CIBERSEGURIDAD EN EL SECTOR ENERGÉTICO

Lucas A. Giraldo-Ríos MsC, MBA, PhD(c)
Maestría en Ciberseguridad y Ciberdefensa
Escuela Superior de Guerra

Lucas Adolfo Giraldo Rios PhD (c)

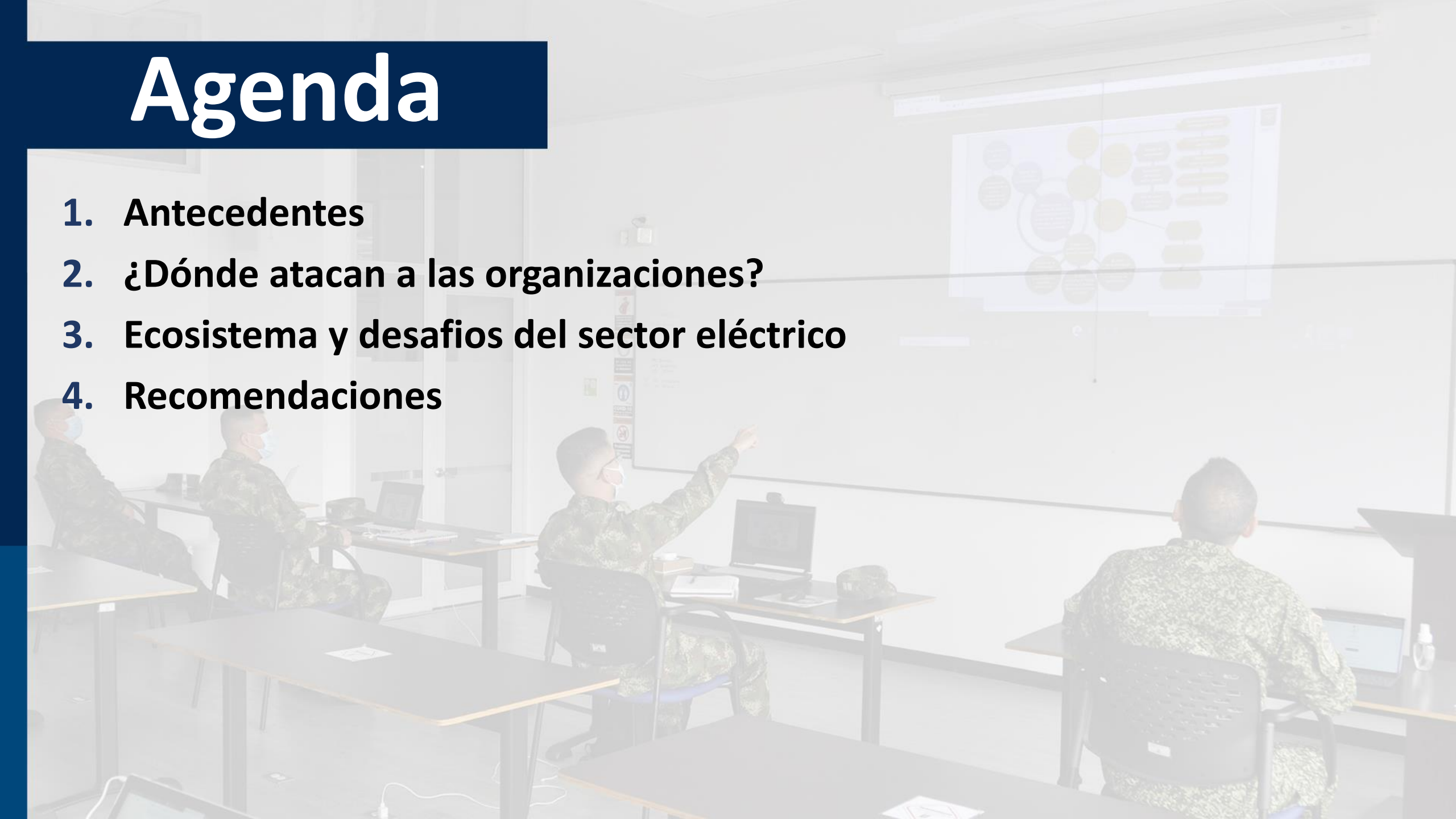
Administrador de Empresas (UdeA), Especialista en Gestión Financiera Empresarial (UdeM), Magister en Innovación (EAN) y Magister en Administración (Nebrija), actualmente candidato a doctor en Ingeniería, Industria y Organizaciones de la Universidad Nacional de Colombia.

Gerente de Consultoría en la firma RSM, asesor de DNP en la subdirección de seguridad y defensa y más de 18 años de experiencia en el sector empresarial en empresas de alimentos, tecnología, servicios, gremiales y educativos en el ámbito nacional e internacional.

Adicionalmente cuenta con más de 15 años de experiencia docente en las universidades Nacional de Colombia, Escuela Superior de Guerra, Universidad Asturias, Instituto Europeo de Posgrados, Universidad Espíritu Santo (Ecuador) entre otras, en temas de Ingeniería Económica, Mercados de Renta Fija y Variable, Análisis y Planeación Financiera, Estrategia, Innovación, Prospectiva, Sistemas de Información Gerencial, Gobierno de TI, Transformación Digital, Digitalización, ciberseguridad y ciberdefensa.

