

GLOBAL CX FORUM

25° CONGRESO MÉXICO

imt.
ORGANIZA



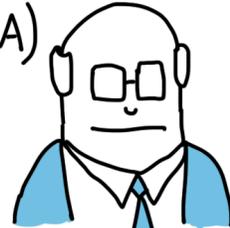
Ciberseguridad en tiempos de pandemia que aceleraron la era digital

Humanizing the Digital Experience

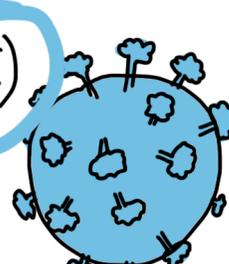
DIGITAL TRANSFORMATION IS **YEARS** AWAY. I DON'T SEE OUR COMPANY HAVING TO CHANGE ANY TIME SOON.



WHO LED THE DIGITAL TRANSFORMATION OF YOUR COMPANY ?

A)  THE CEO

B)  THE CTO

C)  COVID-19

BUSINESSILLUSTRATOR.COM

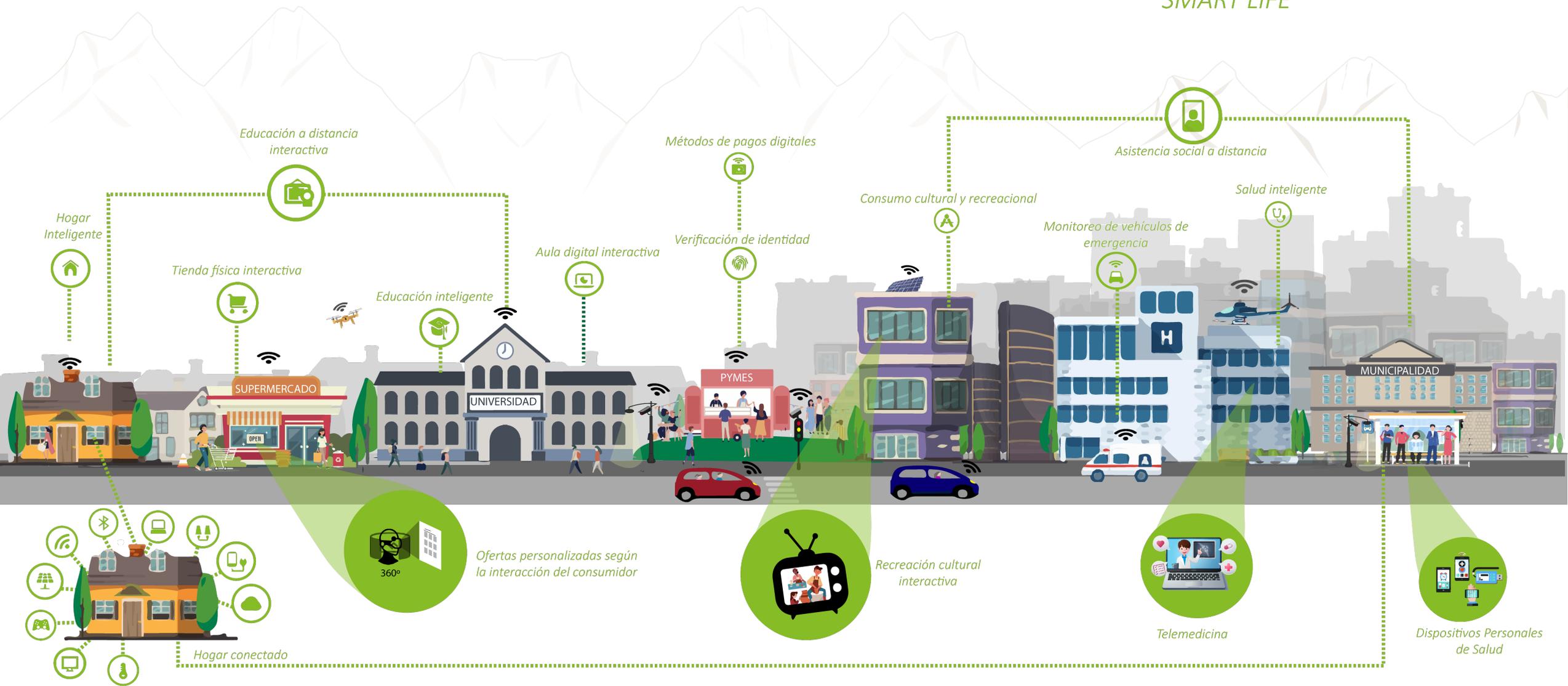


TOM FISH BURNE

© marketoonist.com

Una mirada hacia el arte de lo posible: Sociedad digital.

