Microsoft

Ciberseguridad en contexto.

Gustavo Gómez
Technical Specialist - Security and Compliance

Wilmer Prieto Gómez
Technical Specialist - Security

Microsoft

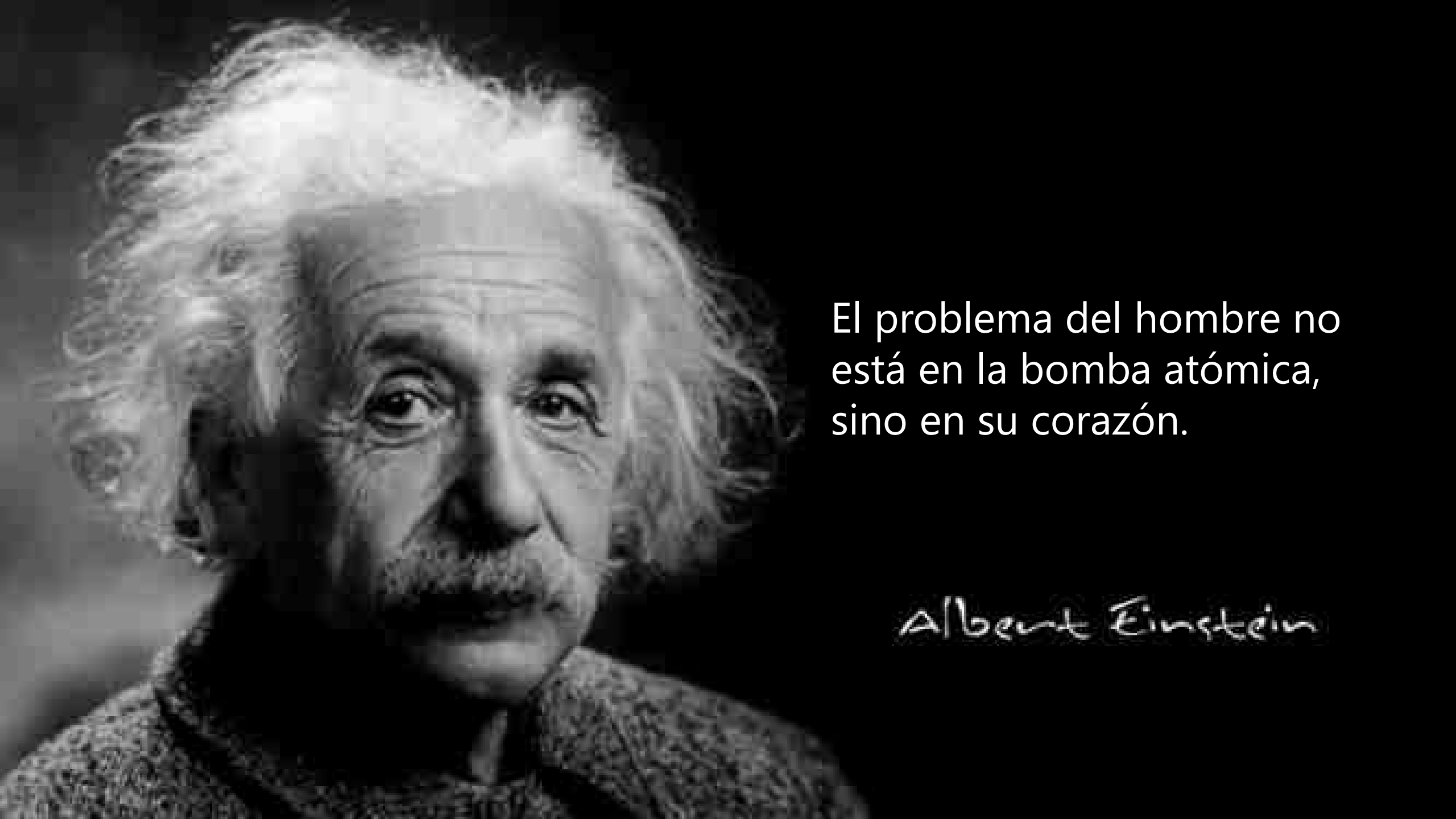
Máster en Dirección y Administración de Empresas (MBA).
Especialista en Transformación Digital.
Especialista en Marketing Digital.
Ingeniero de Sistemas.

CISM, CRISC, CDPSE, ISO31000-LM
ECPD, COBITF, CSXF, CSXA, SFC, CEH
wprietogomez@microsoft.com

Wilmer Prieto Gómez

Agenda

- Competitividad digital.
- Estado actual de la ciberseguridad.
- Comprendiendo la ciberseguridad.
- Enfoques integrales en Ciberseguridad.

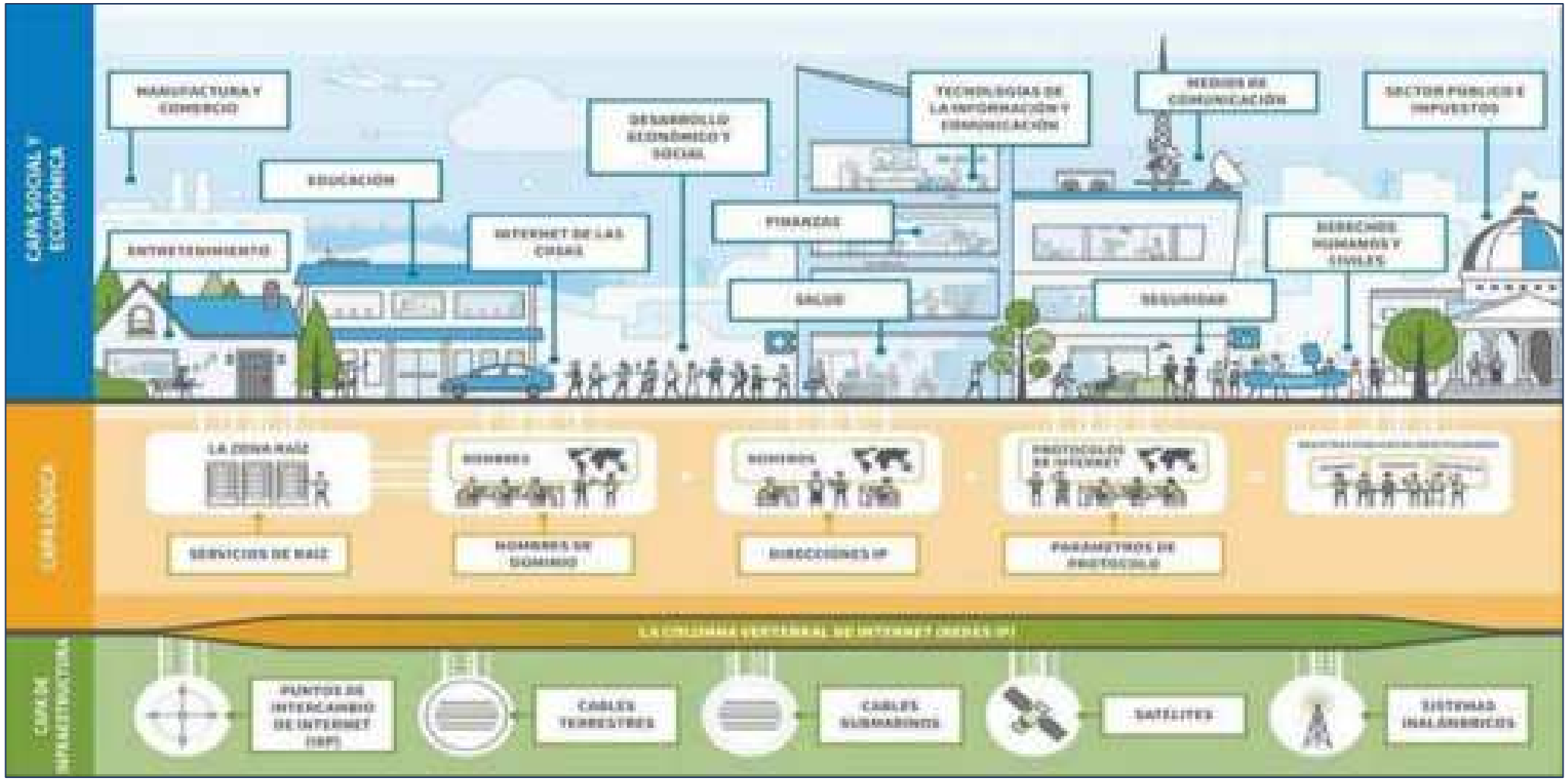

El problema del hombre no está en la bomba atómica, sino en su corazón.
Albert Einstein

Competitividad digital

1

La transformación digital es un concepto global que abarca lo local.

Gobernanza de Internet



Fuente: https://nic.ar/es/enterate/novedades/que-es-gi

Aceleración en la transformación digital

Inteligencia Artificial

Tecnologías Móviles

Desarrollo Productivo

Competitividad

Economía Digital

Ciudades Inteligentes

Ciencia

Design Thinking

I + D + Innovación

IoT

Blockchain

Cloud

Agilismo

Big Data

DevOps

Industria 4.0

Analítica

Tecnologías Emergentes

Lean

Instituto para el Desarrollo Gerencial (IDM)

Institute for Management Development (IMD)

Fundada por ejecutivos de empresas para ejecutivos de empresas. Es una institución académica independiente con raíces suizas y alcance global. Se esfuerzan por ser el socio de aprendizaje de confianza elegido por personas y organizaciones en todo el mundo.

https://www.imd.org/

Centro de Competitividad Mundial

https://www.imd.org/centers/world-competitiveness-center

El Centro de Competitividad Mundial lleva a cabo su misión en cooperación con una red de 58 instituciones asociadas en todo el mundo para proporcionar a los diferentes gobiernos, comunidades empresariales, y académicas los siguientes servicios:

- Informes especiales de competitividad.
- Informes de pronóstico de competitividad.
- Talleres / Mega Inmersiones sobre competitividad.
- Anuario de Competitividad Mundial de IMD.
- Ranking mundial de competitividad digital de IMD.
- Ranking mundial de talentos de IMD.

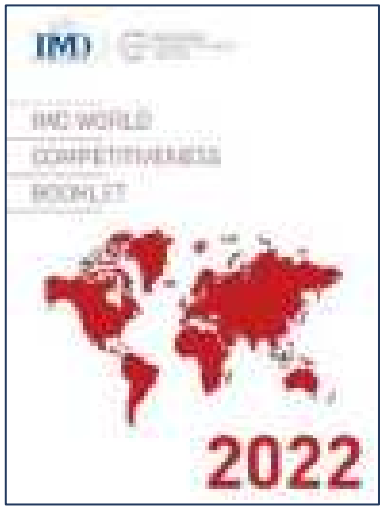
IMD WORLD COMPETITIVENESS CENTER

Generalidades del Ranking

https://www.imd.org/centers/world-competitiveness-center/rankings/world-competitiveness/

- El Ranking Mundial de Competitividad Digital presenta la clasificación general para 2022 de las 62 economías cubiertas por el estudio.
- Las clasificaciones se calculan sobre la base de los 52 criterios clasificados: 32 Definidos y 20 datos obtenidos por encuesta.
- Los países están clasificados de mayor a menor competitividad digital, indicando el valor del índice o “puntuación” para cada país.

Ranking Mundial de Competitividad Digital



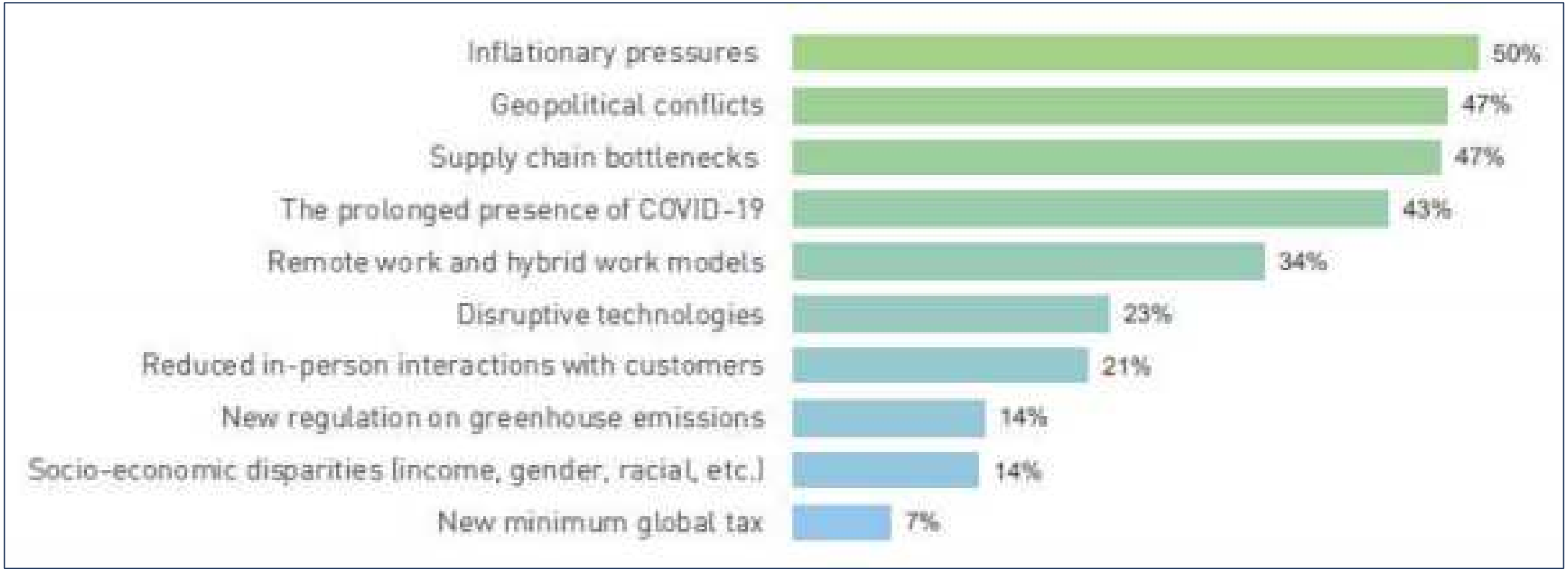
Ranking de competitividad 2022

Conocimiento	Tecnología	Preparación futura
Conocimientos necesarios para descubrir, comprender y construir nuevas tecnologías. • Talento Humano. • Entrenamiento y Educación. • Concentración científica.	Contexto general que habilita el desarrollo de tecnologías digitales. • Marco regulatorio. • Capital. • Marco tecnológico.	Nivel de preparación del país para explotar la transformación digital. • Actitudes adaptativas. • Agilidad empresarial. • Integración de TI.

