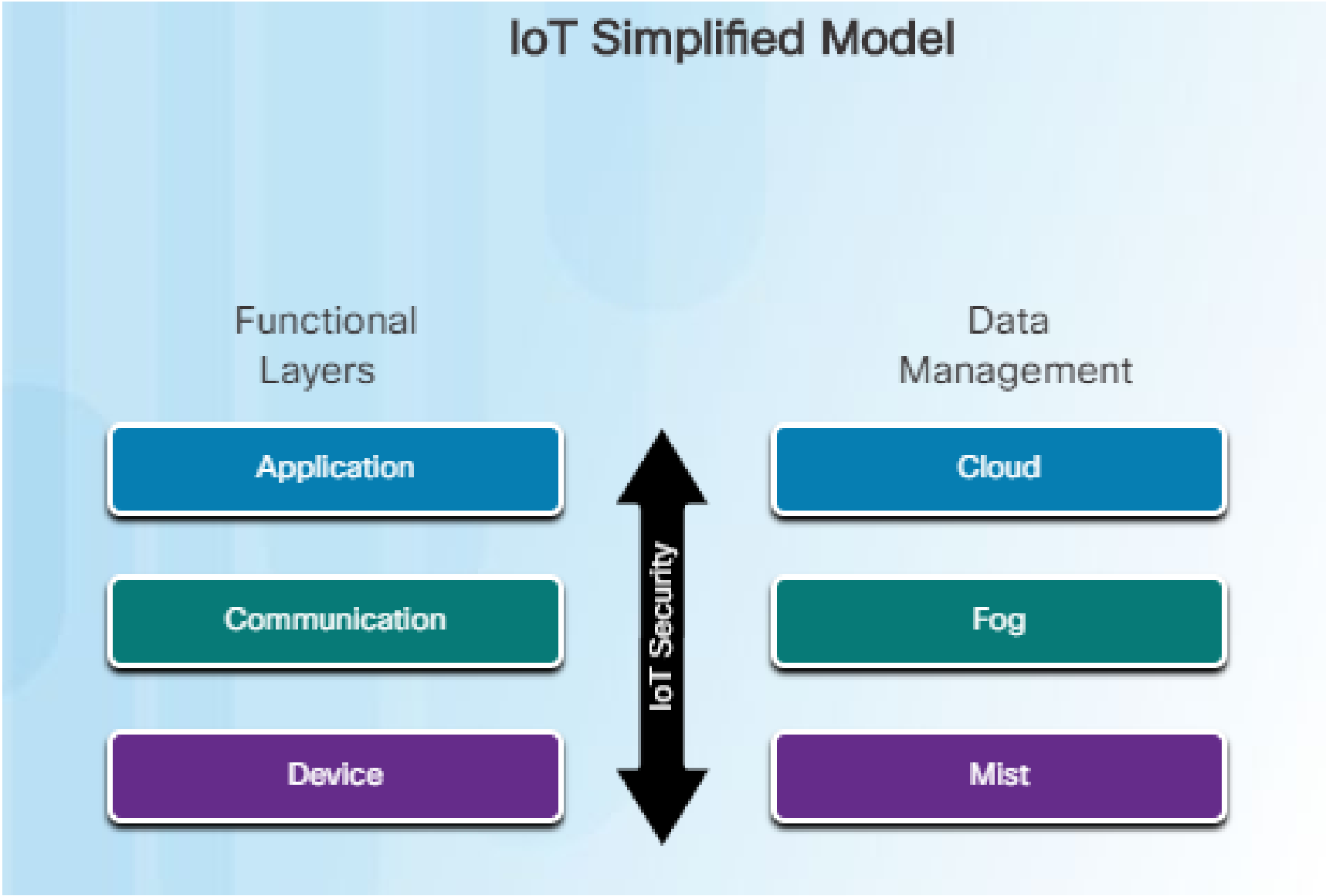
Arquitectura ETSI M2M



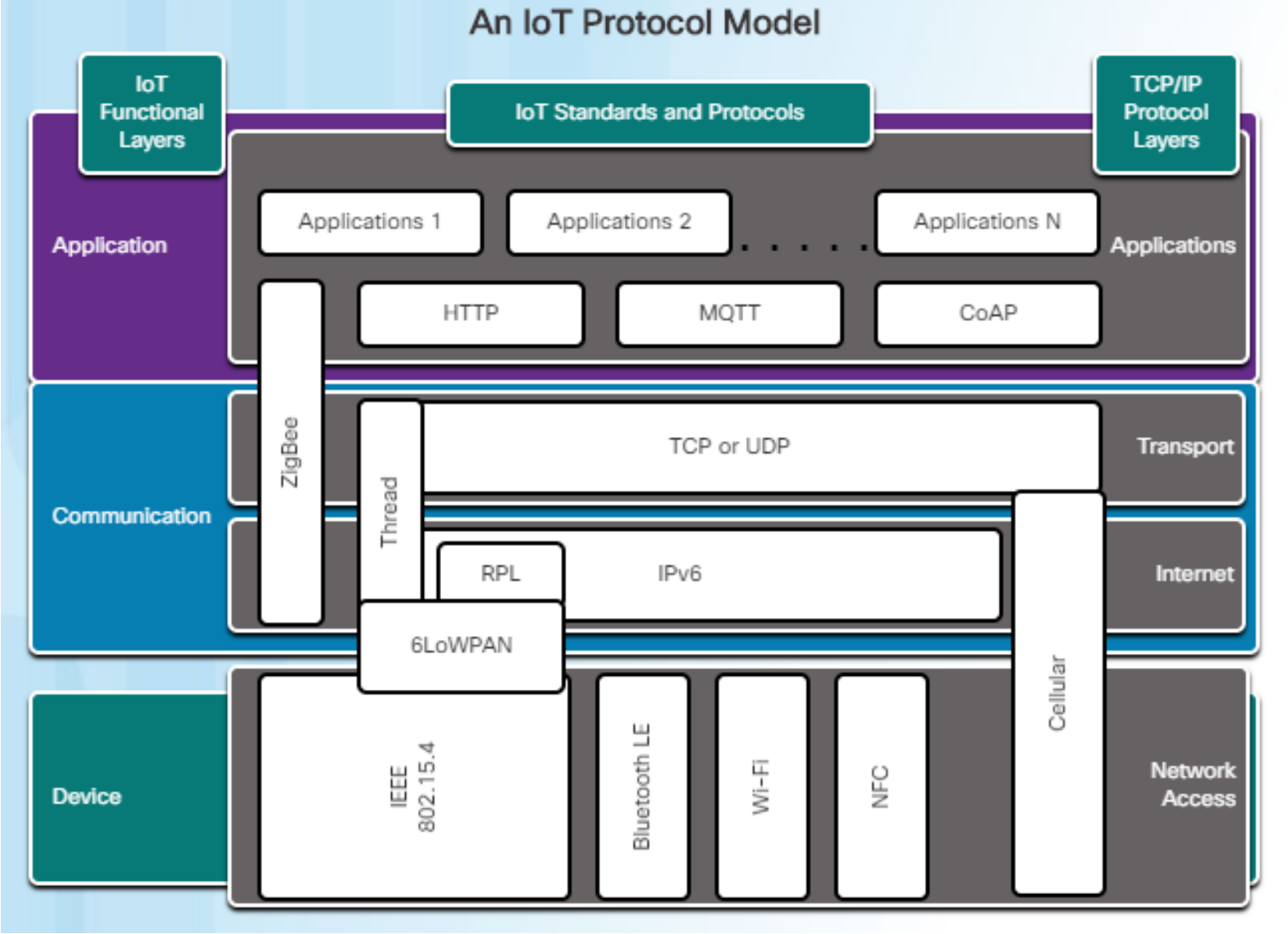
Otros modelos IoT



Modelo simplificado IoT

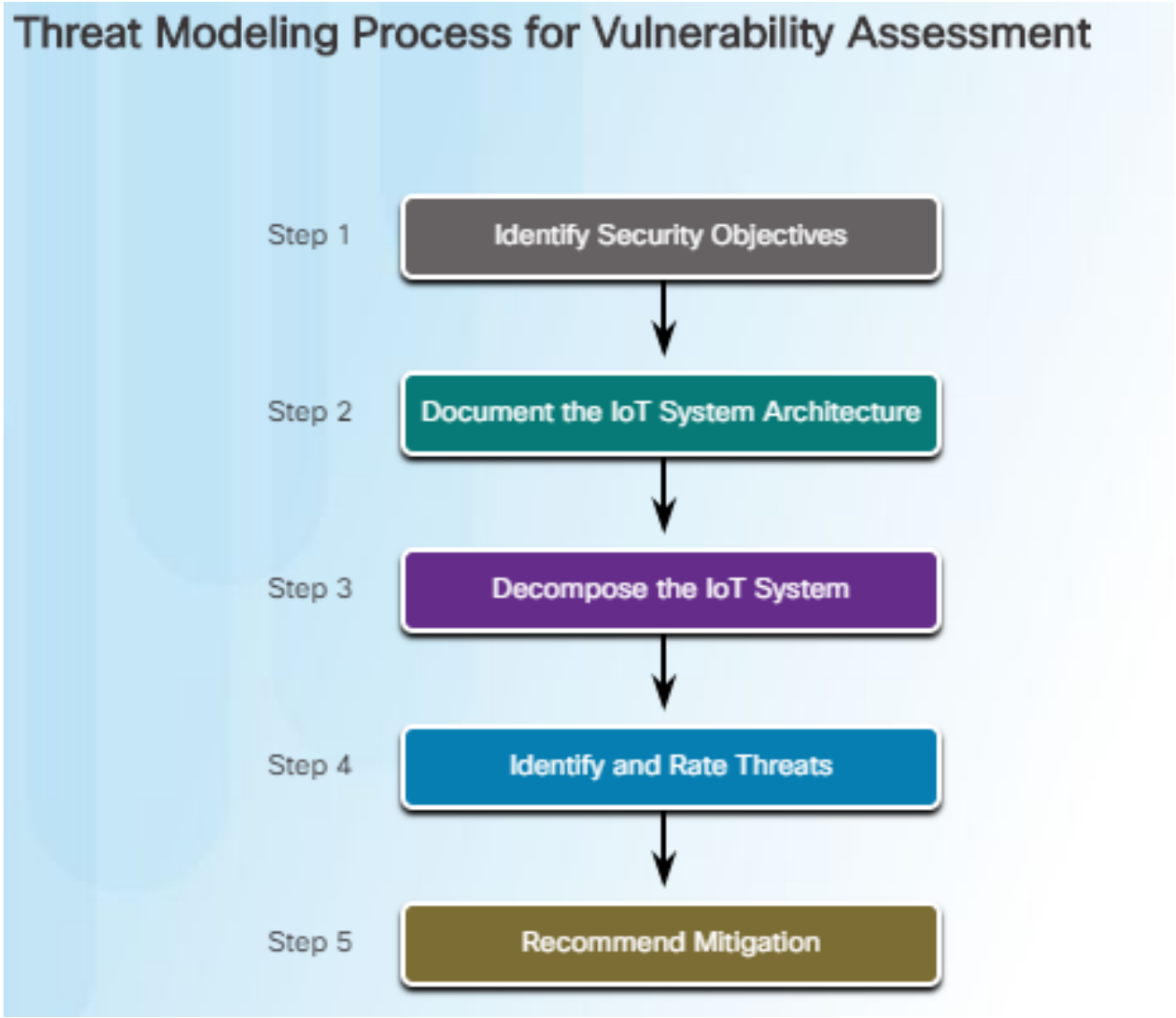


Modelo de Seguridad en IoT



Modelo de análisis de amenazas en IoT

Universidad Rey Juan Carlos



Vectores de ataque en IoT

Universidad Rey Juan Carlos

Los dispositivos IoT son **sistemas empotrados**, menos complejos que los PCs, los fabricantes implementan sus propias soluciones, descartando sistemas operativos de uso común como Windows, Android, Linux, etc. Es el propio fabricante de HW el que se encarga del **mantenimiento de su SW**, y no disponen de la experiencia y recursos para poder dar una respuesta aceptable ante posibles brechas de seguridad. Además, los dispositivos no se diseñaron inicialmente para estar conectados a la red. Algo similar sucede con los sistemas de control industrial (SCADA), diseñados para situarse en redes aisladas y actualmente se empiezan a conectar a Internet.

Vectores de ataque en IoT

- **Security by Default**: necesidad de establecer una configuración por defecto lo más segura posible para un dispositivo en su fabricación.
- Interfaz poco amigable, por lo que buscan una instalación sencilla por el usuario.
- Ubicación física de **fácil acceso**.
- Al disponer de **actuadores**, pueden hacer cambios en el "mundo real" que pueden afectar a la seguridad y salud de las personas.