Agenda

1. Antecedentes
2. ¿Dónde atacan a las organizaciones?
3. Ecosistema y desafios del sector eléctrico
4. Recomendaciones



Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

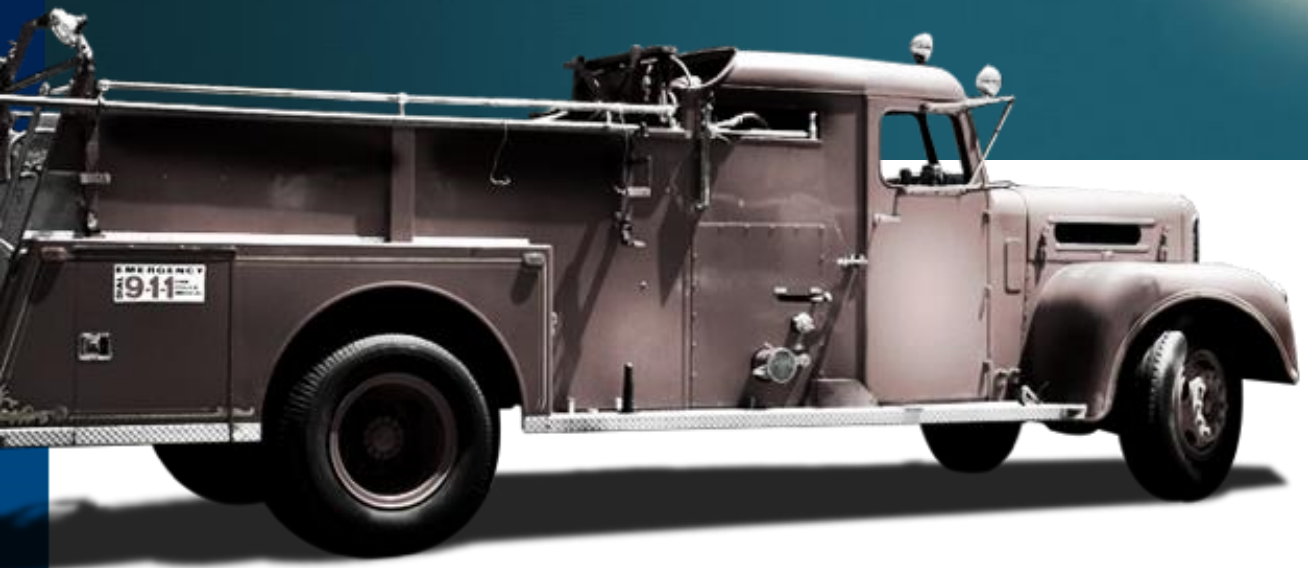
1

Antecedentes

La luz nace también **EN UNA GOTA DE AGUA**

1901

2022

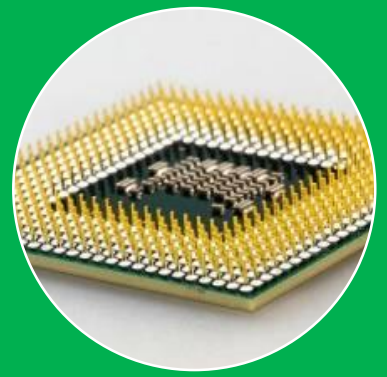


LA LUZ ES SÍMBOLO DE DESARROLLO UNIVERSAL

Habilitadores en los sectores

Capacidad de Transmitir

x2 / 9 meses



Capacidad de Procesar

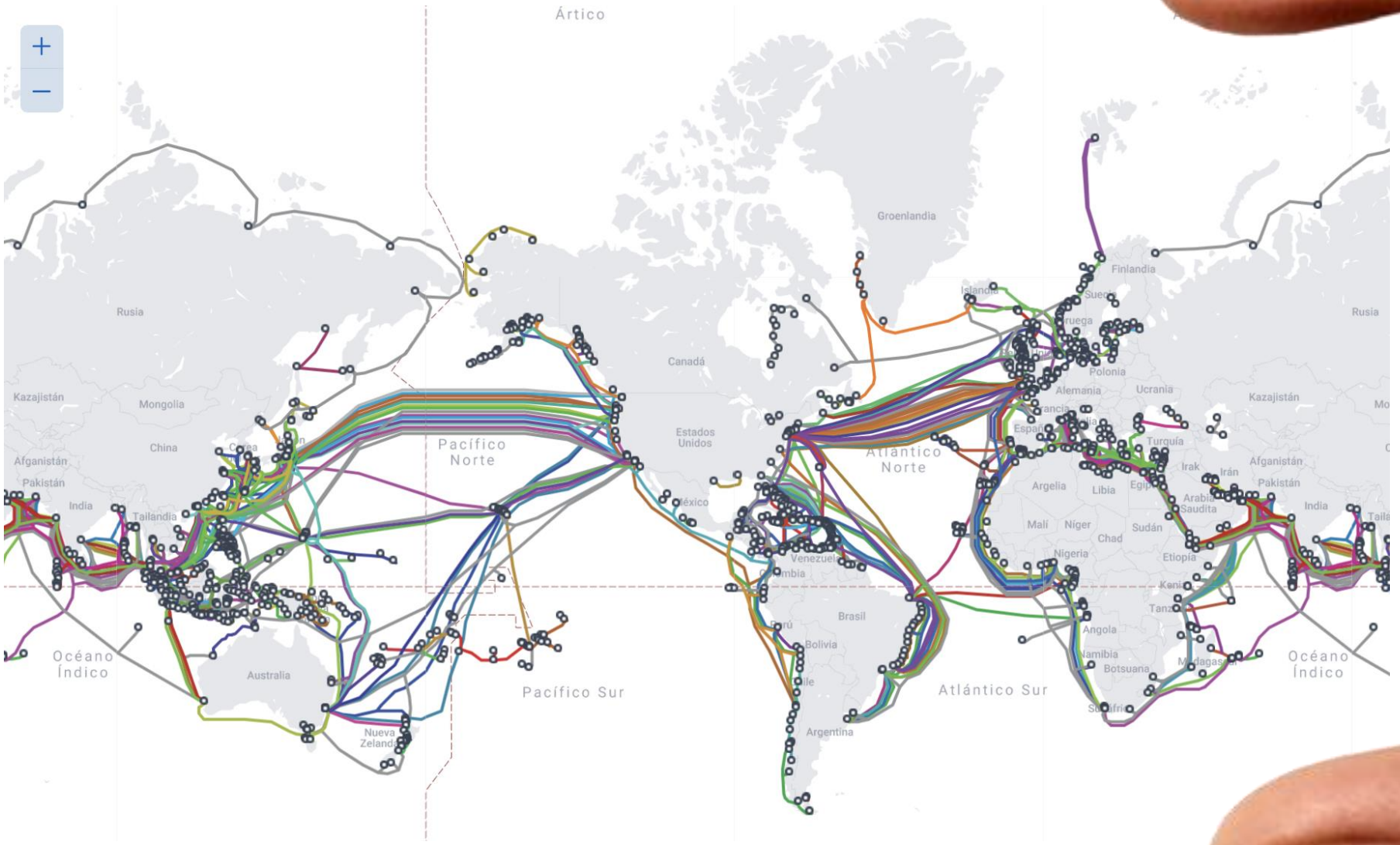
x2 /18 meses

Capacidad de Almacenar

X2 / 13 meses

Moor´s Law (Moore, G, 1975), Butter´s Law (Butters G, 1976), Kryder´s Law (Kryder, M, 1945)

Conexión fibra hoy



Ejemplos del cambio:

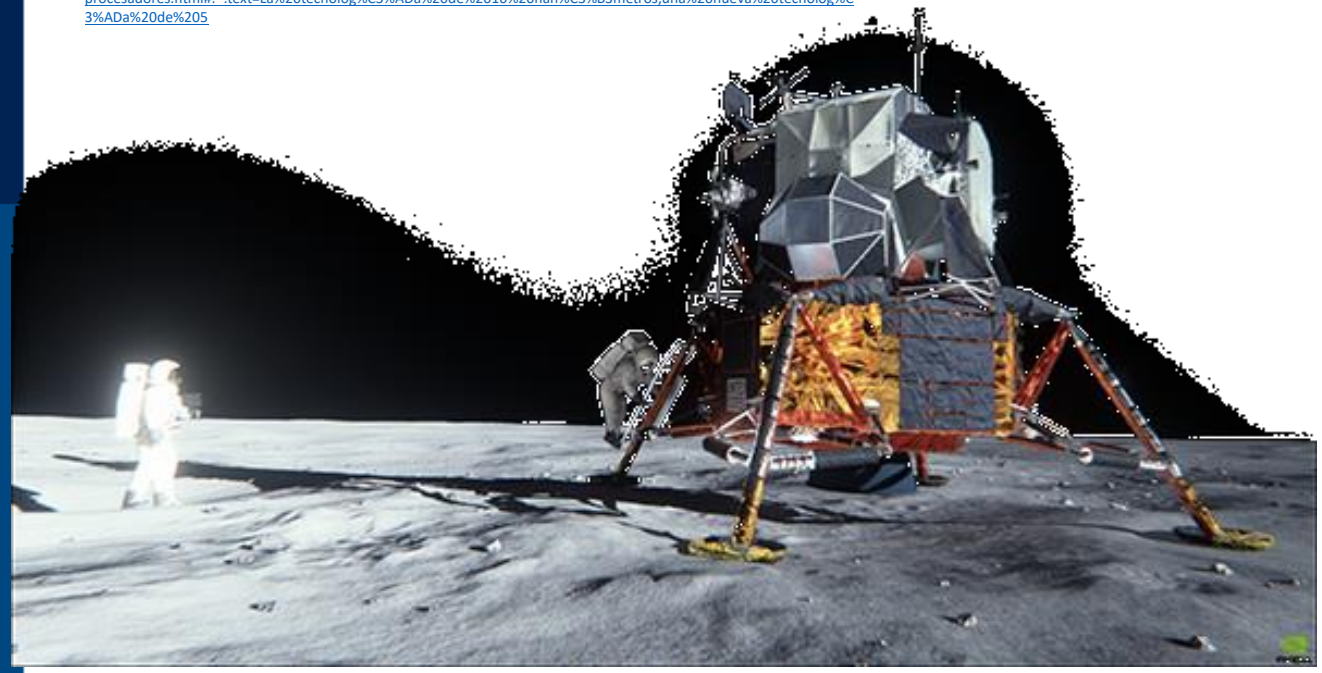
El computador del Apolo XIV, que alunizó en 1971, tenia 12.000 transistores, un iphone 6+ cuentan con 2.3 millones de transistores.

PROCESADORES

30.000 millones de transistores en el tamaño que ocupa una uña

• La industria crea chips cada vez más cerca de los límites del átomo

Fuente: La vanguardia (2017), https://www.lavanguardia.com/tecnologia/20170630/423774241459/tamano-chips-procesadores.html#:~:text=La%20tecnolog%C3%ADa%20de%2010%20nan%C3%B3metros,una%20nueva%20tecnolog%C3%ADa%20de%205



Si un auto de 1971 hubiera avanzado a la velocidad del microchip, hoy este auto debería:

Recorrer en 2 horas, 1.000.000 kms, con 4 galones de gasolina y deberían costar $30.000 COP

¿Y dónde están los cambios?

Internet de las cosas

Conectividad

Robótica

Biotecnología

Realidad aumentada

Realidad virtual

Seguridad

Virtualidad

Banca

Logística

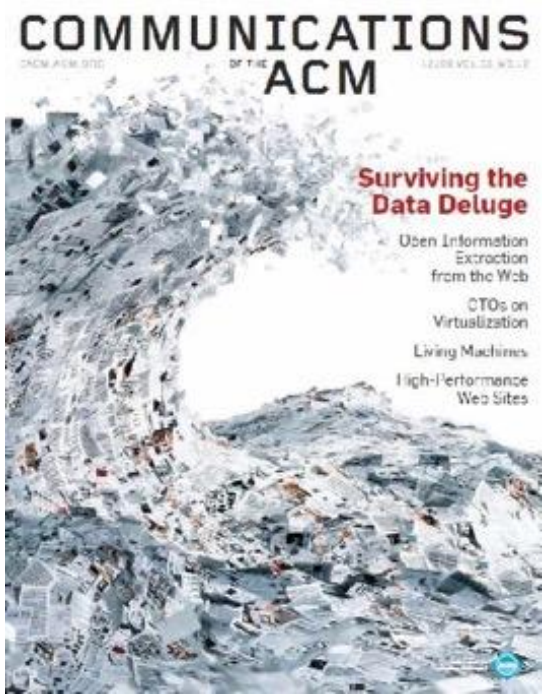
Farmacéutico

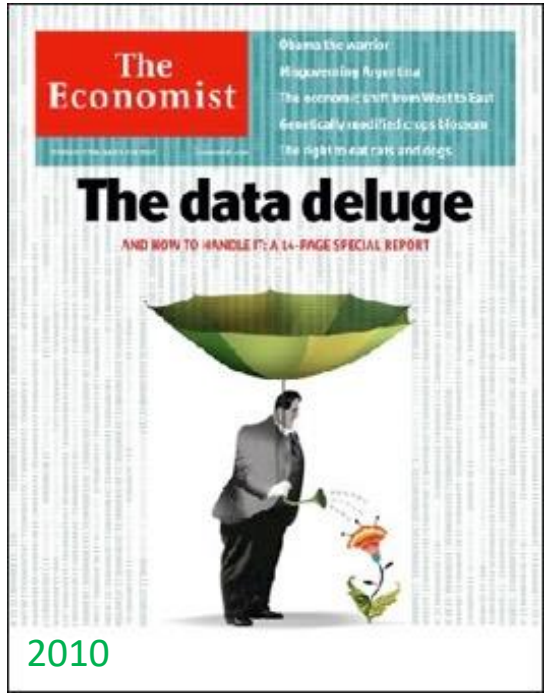
Gobierno

Transporte

Energía

Los DATOS que nos entregan los clientes son abundantes en las organizaciones…





… y también se pueden monetizar a través de la toma de decisiones.

… se vinculan articuladamente con la tecnología y las personas para cambiar los modelos de negocio.

Fuente: Internet, portadas de revistas.


EL DATO

1.4 millones

petabytes

de almacenamiento

15 siglos

de video HD

Fuente: Gartner Insight Study 2021

No solo tenemos más datos…

tenemos más fuentes

Fuentes tradicionales:

- Maquinaria industrial
- Medios de comunicación social
- Sensores IoT
- Entrevistas
- Documentos internos

Fuentes no tradicionales:

- Imágenes
- Audio
- Video
- Web profunda
- Machine Learning

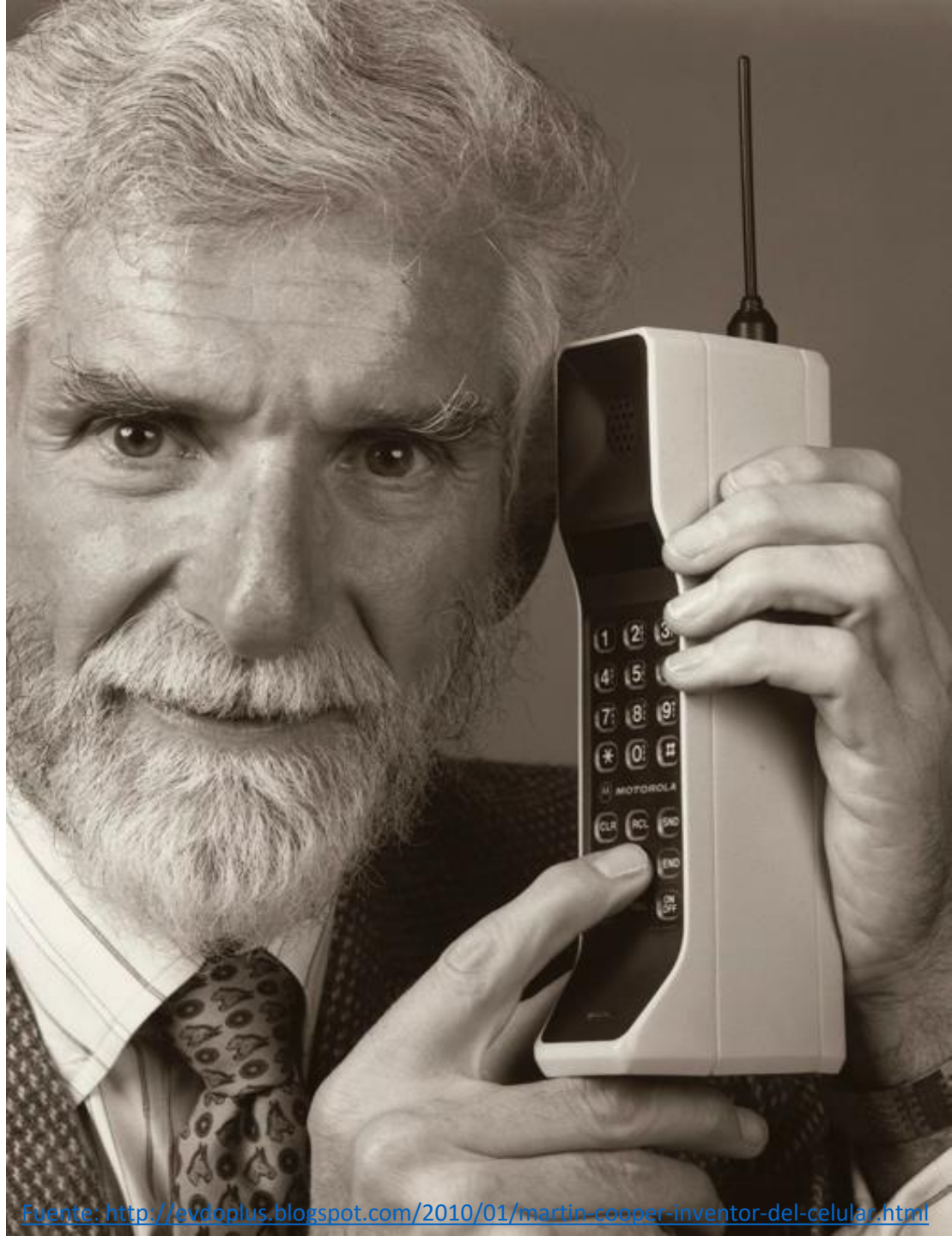
Gratuidad:

- Acceso
- Ubicuidad

Rompimiento de fronteras físicas y psicológicas.

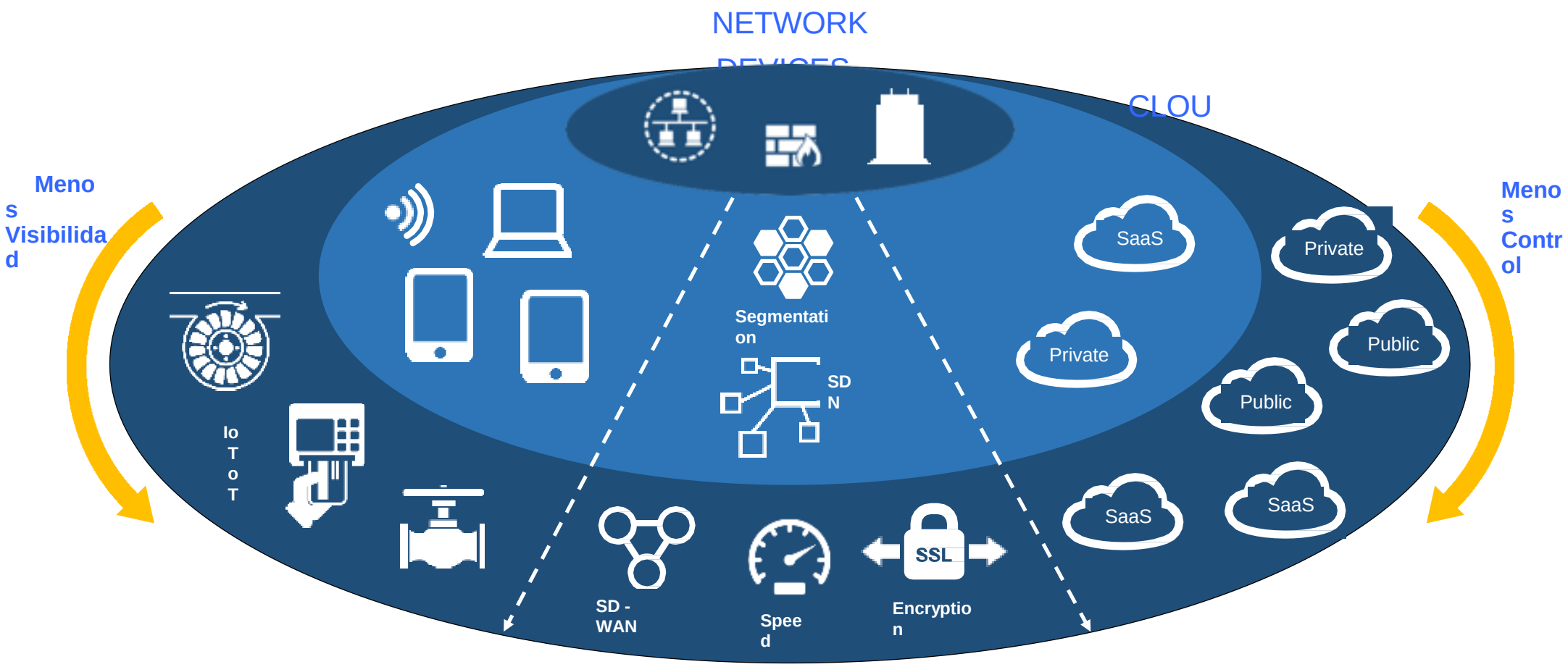
Desafíos del dato:

- Administración
- Arquitectura
- Cumplimiento regulatorio global



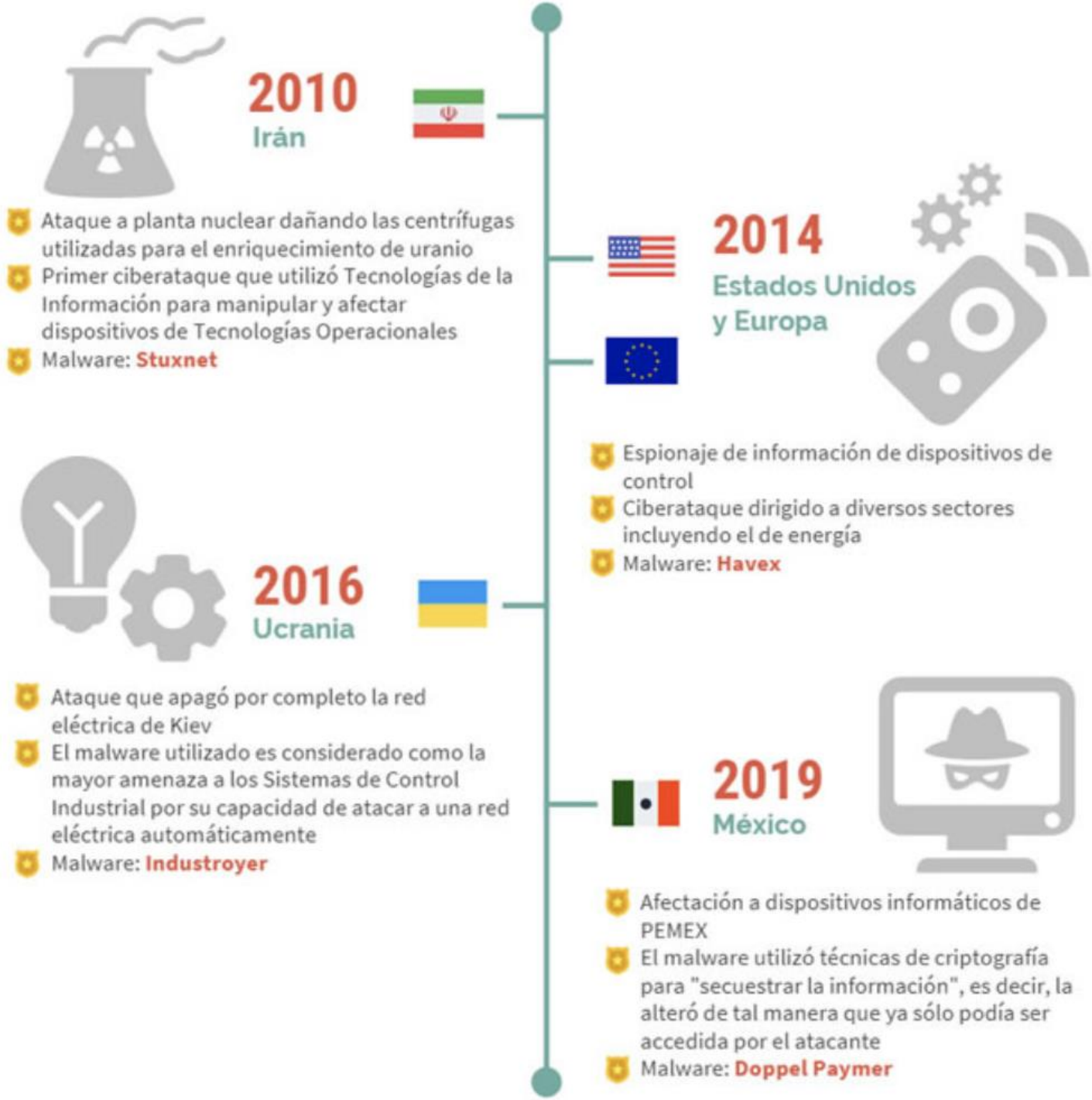
Fuente: http://evdoplus.blogspot.com/2010/01/martin-cooper-inventor-del-celular.html