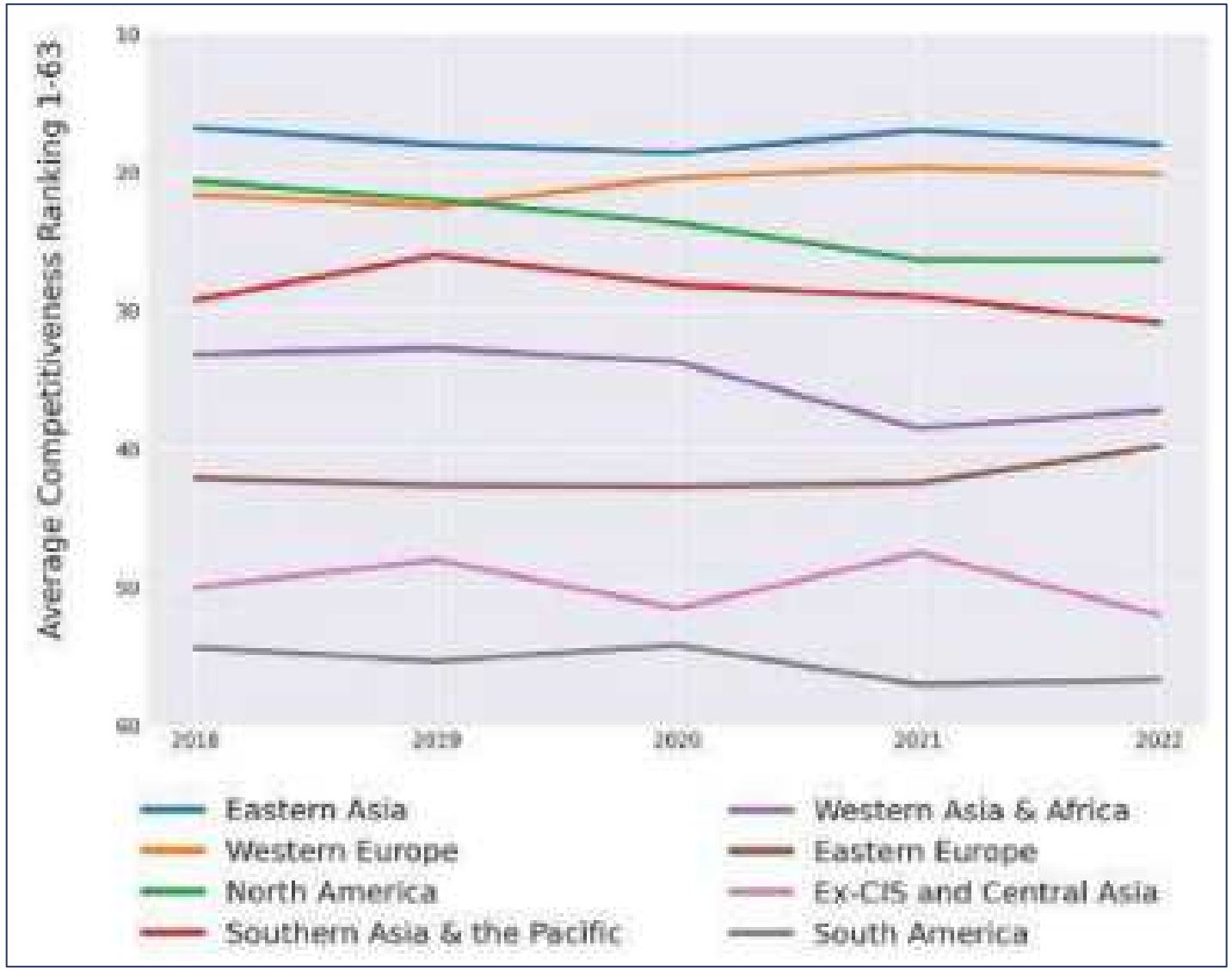
- Evalúa la capacidad de una economía para adoptar y explorar la tecnología digital.
- Tecnologías que conducen a la transformación en las prácticas gubernamentales, los modelos de negocio y la sociedad en general.

Tendencias más importantes que impactarán en los negocios en 2022 según los ejecutivos

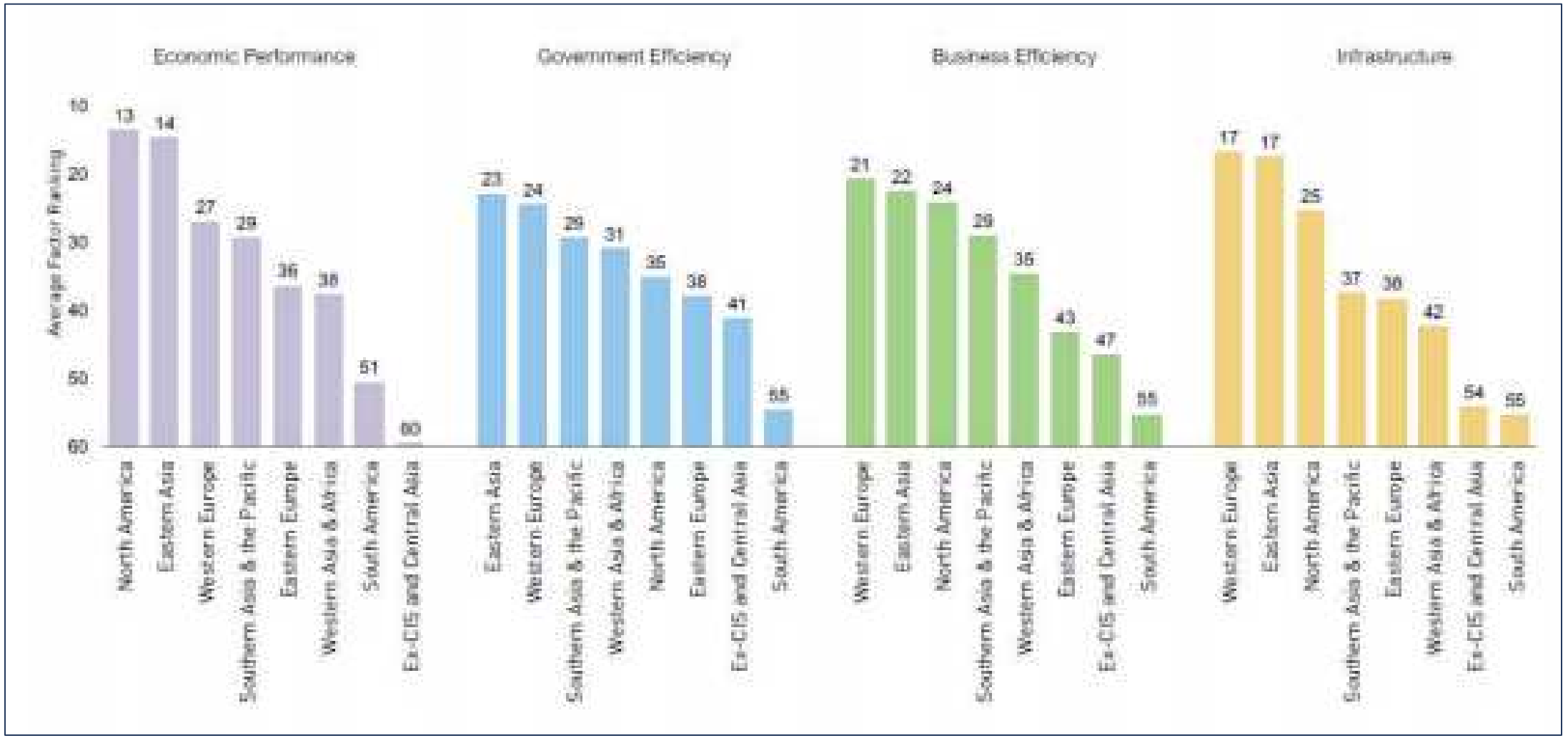
Encuesta de opinión ejecutiva (IMD 2022)



Posiciones de ranking promedio por región en Competitividad General 2018-2022



Rango de factor promedio por región, 2022



Mejoras/disminuciones en la competitividad general por país 2021-2022

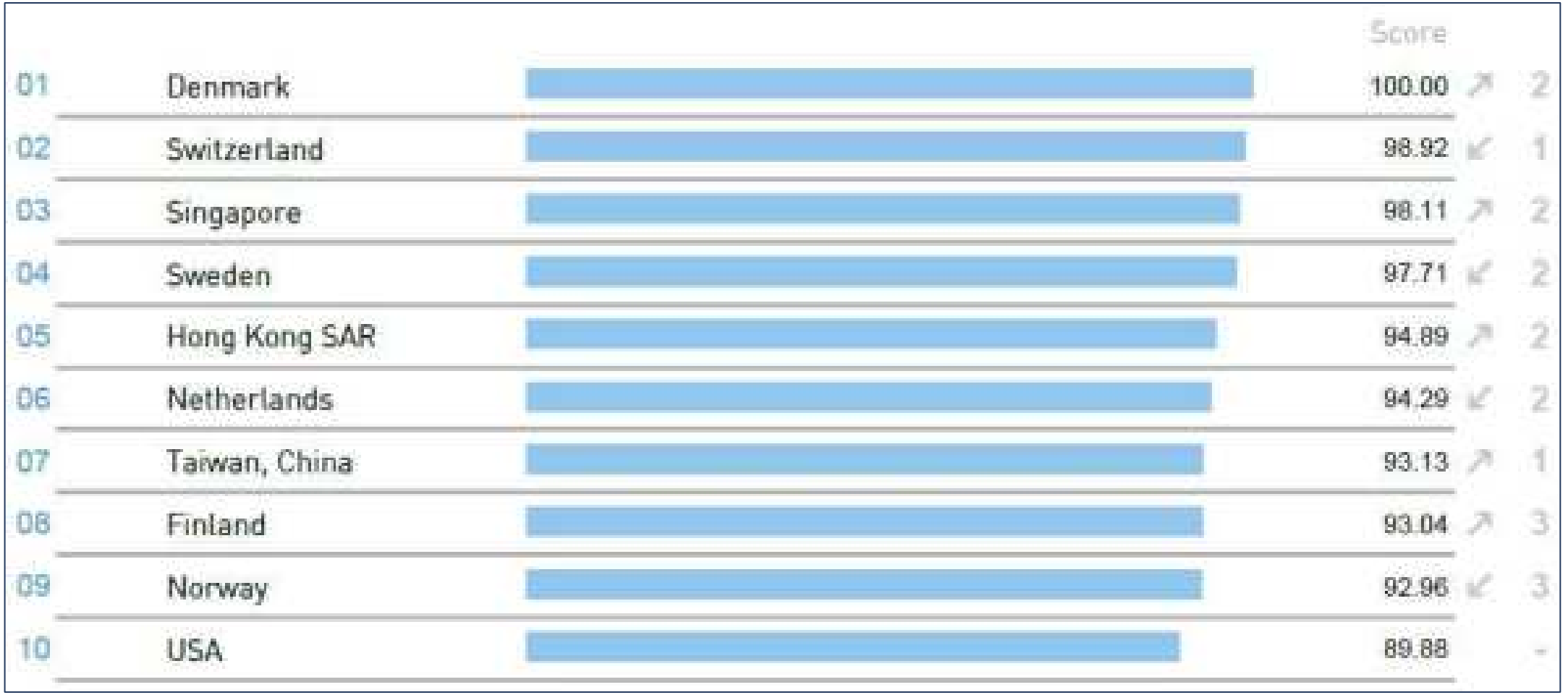
Tendencias generales

- Los países en las primeras posiciones del ranking fomentan el desarrollo continuo de una economía intensiva en conocimiento que es capaz de explorar, adoptar y producir tecnologías digitales a escala, innovando la forma en que operan las empresas y el gobierno y sus interacciones con la sociedad.

- Más específicamente, en diferentes grados, las economías lideres mantienen su competitividad digital a través de su desempeño en la preparación futura particularmente permaneciendo adaptables y ágiles.

- Su competitividad digital también se beneficia de un sólido desempeño en talento humano, capacitación, y educación.

Ranking de competitividad digital 2022 (Top 10)



Ranking de competitividad digital 2021 y 2022 (Hispanos).