Tipos de ataque en IoT

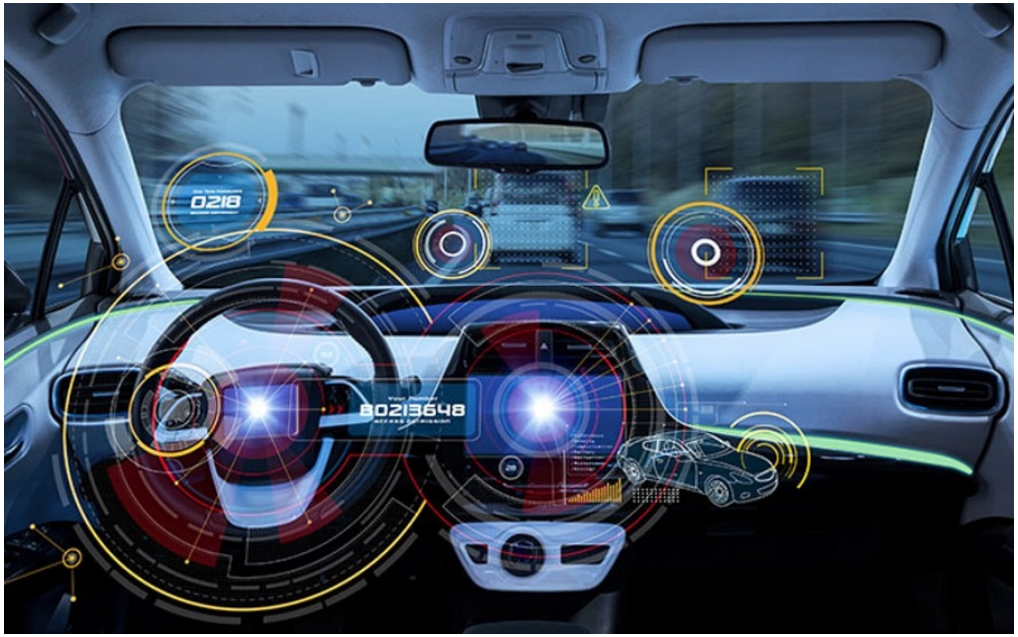
- Captura de nodos (Node Capture)
- Ataque de denegación de servicio (DoS)
- Denial of Sleep Attack
- Ataque distribuido de denegación de servicio (DDoS)
- Ataque de nodo falso (Fake Node/Sybil Attack)
- Ataque de reenvío de información (Replay Attack)
- Ataque de canal lateral (Side-Channel Attack)

Vectores de ataque en IoT

- **Ataque por fuerza bruta** para «obtener» una clave, normalmente la utilizada por el protocolo Telnet. El cual es utilizado por algunos dispositivos de IoT para el acceso de forma remota.
- **Ataques por denegación de servicio** que producen indisponibilidad de los dispositivos por saturación.
- **Utilización como plataforma de ataque hacia otros dispositivos** del entorno, ya que por defecto suelen estar menos fortificados y son más accesibles desde el exterior de la red donde se encuentran.
- **Obtención de datos** de carácter personal de los usuarios como: hábitos de uso, contraseñas de acceso a servicios web e incluso datos de tarjetas de crédito.

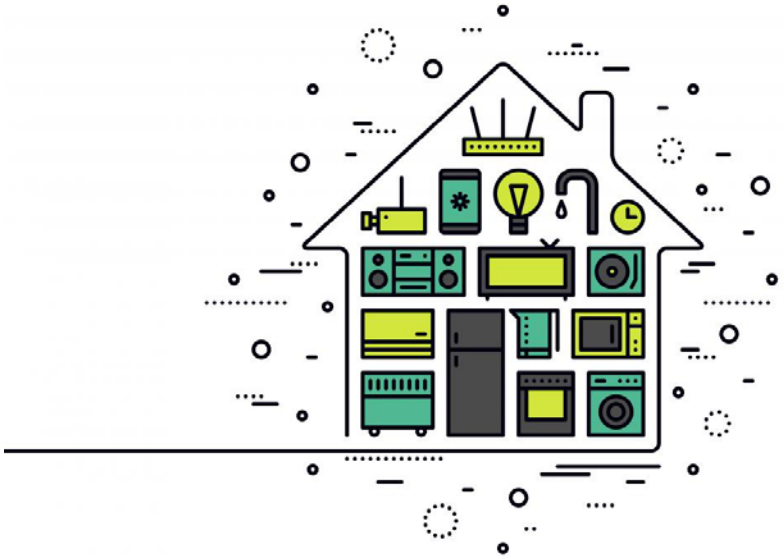
Seguridad en la comunicación

- Si la comunicación es vulnerable, un atacante puede acceder a datos privados o personales o a datos técnicos que puede usar para realizar otro ataque y controlar el dispositivo.
- Canal de comunicación cifrado para evitar MitM.



Seguridad en el software

- Sistema operativo
- Interfaces web públicas
- Uso de servicios en la nube
- Instalación / uso de aplicaciones de market propio
- Apps móviles



Seguridad en la configuración

- Más funcionalidades habilitadas por defecto de las necesarias
- Por ejemplo, protocolos o puertos en un router.

Seguridad en la autenticación/autorización

Universidad Rey Juan Carlos

- Uso de contraseñas seguras (forzar contraseñas seguras, que expiren, que no se repitan, que no sean las de por defecto…)
- Empleo del doble factor de autenticación
- Mecanismos de recuperación de contraseñas

Seguridad en el hardware

- Menos frecuentes pero más críticas
- Acceso físico al dispositivo
- Ingeniería inversa
- Acceso directo al almacenamiento (memoria o disco duro):
  - En memoria pueden estar las claves criptográficas, credenciales de acceso o información sensible
  - Contramedidas: antimanipulación y cifrado
- Borrado incorrecto de memoria
- Actualización del firmware

Seguridad en el hardware

- Hardware Sensors
  - Environment manipulation
  - Tampering
  - Damage
- Device Memory
  - Default username and password
  - Sensitive data
  - Plaintext usernames and passwords
  - Encryption keys
- Device Physical Interfaces
  - Removal of storage media
  - Reset to insecure state
  - Device ID/Serial number
  - Serial interface connections
  - User and Administrative access
  - Privilege escalation
- Device Firmware
  - Backdoor Accounts
  - Hardcoded credentials
  - Encryption keys
  - Firmware version display
  - Firmware version last update date
  - Vulnerable services
  - Security related function API exposure
- Firmware Update Mechanism
  - Update sent without encryption
  - Updates not signed
  - Update location writable
  - Update verification and authentication
  - Malicious update
  - Missing update mechanism
  - No manual update mechanism

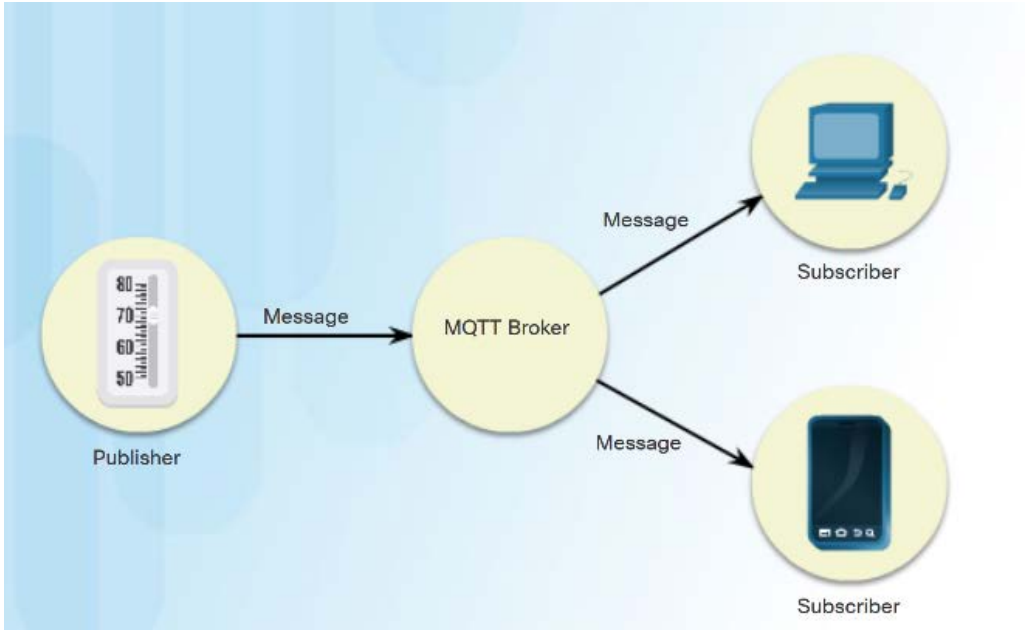
Seguridad en protocolos

Universidad Rey Juan Carlos

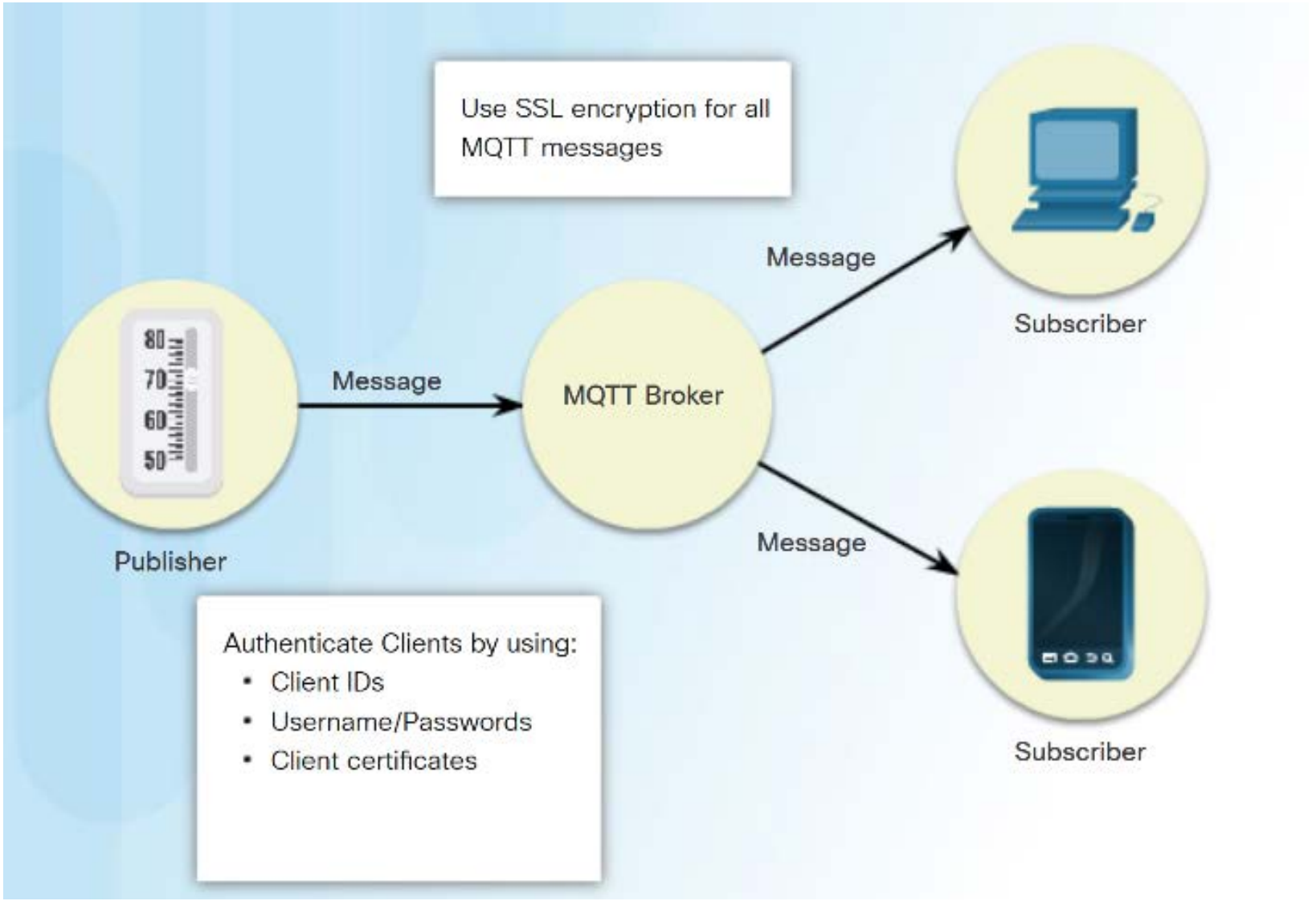
- Veamos ejemplos en:
  - MQTT
  - CoAP
  - UPnP

MQTT (Message Queuing Telemetry Transport)

- Desarrollado por IBM para IoT con comunicacion M2M
- Usa el modelo publish-subscribe
- Un cliente bien publica bien se suscribe a un topic o tema (humedad, temperatura, luz…)
- Diseñado para recoger mucha información de distintos dispositivos