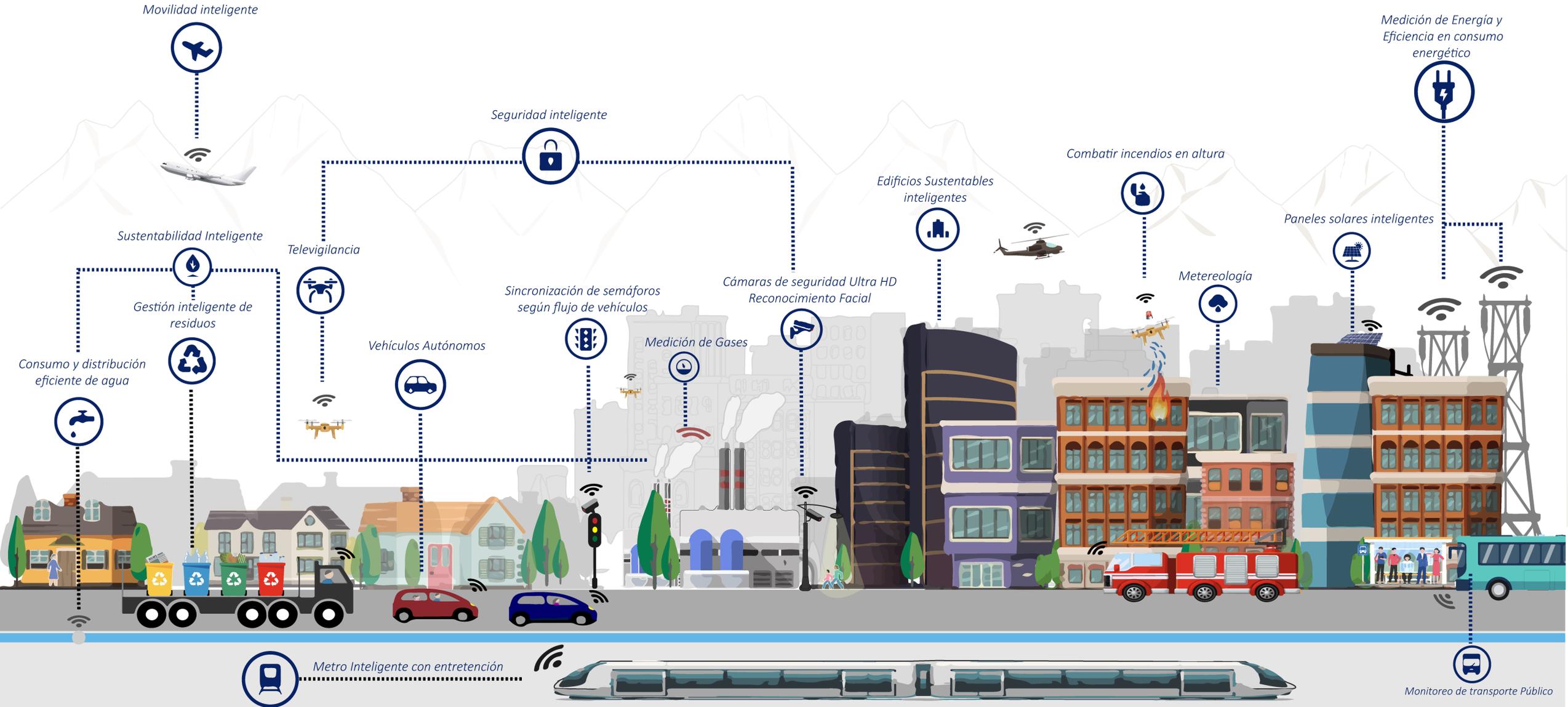
VIDA INTELIGENTE SMART LIFE



*Una mirada hacia el arte de lo posible:
Sociedad digital.*