País	2021	2022
España	39	36 ↑
Chile	44	45 ↓
Perú	58	54 ↑
México	55	55 –
Colombia	56	57 ↓
Brasil	57	59 ↓
Argentina	63	62 ↑
Venezuela	64	63 ↑

Ranking de competitividad digital 2020, 2021 y 2022

Programa Europa Digital 2021-2027

Comisión Europea

La Comisión Europea, a través de una propuesta de reglamento del Parlamento Europeo y del Consejo de Europa, ha establecido el programa Europa Digital 2021-2027.

En un contexto de transformación digital en todos los ámbitos de la sociedad, que afecta a la vida diaria de los ciudadanos, las inversiones en infraestructuras digitales son clave para mejorar y modernizar la interacción entre administraciones y ciudadanía, en aras de la prosperidad futura.

https://eur-lex.uropa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018PC0434&from=ES

Programa Europa Digital 2021-2027

Objetivos Específicos.

1. **Informática de alto rendimiento.** Desarrollar y fortalecer las capacidades de la Unión Europea en materia de informática de alto rendimiento y de procesamiento de datos, garantizando su uso tanto en el sector privado (industria y especialmente, en las pequeñas y medianas empresas) como en áreas de interés público.
2. **Inteligencia artificial.** Europa Digital, en inteligencia artificial, se fija como objetivo desarrollar y reforzar las capacidades esenciales en Europa: concretamente, los recursos de datos y los repositorios de algoritmos de inteligencia artificial; para que sean accesibles a todas las empresas y administraciones públicas.
3. **Ciberseguridad y confianza.** La Comisión Europea, a través de este programa, persigue fomentar el desarrollo de las capacidades básicas para garantizar y asegurar la economía digital, la sociedad y la democracia de la Unión Europea; con el objetivo de mejorar la competitividad y el potencial industrial en materia de ciberseguridad.

Programa Europa Digital 2021-2027

Objetivos Específicos.

4. **Competencias digitales avanzadas.** el programa Europa Digital se centra en el desarrollo de unas competencias adecuadas en los ciudadanos de hoy y en los del mañana, en ámbitos como la informática de alto rendimiento, la inteligencia artificial y la ciberseguridad. Este desarrollo debe conllevar un proceso fácil de adquisición para toda la ciudadanía y para ello, se debe ofrecer a estudiantes, jóvenes recién titulados y personal en activo todos los medios y herramientas necesarias para poder desarrollar dichas competencias.
5. **Despliegue.** mejor uso de las capacidades digitales e interoperabilidad. Este objetivo consiste es extender al conjunto de la economía, sociedad y áreas de interés público el uso de las capacidades digitales, especialmente la informática de alto rendimiento, la inteligencia artificial y la ciberseguridad. De igual forma, aquellos proyectos que fomenten el despliegue de soluciones interoperables, así como la facilitación de acceso a la tecnología y al conocimiento a todas las empresas, se considerarán proyectos de interés común.

Politica de Gobierno Digital

Transformación digital pública

https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

CONPES clave

Transformación Digital para Colombia

Documento

CONPES

3920

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL
REPÚBLICA DE COLOMBIA
DEPARTAMENTO NACIONAL DE PLANEACIÓN

POLÍTICA NACIONAL DE EXPLOTACIÓN DE DATOS (BIG DATA)

Documento

CONPES

3975

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL
REPÚBLICA DE COLOMBIA
DEPARTAMENTO NACIONAL DE PLANEACIÓN

POLÍTICA NACIONAL PARA LA TRANSFORMACIÓN DIGITAL E INTELIGENCIA ARTIFICIAL

Aceleración en la transformación digital

¡Acelera este ciclo de retroalimentación!

Construir

Convertir las ideas en productos

- Producto mínimo viable.

Conserje: Iniciar con un [illegible]te

Medir

Analizar como responden los clientes

- Experimente moviendo los [illegible]meros cerca a lo [illegible]o.
- [illegible]véalo usted mismo.
- [illegible]as divididas para [illegible]zar causa/efecto.

Aprender

Pivotear o perseverar

- Pivotee.
- ¿Cuales actividades generan valor? ¿Cuáles son un desperdicio?
- Los cinco porque: Encuentre y solucione su causa raíz.

Estado actual de la ciberseguridad

Los 10 principales riesgos que enfrenta el mundo en 2022

Hallazgos clave

- **Fuentes de energía.** La tensión entre los objetivos ecológicos y la necesidad de mantener bajos los costos de la energía resultará políticamente tóxica este año, con un aumento de costos de la energía, una mayor volatilidad de los precios y una creciente presión sobre los consumidores para que cambien su comportamiento.

- **Empresas expuestas.** Aunque las marcas más importantes del mundo están obteniendo beneficios récord se enfrentan a pérdida de cultura, debido, entre otras cosas, a la exposición en las redes sociales, en el que los consumidores tienen el poder y que hace que las empresas deben volverse más atractivas para las nuevas contrataciones.

- **Mundo Tecnopolar.** El futuro está siendo moldeado por empresas de tecnología y proyectos descentralizados de blockchain y los estados no podrán detener esta tendencia.

EURASIA GROUP'S TOP RISKS FOR 2022
https://www.eurasiagroup.net/issues/top-risks-2022

eurasia group politics first

Crimen ciber-dependiente

Hallazgos clave

- **El Crimen como servicio 'Crime-as-a-service - CaaS'.** Es una tendencia en aumento.
- **El uso expansivo de la infraestructura gris.** Mejora la seguridad operativa de los delincuentes.
- **Crimen Ciber-dependiente.** Los grupos delincuenciales en línea (Cibercrimen), exhiben una considerada resiliencia y están en continua evolución.
- El **Ransomware** sigue siendo la amenaza más dominante que permite a los delincuentes aumentar la presión, amenazando con la publicación de datos si las víctimas no realizan los pagos.
- La cantidad de **CSMA** detectado en línea sigue aumentando, agravado esto aún más por la crisis del COVID-19, lo cual genera graves consecuencias en la capacidad de las autoridades encargadas de hacer cumplir la ley.

Internet Organised Crime Threat Assessment (IOCTA) 2021
www.europol.europa.eu

Tricotomía del cibercrimen

Internet Organised Crime Threat Assessment (IOCTA) 2017 www.europol.europa.eu

Crimen ciber-dependiente

Hallazgos clave

- En **Colombia** se evidenció un **incremento** en los **delitos cibernéticos** de un **89%** respecto al año anterior.
- El delito que registró el mayor número de denuncias fue el "**Hurto por medios informáticos**" con **16.654 casos**.
- Por motivos de la pandemia del **COVID-19**, los delitos de mayor incremento fueron:
  - Suplantación de sitios web.
  - Violación de datos personales.
  - Interceptación de datos informáticos.

TENDENCIAS CIBERCRIMEN COLOMBIA 2019 - 2020
https://caivirtual.policia.gov.co/#ciberseguridad

Explotación sexual infantil en línea

Top 5 países consumidores de Material de Explotación Sexual Infantil en línea.

7.139 URLs bloqueadas en **2020**.

4.163 URLs bloqueadas en **2019**.

Holanda

Grecia

Estados Unidos

Rusia

Latvia

En el 2020 fueron reportados al **CAI Virtual:**

225 Casos de **GROOMING**.

637 Casos de **SEXTORSIÓN**.

50 Casos de **CYBERBULLYING**.

Comprendiendo la ciberseguridad

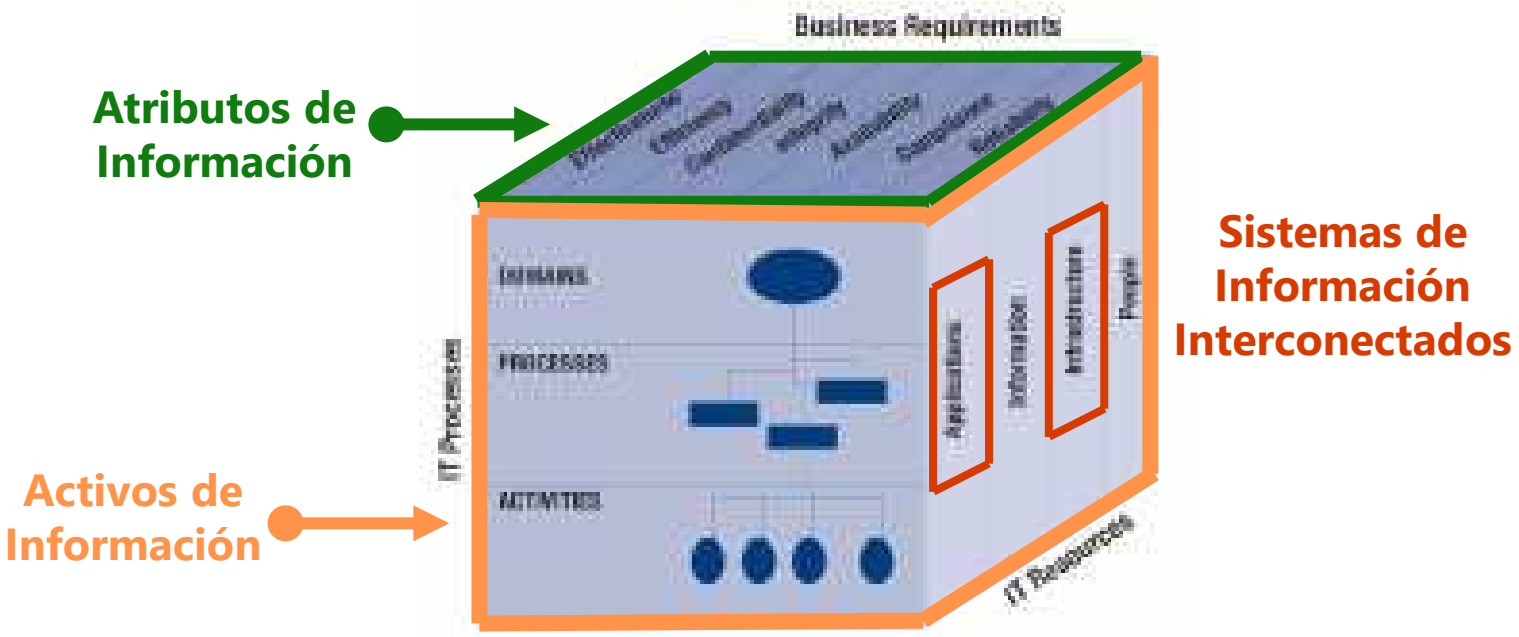
¿Que es la ciberseguridad?

Fuente: ISACA, Cybersecurity Fundamentals Glossary, ISACA, USA, 2022.

"La protección de los activos de información abordando las amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados"

¿Que es la ciberseguridad?

*"La protección de los **activos de información** abordando las amenazas a la **información procesada, almacenada y transportada** por **sistemas de información interconectados**"*



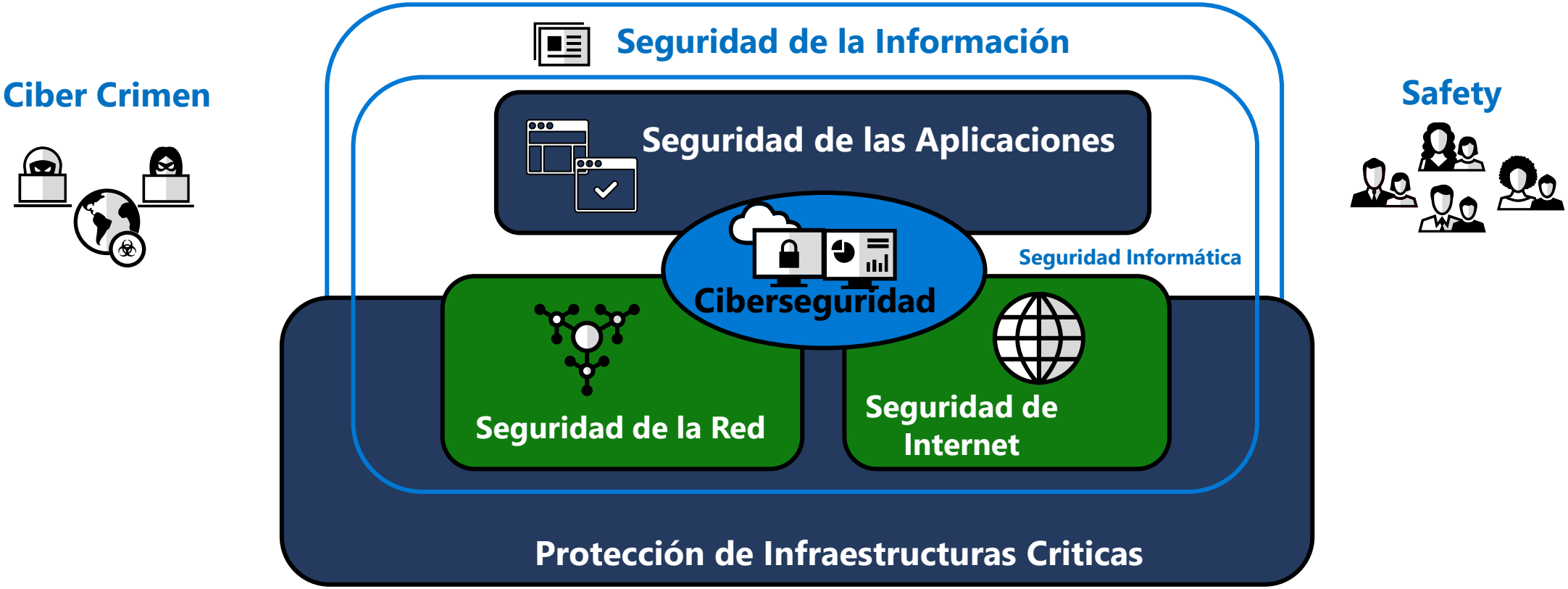
¿Que es la ciberseguridad?