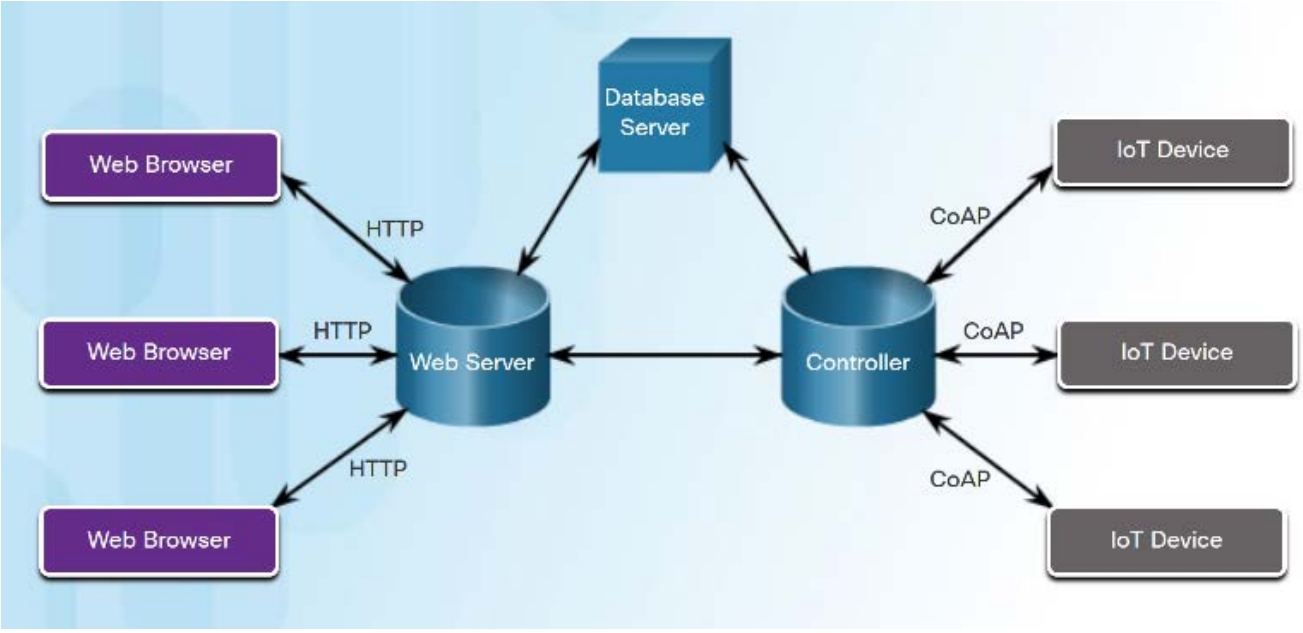


Seguridad en MQTT



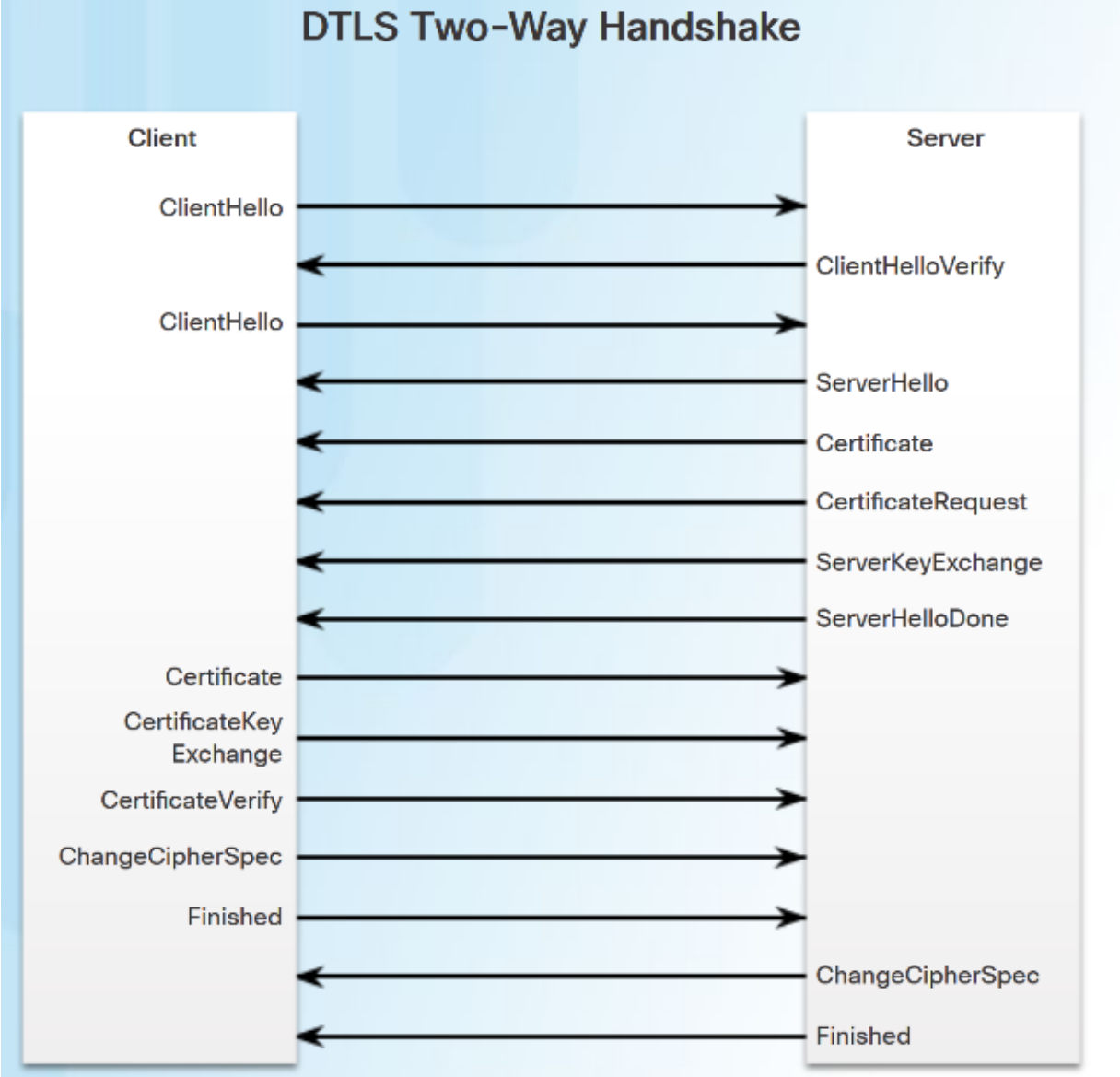
CoAP (Constrained Application Protocol)

- Diseñado para la comunicación M2M y usa UDP
- Sensores y otros nodos pueden conectarse y publicar entre sí, aunque sigue modelo cliente-servidor
- Soporta los métodos HTTP: GET, POST, PUT y DELETE
- Puede observar un recurso (muy útil informar a un servidor de cambios de estado

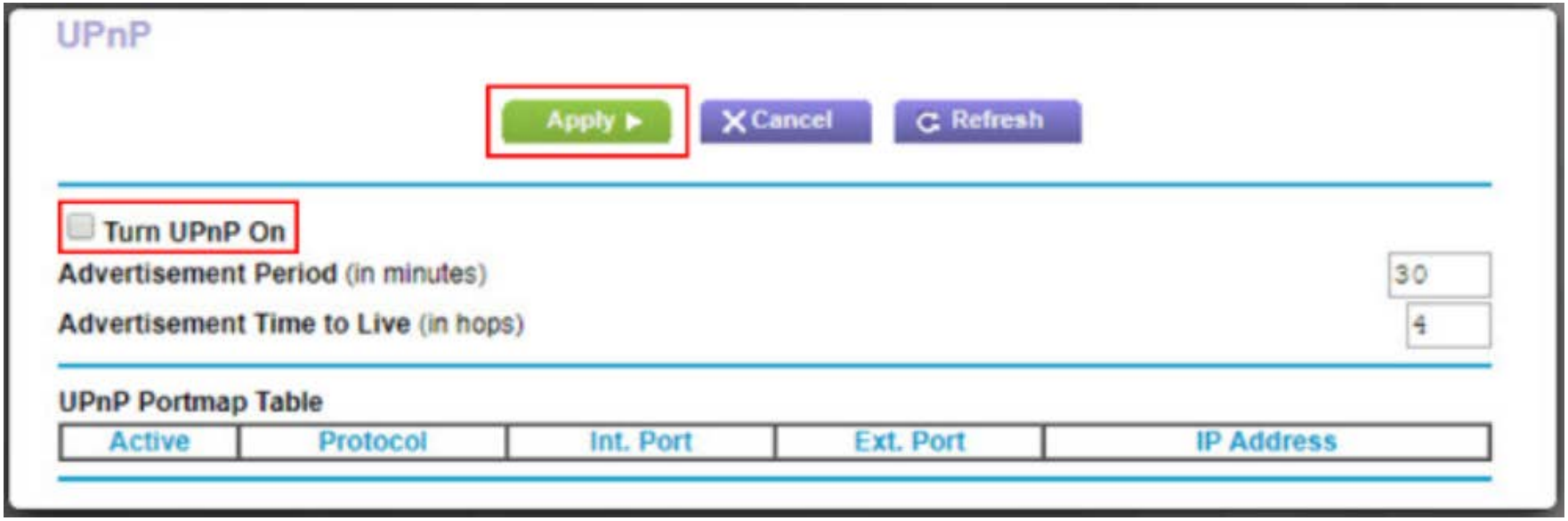


Seguridad en CoAP

Universidad Rey Juan Carlos



UPnP


UPnP
Apply
Cancel
Refresh
Turn UPnP On
Advertisement Period (in minutes)
30
Advertisement Time to Live (in hops)
4
UPnP Portmap Table
Active
Protocol
Int. Port
Ext. Port
IP Address

Seguridad en los usuarios

- Ingeniería social
- Phising

Modelos de control de acceso

Universidad Rey Juan Carlos

Un analista de seguridad debería familiarizarse con los diferentes modelos básicos de control de acceso para entender major cómo los atacantes los rompen

- Mandatory access control (MAC)
- Discretionary access control (DAC)
- Non-Discretionary access control
- Attribute-based access control (ABAC)

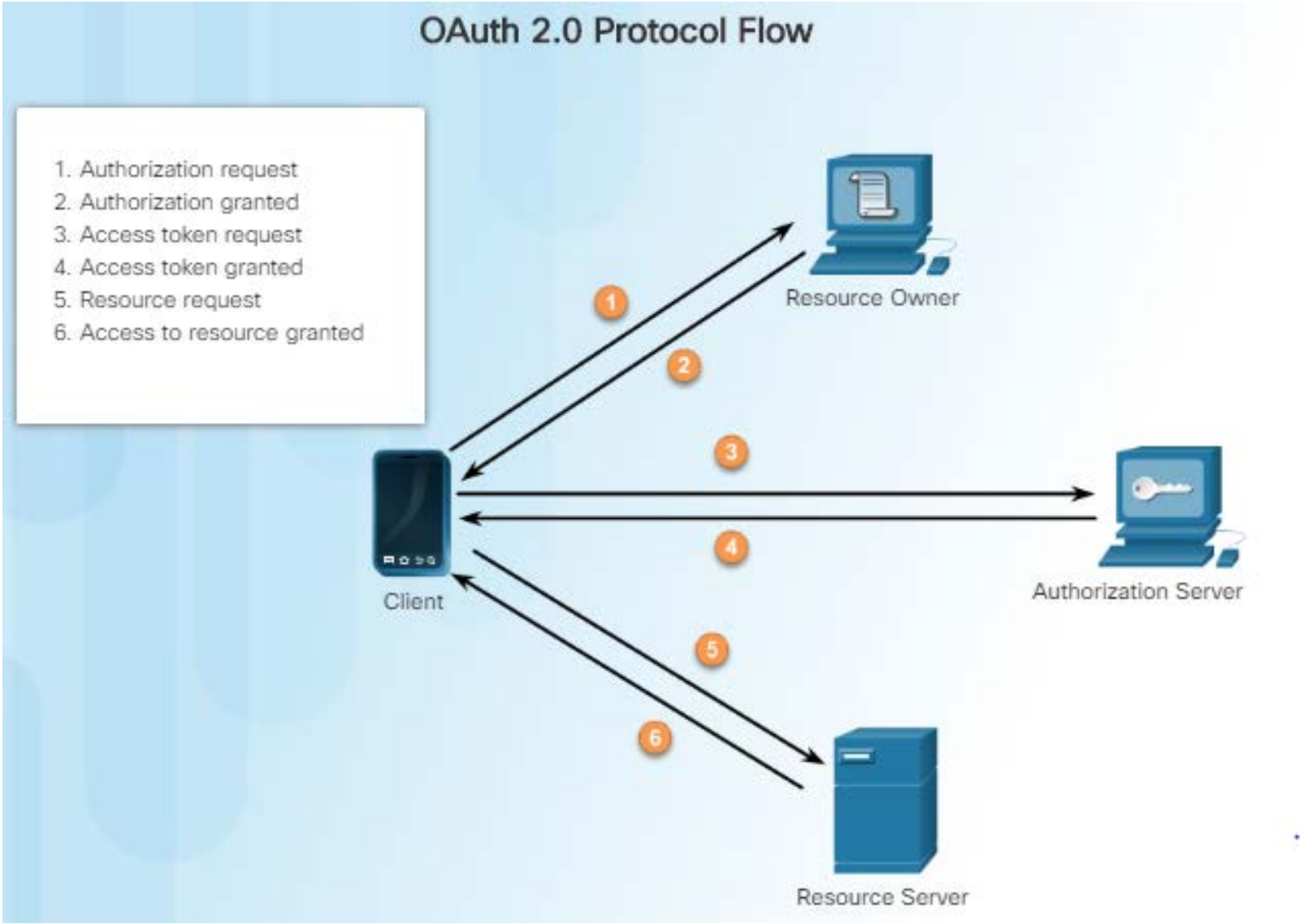
Dos aspectos importantes en el control de acceso son:

- Principio de mínimo privilegio
- Escalado de privilegios

Gestión de identidad y control de acceso

- La Gestión de la identidad y control de acceso (Identity and access management o IAM) es el principio de seguridad que define quién puede acceder a qué recursos y los privilegios que tienen cuando obtienen ese acceso.
- OAuth 2.0 Authorization Framework es un protocolo estándar para la autenticación y autorización basada en Internet.
- Oauth 2.0 se emplea para el control de acceso de los dispositivos IoT para hacerlos más seguros haciendo que sea un servidor el que gestione la autorización de los recursos.

OAuth 2.0 Authorization Framework

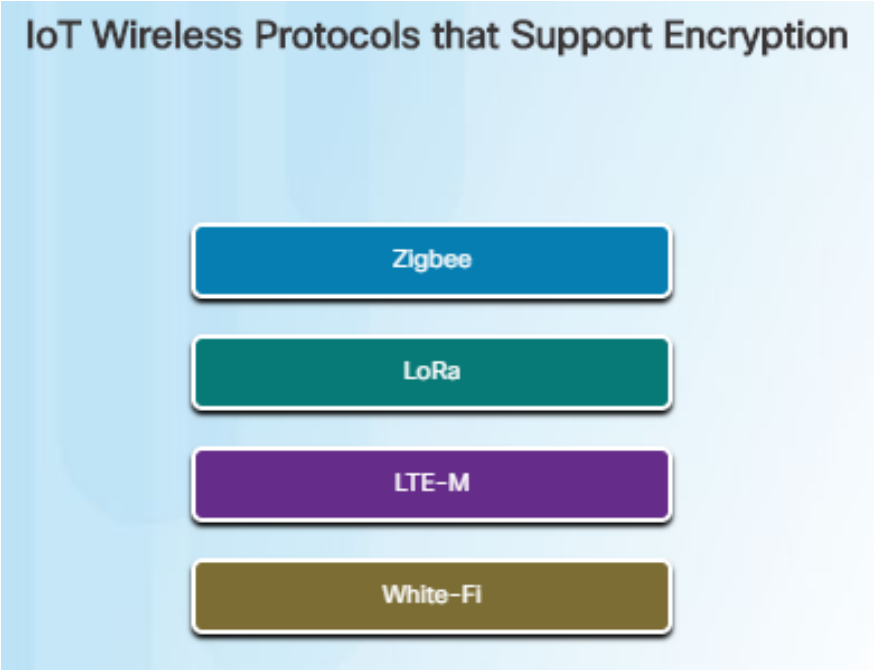


Gestión de identidad en dispositivos IoT

- La gestión de identidad hace referencia en IoT a la identificación de los dispositivos y gestionar su acceso a los datos.
- Es común el intercambio de información sensible entre dispositivos IoT y el acceso a esos datos debe controlarse.
- Además de gestionar el acceso a información de otros recursos, se debe gestionar el acceso a los propios recursos del dispositivo.
- A mayor número de dispositivos IoT conectados, más relaciones se deben establecer y gestionar.
- El Identity Resource Management (IRM) ayuda a las entidades a gestionar un gran número de identidades y relaciones manteniendo los recursos seguros.