CIUDAD INTELIGENTE

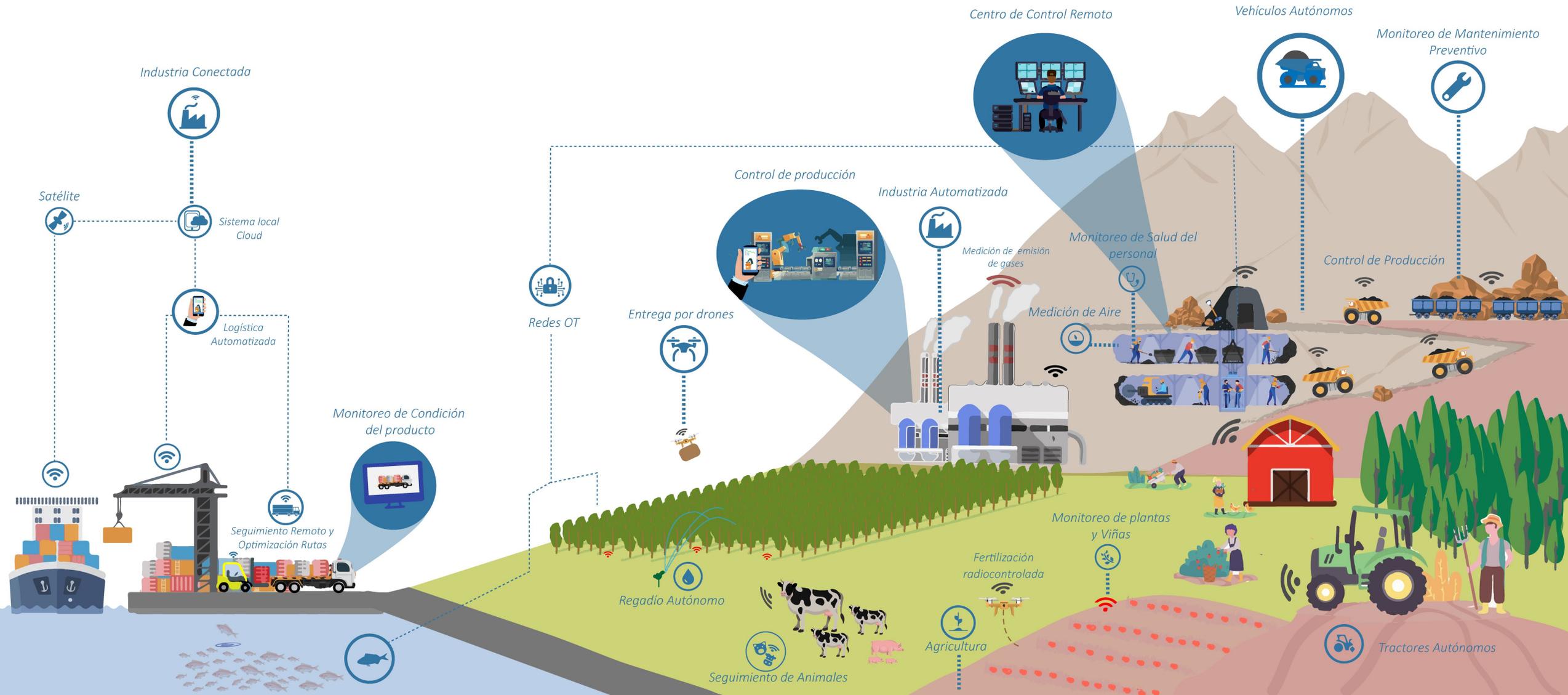
SMART CITY

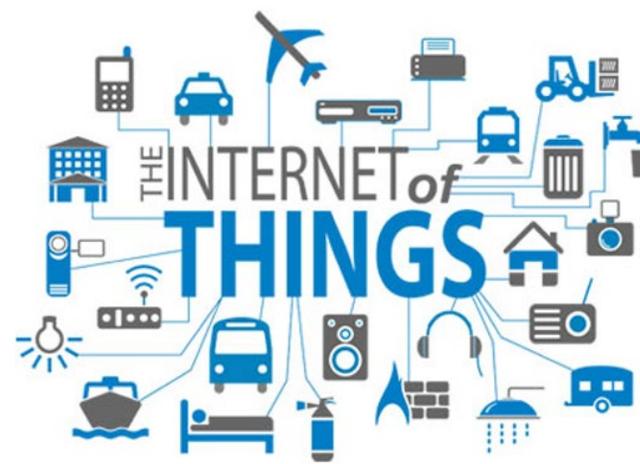


*Una mirada hacia el arte de lo posible:
Sociedad digital.*

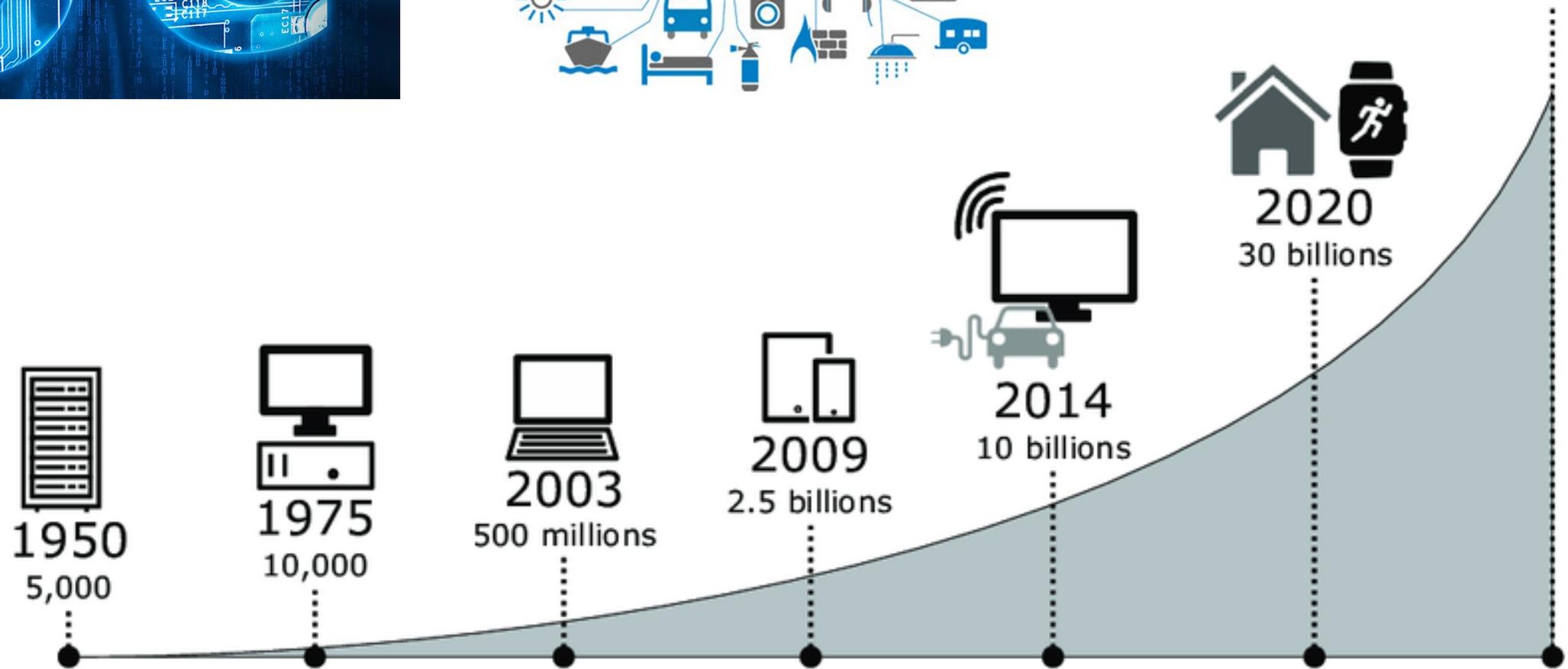
PRODUCCIÓN INTELIGENTE

SMART PRODUCTION






2050
>100 billions