Los datos y su acceso crean una superficie de ataque mucho mayor



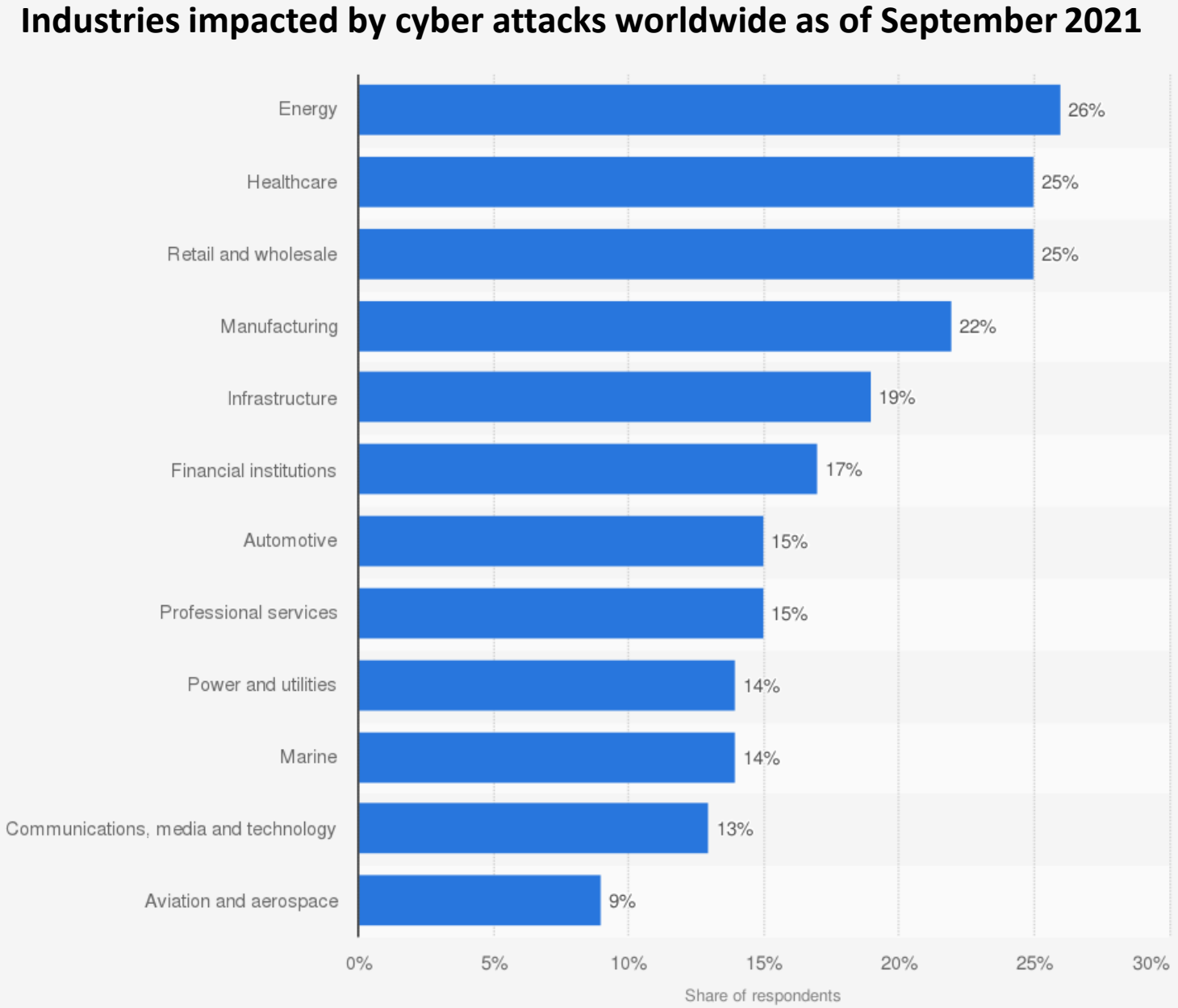
S U P E R F I C I E D E A T A Q U E D I G I T A L

Sucesos relevantes en el sector eléctrico a nivel global



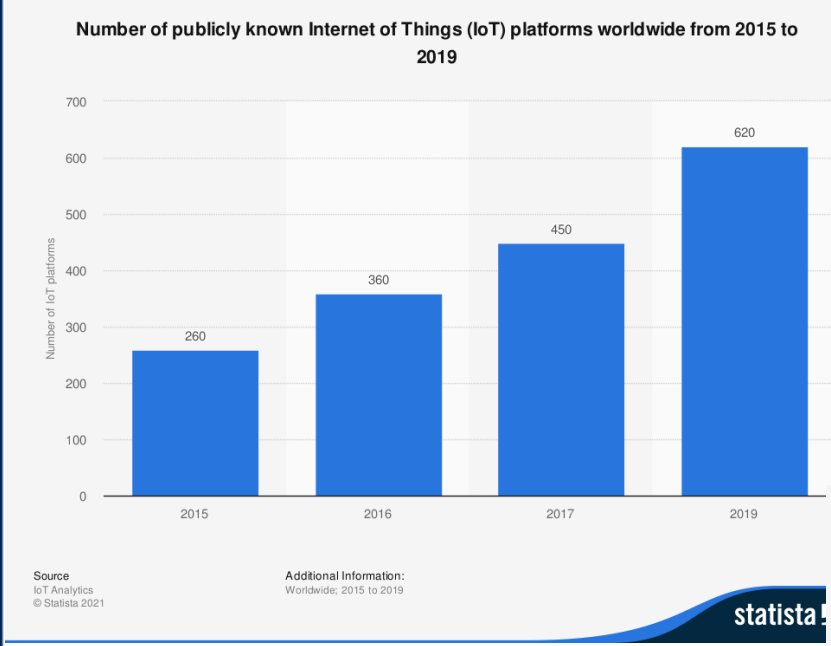
Las redes eléctricas son responsables de proporcionar electricidad a los productores y consumidores, lo que permite que continúe la vida tal como la conocemos.

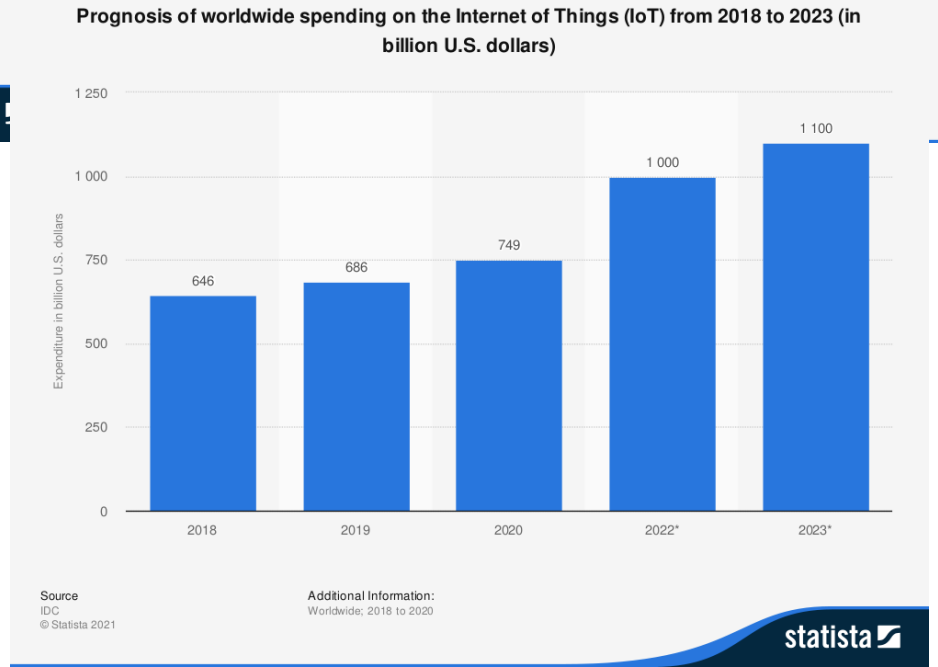
Las amenazas cibernéticas y los adversarios continúan adaptándose y evolucionando, demostrando un cambio en su enfoque para centrarse más en las cadenas de suministro (supply chain) y también en comprometer sistemas de control industrial (ICS).



¿Y cómo llegamos a las redes de energía?