Cifrado

- Las contraseñas se deben cifrar siempre
- Los datos en IoT se deben cifrar pues pueden contener información sensible
- Muchos dispositivos IoT antiguos no soportaban cifrado y son vulnerables
- Muchos dispositivos IoT se comunican de forma inalámbrica, siendo más fácil interceptar su transmisión si no va cifrada

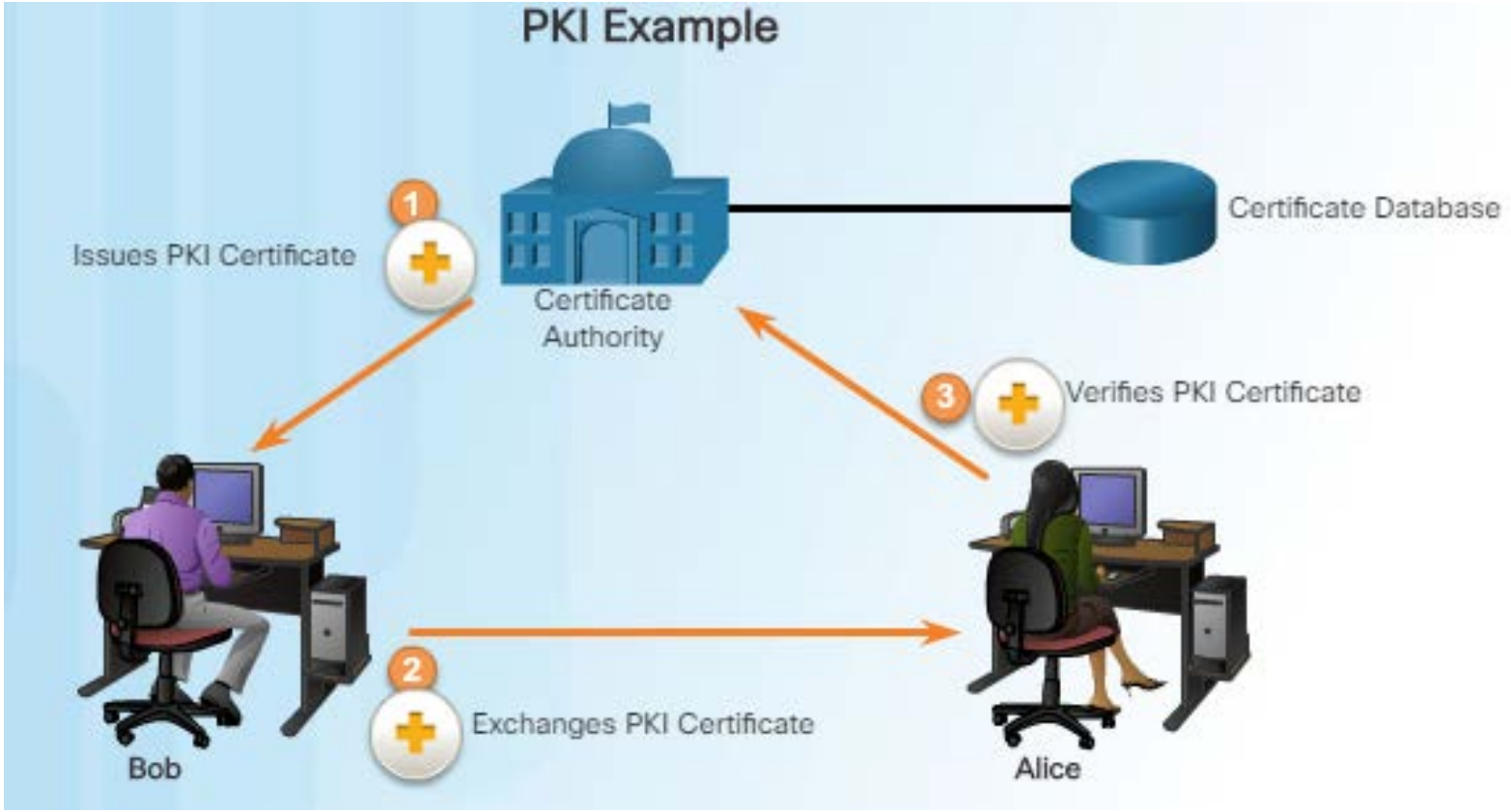


Cifrado en sistemas empotrados

- La mayoría de los dispositivos IoT no tienen el poder de procesamiento o los recursos necesarios para los algoritmos de cifrado más robustos.
- Deben emplearse algoritmos de cifrado ligeros, por HW o por SW.
- Además no existe un estándar, lo que hace que muchos dispositivos IoT no soporten ningún tipo de cifrado.

Cifrado en sistemas empotrados

- Cifrado de clave simétrica
- Cifrado de clave pública (PKI)



3. Cloud Computing

Universidad Rey Juan Carlos

- Definición de Cloud Computing
- Modelo de referencia
- Seguridad en entornos cloud

Definición de Cloud Computing

Universidad Rey Juan Carlos

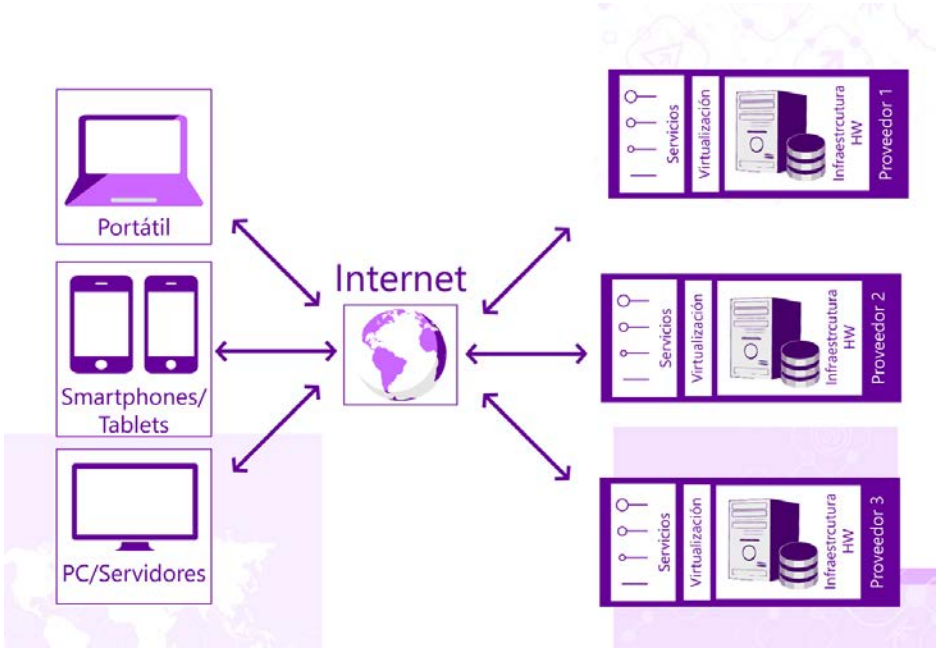
Modelo que permite **acceso remoto**, según nuestras necesidades y **bajo demanda**, y a través de una red de comunicaciones, a un conjunto compartido de **recursos** de cómputo **configurables** (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser **reservados y liberados** de manera rápida con un mínimo esfuerzo e intervención por parte del proveedor.

NIST (National Institute of Standards and Technology del US Department of Commerce)

Definición de Cloud Computing

Modelo de computación que permite al proveedor tecnológico ofrecer servicios informáticos a través de internet. De esta forma los recursos, es decir, el hardware, el software y los datos se pueden ofrecer a los clientes bajo demanda.

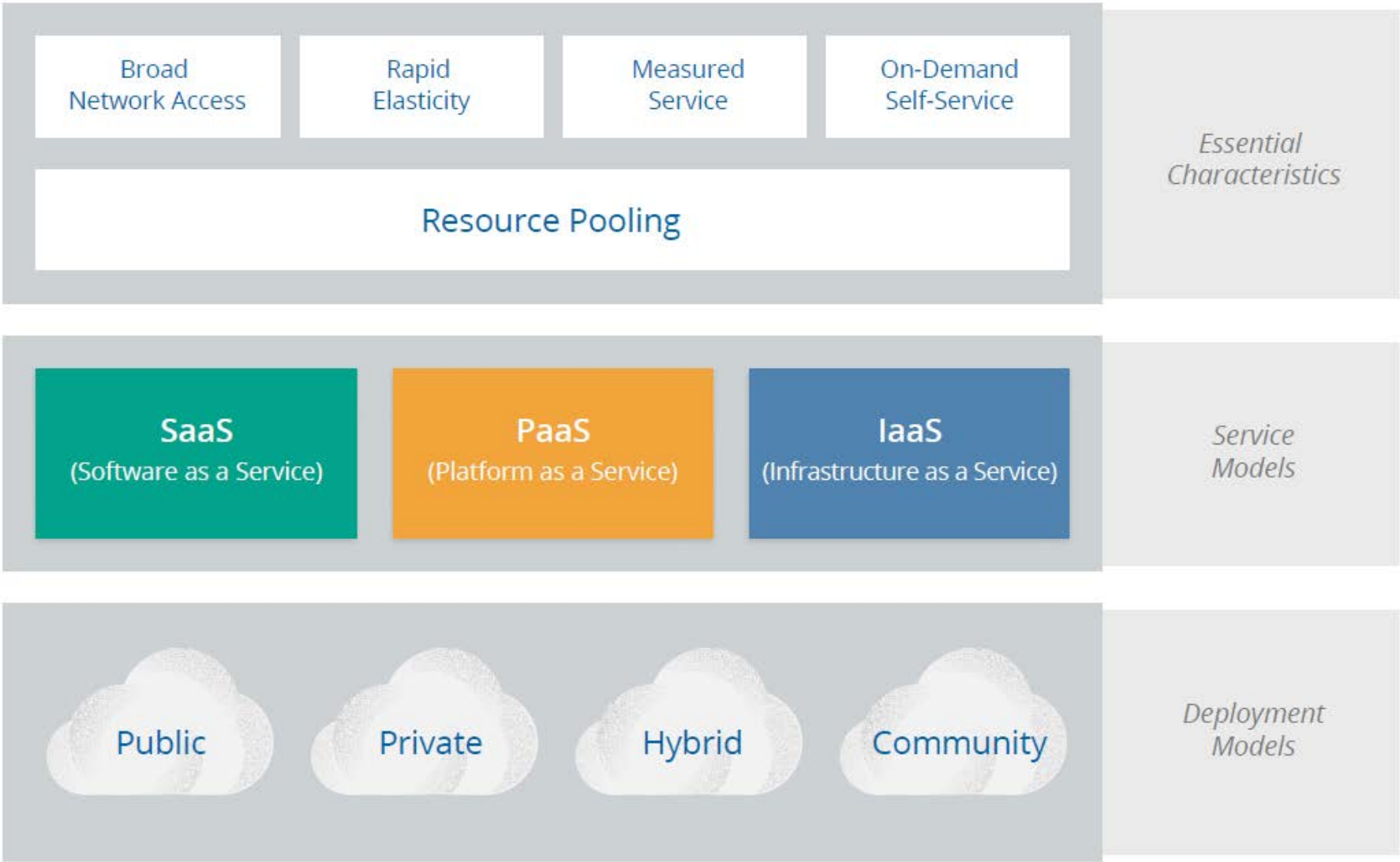
INCIBE



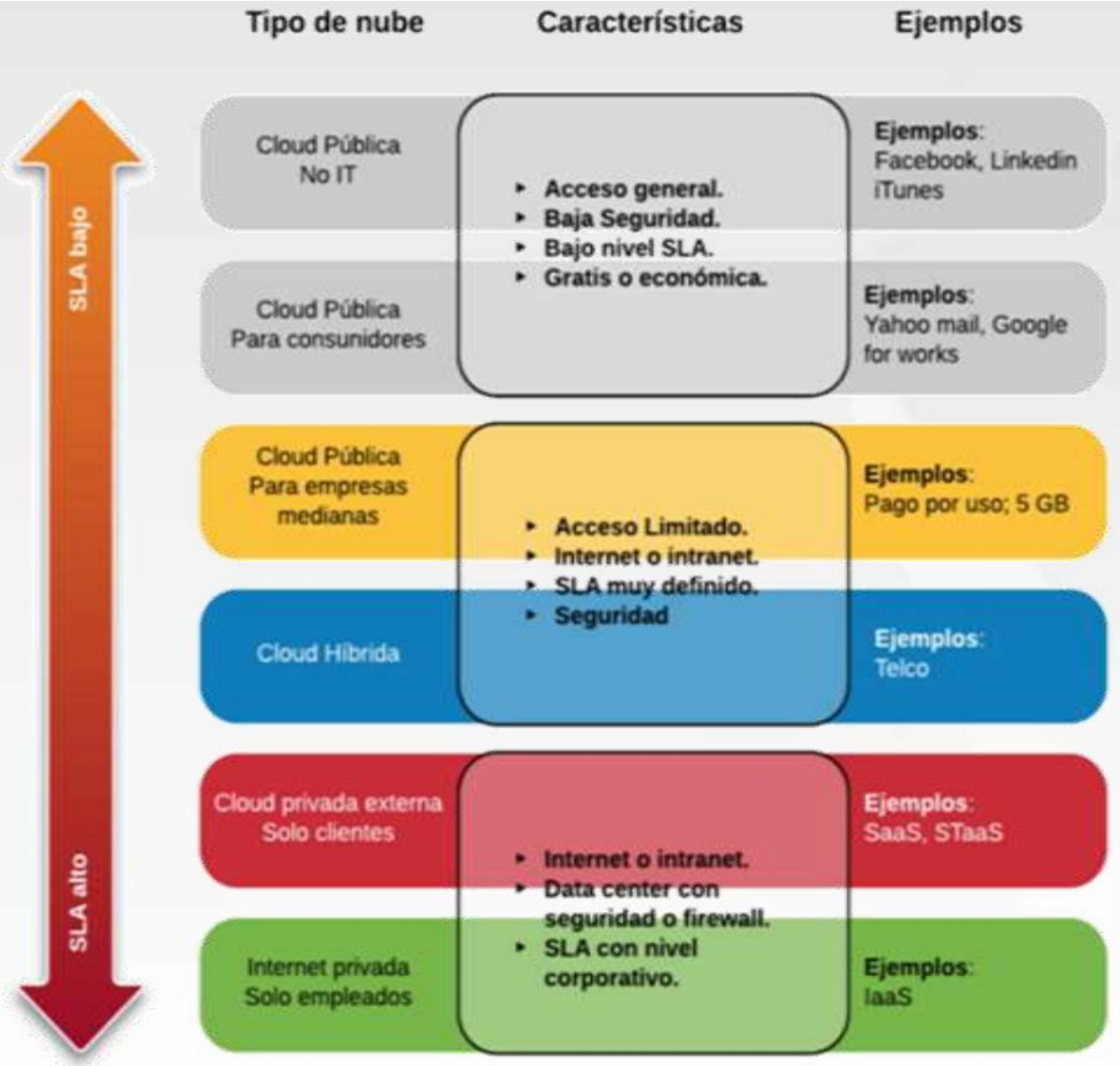
Definición de Cloud Computing

- **Disponibilidad de recursos masivos** que se emplean bajo demanda.
- Modelo de **pago por uso**.
- Capacidad de que **clientes heterogéneos** realicen **accesos remotos, ubicuos y dinámicos** a través de la red.
- **Agrupación de recursos y utilización en modo multi-tenant**.
- **Elasticidad y dinamismo**, los recursos deben poder reservarse y liberarse según las necesidades de los clientes en cada momento.
- Los productos se convierten en servicios, y estos son proporcionados como **suministros**.