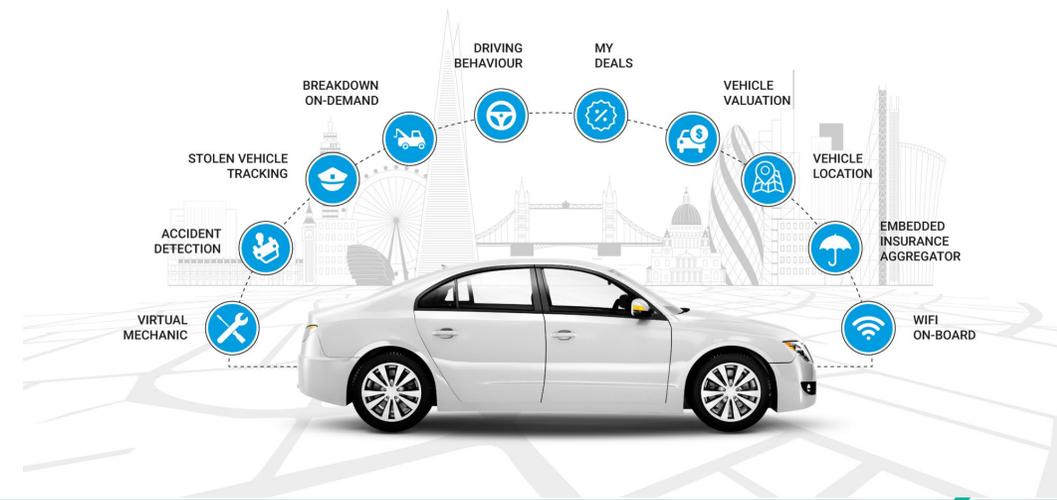
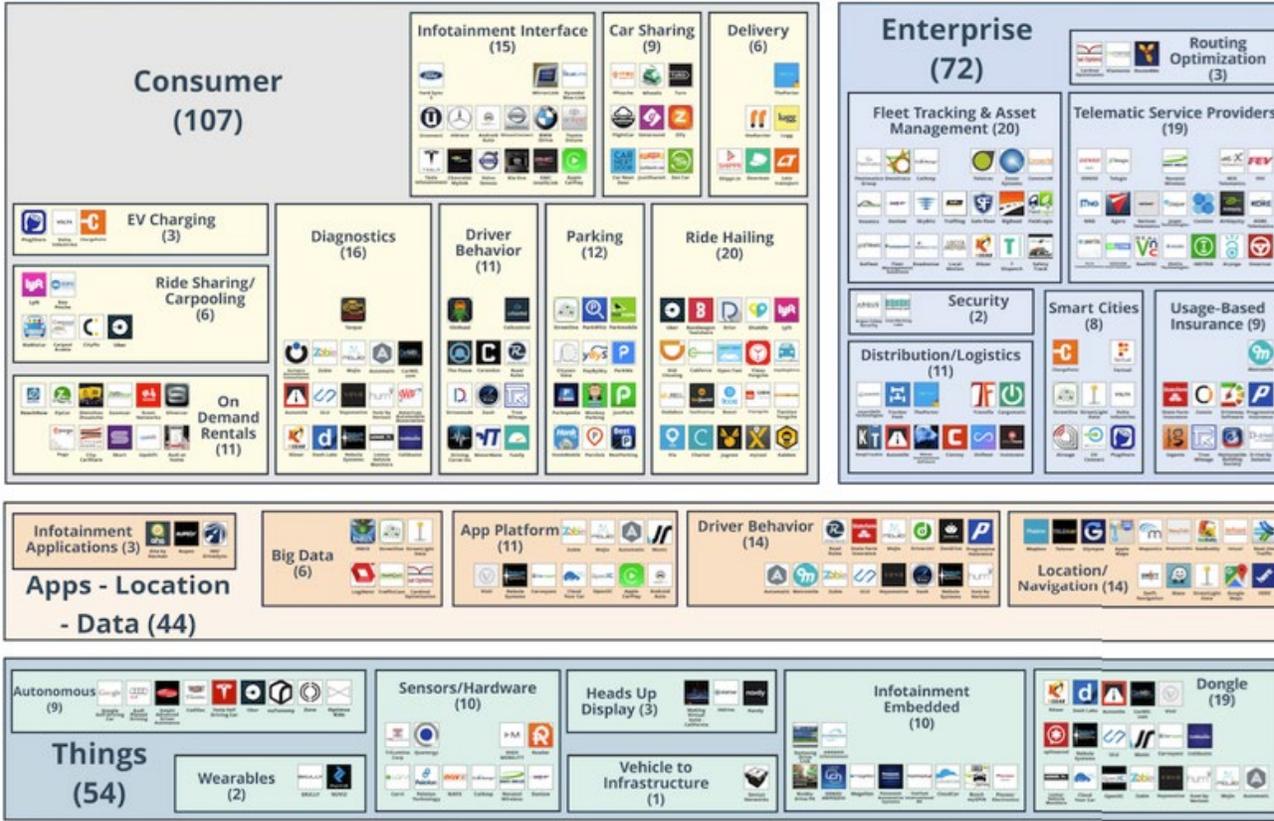
The Healthcare Internet of Things (IoT) Market Map