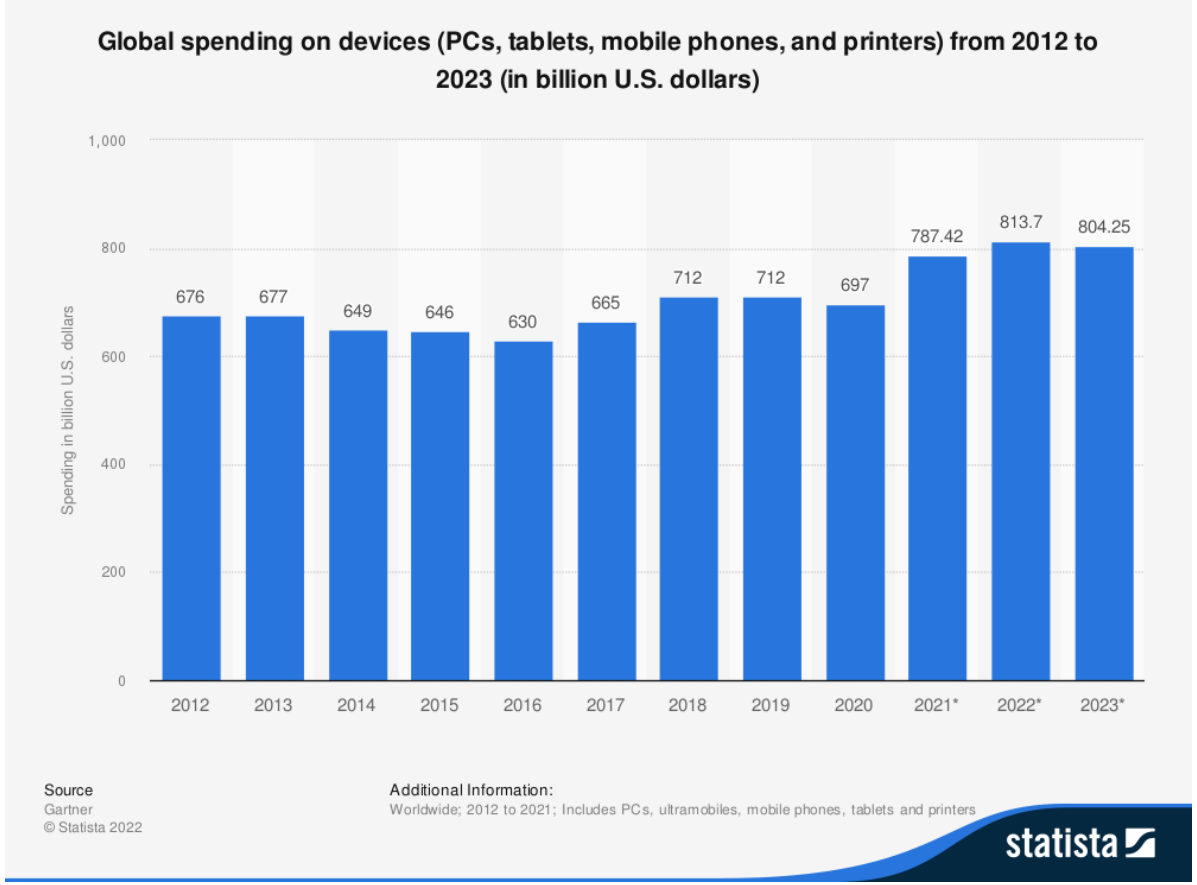
1. Integración y crecimiento de la IoT

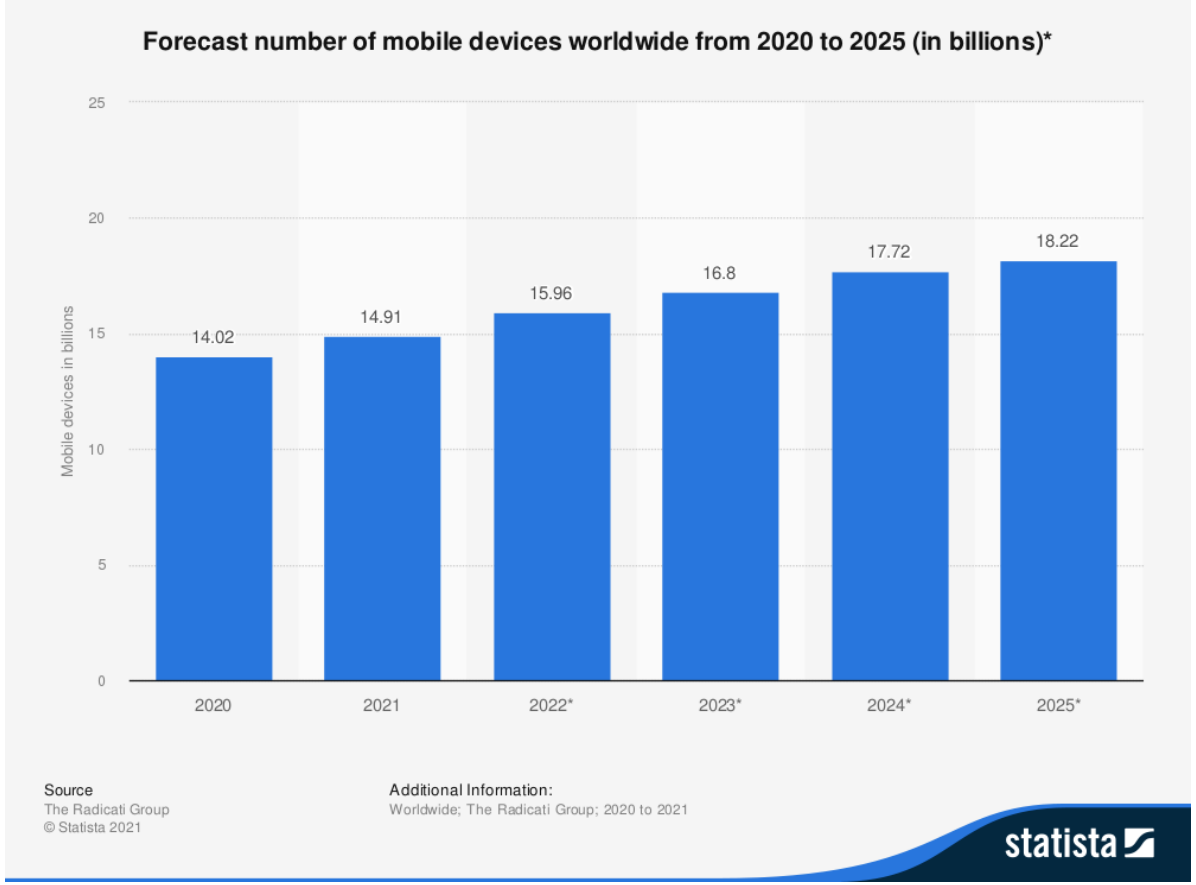




¿Y cómo llegamos a las redes de energía?

2. Crecimiento de conectividad de dispositivos





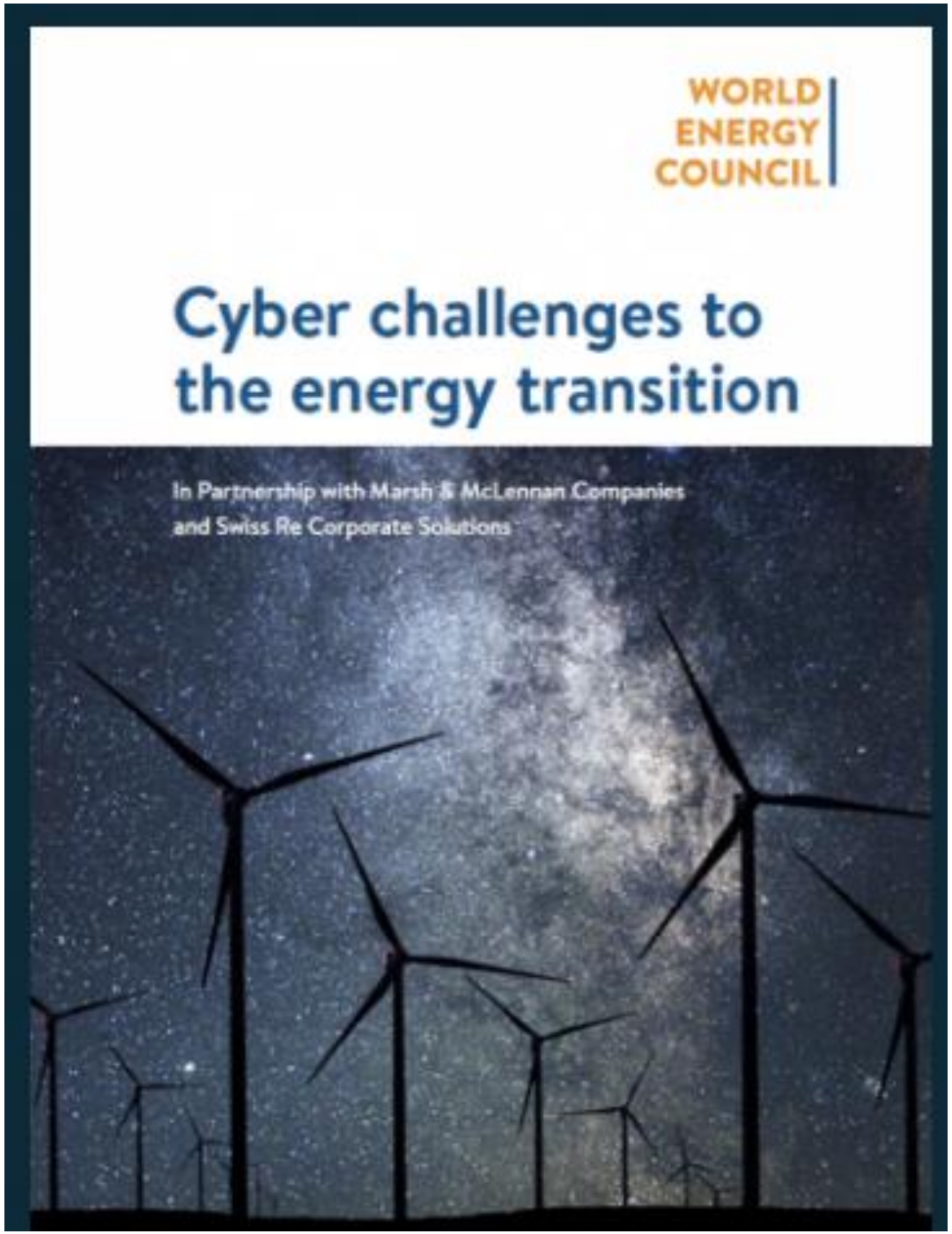
¿Y cómo llegamos a las redes de energía?

Integración y crecimiento de la IoT

Crecimiento de conectividad de dispositivos

amenazas continúan enfocando sus esfuerzos contra las redes de tecnología de la información (TI) para usarlas como punto pivote al intentar lograr el compromiso de las redes de tecnología operativa (OT).

- falta de visibilidad en sus propias redes,
- una extensa cadena de suministro susceptible a compromisos,
- segmentación inadecuada de TI y OT,
- la incapacidad de responder rápidamente a las amenazas actuales.



recomienda que: "…las empresas energéticas consideren los riesgos cibernéticos como riesgos empresariales fundamentales"

Las empresas deben cooperar para evaluar, comprender y crear una fuerte resistencia a estos riesgos, que amenazan:

- Continuidad del servicio,
- Reputación
- Los datos y los sistemas.

Aproximádamente, 9 de cada 10 organizaciones que utilizan ICS han sufrido una brecha de seguridad en dichos sistemas

Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks - Fortinet, Mayo 7, 2018

Hoy se hace imposible pensar en una red inteligente de distribución de energía sin ciberseguridad.

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

2

Dónde atacan a las organizaciones

Impactos y puntos de entrada hacia una red OT

Cuando los controles de los dispositivos físicos de una red OT se conectan con otras redes de datos, la superficie de ataque disponible para que un adversario comprometa a una organización industrial se expande.

AISLAMIENTO

Tradicionalmente, la red OT se encuentra aislada de la red IT. Dado esto, la ciberseguridad no es usualmente una prioridad para la red OT. Por lo tanto, la implementación de medidas de seguridad e higiene deben tomarse en consideración como parte de buenas prácticas.

VECTOR DE ENTRADA

Spear-phishing, estaciones de trabajo comprometidas y el robo de credenciales son los tipos vectores de ataque más comunes dentro de la industria. Esto marca la importancia del uso de 2FA, concientización hacia los empleados y monitoreo continuo de indicadores de compromiso (IoC)

SABOTAJE

Los ciberatacantes han obtenido mayor expertise en cuanto a la obtención de información para lograr un sabotaje. Se han observado desarrollos, ventas y herramientas especializadas para penetrar redes OT, representando un mayor riesgo.

SEGMENTACIÓN

La falta de segmentación dentro de una red OT es una de las vulnerabilidades más explotadas. Esto permite que un malware que se haya infiltrado exitosamente a una red OT se expanda lateralmente con mucha facilidad.

BRECHA IT / OT

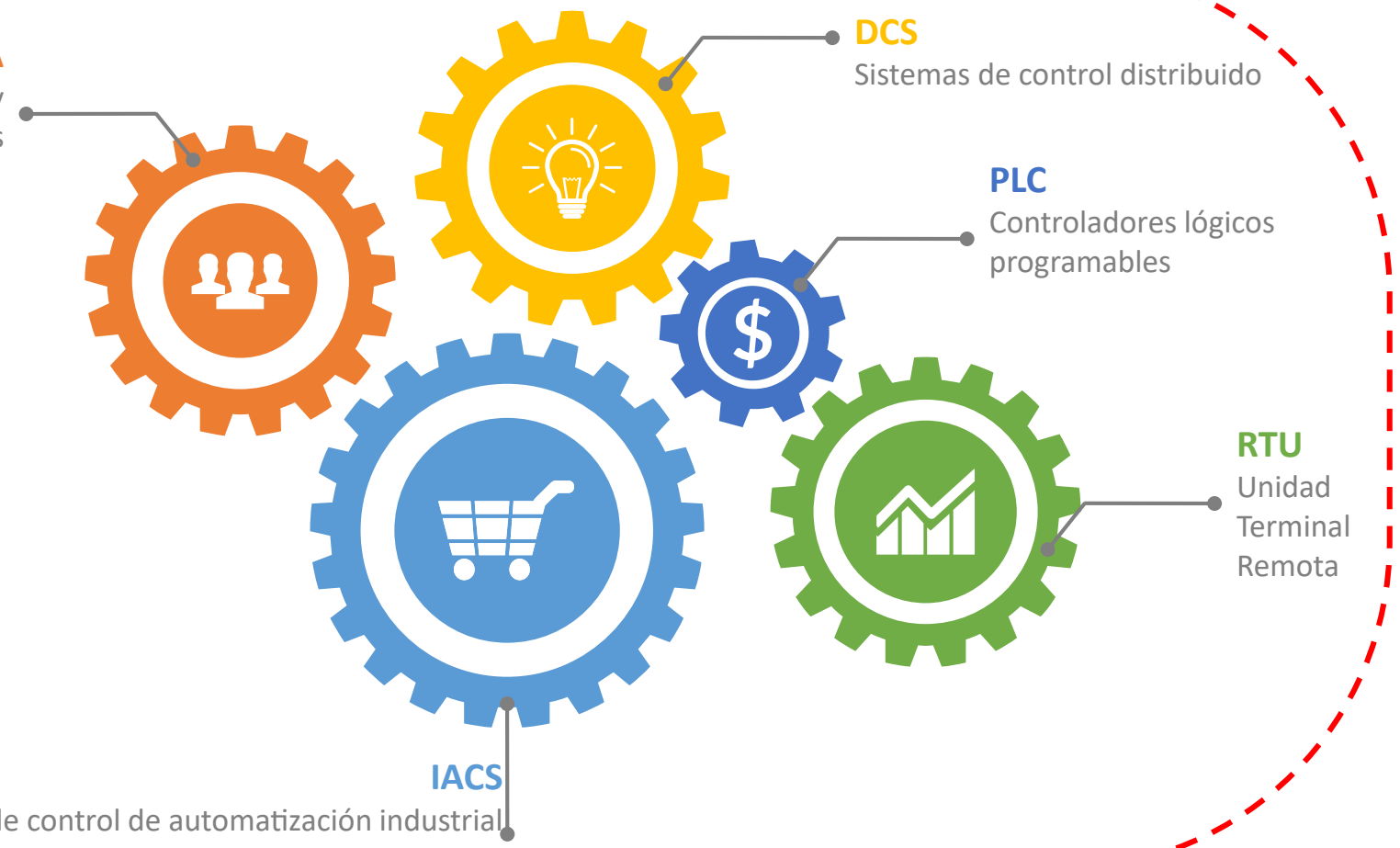
La brecha cultural entre IT y OT genera riesgos dentro de la organización. Particularmente, aquellas organizaciones que poseen la administración de ambas áreas divididas son más susceptibles a sufrir ciberataques