Modelo de referencia



Modelo de referencia



Responsabilidades del proveedor

- Seguridad física y ambiental
- Acceso físico de los empleados
- Detección y supresión de incendios
- Continuidad de la energía eléctrica
- Control del clima y la temperatura para los servidores y otros dispositivos de hardware
- Saneamiento para los dispositivos de almacenamiento desmantelado

Responsabilidades del cliente

Universidad Rey Juan Carlos

- Comprender y calificar el perfil del riesgo de las cargas de trabajo que intentan mover a la nube.
- Considerar las responsabilidades de que sus controles técnicos cumplan con los requerimientos de seguridad, privacidad y de cumplimiento.

Ventajas del Cloud Computing

Universidad Rey Juan Carlos

- Es probable que los estándares de seguridad de datos sean más altos en el entorno del proveedor que en el cliente, especialmente si el proveedor de la nube cuenta con las normas ISO y otros estándares clave de la industria.
- Posiblemente, el proveedor de la nube tenga mejores recursos físicos y financieros que el cliente, para contrarrestar las amenazas a la seguridad de los datos a las que se enfrenta su infraestructura.
- Los datos aún estarán disponibles, incluso si se pierde un portátil.
- El cliente puede concentrar más recursos y esfuerzos hacia un aspecto más estratégico y trascendente, que tenga un impacto directo sobre los procesos de negocio de la organización, transfiriendo al proveedor la responsabilidad de la implementación, configuración y mantenimiento de la infraestructura necesaria para que se ejecute la aplicación.

Desventajas del Cloud Computing

- Los datos del cliente estarán almacenados fuera de la red empresarial, y posiblemente en el exterior, lo que puede infringir las leyes y las normas de protección de datos.
- Falta de control sobre recursos. Al tener toda la infraestructura e incluso la aplicación corriendo sobre servidores que se encuentran en la nube, es decir, del lado del proveedor, el cliente carece por completo de control sobre los recursos e incluso sobre su información, una vez que ésta es subida a la nube.
- Dependencia. En una solución basada en cómputo en la nube, el cliente se vuelve dependiente no sólo del proveedor del servicio, sino también de su conexión a Internet, debido a que el usuario debe estar permanentemente conectado para poder alcanzar al sistema que se encuentra en la nube.

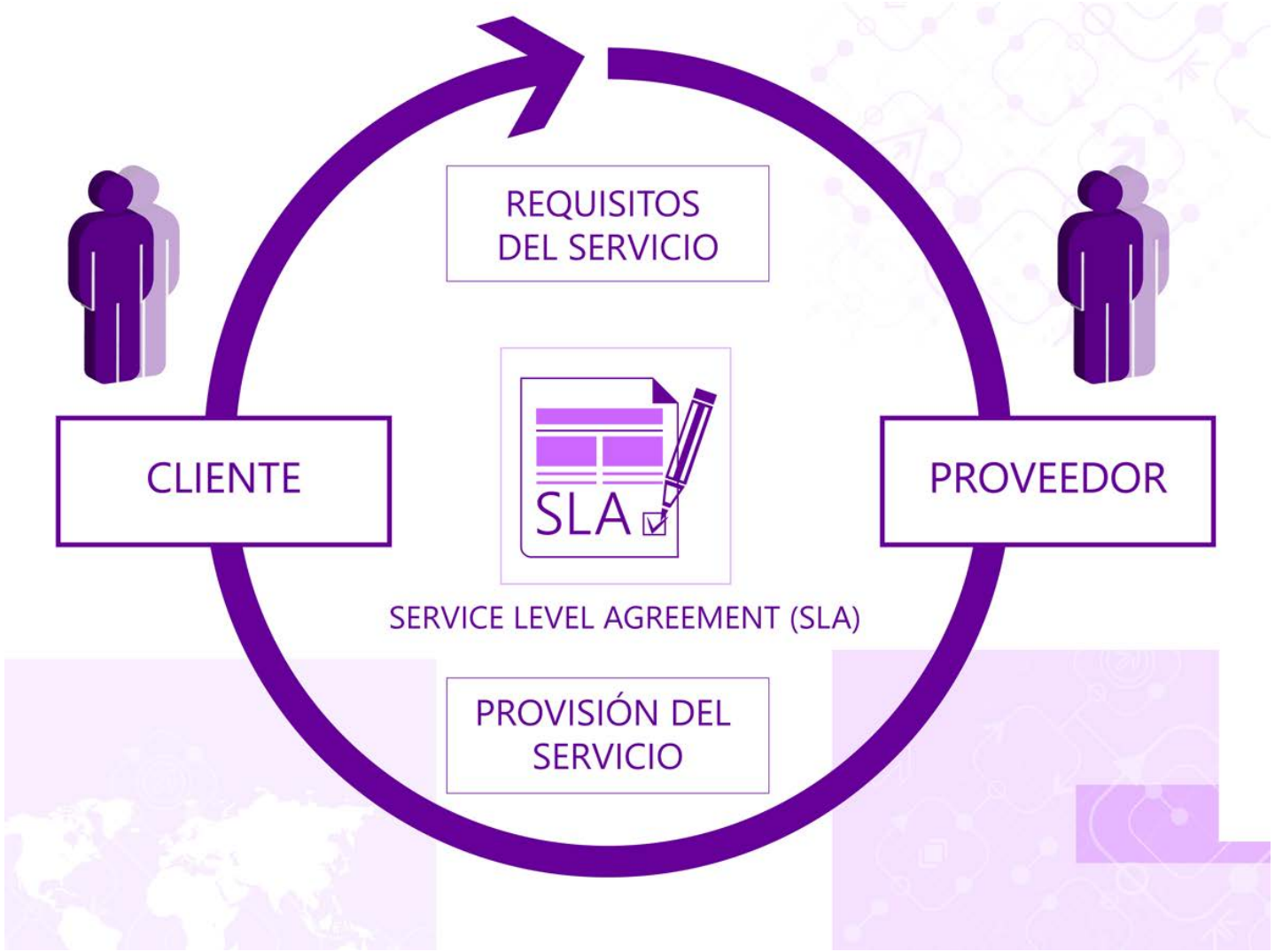
Seguridad en entornos Cloud

Muchas organizaciones no cambian de paradigma o lo están haciendo muy lentamente porque **les asusta** la indefinición que suele percibirse en los entornos cloud, la pérdida de control sobre sus activos y la deslocalización de estos. La mayor parte de estudios y encuestas identifican como mayor preocupación en la transición a un contexto cloud la **ciberseguridad**. Y esto en casi todos los roles de una organización, no sólo en los técnicos. Pero ¿hasta qué punto esta preocupación está justificada en la actualidad?

- Security as a Service (sistemas de gestión de la identidad, antivirus, IDS/IPS,…)

¿Qué cambia en cloud?

- Pérdida de control sobre la infraestructura tecnológica
- Preocupación por confidencialidad y la disponibilidad
- Cautividad de los proveedores escogidos
- Ausencia de estándares específicos para cloud
- Ausencia de metodologías de auditoría para cloud
- Vulnerabilidades específicas cloud


REQUISITOS DEL SERVICIO
CLIENTE
SLA
PROVEEDOR
SERVICE LEVEL AGREEMENT (SLA)
PROVISIÓN DEL SERVICIO

El cliente y el proveedor deben:

- Definir claramente las fronteras para los datos
- Dejar claros los aspectos relacionados con la propiedad intelectual
- Definir conjuntamente los procedimientos para responder ante incidentes
- Acordar los procedimientos para obtener evidencias digitales
- Realizar auditorías o hacer visibles sus relaciones con terceros y cómo pueden afectar éstas a la ciberseguridad

Seguridad en entornos Cloud

La preocupación por la ciberseguridad en entornos cloud ha hecho que desde el año 2008 se intenten clasificar los **riesgos, amenazas y vulnerabilidades específicos del paradigma** para intentar también proponer soluciones, defensas y contramedidas particulares que generen confianza en los potenciales clientes. El problema es que **no hay una propuesta estándar**, aunque cada vez existe un acuerdo mayor en los aspectos más importantes.

Análisis de riesgos específicos para cloud computing que realizó **ENISA** en el año 2009, los 10 riesgos más importantes son

Pérdida de gobernanza
Cautividad del proveedor
Fallos de aislamiento entre usuarios
Inclumplimiento de normativas y regulaciones
Compromiso de la interfaz o API de acceso
Compromiso de datos
Borrado reversible de datos
Malicious insider
Pérdida de disponibilidad
Transferencia de riesgos desde el modelo tradicional

- La **Cloud Security Alliance (CSA)** identificó en 2013 en su lista The Notorious Nine las nueve amenazas más importantes en entornos cloud.

1. Data breach
2. Pérdida de datos
3. Secuestro de cuenta
4. API insegura
5. Denegación de servicio
6. Malicious insider
7. Abuso de los servicios (impago por parte del cliente)
8. Selección de proveedor inadecuada
9. Mala gestión de multy-tenancy

La CSA actualizó en 2017 la lista a las Treacherous 12 y en 2019 a las Egregious 11:

1. Data Breaches
2. Misconfiguration and inadequate change control
3. Lack of cloud security architecture and strategy
4. Insufficient identity, credential, access and key management
5. Account hijacking
6. Insider threat
7. Insecure interfaces and APIs
8. Weak control plane
9. Metastructure and applistructure failures
10. Limited cloud usage visibility
11. Abuse and nefarious use of cloud services

Seguridad en entornos Cloud

Universidad Rey Juan Carlos

- Los riesgos y amenazas que más preocupan son los mismos.
- Un primer grupo tiene que ver con **aspectos legales, organizativos y estratégicos**.
- El segundo grupo es el que incluye a los **riesgos puramente tecnológicos**, es decir, aquellos que pueden afectar a la **confidencialidad, integridad, disponibilidad y control de acceso** por vulnerabilidades de las tecnologías y modelos que subyacen al paradigma.
- En este contexto, cabe destacar que los patrones de ataque que más se observan en la actualidad son las inyecciones de comandos y código, los forgeries y los diferentes secuestros de sesión y/o cuenta debidos a los esquemas IAAA débiles, normalmente basados, todavía en la actualidad, en un único factor de autenticación (par nombre de usuario-contraseña).

Cuatro pilares básicos:

- la utilización de **protocolos de red seguros**
- la **encriptación de datos** a diferentes niveles
- la definición de **políticas y procedimientos** adecuados para el paradigma
- el uso de **esquemas IAAA** fuertes

Y en cada uno de estos cuatro aspectos las dos partes, proveedor y cliente, deben cumplir con su papel correctamente.

Esquemas IAAA en entornos Cloud

Universidad Rey Juan Carlos

I → Identificación del usuario asignando una identidad digital

A → Autenticación para comprobar que un usuario es quien dice ser

A → Autorización del acceso del usuario a diferentes recursos o activos

A → Auditoría (Accountability), trazabilidad de lo que hace el usuario para pedirle responsabilidades o facturarle

Compromiso entre Seguridad, Flexibilidad y Facilidad de uso

Esquemas IAAA en entornos Cloud

Universidad Rey Juan Carlos

Integrar el esquema IAAA en todos los dispositivos de manera inteligente, para que sean lo más sencillos y transparentes para el usuario, manteniendo los niveles de seguridad y control adecuados

IAAA federados con varios repositorios de credenciales, pero los atributos de identidad están en un único repositorio (encargado de verificarlos en cada proceso de identificación y autenticación). Los usuarios emplean esa identidad para acceder a diferentes recursos, aplicaciones o servicios de distintos proveedores. No es necesario manejar esquemas diferentes para cada uno de ellos. Los proveedores confían los unos en los otros.