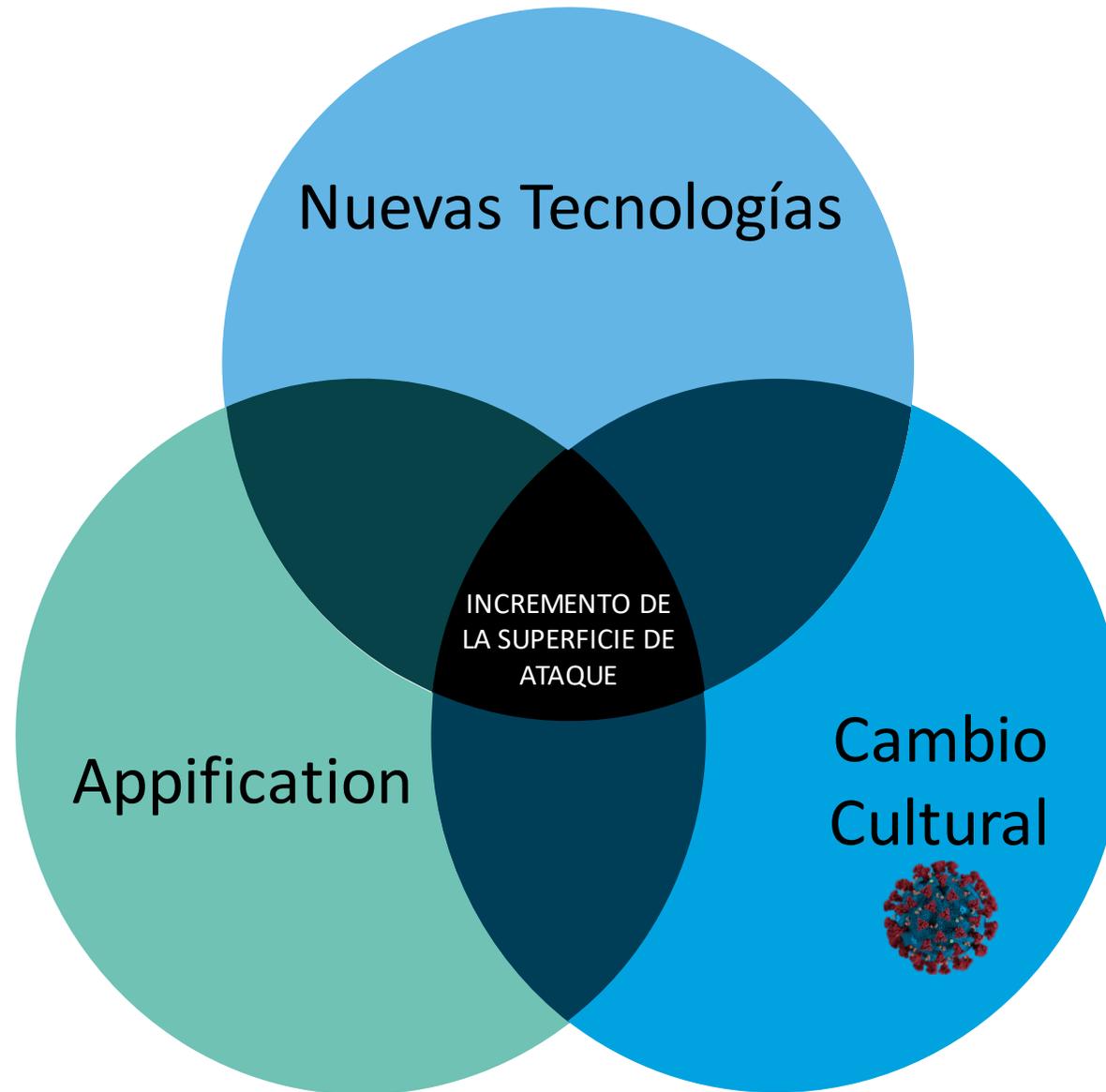


Connected Cars Landscape

DESIGNED BY
Liz Slocum Jensen

POWERED BY
spoke







APT36
Iran



APT38
China



APT37
Corea del Norte



APT32
Vietnam



APT34
Iran



APT18
China



APT3
Corea del Norte



FANCY BEAR
Rusia



LAZARUS



APT35
Iran



- Americas
- 16. United States
 - 37. Chile
 - 40. Paraguay
 - 42. Canada
 - 52. Dominican Republic
 - 53. Costa Rica
 - 61. Panama
 - 63. Argentina
 - 64. Uruguay
 - 65. Colombia
 - 66. Brazil
 - 74. Peru
 - 77. Mexico
 - 81. Ecuador
 - 84. Trinidad and Tobago
 - 89. Venezuela
 - 96. Guatemala



39. Chile 57.14

39th National Cyber Security Index
 88th Global Cybersecurity Index
 56th ICT Development Index
 38th Networked Readiness Index

Population 18.2 million
 Area (km²) 756.1 thousand
 GDP per capita (\$) 25.4 thousand

NCSI FULFILMENT PERCENTAGE

Version 3 Dec 2020 Choose a version

GENERAL CYBER SECURITY INDICATORS



BASELINE CYBER SECURITY INDICATORS



INCIDENT AND CRISIS MANAGEMENT INDICATORS



Version 25 Jan 2021 Choose a version

GENERAL CYBER SECURITY INDICATORS



BASELINE CYBER SECURITY INDICATORS



INCIDENT AND CRISIS MANAGEMENT INDICATORS



Datos relevantes para LA



Costo de una fuga de información - 2020

- 1er año del estudio para Latinoamérica. Incluye Argentina, Chile, Colombia y México.
- USD 1,67M vs 3,6M fue el promedio del costo de una brecha de seguridad en LATAM vs Global.
- USD 52,56 es el costo promedio por registro, mientras que 150 en PII Global.
- 48% de las brechas son causadas por ataques maliciosos.
- El tiempo promedio para identificar una brecha fue de 241 días (207 G)
- El tiempo promedio para contener una brecha fue de 87 días (73 G)