Reglamento de Ciberseguridad de la UE

La **ciberseguridad** incluye las actividades necesarias para la **protección de las redes y sistemas de información**, de los **usuarios** de dichos sistemas y de **otras personas** afectadas por las **ciberamenazas**.

Ciberseguridad y otros dominios de la seguridad

Fuente: ISO/IEC 27032 2012



Índice global de ciberseguridad 2020

International Telecommunication Union (ITU)

La UIT es el organismo especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación – TIC. https://www.itu.int/es/Pages/default.aspx

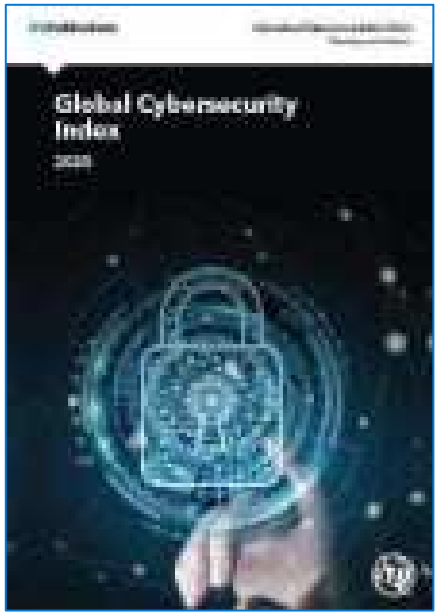
Countries Measured	Collection Year	Focal Points from Countries	Submitted Questionnaires	Median Overall Score Growth since 2018
194	**2020**	**169**	**150**	**9.5%**

https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Aspectos generales

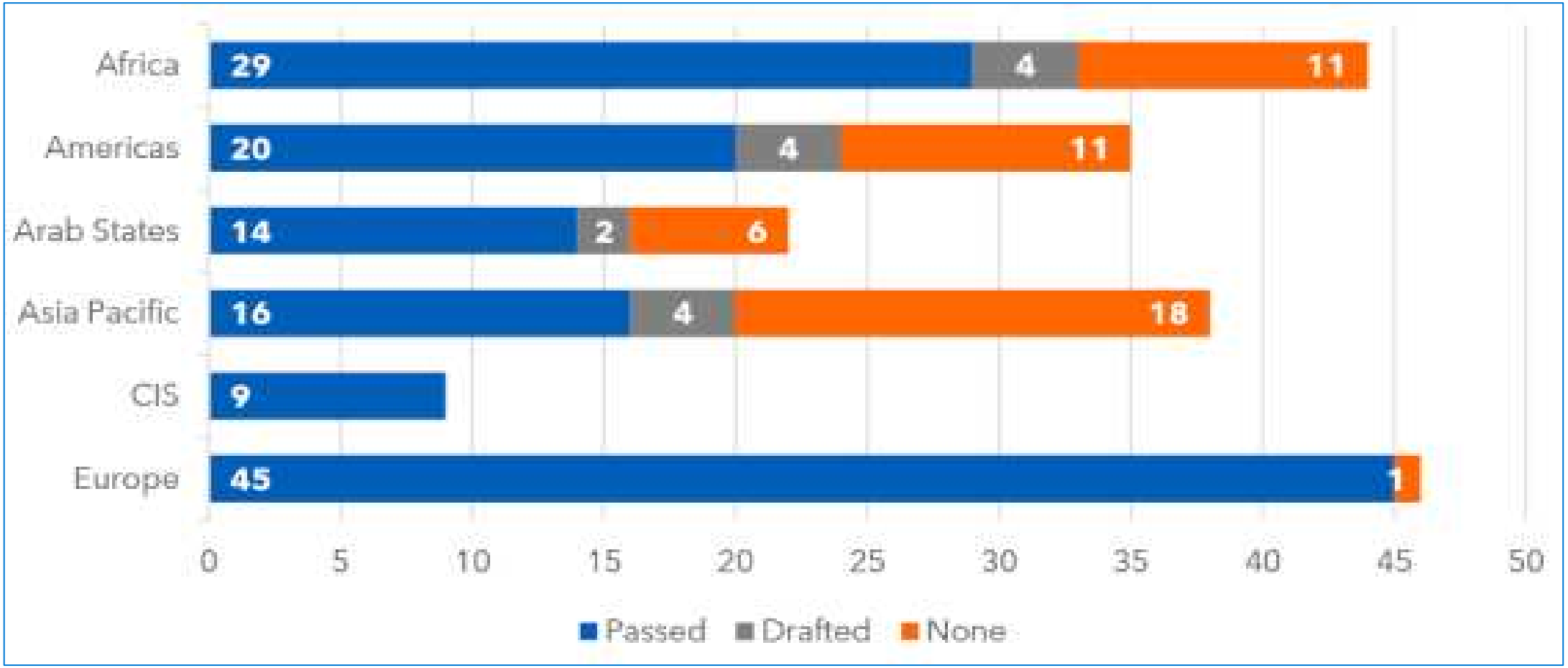
Índice global de ciberseguridad 2020

- El Índice mapea 82 preguntas sobre los compromisos de ciberseguridad de los Estados miembros en cinco pilares:
  - Medidas legales.
  - Medidas técnicas.
  - Medidas organizativas.
  - Medidas de desarrollo de capacidades.
  - Medidas de cooperación.



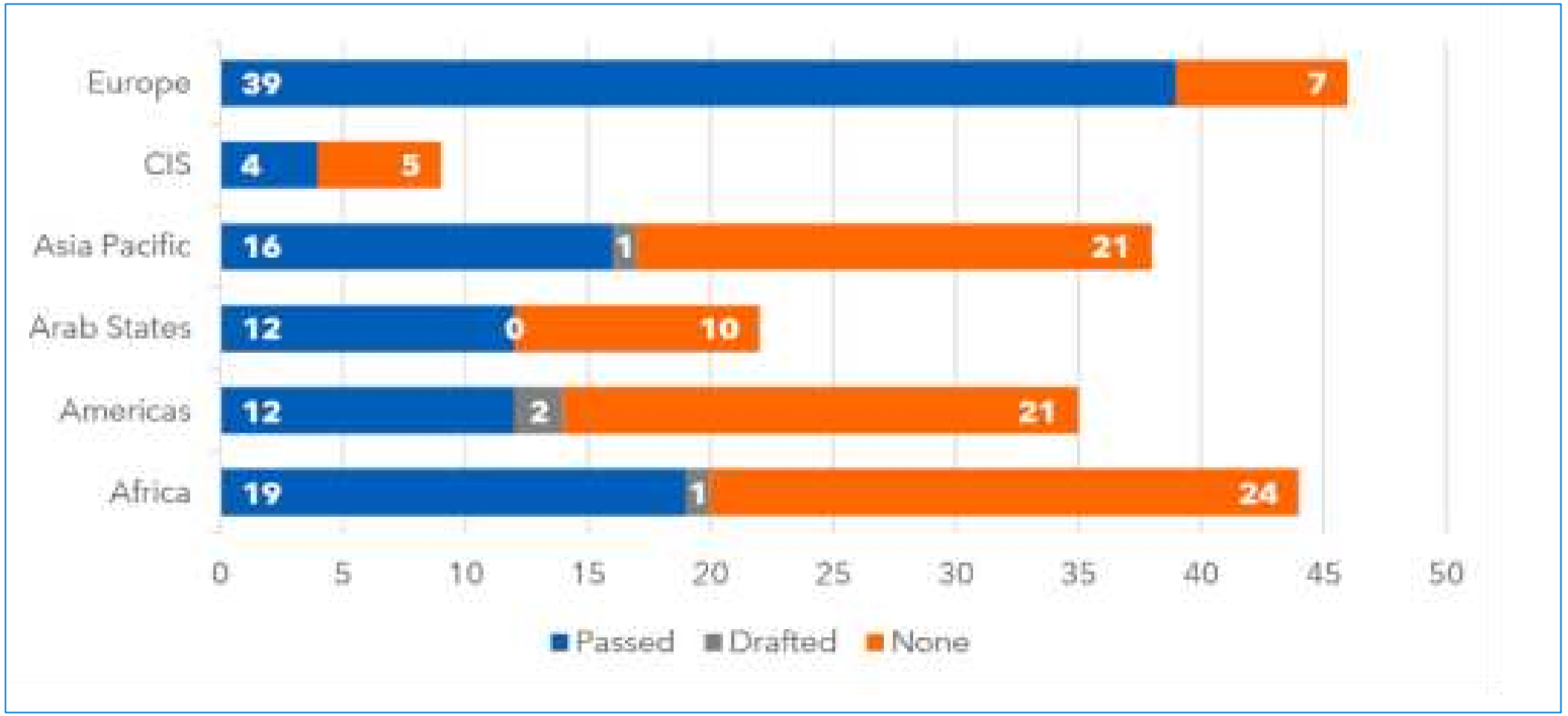
Medidas legales: Planificación de futuras intervenciones

Países con legislación de protección de datos



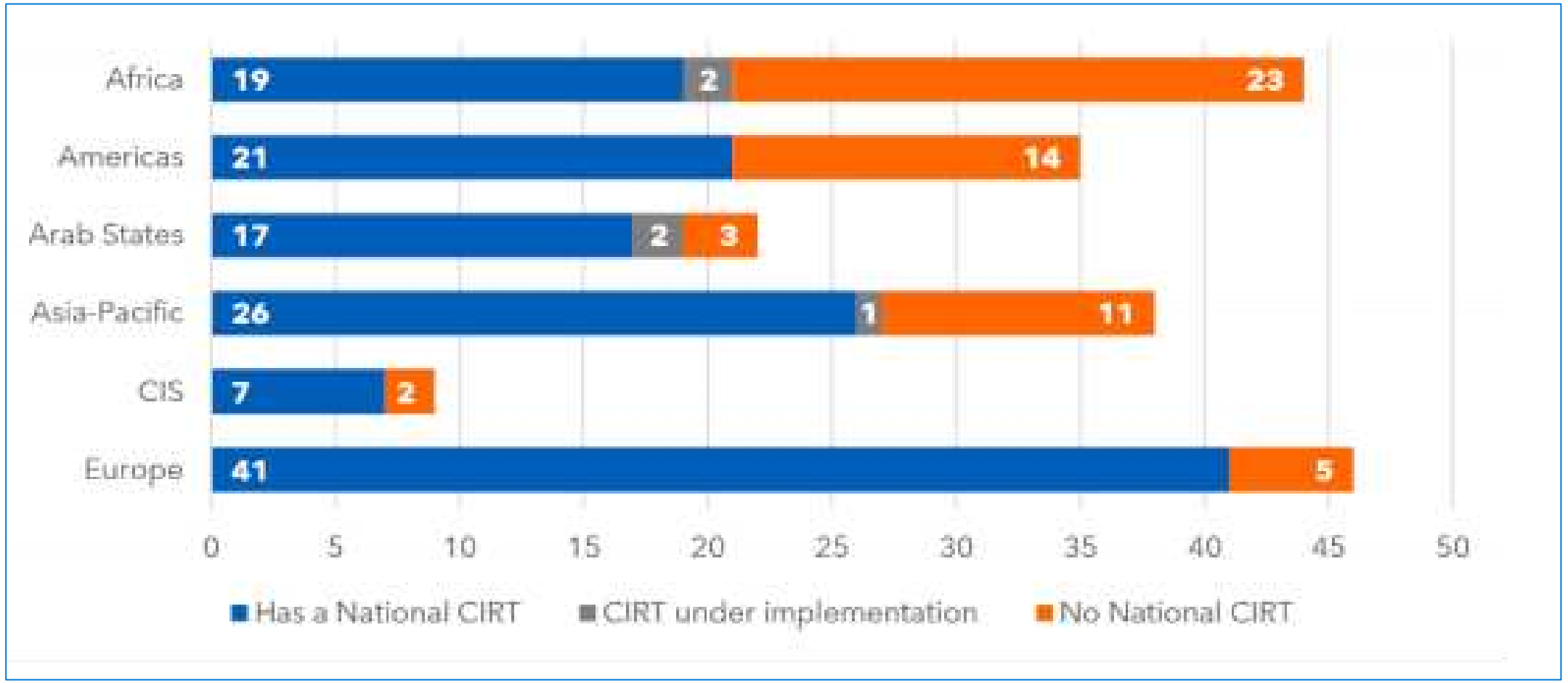
Medidas legales: Planificación de futuras intervenciones