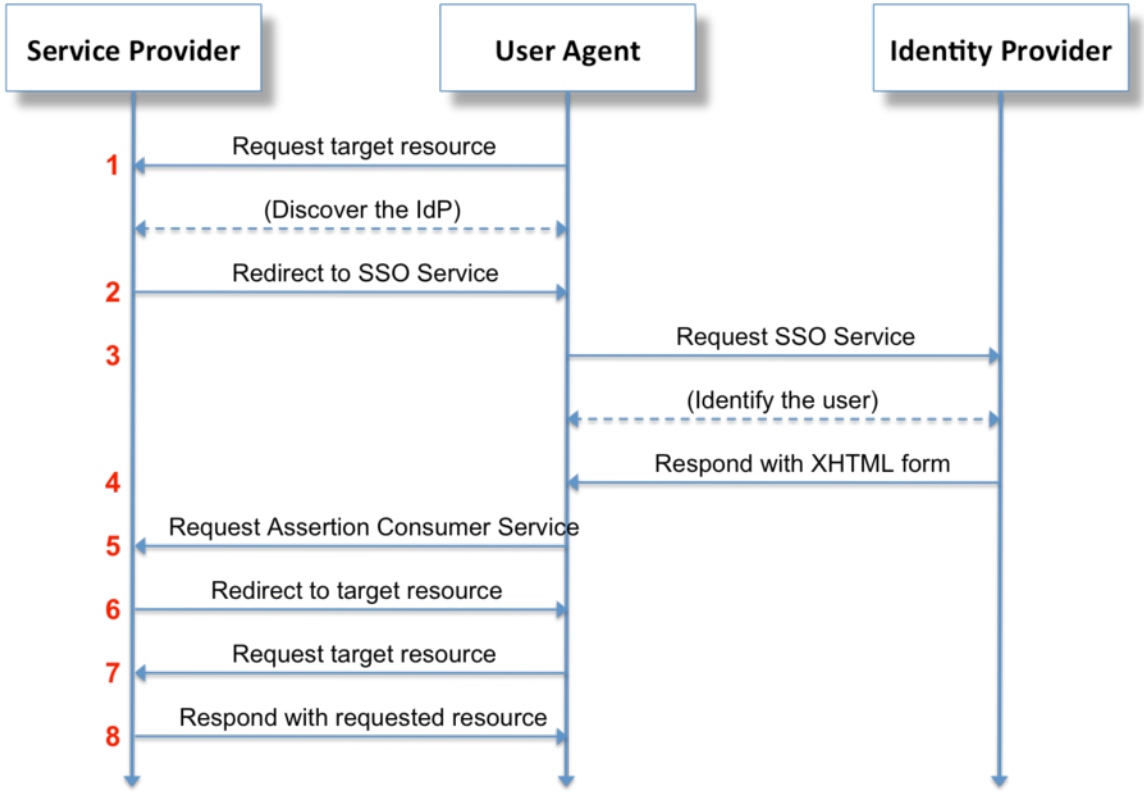
Esquemas centralizados clásicos no eran escalables ni lo suficientemente dinámico para el aprovisionamiento y liberación de identidades. Y cada proveedor con su esquema… número elevado de usuario-contraseña (uno por cada servicio)

Las soluciones más extendidas en esquemas federados son:

- SAML: Identificación y autenticación
- OAuth: Autorización

SAML (Security Assertion Markup Language):

Estándar de OASIS de 2002 (v2.0 en 2005) que define un esquema XML que permite a un usuario identificarse y autentificarse en un sitio y que no lo tenga que repetir en sitios de confianza (SSO).

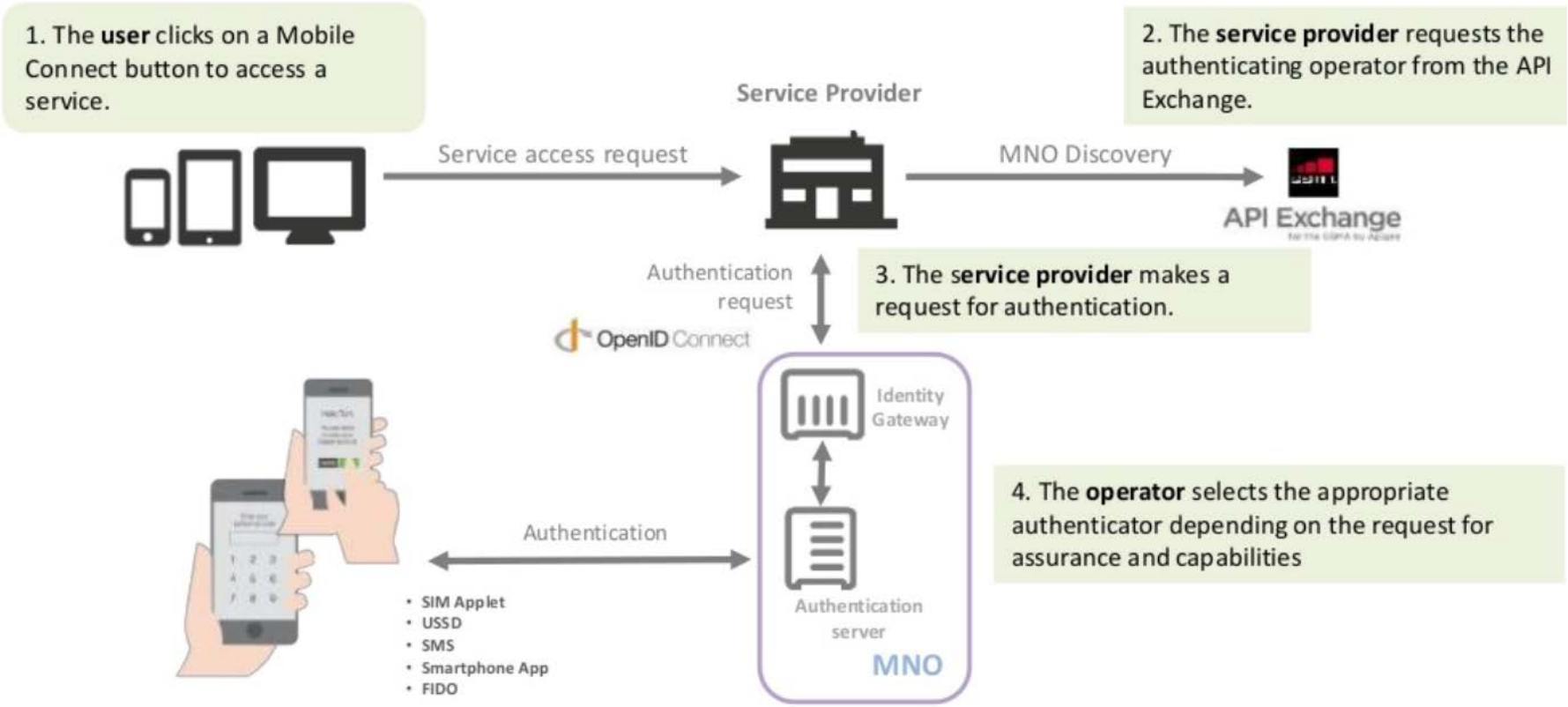


Esquemas IAAA en entornos Cloud

- Como has podido ver, existen **soluciones federadas** para resolver el problema de IAAA en entornos cloud de manera sencilla y flexible para los usuarios, pero también segura.
- Esta seguridad se basa principalmente en la **autenticación multi-factor**, que además de basarse en algo que se conoce (nombre de usuario y contraseña) se basa en algo que se posee (algún tipo de token o smart card, la SIM del teléfono) e incluso en algo que es (aprovechando las capacidades biométricas de estos dispositivos móviles, que permiten escanear la huella dactilar, reconocer la cara o capturar una firma, por ejemplo).
- Sin embargo, la adopción de estos esquemas está siento lenta, con muchos proveedores a distintos niveles (tanto IaaS como PaaS o SaaS) se basan todavía en un **par usuario-contraseña sobre https** o como mucho en la utilización de HMAC.

Esquemas IAAA en entornos Cloud

OpenID Connect = OpenID + OAuth



Esquemas IAAA en entornos Cloud

mobile connect

Authentication

Simple, secure log-in and 2-factor authentication for the user when a PIN or fingerprint is requested for extra security.

Authorisation

Allowing end users to authorise requests from service providers – such as payments and permissions – directly from their mobile phone.

Identity

Enabling end users to confirm or share their personal data with digital services quickly and securely.

Attributes

Utilising device and network information for ID verification and fraud prevention.

4. Infraestructuras críticas

Universidad Rey Juan Carlos

1. Definición de infraestructura crítica
2. Características de las infraestructuras críticas
3. Principales amenazas a las ICs
4. Marcos y planes aplicables a ICs
5. Contramedidas en ICs

Definición de infraestructura crítica

Universidad Rey Juan Carlos

"Las *infraestructuras estratégicas* cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los *servicios esenciales*".

Infraestructura estratégica: "las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales".

Servicio esencial: "el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas".

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas

Definición de infraestructura crítica

Universidad Rey Juan Carlos

Características de infraestructura crítica

Algunas de las características comunes a las infraestructuras críticas son:

- Haber adoptado un alto nivel de automatización para su operación control
  - Aparecen las *infraestructuras de información críticas*
- Existir una gran interrelación entre todas ellas
- Estar en la mayor parte de los casos distribuidas geográficamente incluso en diferentes naciones

Amenazas a infraestructuras críticas

Amenazas:

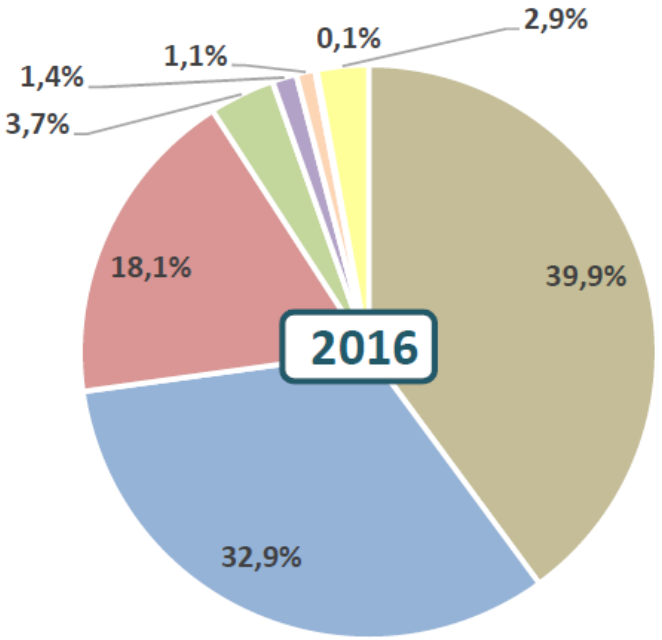
- Catástrofes naturales
- Fallos técnicos
- Errores humanos (Ingeniería social)
- Crimen internacional y Terrorismo
- APTs
- Dispositivos físicos
- Vulnerabilidades y 0-days

Incidentes de ciberseguridad reportados

Universidad Rey Juan Carlos

Tipo de incidente	INCIDENTES GESTIONADOS 2014	2015	2016
Acceso no autorizado	6.785	16.054	14.373
Fraude	4.274	13.410	11.843
Virus, troyanos, gusanos, spyware	1.745	15.177	6.513
SPAM	1.006	1.275	1.325
Denegación de servicio	788	794	495
Escaneos de red	426	335	381
Robos de información	80	26	37
Otros	2.781	2.905	1.038

Porcentaje del total de incidentes gestionados



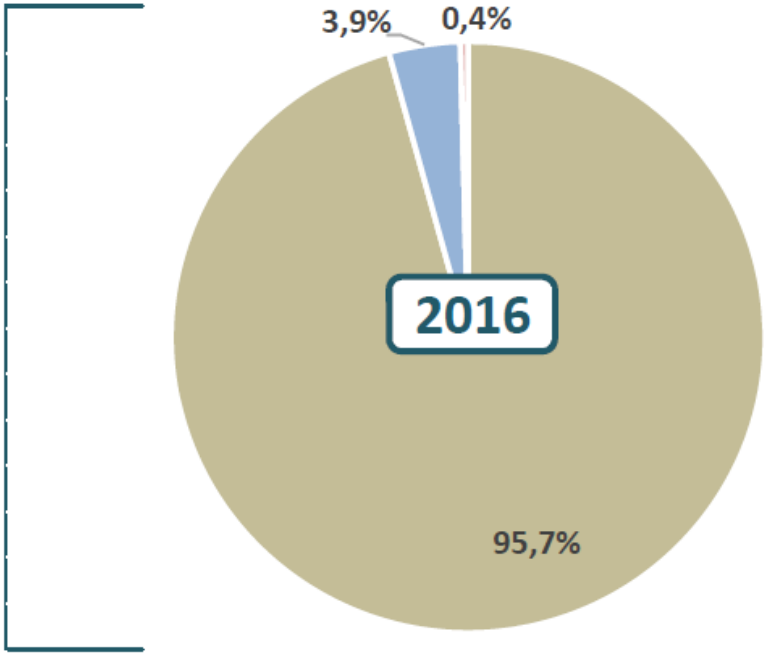
Estudio sobre la cibercriminalidad en España. Ministerio del Interior. 2016

Incidentes de ciberseguridad reportados

Universidad Rey Juan Carlos

Incidentes por público objetivo	INCIDENTES GESTIONADOS		
	2014	2015	2016
Ciudadanos y empresas	14.715	45.693	110.293
Red académica (RedIris)	3.107	4.153	4.485
Infraestructuras Críticas (IICC)	63	130	479

Porcentaje del total de incidentes gestionados



Estudio sobre la cibercriminalidad en España. Ministerio del Interior. 2016

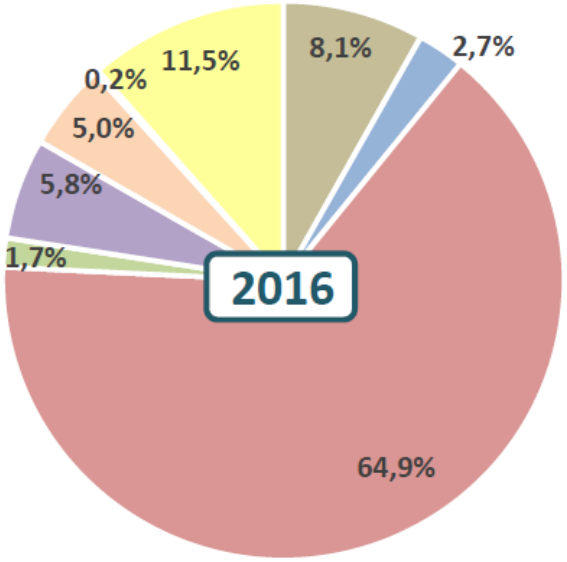
Incidentes en Infraestructuras Críticas

Universidad Rey Juan Carlos

>> 3.2. Incidentes gestionados en relación con las infraestructuras críticas

Tipo de incidente	INCIDENTES GESTIONADOS 2014	2015	2016
Acceso no autorizado	2	15	39
Fraude	6	8	13
Virus, troyanos, gusanos, spyware	31	75	311
SPAM	0	0	8
Denegación de servicio	2	10	28
Escaneos de red	1	7	24
Robos de información	9	2	1
Otros	12	13	55