ACTORES EXTERNOS

Actores patrocinados por entes gubernamentales representan aquellos ciberatacantes de mayor amenaza y han demostrado su habilidad para cometer daños de consideración.

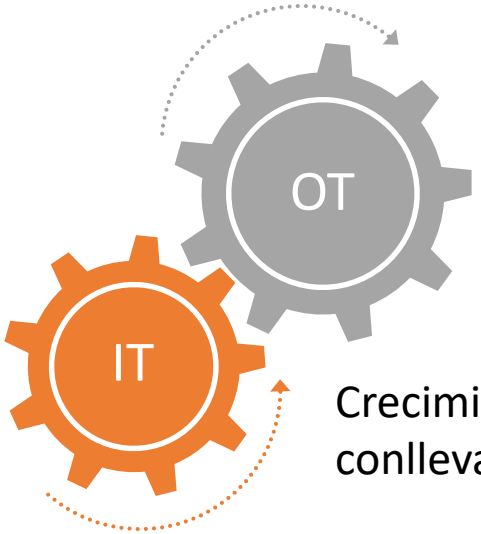
Amenazas contra ICS

Los sistemas de control industrial (ICS) corresponden a la instrumentación necesaria para controlar procesos industriales



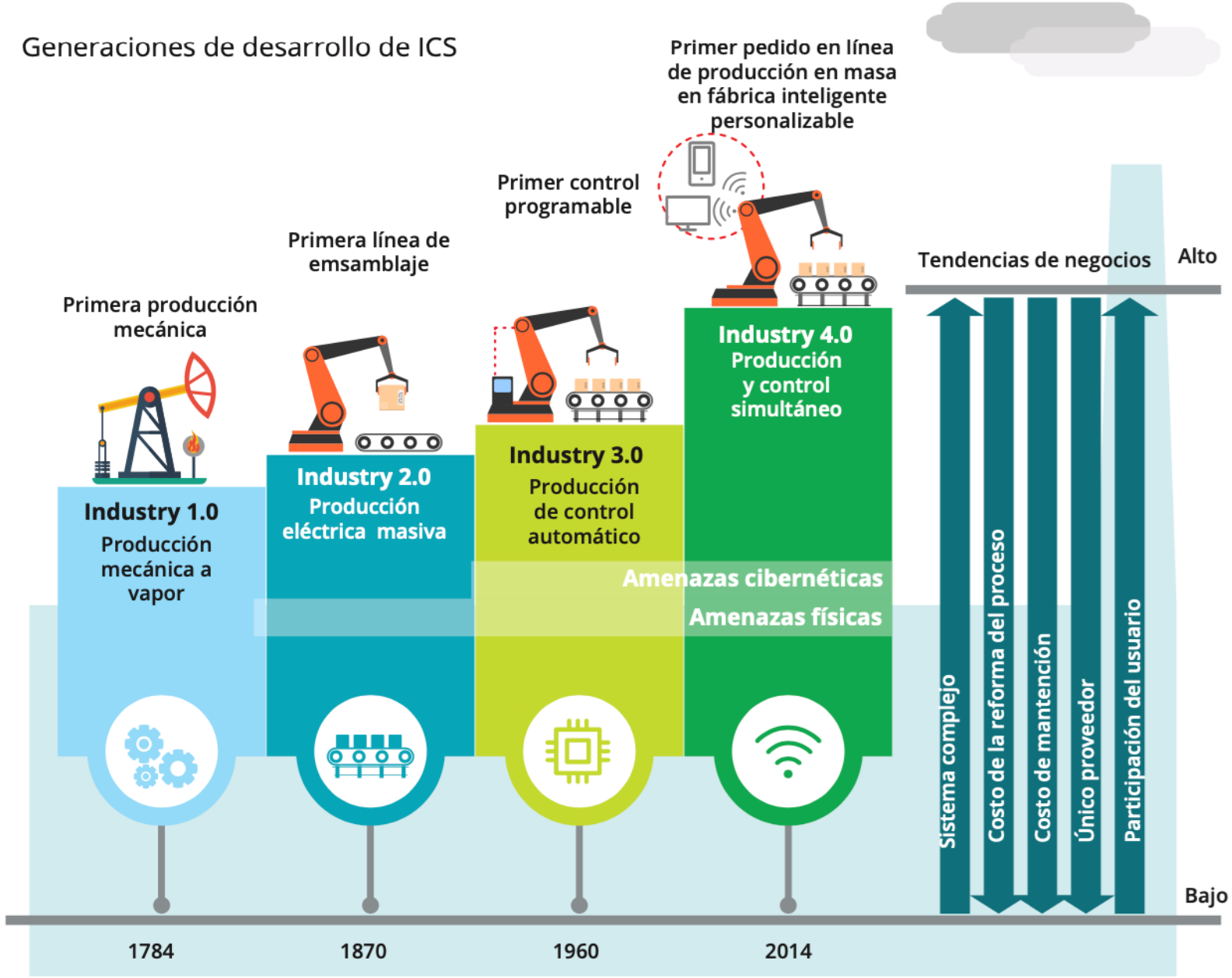
Las organizaciones utilizan sistemas de control automatizado que permite la autogestión y acceso remoto para los procesos requeridos de ICS. Si bien estos procesos permiten una mayor eficiencia y flexibilidad, éstos también introducen nuevos vectores de ataques y ciberamenazas.

Amenazas contra ICS

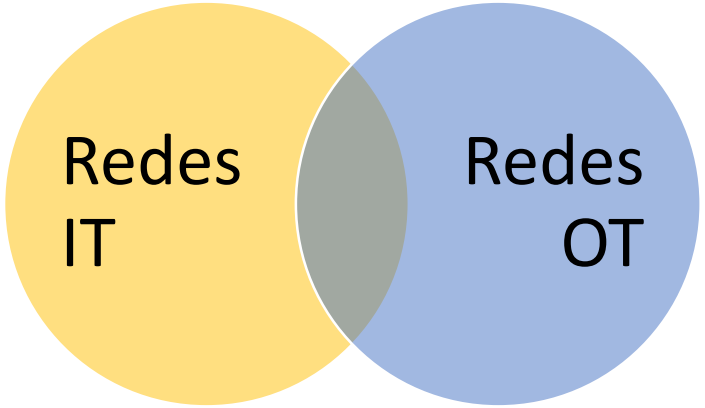


Crecimiento integración conlleva riesgos como:

- Creciente cercanía entre las áreas de TI y OT.
- Modelos de fuerza laboral remotos.
- Uso de terceros para la gestión y mantenimiento de sistemas.
- Incremento en uso de tecnología móvil y el uso de soluciones TI.



Amenazas contra ICS



Dos tercios de sistemas OT están conectados — 32% directamente a internet, y otro 32% por medio de un Gateway a la organización[1].

Si bien la tendencia es incuestionablemente hacia la convergencia, muchas organizaciones han encontrado que esta transición es más complicada —y riesgosa— que lo

1: Barbara Filkins, "The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns," SANS Analyst Program, July 2018.

¿Cómo y donde convergen?

Ambientes OT

contemplan tanto el software como hardware que ejerce cambios a través de un monitoreo directo o control de un dispositivo físico, proceso y/o eventos.

Ambientes IT

se enfocan en la capacidad para almacenar, obtener, transmitir y manipular información.

	OT	IT
Información	• Ejecución de cambios o detección de dispositivos físicos, procesos y eventos	• Almacenamiento, manipulación, obtención y transmisión de información
Objetivos	• Seguridad física (clientes y trabajadores) • Disponibilidad • Integridad • Confidencialidad	• Disponibilidad • Integridad • Confidencialidad
Impacto por ciberataque	• Daño ambiental • Pérdida de vida • Pérdida de ingresos por minuto/hora • Riesgo a seguridad nacional • Disrupción a cadena de suministro • Daño reputacional • Penalidades regulatorias • Fuga de información	• Disrupción de Operaciones • Fuga de Información • Daño reputacional • Fuga de información sensible
Parchado	• Complejo de ejecutar • Realizado por fabricantes (remotamente)	• Programadas oportunamente • Realizada por equipo de ITCiclo
Ciclo de vida	• vida-20-30 años, cada vez menor debido a convergencia con IT	• IT-3-5 años
Procesamiento	• Limitado, desactualizados	• Altamente escalable

Barbara Filkins, “The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns,” SANS Analyst Program, July

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

3

Ecosistema y desafios del sector electrico

Problemas en el sector eléctrico

Acceso no autorizado, como habilitador para el ciber-espionaje tanto para obtener una ventaja económica como para potencialmente permitir ataques futuros más destructivos por parte de actores patrocinados por estados. El acceso no autorizado se obtiene mediante métodos tradicionales y conocidos, como lo son el envío de correos electrónicos con archivos adjuntos y enlaces (phishing), así como a través del compromiso de la cadena de suministro o por medio de amenazas internas.

El ransomware y las amenazas al almacenamiento en la nube siguen siendo generalizadas para las organizaciones de energía y servicios públicos debido a su naturaleza operativa de 24x7, lo cual les impide estar inactivas por cualquier período de tiempo. Este requisito es algo que los ciber-delincuentes y las amenazas persistentes avanzadas (Advanced Persistent Threats - APT) conocen.