Personal

Empleado

Cliente

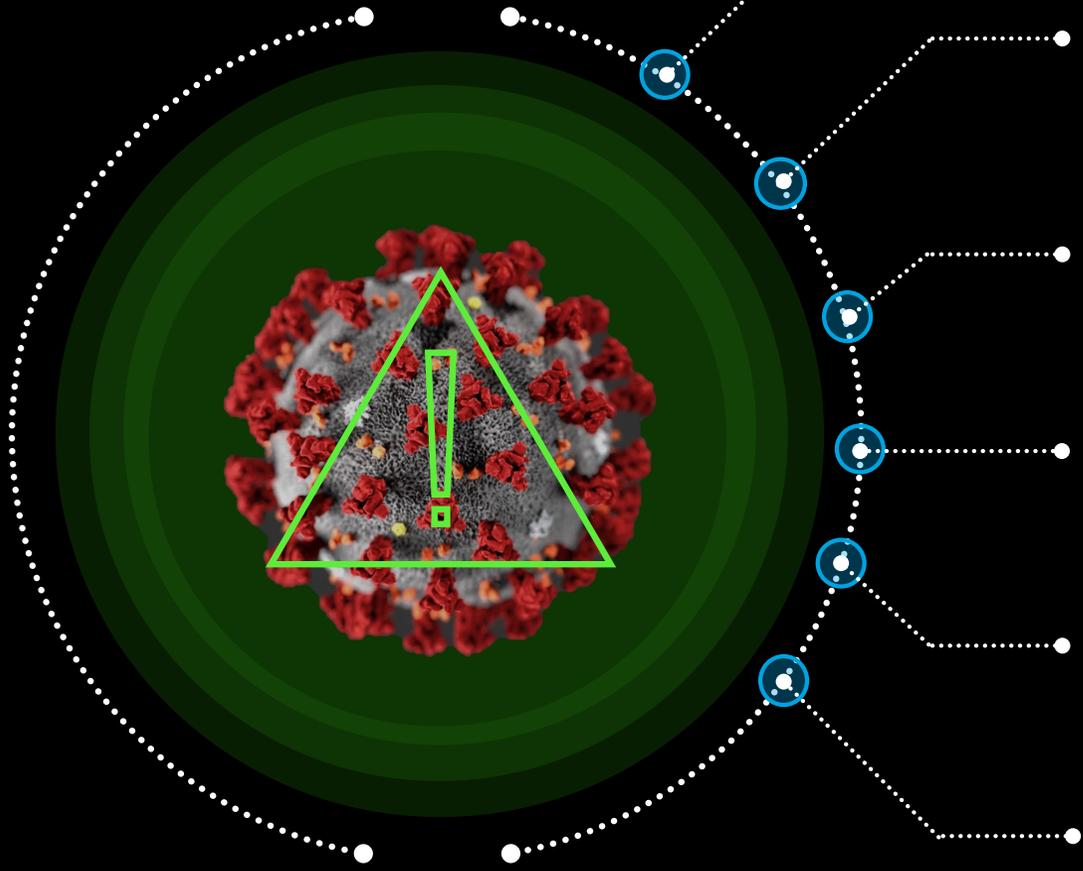


+ VISION

EL IMPACTO EN LAS ORGANIZACIONES

Dónde deben focalizarse el Directorio y los ejecutivos (C-suite) respecto de los riesgos de Cyber.





Trabajo Remoto

Se trae la casa a la red de la institución (BYOH)



Aumentan sitios ilegales, malware y spam

Se aprovecha la pandemia para dirigir ataques y confundir al usuario



Aumentan e-Commerce

Proliferan sitios para facilitar las compras de insumos y realizar trámites



Utilización de Dispositivos / Computadores personales

Software desactualizado, sin antivirus, sin backup



Seguridad en red hogareña

Computadores en ambientes no controlados con navegación irrestricta



Aumento de conexiones hacia institución

Todos los trabajadores ingresando a la red desde los hogares.

Políticas y procedimientos para eliminar la confusión y reforzar los controles de seguridad y procesos en el trabajo remoto



Control de **herramientas**: Uso de herramientas aprobadas, sobre todo para la colaboración remota.

Concientización de usuarios. Realizar entrenamientos y comunicados acerca del adecuado uso y responsabilidad de la seguridad por los empleados remotos



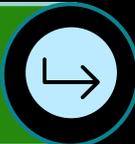
Protección de la información a través de controles y procesos para proteger información crítica (encriptación, dlp)

Contraseñas: incrementar niveles si no están en mejores prácticas y fortalecer con autenticación multi-factor



Seguridad en estaciones de trabajo: Antivirus, protección del endpoint, **implementación de parches** y realización de backups en forma remota

Conexiones Remotas: tener capacidad extra para conexiones (VPN) y establecer requerimientos mínimos a cumplir por dispositivos en el acceso remoto.