Porcentaje del total de incidentes gestionados



Estudio sobre la cibercriminalidad en España. Ministerio del Interior. 2016

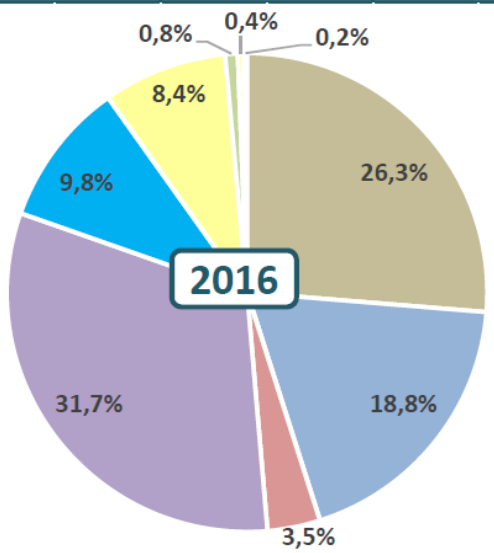
Incidentes en Infraestructuras Críticas

Universidad Rey Juan Carlos

>> 3.4. Incidentes gestionados por sector estratégico

Sector estratégico	INCIDENTES GESTIONADOS 2014	2015	2016
Energía	34	46	126
Transporte	14	24	90
Tegnologías Información y Comunicac. (TIC)	6	17	17
Sistema tributario y financiero	3	17	152
Alimentación	0	12	47
Agua	0	5	40
Industria nuclear	4	5	4
Administración	2	1	2
Espacio	0	0	0
Industria química	0	0	0
Instalaciones de Investigación	0	0	0
Salud	0	0	0
Todos los sectores afectados	0	3	1

Porcentaje del total de incidentes gestionados



Estudio sobre la cibercriminalidad en España. Ministerio del Interior. 2016

Protección de infraestructuras críticas: “el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia”.

Protección de infraestructuras críticas

Universidad Rey Juan Carlos

Objetivos en la protección:

- Prevenir los ataques informáticos contra las infraestructuras de información críticas.
- Reducir la vulnerabilidad nacional a los ciberataques.
- Reducir al mínimo los daños y el tiempo de recuperación cuando estos ataques se producen.

Para alcanzar estos objetivos se han desarrollado diferentes normativas, estándares y grupos especializados que proporcionan mejores prácticas.

Marcos y Planes en infraestructuras críticas

Universidad Rey Juan Carlos

País	Plan/Marco	Agencia
Estados Unidos	National Infrastructure Protection Plan 2013 (NIPP)	U.S. Department of Homeland Security
	CIP (Critical Infrastructure Protection)	North American Electric Reliability Corporation (NERC)
Canadá	Strategy for the Protection of National Critical Infrastructure	Canadian Security Intelligence Service + NERC
Alemania	CERT-Bund	Federal Office for Information Security
Francia	Libro Blanco para la Seguridad y Defensa Nacional	Sécretariat Général de la Défense Nationale
Reino Unido	National Infrastructure Protection Plan 2013 (NIPP)	Centre for the Protection of National Infrastructure
España	Plan Nacional de Protección de Infraestructuras Críticas (Ley PIC)	Centro Nacional de Protección de Infraes-trucuturas Críticas (CNPIC)

Marco Europeo de infraestructuras críticas

- European Programme of Critical Infrastructure Protection (EPCIP) en 2006, revisado en 2013 para incluir las dependencias transfronterizas entre distintas ICs y entre diferentes sectores
- La Directiva europea sobre Infraestructuras Críticas de 2008 establece el procedimiento para identificar las ICs y cómo protegerlas.
- El EPCIP facilita la compartición de información entre los estados miembros y se ha creado una herramienta online específica para ello, la Critical Infrastructure Warning Information Network (CIWIN).

Marco Español de infraestructuras críticas

Plan Nacional de Protección de Infraestructuras Críticas desarrollado por el **CNPIC (Centro Nacional de Protección de Infraestructuras ~~Críticas~~ y Ciberseguridad)** en España.

Ley 8/2011 de Protección de Infraestructuras Críticas complementada por el Real Decreto 704/2011. Entre las principales aportaciones de esta ley destacamos las siguientes:

- Crear el **Sistema Nacional de Protección de Infraestructuras Críticas**
- Poner las bases para el **Sistema de Planificación PIC**
- Generar el **Catálogo Nacional de Infraestructuras Estratégicas**
  - Para facilitar esta información se ha desarrollado el **sistema HERMES**
- Establecer el **CERT (Cyber Emergency Response Team)** para la gestión de incidentes de ciberseguridad
  - **INCIBE (Instituto Nacional de Ciberseguridad)**

Marco Español de infraestructuras críticas

Universidad Rey Juan Carlos

Marco Español de infraestructuras críticas

Universidad Rey Juan Carlos

Andalucía CERT

Basque Cybersecurity Centre

Caixabank CSIRT

CCN-CERT

Cert Oesía

CertUC3M

CESICAT-CERT

CNPIC

CSIRT.gal

CSIRT-CV

CSIRT CARM

CSIRT Global Telefónica

CSUC-CSIRT

Deloitte EDC

Entelgy Innotec Security - CSIRT

ERIS-CERT

Ertzaintza SCDTI

esCERT-UPC

ESP DEF CERT

eSOC Ingenia

EULEN-CCSI-CERT

everis CERT

Global CSIRT

Guardia Civil - Ciberinteligencia y Ciberterrorismo

Marco Español de infraestructuras críticas

Universidad Rey Juan Carlos

Guardia Civil - Departamento de Delitos Telemáticos

IBERDROLA Cyber-Security Incident Response Team

ICA SYS CiberSOC

INCIBE-CERT

ITS-CERT

MAPFRE-CCG-CERT

Minsait CSIRT

MNEMO-CERT

NestleSOC

NUNSYS-CERT

OSSI-CERT SERMAS

Policía Nacional

PROSEGUR CERT

RedIRIS

RENFE CERT

Repsol CERT

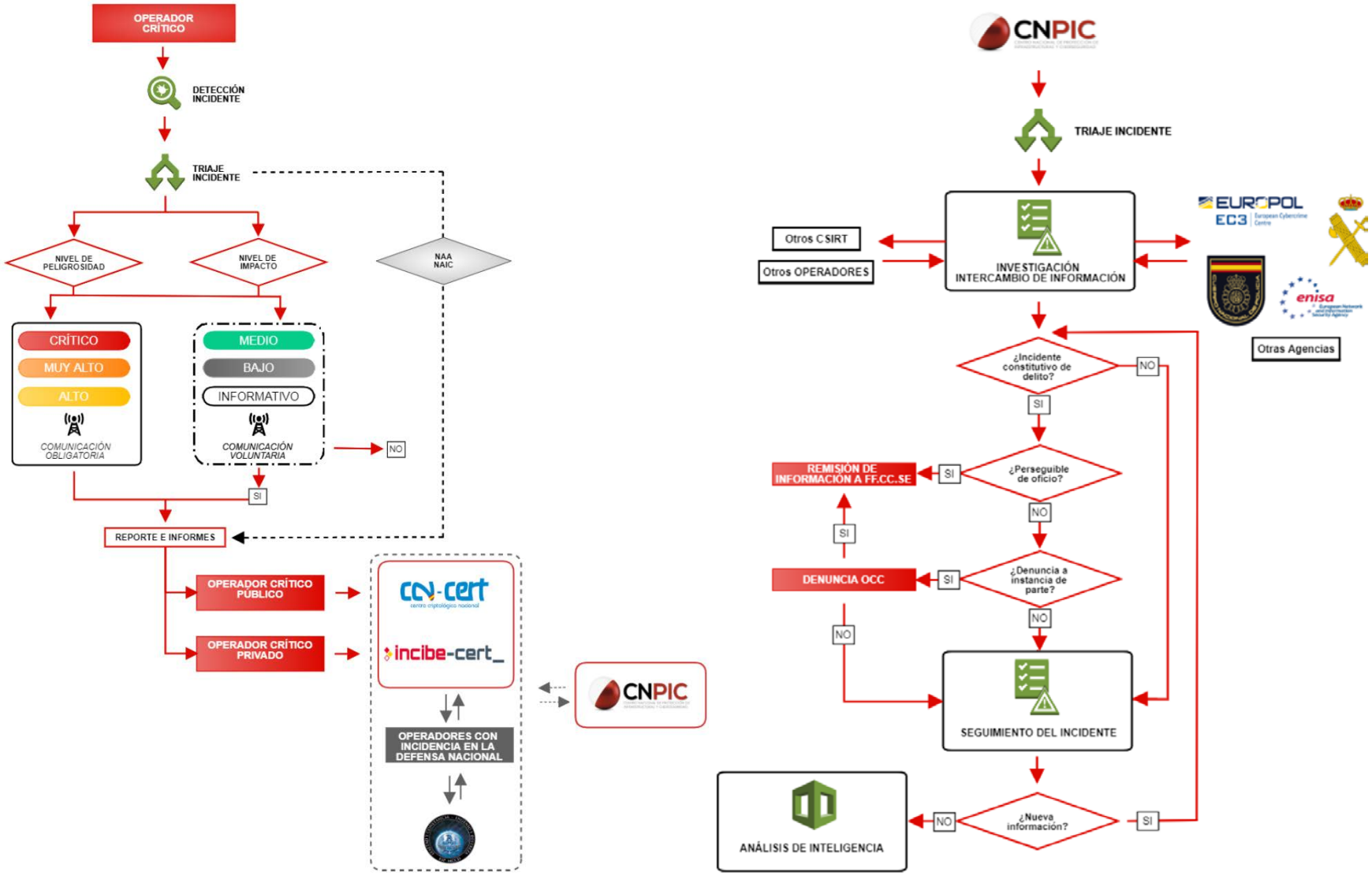
S21sec CERT

S2 Grupo CERT

SIA-CEC CERT

UCIBER - Mossos d'Esquadra

Notificación de incidentes en ICs



Notificación de incidentes en ICs

Universidad Rey Juan Carlos

Nivel de Alerta en Infraestructuras Críticas (NAIC)

Contramedidas en ICs

- **Puesto de operador:** centros de control con sistemas HMI o SCADA para supervisar y/o controlar las infraestructuras críticas distribuidas

Controles del puesto de operador

- Configuración segura del HW y SW
- Establecimiento de medidas antimalware
- Capacidad para la recuperación de datos
- Uso controlado de privilegios de administración
- Acceso basado en el “Need to know”

Contramedidas en ICs

Otras contramedidas

- Utilización de HIDS
- Honeytokens
- Indicadores IOC
- Herramientas como EMET o CrystalAEP
- Reputación de seguridad del proveedor HW y SW

Entornos Legacy

Equipos móviles

5. Advanced Persistent Threat (APT)

Universidad Rey Juan Carlos

- Definición de APT
- Objetivos y consecuencias de APT
- Ejemplos de APTs
- Fases de una APTs
- Contramedidas para APTs

Definición de APT

Advanced Persistent Threat (APT): amenaza dirigida a una determinada persona, organización, gobierno o incluso país, que se caracteriza por ser avanzada, persistente en el tiempo, sofisticada, y normalmente organizada y financiada.

"An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives".

National Institute of Standards and Technology (NIST)

Definición de APT

- Amenaza sofisticada
- Afecta a una organización o sector concreto
- Múltiples vectores de ataque
- Equipo de personas multidisciplinar:
  - *Personas* con conocimientos muy avanzados
  - *Tecnologías* sofisticadas
  - Coordinados mediante *procedimientos*
- Organizadas, premeditadas y persistentes en el tiempo
- Buscan objetivos específicos
- Usan firmas de ataque únicas
- Financiado, para perdurar o incluso reintentar

Definición de APT

Probabilidad de sufrir un APT vs Nivel de preparación para afrontarlo
(ISACA, 2015 Advanced Persistent Threat Awareness)

	Muy probable	Probable	No muy probable	Nada probable
Muy preparada (Plan desplegado, probado y documentado)	45%	15%	2%	0%
Preparada (con gestión de incidentes pero no cubre APTs)	35%	58%	46%	29%
No muy preparada	18%	25%	49%	57%
Nada preparada	2%	2%	4%	14%
Total	22%	51%	26%	1%

Definición de APT

Objetivos de un APT:

- Personas físicas (recuerda el ataque dirigido a “celebrities” durante el mes de septiembre de 2014, en el que se difundieron fotos comprometedoras que presuntamente habían sido robadas de la plataforma iCloud de Apple)
- Organizaciones privadas
- Organizaciones gubernamentales
- Organizaciones militares
- Incluso países enteros

Consecuencias de una APT

Universidad Rey Juan Carlos

Las consecuencias son muy variadas y dependen de la acción maliciosa y del objetivo. Algunos ejemplos son:

- Pérdidas directas provocadas como consecuencia directa del ciberdelito en sí (robo de propiedad intelectual, extracción de información confidencial, costes incurridos por la falta de disponibilidad de un determinado sistema, etc.).
- Costes de remediación e indirectos generados por el tiempo y esfuerzo dedicado a resolver la intrusión e investigarla.
- Costes asociados a reforzar las líneas de defensa y contramedidas, y a devolver la estabilidad a los sistemas.
- Costes asociados a la reputación de las personas o de las organizaciones afectadas. Estos costes son normalmente intangibles y causan la pérdida de confianza por parte de clientes, empleados, colaboradores e inversores, pérdida de oportunidades de negocio, etc.