Países con medidas de notificación de brechas de seguridad



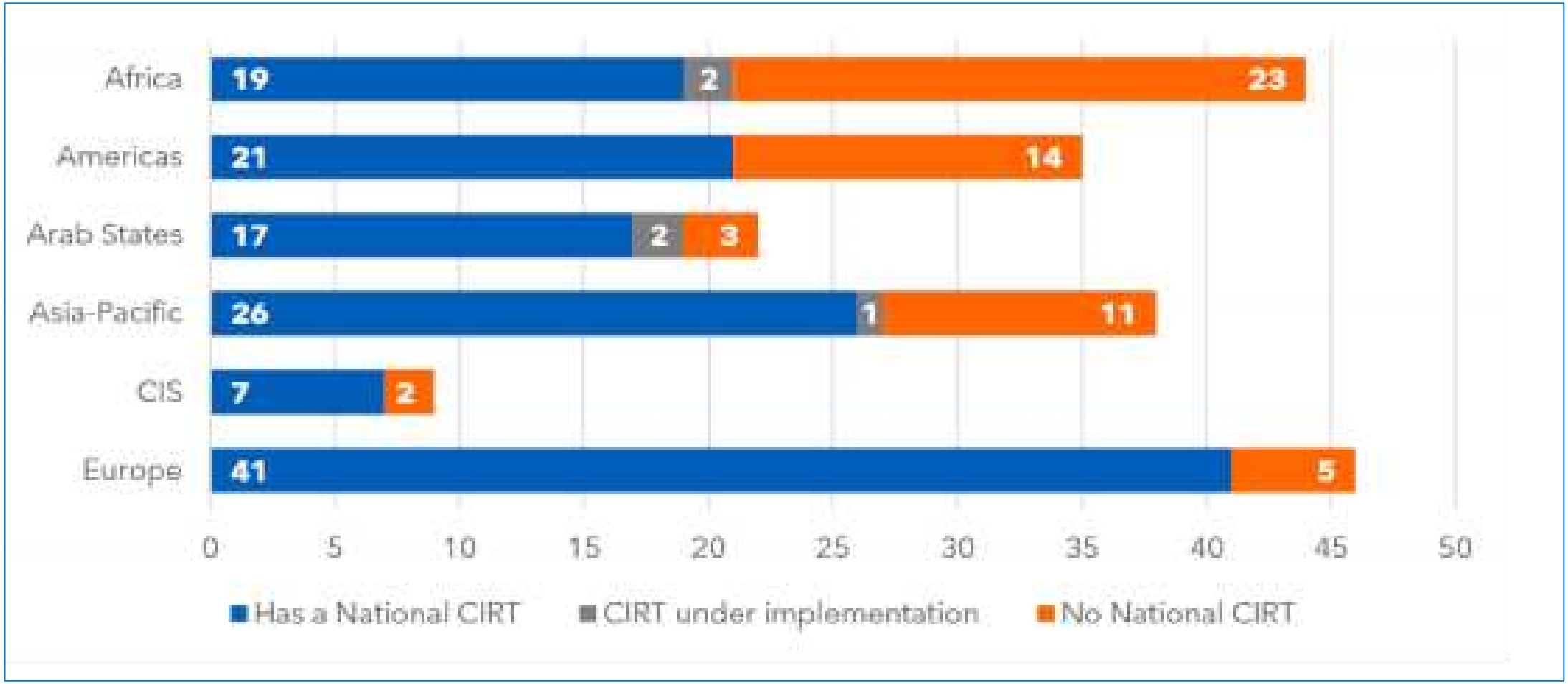
Medidas técnicas: mayor despliegue de CIRT/CERT

Número de países con un CIRT nacional



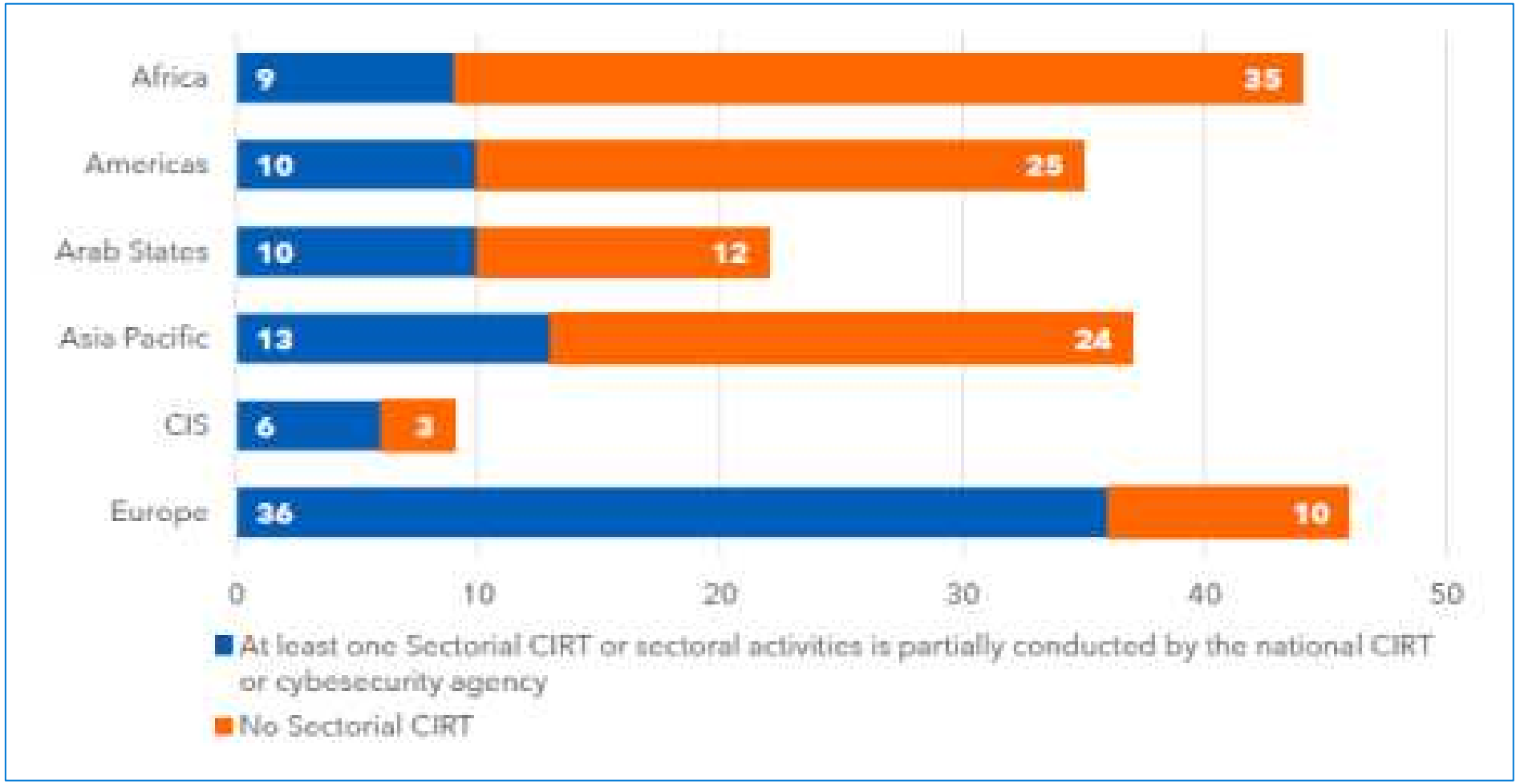
Medidas técnicas: mayor despliegue de CIRT/CERT

CIRTs por región



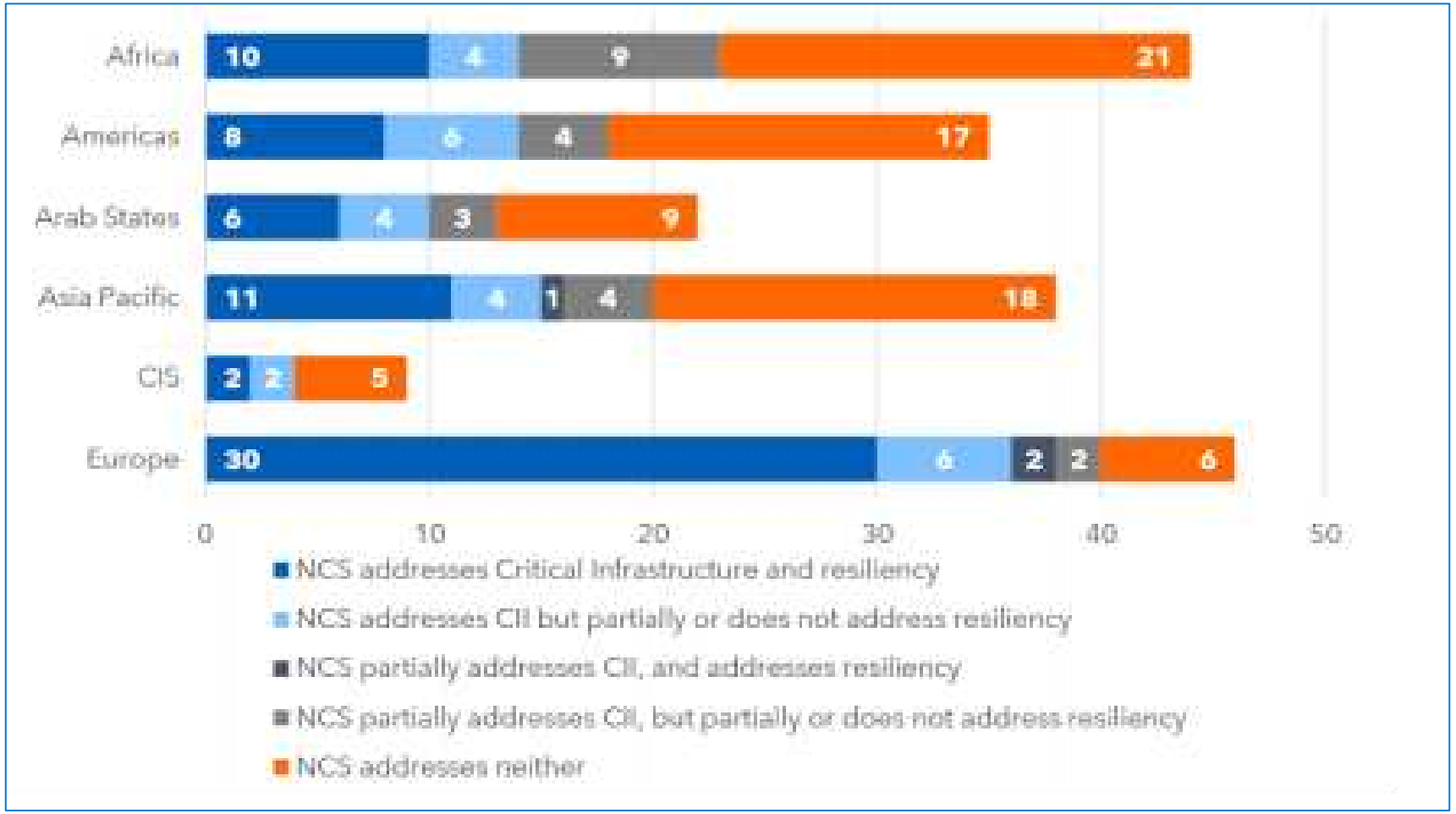
Medidas técnicas: mayor despliegue de CIRT/CERT

Número de CIRT sectoriales



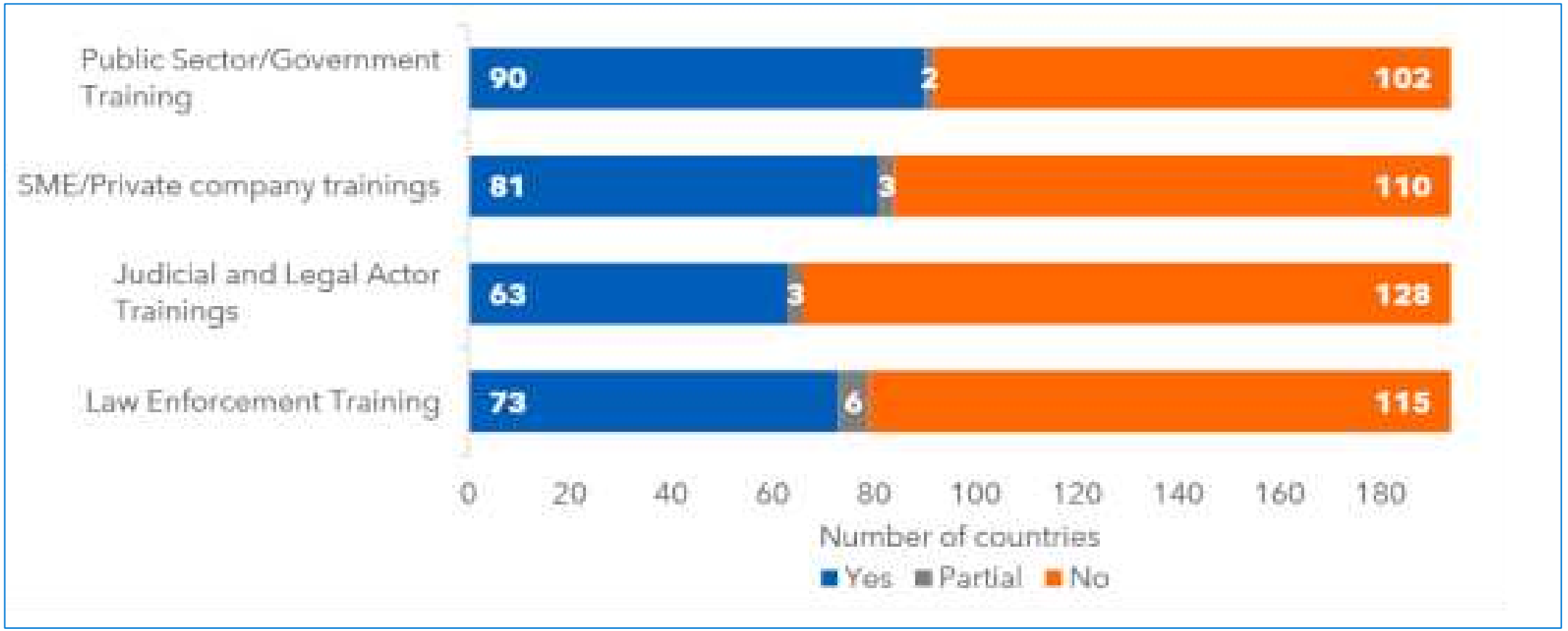
Medidas organizativas: alineación de la estrategia