Gestión de **accesos remotos**: **monitoreo y control** sobre los accesos de los usuarios y usuarios con elevados privilegios

Seguridad en **Cloud** y **Nuevos sitios** web/aplicaciones para responder a la situación del COVID-19



Respuesta ante incidentes de ciberseguridad: reforzar procedimientos y herramientas para responder a un aumento de las alertas de seguridad y tener capacidad para responder remotamente.

+ VISION

EL IMPACTO EN LOS CLIENTES

Dónde deben focalizarse el
Directorio y los ejecutivos (C-suite)
respecto de los riesgos de Cyber y las
regulaciones.



Los individuos están tratando de manejar un "agotamiento digital" significativo que proviene de todos los aspectos de sus vidas

Controlado por el usuario



Mínimamente controlado por el usuario

Los consumidores con cuidado de la privacidad quieren más control sobre sus datos personales, pero están dispuestos a recompensar a aquellos que ganan su confianza

Los consumidores se sienten abrumados...



Casi la mitad de los consumidores (47%) sienten que tienen poco o ningún **control de sus datos personales**

... y quieren más control



La gran mayoría (86%) de los consumidores creen que deben ser capaces de **optar por no participar de la venta de sus datos** por los retailers

Pero están dispuestos a compartir...



Al compartir datos personales con los retailers, los consumidores esperan recibir **mejores precios, descuentos u ofertas** (71%) como incentivos

... y recompensar a aquellos que ganan su confianza



Aquellos que están satisfechos con las políticas de privacidad son más propensos a ser abiertos o neutrales al **compartir datos personales** (73%), en comparación con aquellos que no están satisfechos o no son conscientes (57%)

Fuente: Deloitte – Encuesta de privacidad de datos para consumidores de EE. UU. (N.o 2.000)

Monitoreo Activo

Activación de soluciones y procedimientos que permitan detectar accesos incorrectos en cortos períodos de tiempo.

Respuesta ante Incidentes

Definir procedimientos que involucren a todas las áreas técnicas, compliance, legales y comunicaciones

Desarrollo Seguro - DevSecOps

Utilización de metodologías y herramientas que permita automatizar la integración de Seguridad en todas las fases del ciclo de vida del Desarrollo.

Control de Fraudes

Implementación de soluciones que permitan a través de motores de confianza y riesgo adaptativo.

Orquestación de Seguridad

Implementar soluciones que permitan robustecer y centralizar la autenticación y autorización de todos los canales basado en el contexto

Privacy by Design

Considerar en el diseño de soluciones los aspectos que permitan el cumplimiento de los controles de privacidad de datos



+ VISION

EL IMPACTO EN NUESTRO DIA A DIA

Dónde debemos focalizarnos como
individuos en la protección de
nuestros datos



ANTIVIRUS



Utilice software antivirus, con actualizaciones automáticamente y que ejecute periódicamente y al bajar archivos.

VPN



Utilice siempre VPN para ingresar a las aplicaciones alojadas en la red de la oficina o dejar archivos en carpetas compartidas de la oficina

SOFTWARE AUTORIZADO



Evite utilizar software no autorizado para compartir archivos, realizar conferencias o navegar en internet

Atención Constante

Revisar los mails antes de abrir archivos o clickear en vínculos, revisar sitios web a los que se ingresa antes de realizar compras. Evitar compras por redes sociales.

Seguridad WiFi

Cambie las claves por defecto del router, wifi o cualquier otro dispositivo de la red del hogar
Utilice sólo redes wifi con contraseña



Actualización

Realice actualizaciones frecuentes de los dispositivos



Conectividad

De preferencia, use una red aislada distinta al del resto de la casa



Uso

No utilice dispositivos del trabajo para uso personal o entretenimiento



Contraseña

Utilice Multi-factor o contraseñas seguras. No publique ni comparta contraseñas



Descargas

No descargue archivos que puedan ser sospechosos



Cloud

Proteja las cloud personales y encripte archivos importantes

COVID-19 cyberthreats

CYBER SAFETY CHECKLIST



Back up online and offline files regularly and securely



Strengthen your home network



Use strong passwords



Keep your software updated



Manage social media profiles



Check privacy and security settings



Avoid opening and delete suspicious emails or attachments



INTERPOL

BE VIGILANT . BE SKEPTICAL . BE SAFE



Nicolás Corrado
Socio Lider
Cyber & Strategic Risk
Risk Advisory
Deloitte Chile
nicorrado@deloitte.com

Deloitte.