	Maldocs	***Fuerza Bruta***	***Wipers***	***Malware IoT***	***Troyano Acceso Remoto (RAT)***	***Validadores de cuenta***	***Rasomware***
	Documentos infectados	*Intento de descifrar una contraseña o nombre de usuario, de buscar una página web oculta o de descubrir la clave utilizada para cifrar un mensaje, con el método de prueba y error.*	*Ataque que busca borrar el contenido que haya en una memoria o disco*	*diseñado para tomar el control de los dispositivos conectados a Internet.*	*Aplicaciones que parecen genuinas pero que contienen malware y que pueden descargarse involuntariamente en un dispositivo.*		*Es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.*
Amenazas en servicios en la nube			■		■		■
Vulnerabilidades y configuraciones erroneas		■	■			■	■
Ataques a cadenas de suministro		■	■			■	■
Amenazas internas	■					■	■
Ataques contra ICS	■		■			■	
Espionaje	■		■		■	■	
Ataques de Ransomware			■	■		■	
Troyanos de acceso remoto (RATs)		■			■		■
TOTAL	**3**	**3**	**6**	**1**	**3**	**6**	**5**

Fuente: Deloitte & Fortinet

7 desafíos de la ciberseguridad en el sector energético

Los desafíos dentro del sector energético deben contemplar factores adicionales en relación a otras industrias, convirtiéndolo en la industria donde mayor foco se debe poner en seguridad física y disponibilidad del servicio. Los siguientes tópicos corresponden a una lista de desafíos que el sector energético debe tener en consideración:

Ciberseguridad para infraestructuras de energía removable

Las nuevas formas de energía, como la energía renovable a través de la energía solar o eólica, por lo general están menos centralizadas. Esto no solo crea nuevos desafíos para la distribución y el almacenamiento, sino también para la ciberseguridad.

Seguridad física

Las instalaciones de energía tienen maquinaria y procesos físicos que podrían causar lesiones físicas en el caso de existir una falla. En el panorama actual de amenazas, los cibercriminales pueden interrumpir las operaciones de la infraestructura crítica creando problemas de seguridad para los empleados en el sitio e incluso para los residentes cercanos. Además, las interrupciones en los procesos de generación, transmisión y distribución también pueden hacer que la energía no sea segura para los consumidores. Cualquiera de estas eventualidades traería graves consecuencias para la organización, desde demandas hasta el cierre de operaciones por parte de los reguladores.

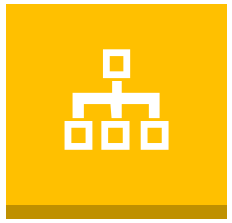
Productividad y tiempo de actividad

Los ciberataques a las compañías de energía con frecuencia están diseñados para causar demoras e interrupciones en las operaciones, dejando a las organizaciones con daños financieros significativos. Junto con la interrupción de la continuidad del negocio, la debido a la ineficiencia de la red o a eventos de ciberseguridad. Un ejemplo de amenazas hacia OT es el ataque a la red eléctrica de Ucrania ocurrido en diciembre del 2015

7 desafíos de la ciberseguridad en el sector energético

Eficiencia operativa

La falta de integración entre los diferentes elementos acoplados de seguridad junto con la fragmentación arquitectónica aumenta las ineficiencias operativas. Sin la integración entre los entornos de OT y TI, muchos flujos de trabajo de seguridad se deben administrar manualmente, lo que ralentiza los procesos y crea espacio para errores humanos. Además de retrasar la detección, la prevención y las respuestas de amenazas, los silos arquitectónicos crean redundancias en la administración de aplicaciones e incluso en las licencias de software y hardware, lo que aumenta los costos de gastos operativos.

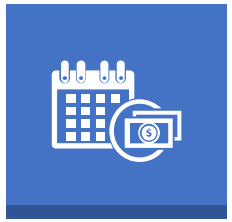


Experiencia al cliente

Las compañías de energía ahora interactúan con su base de clientes a través de una diversidad de medios electrónicos. La seguridad para las comunicaciones electrónicas es crítica, ya que una violación de la seguridad podría exponer datos personales y confidenciales de los clientes.

Integridad del producto

Las empresas de energía se dedican a proporcionar un servicio constante e ininterrumpido en geografías particulares. Se deben evitar las brechas o los ciberataques que provoquen cortes de energía o tiempo de inactividad para brindar un servicio ininterrumpido a los usuarios que con- fían en estas infraestructuras críticas.



Cumplimiento

La energía están sujetos a una amplia variedad de regulaciones y normas y, por lo general, están sujetos a la supervisión directa del gobierno. Si bien las sanciones financieras por incum- plimiento pueden ser altas, un costo aún mayor a menudo proviene del menoscabo de la reputación de la marca, en caso de incumplimiento o interrupción del servicio. Las organizaciones deben poder demostrar el cumplimiento de múltiples regulaciones y normas sin volver a cambiar al personal de las iniciativas estratégicas para preparar informes de auditoría.

¿Quiénes atacan estas infraestructuras?

Tipo de actor	Motivación	Impacto	Tipos de ataques
Amenaza Avanzada Persistente	Ventaja - Estratégica/geopolítica Desestabilizar a un adversario - Competitividad comercial	Disrupción - Infiltración - Espionaje	0-Day Malware especializado Phishing
Terroristas	Social - Religiosa - Política Desestabilizar a un adversario - Competitividad comercial	Disrupción - Destrucción de Servicio	Credenciales comprometidas Malware genérico Crimeware DDoS
Criminal	Ganancia financiera - Robo de Propiedad Intelectual	Pérdida de información - Pérdida financiera Espionaje - Disrupción del Servicio	Credenciales comprometidas Malware genérico Phishing Ingeniería social
Hacktivistas	Medioambiental - Social - Religiosa - Política Difusión y enviar un mensaje	Disrupción del Servicio- Daño reputacional	Credenciales comprometidas Phishing DDoS Doxxing Ingeniería social
Insider	Intensional - Desapercibido	Pérdida de información - Pérdida financiera Espionaje - Disrupción del Servicio	Ingeniería social Phishing Acceso privilegiado

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

4

Recomendaciones

Mantener enfoques y soluciones de ciberseguridad separados para TI y OT añade complejidad y dificulta la gestión, terminando muchas veces en brechas de cobertura.

Una visión integral respecto a la ciberseguridad en la organización simplifica su manejo, y reduce la complejidad.

Se debe tener particular cuidado en no implementar soluciones desde una perspectiva netamente técnica y operacional, y en su lugar hacerlo con la visión estratégica del negocio en consideración. El cuidado es el de evitar instaurar “silos” en la organización, los cuales operen de manera aislada y no interactúen con

Frameworks de ciberseguridad

Seguridad de la información y Ciberseguridad

ISO/IEC27002

Provee las mejores prácticas y recomendaciones para los controles de seguridad de la información y promueve su uso para aquellos responsables de iniciar, implementar y mantener un sistema de gestión de seguridad de la información.

ISO/IEC27001

establece buenas prácticas que luchan contra los riesgos y la amenazas. La certificación mejora las relaciones con los clientes y los proveedores.

Contempla 14 dominios y 114 controles, especificando aquellos requerimientos necesarios para mantener, mejorar e implementar un sistema de gestión de la seguridad de la información.

NIST SP 800-39

Desarrollado por el NIST, tiene como propósito entregar guías para la gestión de riesgos asociados a la seguridad de la información para las operaciones organizacionales. Entrega un acercamiento flexible y detallado para evaluar, responder y monitorear riesgos de forma continua.

CRF (Common Regulatory Framework on Cybersecurity)

CRF entrega los requerimientos para una mejor gestión de riesgos asociados a la ciberseguridad y provee una aproximación consistente con las mejores prácticas y regulaciones de ciberseguridad.

NIST SP 800-53

Creado con el propósito de aumentar la seguridad de un sistema de información. Es aplicable a cualquier componente de información que almacene, procese o transmita información. Los controles contenidos contemplan tanto la parte técnica como operacional, con el propósito de mantener la integridad y confidencialidad. Adopta guías para un acercamiento a la gestión de riesgos en distintos niveles y opera en conjunto con el estándar SP 800-37.

Frameworks de ciberseguridad

Sistemas de control industrial

ISA/EIC 62443:

Entrega un marco de referencia flexible para la mitigación de vulnerabilidades actuales y futuras dentro de un sistema de control y automatización industrial. Provee definiciones estándar dentro del ámbito de la seguridad para los diversos componentes, y establece un lenguaje común para simplificar los procesos de integración de equipos, aplicaciones, redes y dispositivos de control que componen el sistema.

IC-IISF (Industrial Internet Consortium (IIC) Industrial Internet Security Framework)

El incremento del uso de dispositivos IoT (Internet of Things) en la industria ha gatillado el desarrollo de este estándar, el cual tiene como foco el entregar un marco de referencia para abordar la seguridad en dispositivos IIoT (IoT industrial). Aborda las definiciones de dispositivos IIoT vs los sistemas pertenecientes a IT y OT. Contempla la identificación y gestión del riesgo desde el punto de vista del negocio e implementación de mejores prácticas para la protección de las comunicaciones, configuraciones y monitoreo.

NIST SP 800-82

Corresponde a una guía hacia sistemas ICS, SCADA, DCS y PLC para identificar amenazas y vulnerabilidades típicas a estos sistemas. Recomienda medidas de seguridad apropiadas para respuesta ante incidentes y mitigación de los riesgos asociados. Permite la revisión industrias (plantas químicas, aguas, eléctricas, manufactura, aeroespacial, etc.).

IC-IISF (Industrial Internet Consortium (IIC) Industrial Internet Security Framework)

El incremento del uso de dispositivos IoT (Internet of Things) en la industria ha gatillado el desarrollo de este estándar, el cual tiene como foco el entregar un marco de referencia para abordar la seguridad en dispositivos IIoT (IoT industrial). Aborda las definiciones de dispositivos IIoT vs los sistemas pertenecientes a IT y OT. Contempla la identificación y gestión del riesgo desde el punto de vista del negocio e implementación de mejores prácticas para la protección de las comunicaciones, configuraciones y monitoreo.

Frameworks de ciberseguridad

Para el sector eléctrico

IEEE 402 (Physical and electronic Security in substations)

Esta guía describe los procedimientos de seguridad para el suministro eléctrico. Contempla detalles técnicos en cuanto a la determinación de resistencias y polarización eléctrica, variables tales como temperaturas, voltajes son también consideradas como parte de la guía para abordar la seguridad física y electrónica en subestaciones.

ES-C2M2 (Electric Subsector Cybersecurity Capability Maturity Model)

Marco de referencia exhaustivo que tiene como objetivo medir las capacidades en ciberseguridad dentro del sector eléctrico. Contempla cuatro objetivos: Mejora en capacidades de ciberseguridad, evaluación de iniciativas, establecimiento de mejores prácticas y puntos de referencia, priorización de procedimientos para la mejora en ciberseguridad. El modelo posee 10 dominios y cuatro indicadores de nivel de madurez, donde cada dominio agrupa cada práctica en ciberseguridad.