Países que abordan la infraestructura crítica y la resiliencia



Medidas organizativas: alineación de la estrategia

Número de países con programas específicos de educación/formación en ciberseguridad para profesionales



Ranking global

Colombia (Republic of)

Development Level:
Developing Country

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
63.72	9.14	17.58	6.67	14.42	15.93

Source: ITU Global Cybersecurity Index v4, 2020

Enfoques integrales en Ciberseguridad

Desafíos globales en Ciberseguridad y Ciberdefensa

En **2013**, el presidente de EE. UU., Obama, emitió la **Orden Ejecutiva (EO) 13636.**

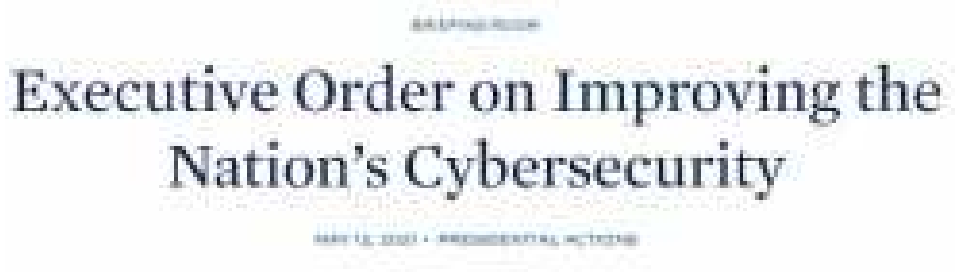
Mejorar la ciberseguridad de las infraestructuras críticas de la Nación

CSX CYBERSECURITY NEXUS

Implementing the NIST Cybersecurity Framework

En **2021**, el presidente de EE. UU., Biden, emitió la **Orden Ejecutiva (EO) 14028.**

Mejorar la Ciberseguridad de la Nación



La **Unión Europea (UE)** publicó una declaración expresando su **solidaridad con los EE.UU**. sobre el impacto de los ciberataques enfrentados en **2020** y **2021**. Además, el **Reino Unido**, **Canadá**, **Australia** y la **OTAN** culparon públicamente a **Rusia** por los ataques de **SolarWinds**.

General Data Protection Regulation (GDPR)

El **Reglamento Europeo de Protección de Datos** es aplicable a partir del **25 de mayo de 2018**. En todos los **estados miembros** para armonizar las **leyes de privacidad de datos** en toda **Europa**.

Aplica sobre los ingresos brutos anuales del grupo empresarial.

Level 1. **2%** del volumen de ingresos anual de la empresa, o **€10M**, lo que sea mayor.

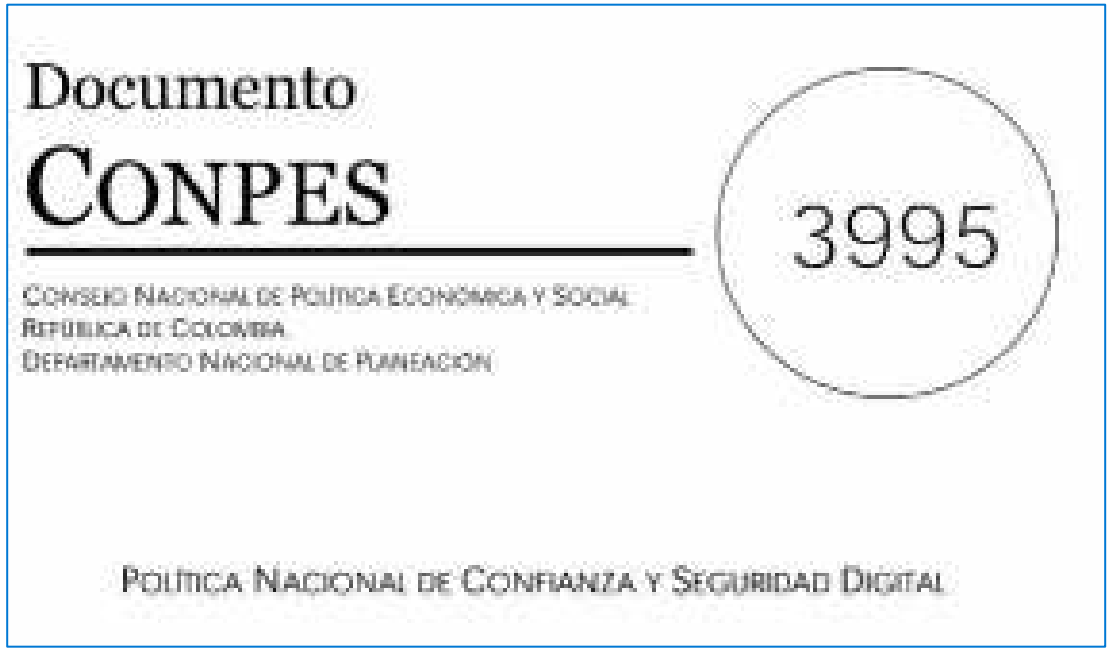
Level 2. **4%** del volumen de ingresos anual de la empresa, o **€20M**, lo que sea mayor.

El **marco de privacidad de datos** adoptará nuevos controles para garantizar que las actividades de **inteligencia de EE. UU**. se limiten a lo necesario y proporcionado para proteger la seguridad nacional, y también creará un nuevo sistema de reparación para abordar las **quejas de los ciudadanos de la UE**.

https://gdpr-info.eu/

CONPES 3995

Confianza y Seguridad Digital



https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

CONPES 3995

Objetivo

Establecer … la confianza digital a través de la mejora la seguridad digital de … iedad incluyente y competitiva en el futuro digital mediante … alización del marco de gobernanza en seguridad … énfasis en nuevas tecnologías.

Objetivos

- **OE 1.** Fortalecer las capa… or privado para aumentar la confian…
- **OE 2.** Actualizar el marco de gobernanza en mate… de desarrollo y mejorar el avance en seguridad digital del país
- **OE 3.** Analizar la adopción de modelos, estándares y marcos de trabajo en … d digital, con énfasis en nuevas tecnologías para preparar al país a los desafíos de la 4RI.

Decreto 338 de 2022
Fortalecimiento de la Gobernanza en Seguridad Digital

CONPES 3995

Sectores de infraestructura critica Nacional

IC NACIONAL

1. Gobierno.
2. Seguridad y Defensa.
3. Tecnologías de Información y de las Comunicaciones.
4. Electricidad.
5. Financiero.
6. Educación.
7. Hidrocarburos, Minas y Gas.
8. Industria, Comercio y Turismo.
9. Ambiente.
10. Salud y Protección Social.
11. Agua.
12. Transporte.
13. Agricultura y Alimentación.

Política Publica

Principios Generales

AMBIENTE DE CONFIANZA

La estrategia debe ayudar a construir un entorno digital en el cual los ciudadanos, así como las entidades de sector publico y privado nacionales e internacionales pueden confiar

LIDERAZGO BIEN DEFINIDO, ROLES Y ASIGNACIÓN DE RECURSOS

La estrategia debe establecerse en el nivel más alto del gobierno, que a posterior será responsable de asignar roles y responsabilidades relevantes, así como los recursos financieros y humanos necesarios.

ARTEFACTOS APROPIADOS EN POLÍTICA

La estrategia debe utilizar los instrumentos de política más apropiados disponibles para cumplir cada uno de sus objetivos, teniendo en cuenta las circunstancias específicas del país.

GESTIÓN DE RIESGOS Y RESILIENCIA

La estrategia debe permitir una gestión eficiente de los riesgos de ciberseguridad e Impulsar la resiliencia de las actividades económicas y sociales.

VISIÓN

Enfoque futurista centrado en la sociedad y un marco de gobierno estructurado.

ENFOQUE INTEGRAL Y PRIORIDADES PERSONALIZADAS

La estrategia debe abarcar las generalidades del entorno digital, pero a la medida de las circunstancias de cada país y a su priorización.

INCLUSIVIDAD

La estrategia debe desarrollarse con la participación activa de todos los partes interesadas relevantes, y debe abordar sus necesidades y responsabilidades.

PROSPERIDAD ECONÓMICA Y SOCIAL

La estrategia debe fomentar la prosperidad económica y social y maximizar la contribución de las TIC al desarrollo sostenible y la inclusión social.

DERECHOS HUMANOS FUNDAMENTALES

La estrategia debe respetar y ser coherente con los valores fundamentales.

Política publica en Ciberseguridad

Política Nacional y Gobierno
En todos los sectores colaboración multidisciplinaria

Justicia
Articulación del sistema judicial

Victimas
Ambiente adecuado de denuncias y seguimiento

Publico/Privado
Sectores publico y privado Todos trabajando por y para la comunidad

Sociedad
Suficientes recursos financieros y humanos

Industria
Acogimiento de las directrices nacionales

Comunicaciones y medios
Comunicaciones responsables

Educación
Desarrollo de competencias ciudadanas

Investigación
Potencialización del uso de las TICs

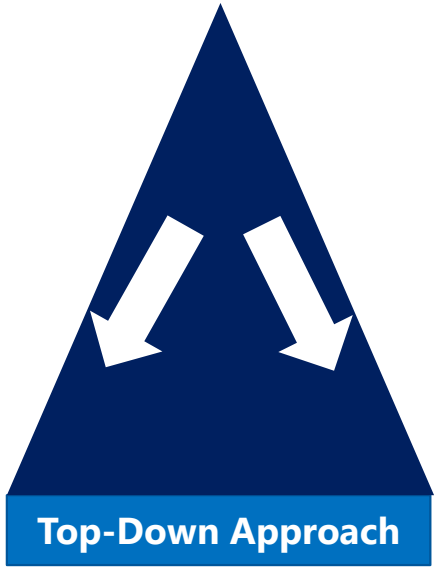
Nación
Desarrollo de ventajas competitivas integrales

El factor humano es la clave del éxito

Fuente: Desarrollo Propio (Wilmer Prieto Gómez)

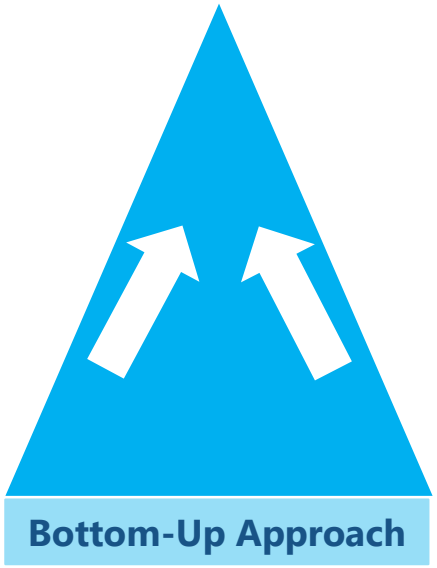
Ciberseguridad y ciberdefensa

Enfoques integrales en Ciberseguridad



1. Automatizar la búsqueda de riesgos que puedan comprometer los objetivos del negocio.
2. Planteamiento de escenarios con el fin de examinar la relación entre los diferentes riesgos.
3. Análisis de los posibles eventos y su impacto en los objetivos del negocio.
4. Enfocarnos en una adecuada gestión de los riesgos.

Teniendo en cuenta lo anterior podremos presentar y sustentar de una forma fácil los casos de negocio.



1. Identificación de riesgo específicos de relacionadas con la ciberseguridad del ecosistema.
2. De lo general a lo particular.
3. Planteamiento pensando en la satisfacción de las necesidades organizacionales.
4. Identificación de escenarios de riesgo altamente interdependientes.

Mantener el interés del C-Level en la organización.

Capacidades particulares a desarrollar

Mejorar la ciberseguridad de las infraestructuras críticas de la Nación

Orden Ejecutiva (EO) 13636

NIST CYBERSECURITY FRAMEWORK

https://www.nist.gov/cyberframework

PRIVACY FRAMEWORK

https://www.nist.gov/privacy-framework

El CORE del Framework

Establece un lenguaje común

Función
Identificar
Proteger
Detectar
Responder
Recuperar

- Describe los resultados deseados.
- Comprensible para todos.
- Aplica para cualquier tipo de gestión de riesgos.
- Define toda la amplitud de la ciberseguridad.
- Abarca tanto la prevención como la reacción.