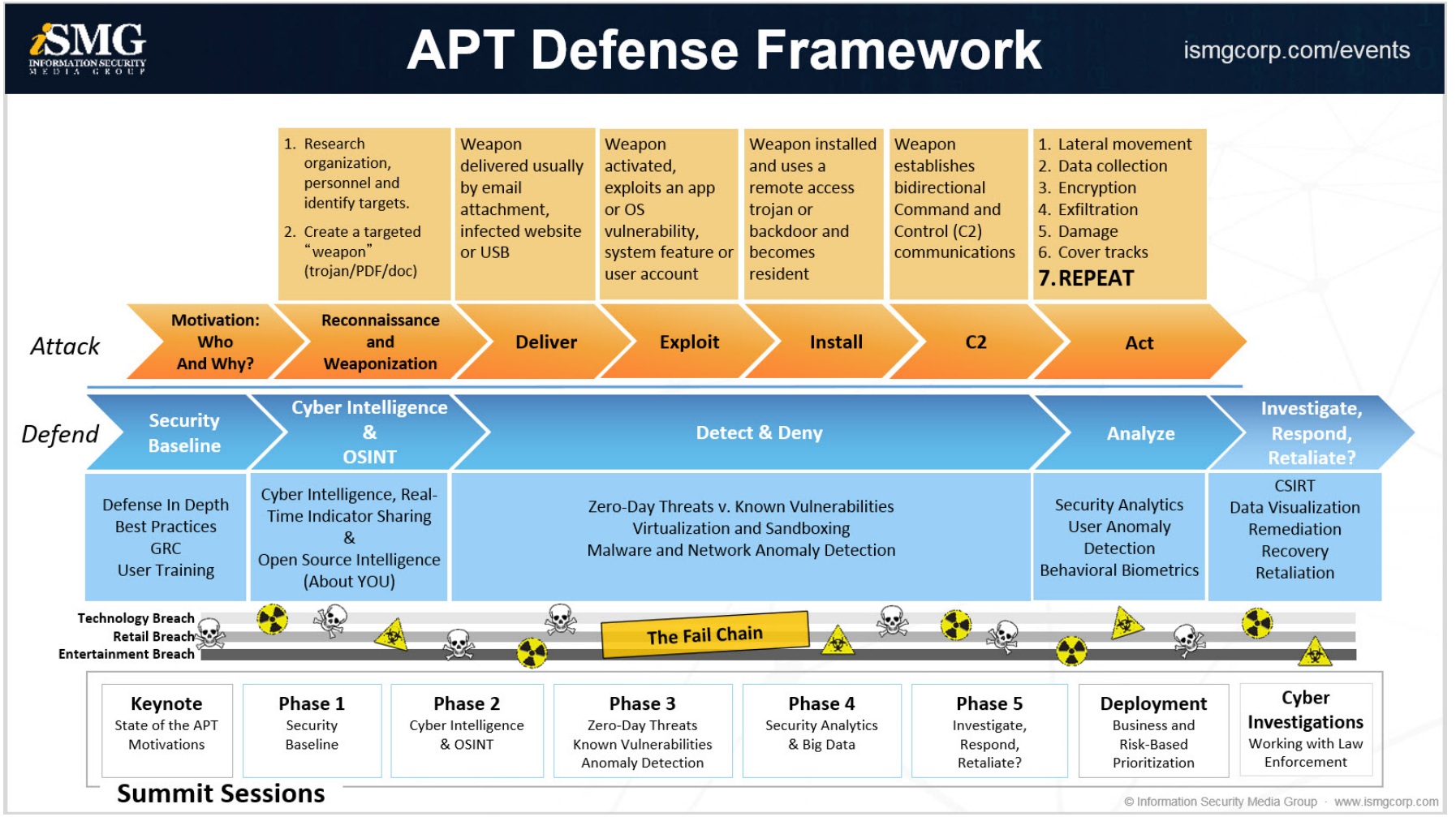
Ejemplos de APTs

Año	APT	Acción maliciosa	Objetivo
2009	Operación Aurora	Robar información confidencial	Multinacionales tecnológicas (Google, Adobe, Juniper)
2009	Operación Ghosnet	Espiar información personal e industrial	Dalai Lama y países del sur/sureste de Asia
2010	Stuxnet	Alterar los procesos industriales controlados por sistemas DCS, PLC y SCADA	Centrales nucleares Iraníes y otras instalaciones críticas
2010	Operación Night Dragon	Robar información confidencial	Multinacionales de los sectores petróleo, químico y energético
2011	Operación Shady RAT	Robar información confidencial	Naciones Unidas y gobiernos de todo el mundo
2011	Nitro	Espiar información industrial (patentes, fórmulas, recetas, etc).	Empresas químicas y ejércitos
2012	Flame	Espiar información industrial (patentes, fórmulas, recetas, etc).	Empresas petrolíferas y del sector gas de Irán, Israel, Sudán, Siria, Líbano, Arabia Saudí
2012	Operación Medre	Robar documentación de carácter industrial (planos AutoCAD)	Países de habla hispana
2012	Duqu	Robar información de infraestructuras críticas utilizando un troyano	Centrales eléctricas, refinerías y oleoductos
2012	Gauss	Robar credenciales y espiar transacciones bancarias	Israel y Líbano
2013	APT1	Atacar países enemigos de China (nombre del ciberejército chino)	Países de habla inglesa
2013	Red October	Espiar información industrial (patentes, fórmulas, recetas, etc).	Empresas petrolíferas y del sector gas de Irán, Israel, Sudán, Siria, Líbano, Arabia Saudí
2014	Dragonfly	Robar información de entornos industriales e infraestructuras críticas	Sectores eléctricos, farmaceúticos, alimentación y bebidas
2014	Sandworm	Robar información de entornos industriales e infraestructuras críticas	Instalaciones NATO Secret y empresas del sector petrolífero
2015	Laziok	Robar información de entornos industriales e infraestructuras críticas	Sector petrolífero y gas de países de Europa del Este

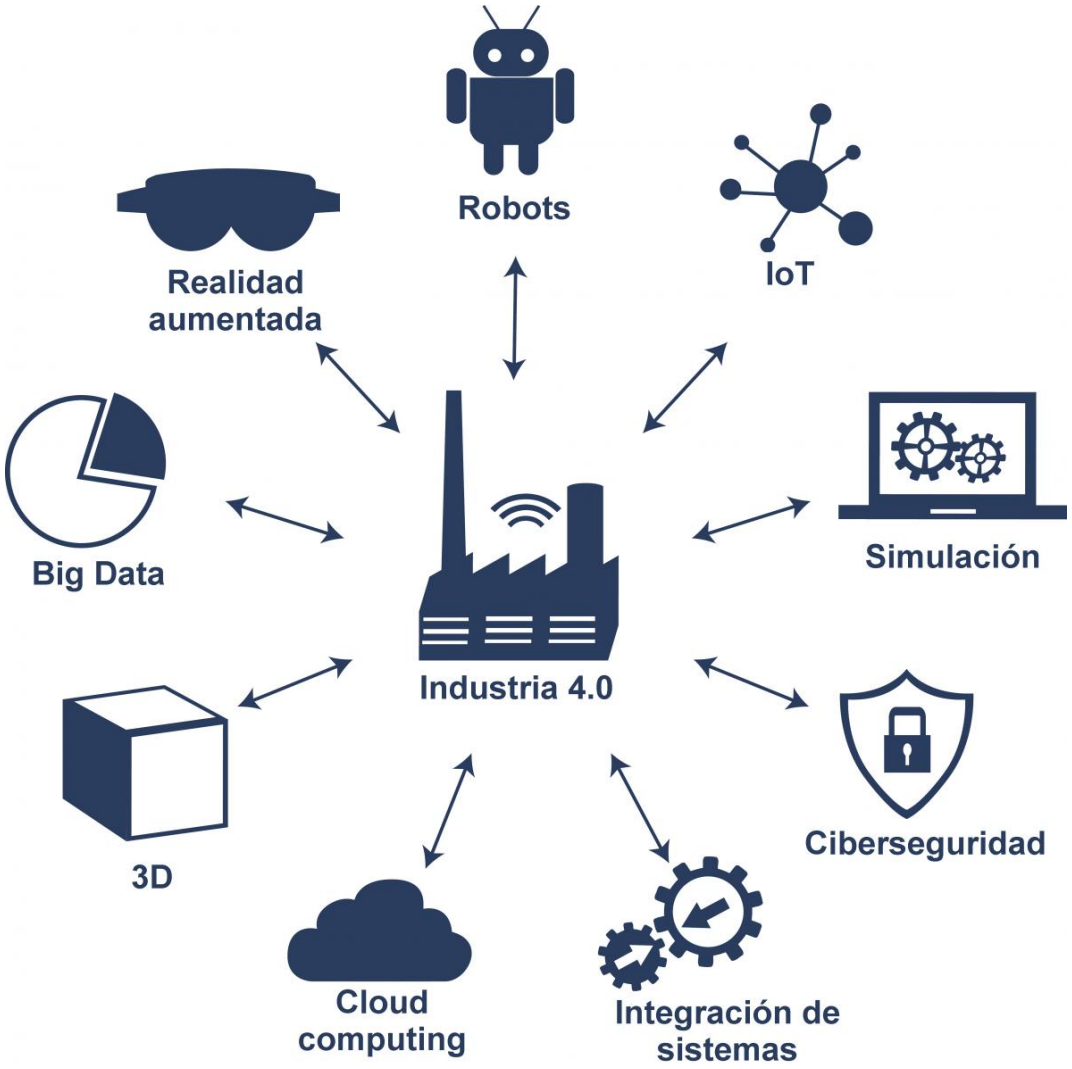
Fases de una APT

- Fase 1: Seleccionar el objetivo y recoger información
- Fase 2: Diseñar el modelo de ataque
- Fase 3: Realizar la intrusión en el sistema objetivo e infectarlo, usando vectores de ataque como:
  - Factor humano: spear phishing, iframe injection (watering holes)
  - Morphing and obfuscation toolkits (descargas de software pirata)
  - Medios físicos (USB…)
  - Overflow, inyección código, forgeries,…
- Fase 4: Actualizar y desplegar malware
- Fase 5: Capturar, extraer y utilizar información sensible

Fases de una APT

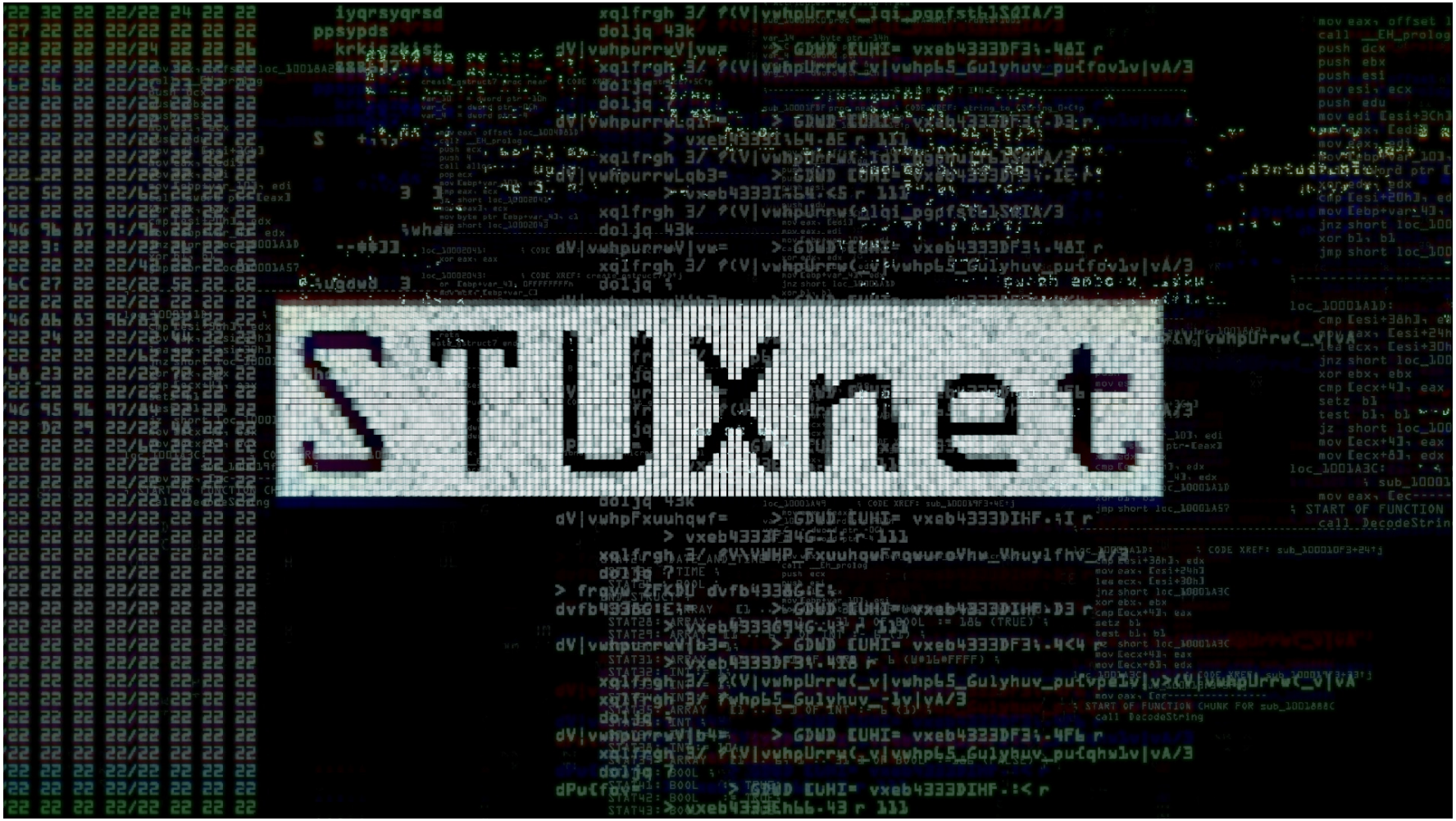


Objetivo: Industria 4.0



Ejemplo de APT: Stuxnet

Universidad Rey Juan Carlos



Contramedidas en APTs