NERC CIP (Northamerican Electric Reliability Corporation - Critical Infrastructure Protection)

Dedicado hacia la protección de la infraestructura crítica, define una serie de requerimientos diseñados para mejorar la seguridad a los activos requeridos para la operación de una red eléctrica. Su propósito es establecer una base de medidas enfocada en el rendimiento, gestión de riesgos y capacidades. Actualmente es un requerimiento mandatorio para plantas eléctricas en EE.UU.

ENISA Smart Grid Threat Landscape and Good Practice Guide

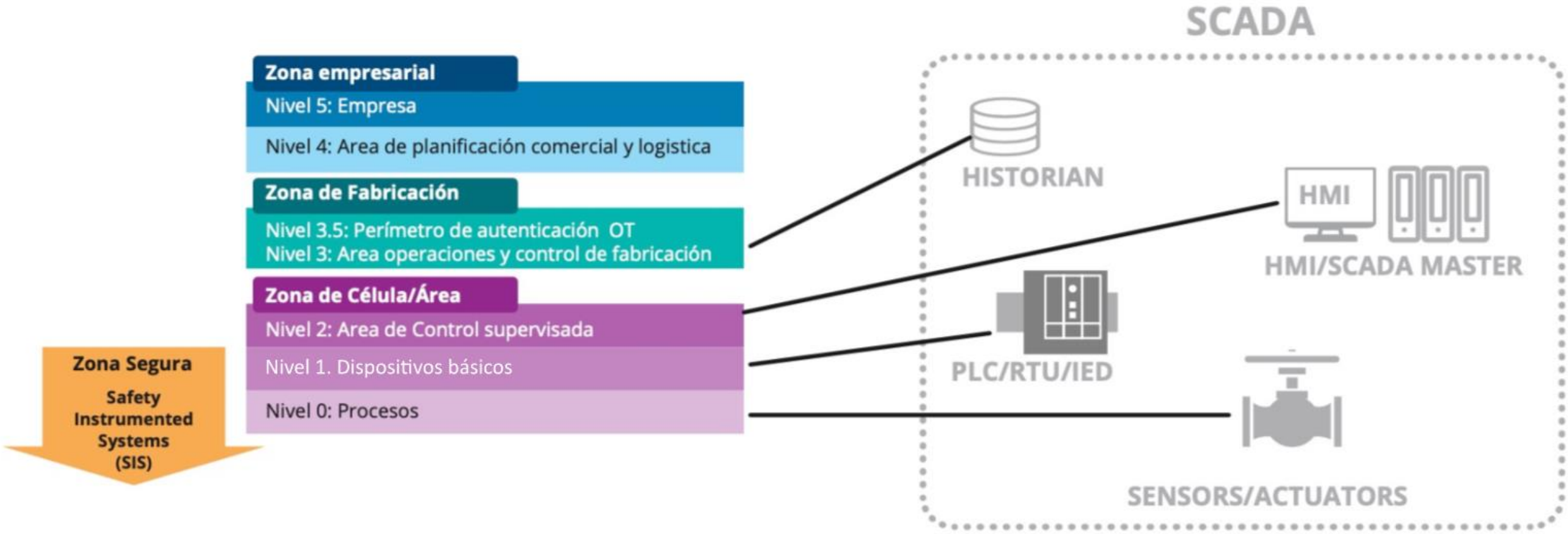
Publicado por ENISA (La agencia de la Unión Europea para Ciberseguridad), provee una guía de buenas prácticas para abordar ciberataques tanto externos como internos, también clasifica distintos elementos de una red eléctrica dada su alta complejidad a nivel de componentes. Describe métodos para identificar distintos niveles de protección hacia los activos para el fortalecimiento de la ciberseguridad, incluyendo la cadena de suministro.

ENISA Appropriate Security Measures for Smart Grids

Documento técnico, el cual define diez dominios que contemplan medidas de seguridad para tres tipos de niveles dentro de una red eléctrica inteligente. Permite el lineamiento de distintos niveles de seguridad con operadores, establece un mínimo nivel de seguridad y resiliencia para lograr a identificación del eslabón más débil. Además, facilita la preparación para una recuperación y medidas de respuesta ante una crisis.

¿Cómo fomentar la arquitectura en TO?

Modelo Purdue



La zona de Célula/Área:

- **Nivel 0:** Activos físicos de alto valor involucrados en el proceso, controlados por sensores y actuadores.
- **Nivel 1:** Dispositivos básicos e inteligentes que detectan y manipulan procesos físicos, como PLC y RTU.
- **Nivel 2:** Sistemas de control de área que supervisan y supervisan los procesos, incluidos HMI y maestros SCADA.

La zona de fabricación consta de:

- **Nivel 3:** Sistemas de operaciones de fabricación en el sitio que administran el flujo para producir la salida deseada. El nivel 3 también puede contener el historiador operativo, una base de datos que captura el control de supervisión, el monitoreo del desempeño y las métricas de garantía de calidad.

La zona empresarial consta de:

- **Nivel 4:** Planificación de negocios en el sitio y aplicaciones de logística, incluidos niveles de ERP, programación, uso de materiales, envío e inventario.
- **Nivel 5:** Infraestructura de TI empresarial y aplicaciones utilizadas por la organización controladora.

Recomendaciones desde los FW y el modelo Purdue

Segmentar la red

04

Uno de los pasos principales para mejorar la seguridad OT es la segmentación de las redes, dado que es uno de los conceptos de arquitecturas más efectivos para este fin. Se debe destacar que el modelado de zonas de segmentación debe contar con dinamismo, y no ser estático: La segmentación tradicional asume un valor de confianza estático tanto para usuarios, aplicaciones y dispositivos; paradigma que se ve cuestionado si consideramos como estos elementos cambian constantemente dentro de una organización, ya sea por cambios del negocio o por amenazas emergentes. El framework de ISA/IEC-62443 entrega guías prácticas para la segmentación de una red. A cada zona se le puede asignar un nivel de seguridad de 0 a 4, con el 0 representando el nivel más bajo de seguridad, y 4 el más alto

Monitorear el tráfico

03

Luego de segmentar una red, es crítico ganar visibilidad sobre el tráfico que circula por cada segmento. Esto permitirá alertar de manera temprana la presencia de una amenaza conocida, o en su defecto podrá asistir a la organización a identificar anomalías (tanto en tráfico como en comportamiento de usuarios) que pudiesen ser predecesoras a un ataque mayor.

Control de accesos y dispositivos

02

Usuarios, aplicaciones y dispositivos deben ser autenticados antes de ser otorgados los permisos para acceder a un segmento de la red OT. Este punto es crítico, considerando que algunos de los ataques más devastadores sobre ambientes OT se han efectuado por medio de cuentas de usuarios y contraseñas comprometidas, lo cual se ve exacerbado cuando no se cuenta con un apropiado nivel de control de acceso. Iniciativas de NAC (Network Access Control), RBAC (Role Based Access Control) y de Gestión de Accesos se alinean con este objetivo.

Proteger puntos de acceso

01

Si bien tradicionalmente los ambientes OT no cuentan con conexiones o puntos de acceso inalámbricos, diversas organizaciones están incrementalmente implementando sensores y otros dispositivos en sus ambientes OT y conectándolos de manera inalámbrica. Los puntos de acceso y dispositivos de comunicación son generalmente un objetivo atractivo para los atacantes. Es necesario que estos componentes cuenten con seguridad por diseño, y que sean administrados desde una interfaz central en lugar de manera particular.

5 prácticas recomendadas para la seguridad en el sector eléctrico

Tradicionalmente, los entornos OT no han contenido conexiones inalámbricas. Sin embargo, en muchos casos, las organizaciones implementan sensores y otros dispositivos en sus entornos OT y los conectan de forma inalámbrica. Esto aumenta la superficie de ataque digital. Los puntos de acceso inalámbrico (AP), así como los switches de red, son objetivos atractivos para los ataques cibernéticos. Ambos necesitan seguridad por diseño, administrada desde una interfaz central, en lugar de estar protegidos por soluciones de seguridad de puntos adicionales administradas a través de múltiples interfaces.

Los dispositivos, usuarios y aplicaciones deben autenticarse antes de que puedan acceder a los segmentos de la red OT. La autenticación segura es crítica y muchas de las brechas de seguridad más dañinas de OT se deben a cuentas de usuario y contraseñas comprometidas exacerbadas por los usuarios que reciben niveles de acceso inapropiados.

Una vez que los firewalls dividen una red OT en zonas, segmentos y conductos, es valioso analizar el tráfico de red para detectar amenazas conocidas y desconocidas, donde el primer requisito es poder visualizar el tráfico de forma integrada. Esto con el objetivo de poder identificar y vigilar la red de forma completa, incluyendo los protocolos de comunicación de ICS / SCADA

Si se produce una brecha de seguridad en la red, la segmentación restringe el movimiento y el impacto de un atacante. La segmentación en una red OT minimiza la exposición a ataques y, por lo tanto, es una práctica recomendada para asegurar OT como se describe en los estándares de seguridad ISA / IEC- 62443 (anteriormente ISA-99).

Un equipo de ciberseguridad no puede proteger los activos los cuales no puede acceder o monitorear. Esto genera una brecha crítica de seguridad para muchas organizaciones. El primer paso para mejorar la postura de seguridad de OT es tener un inventario actualizado de dispositivos y aplicaciones que se ejecutan en una red. Esto se puede lograr mediante una evaluación complementaria de amenazas cibernéticas. Un inventario actualizado de dispositivos y aplicaciones en la red, sirve como base para planificar la arquitectura de seguridad, permitiendo implementar las mejores prácticas en función de las necesidades particulares de una organización.

14 PRINCIPLES OF THE FUTURE ORGANIZATION

1. Globally distributed with smaller teams
2. Connected workforce
3. Intrapreneurial
4. Operates like a small company
5. Focuses on "want" instead of "need"
6. Adapts to change faster
7. Innovation anywhere
8. Runs in the cloud
9. More women in senior management roles
10. Flatter structure
11. Tells stories
12. Democratizes learning
13. Shifts from profit to prosperity
14. Adapts to future employee and manager

Dentro de una red OT, la segmentación de la red interna es imprescindible, los métodos tradicionales finalmente se encuentran sujeto a fallas o a ser atacados debido a la falta de eficacia de seguridad y TCO (Total Cost of Ownership) injustificable.

Los líderes de las organizaciones deben asumir la responsabilidad en cuanto a la protección de los activos de datos de sus organizaciones, necesitando adoptar un enfoque más empresarial orientado tanto a la ciberseguridad y seguridad física en la infraestructura como también de los activos de información.

Gracias

lucas.giraldo@esdegue.edu.co
lucas.Giraldo@rsmco.co

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

Escuela Superior de Guerra
@EsdegCol
Escuela Superior de Guerra
Escuela Superior de Guerra
ISSUU
esdeguecol

4TO FORO XM

Una mirada integral a la transición del sector eléctrico.

17 - 18 de marzo de 2022

Escanea este código para ver las memorias de esta ponencia

Patrocina

TermoemCali

a CONTOURGLOBAL company

Organiza

XM

Sumando energías