Un extracto del Framework Core

El camino conectado de los resultados del marco

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

5 Funciones **23 Categorías** **108 Subcategorías** **6 Referencias informativas**

Tiers de implementación

Marco de Ciberseguridad versión 1.1

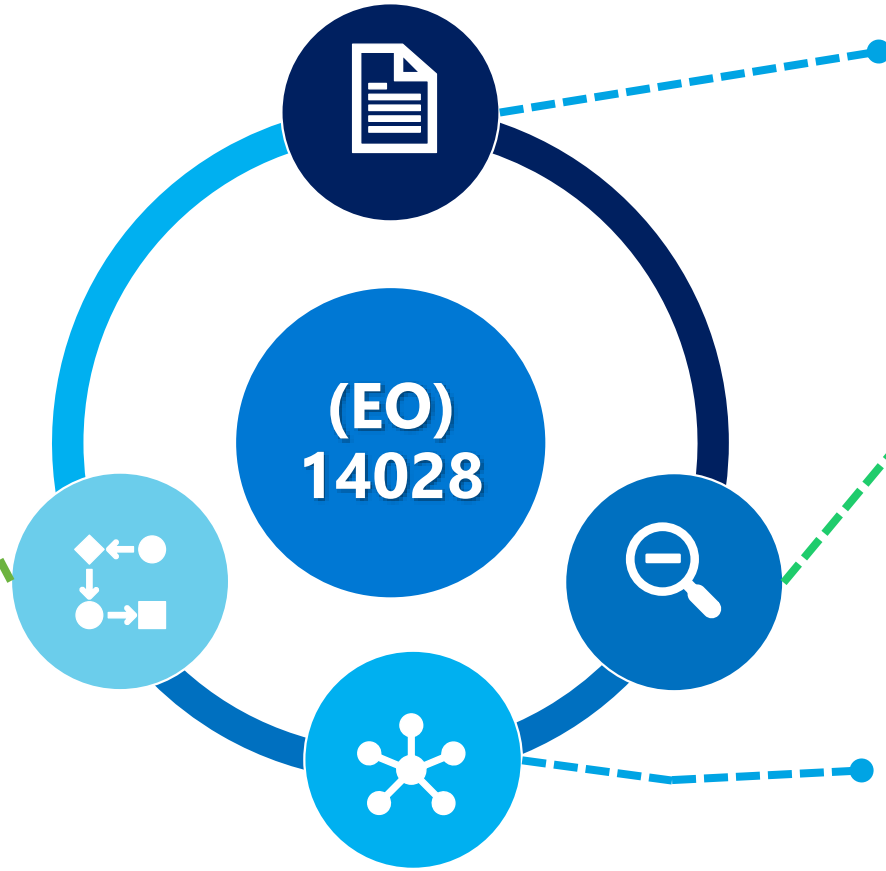
	1	2	3	4
	Parcial	**Riesgo informado**	**Repetible**	**Adaptativo**
Proceso de gestión de riesgos	Funcionalidad y repetibilidad de la gestión de riesgos de ciberseguridad			
Programa de Gestión Integral de Riesgos	La medida en que la ciberseguridad se considera en las decisiones más amplias de gestión de riesgos.			
Participación Externa	**El grado en que la organización:** • supervisa y gestiona el riesgo de la cadena de suministro. • se beneficia al compartir o recibir información de terceros.			

Capacidades particulares a desarrollar

Mejorar la Ciberseguridad de la Nación

Multifactor Authentication

(MFA)



Zero Trust Architecture

(ZTA)

Endpoint Detection and Response

(EDR)

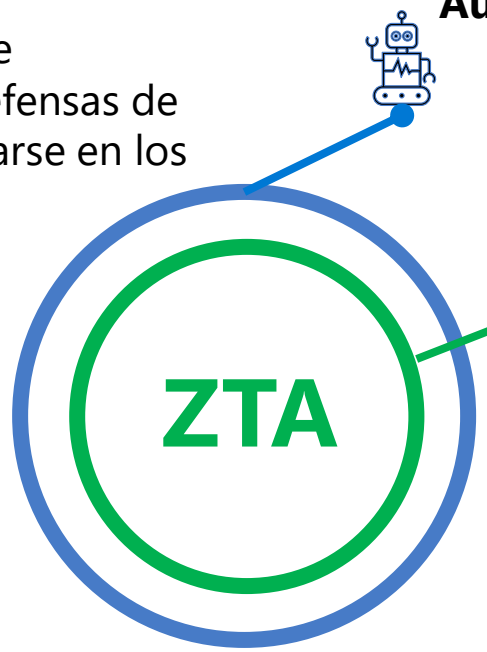
Extended Detection and Response

(XDR)

https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

Zero Trust Architecture (ZTA)

ZT es el término para un conjunto en evolución de paradigmas de ciberseguridad que mueven las defensas de perímetros estáticos basados en la red para centrarse en los usuarios, los activos y los recursos.



Automatización y orquestación

(ITSM, SIEM, SOAR, CASB, SASE, SSE, EDR, XDR)

Visibilidad y Analítica

(MITRE ATT&CK, MITRE D3FEND, CTI, OSINT, SIEM, SOAR, SASE, SSE, EDR, XDR, EPP)

Cargas de trabajo

(CWPP, Traffic Light Protocol-TLP)

Personas

(FCAPS Model, CIS Controls v8, Defensa en Profundidad)

Dispositivos

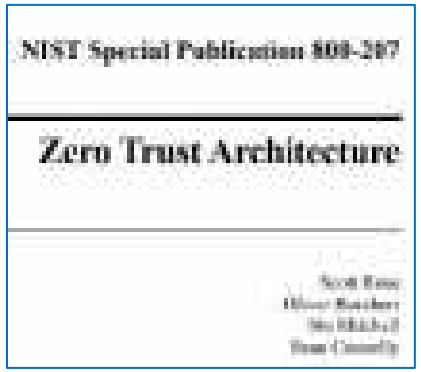
(FCAPS Model, CIS Controls v8, Defensa en Profundidad)

Redes

(FCAPS Model, ITSM, CASB, SASE, CIS Controls v8, Defensa en Profundidad)

Datos

(GDPR, Normativas nacionales e internacionales, requerimientos contractuales)


NIST Special Publication 800-207

Zero Trust Architecture

NIST SP 800-207 – Zero Trust Architecture

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Plataformas de Inteligencia en Seguridad (SIP)

SIP se refiere a la recopilación y el análisis de datos para comprender los motivos, los objetivos y los comportamientos de ataque de los agentes de amenaza.

Los adversarios y su ciclo de vida

Cyber Kill Chain

MITRE ATT&CK™

ATT&CK Móvil

ATT&CK Empresarial

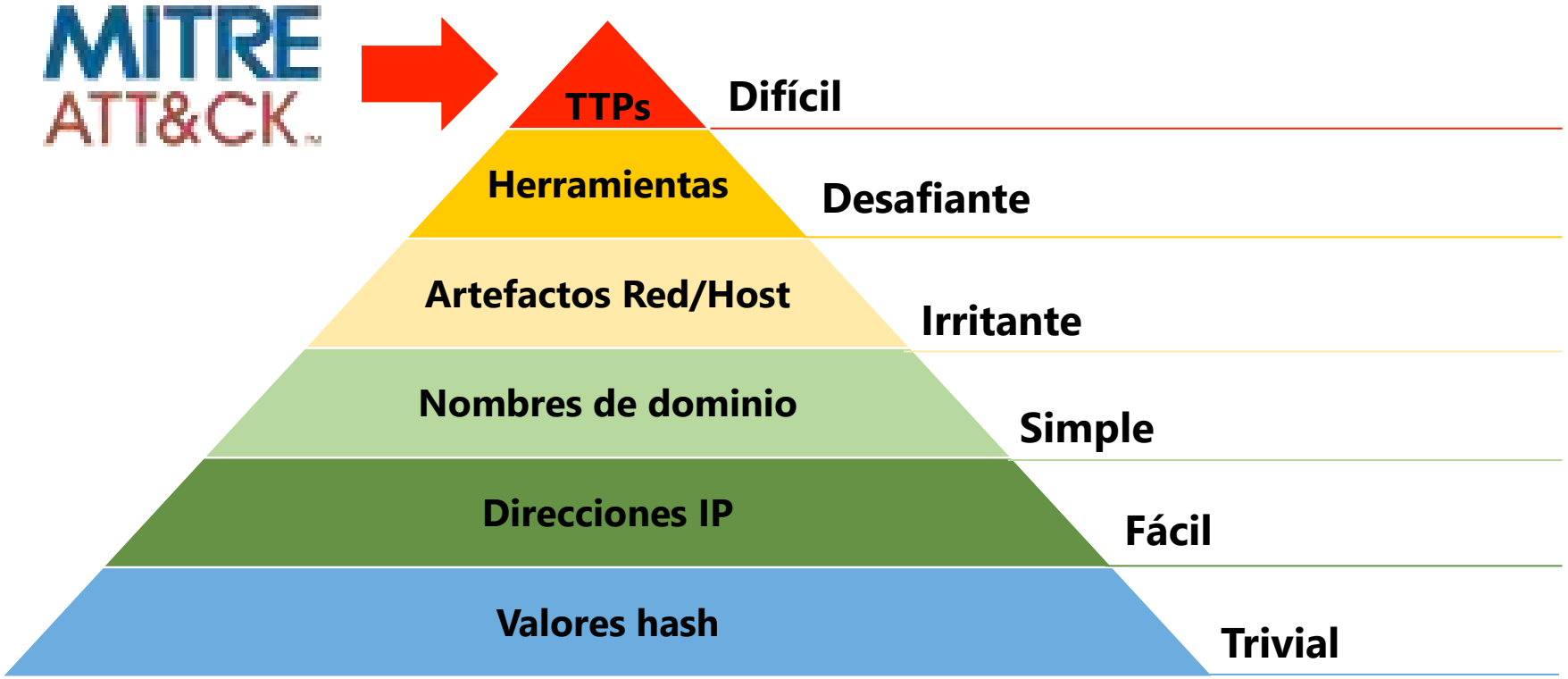
MITRE ATT&CK

Una base de conocimientos de comportamiento del adversario

- Basado en observaciones del mundo real.
- Gratis, abierto y accesible a nivel mundial.
- Un lenguaje común.
- Impulsado por la comunidad.

La pirámide del dolor

David Bianco



Fuente: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

MITRE D3FEND

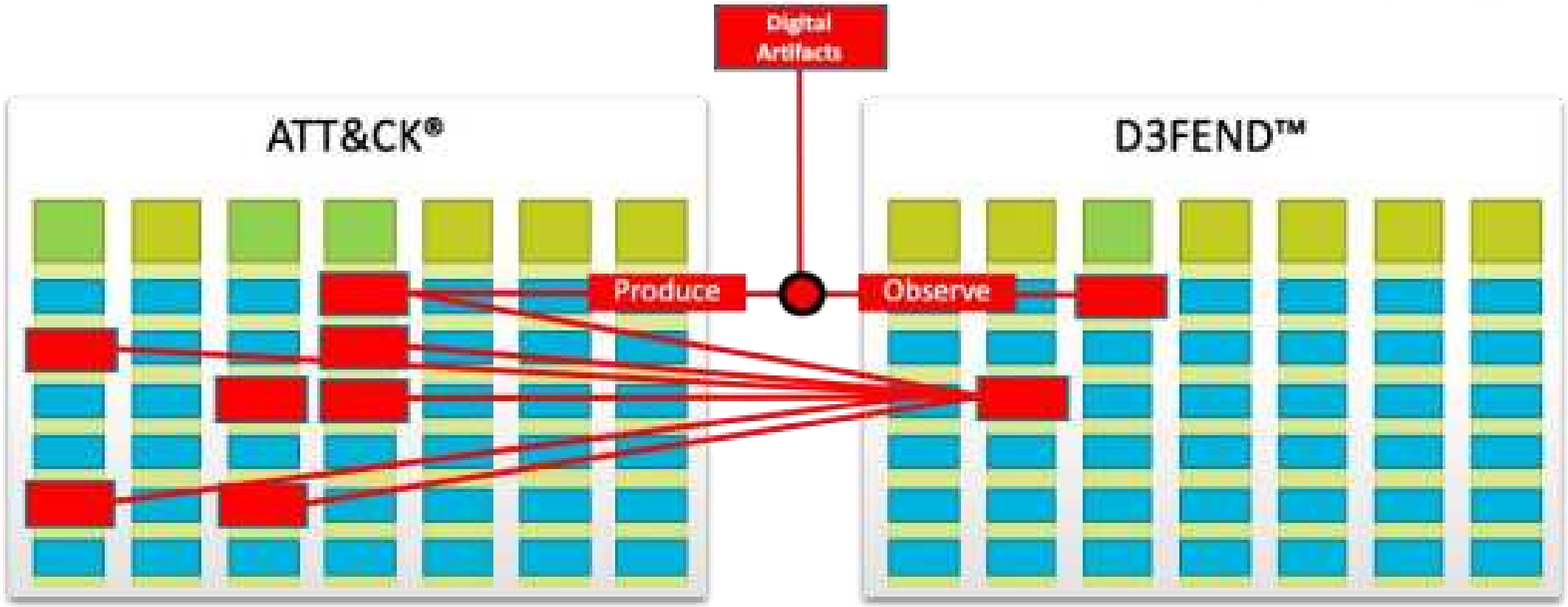
Acerca del proyecto de gráfico de conocimiento

- **D3FEND** es una **base de conocimiento**, pero más específicamente un **gráfico de conocimiento, de técnicas de contramedidas de ciberseguridad**.
- Es un **catálogo de técnicas defensivas de ciberseguridad** y sus **relaciones con técnicas ofensivas/adversarias**.
- El objetivo principal del lanzamiento inicial de **D3FEND** es ayudar a **estandarizar el vocabulario** utilizado para describir la funcionalidad de la tecnología de **ciberseguridad defensiva**.

MITRE
D3FEND™

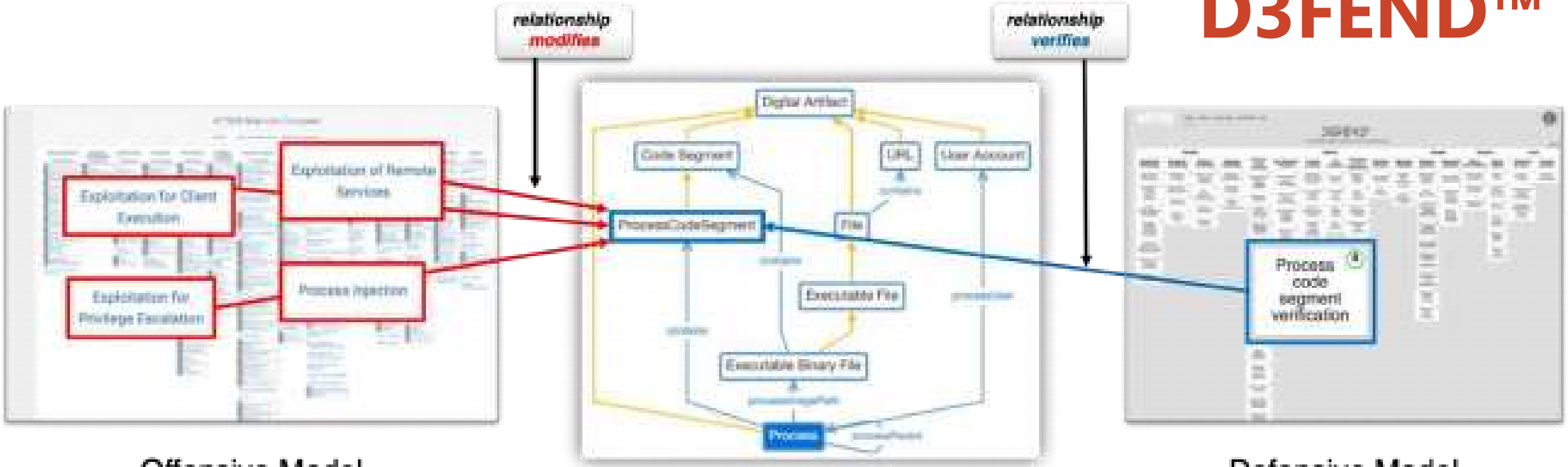
Relaciones Simplificadas de Técnicas Ofensivas y Defensivas

Subtitle or descriptive text



Ontología de artefactos digitales

MITRE D3FEND™



Offensive Model

Digital Artifact Ontology
(simplified)

Defensive Model


“Las huellas de las personas que caminaron juntas nunca se borran. ”
Proverbio Africano

Visión Tecnológica Microsoft

5

Microsoft

Máster en Dirección y Administración de Empresas (MBA).
Magister en Seguridad de Sistemas de Información.
Especialista en Gerencia de Telecomunicaciones
Especialista en Marketing Digital
Ingeniero de Sistemas

CISM, CCSK
Microsoft CSAE, Microsoft COAA
Microsoft IPAA, Microsoft IAAA
Microsoft 365F, Microsoft AzureF
Microsoft SCIF, Microsoft OpenHack SCI
Symantec CSC, AWS CCP

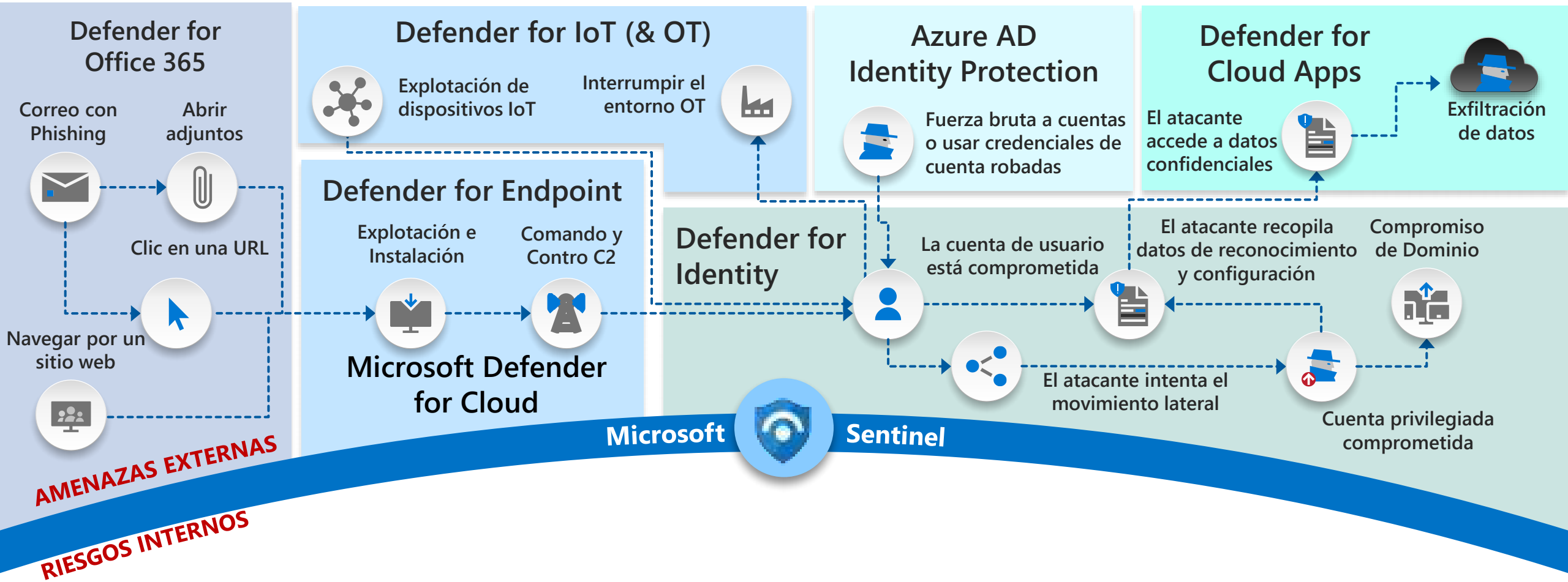
gugom@microsoft.com

Gustavo Gómez

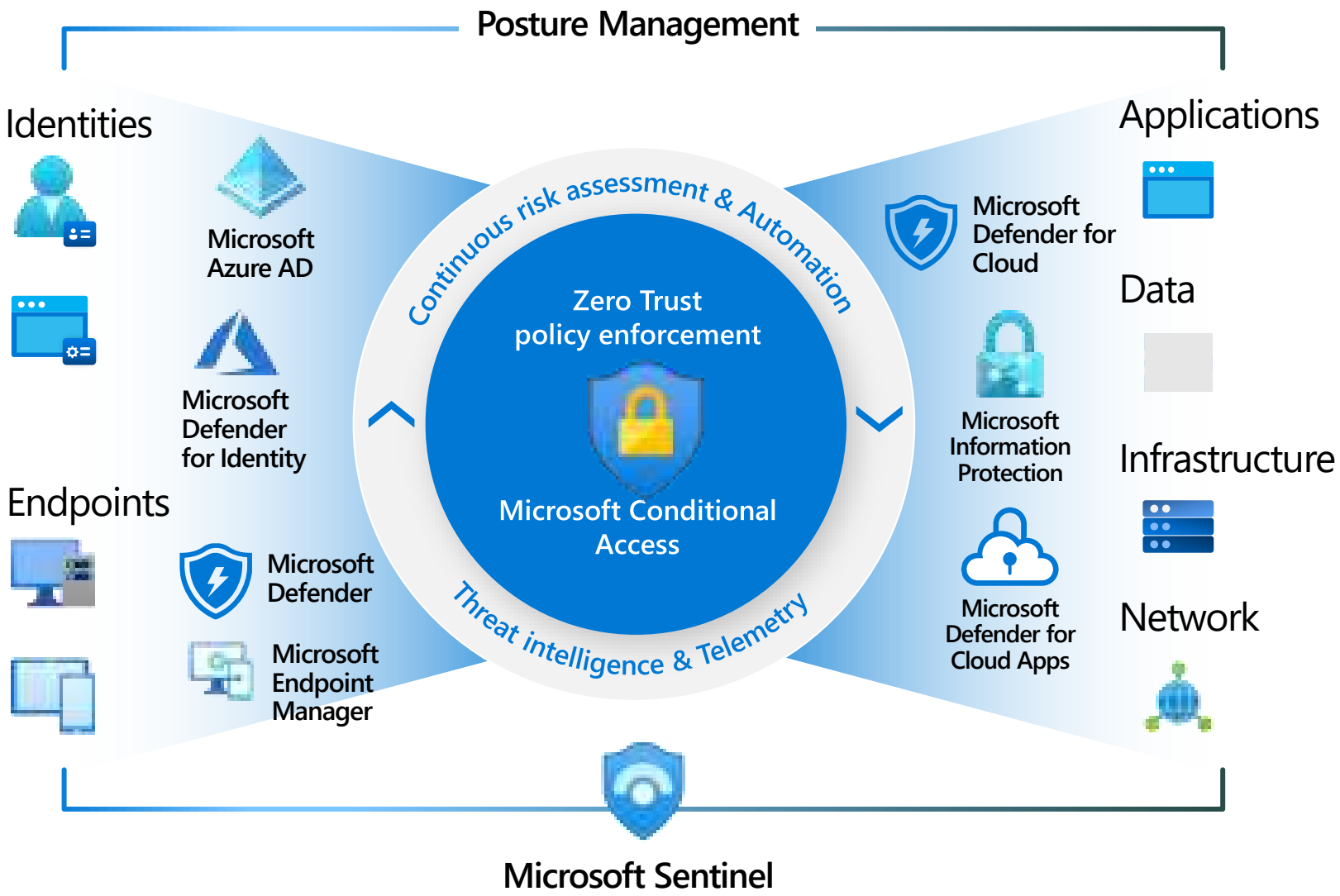
Defender a través de cadenas de ataque

Amenazas internas y externas

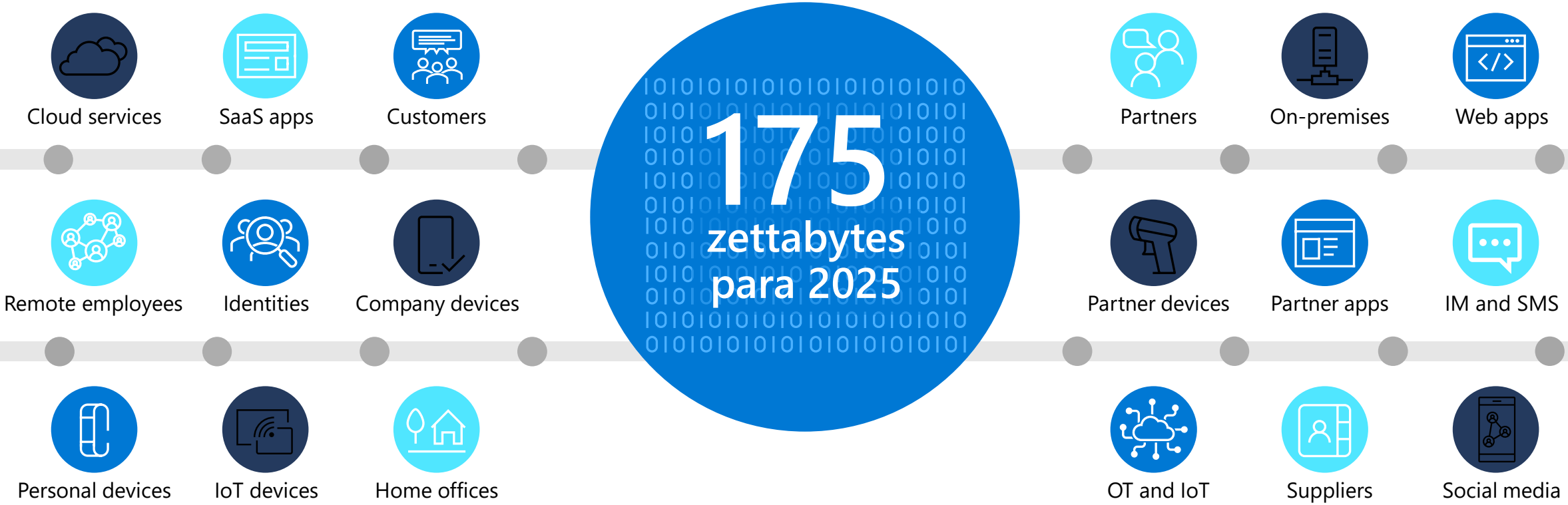
Microsoft December 2021 – https://aka.ms/MCRA



Microsoft Zero Trust Capabilities



La proliferación de la información sigue acelerándose



Sources:
1. IDC Data Age 2025

Microsoft para ayudar a proteger los datos de su empresa

Comprender su panorama de datos

Dónde se encuentra su información confidencial, cómo se accede, comparte y edita

Protección de sus datos

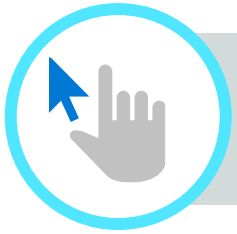
Identificar y prevenir el intercambio, la transferencia y el uso riesgosos o inapropiados de datos confidenciales

Protección contra amenazas internas

Identifique las amenazas internas a sus datos más importantes

Protección y gobernanza de la información

Clasifique, gobierne y proteja información dondequiera que viva



Prevención de pérdida de datos

Evitar el intercambio accidental o inapropiado de datos

Gestión de riesgos internos

Identificar y mitigar los riesgos internos

Microsoft para ayudar a proteger los datos de su empresa

Conocer los requisitos regulatorios
Evaluar el cumplimiento y responder a los requisitos reglamentarios

Gerencia de Cumplimiento
Simplifique el cumplimiento y reduzca el riesgo

Comprender sus datos de extremo a extremo
Descubra, conserve, recopile, procese, elimine y analice sus datos en un solo lugar

Advanced eDiscovery
Responder eficientemente a asuntos legales e investigaciones

Reducción del volumen de contenido
Centrarse en los activos más relevantes

Auditoría avanzada
Reduzca el volumen de activos, el tiempo y los costos durante las investigaciones

Use Microsoft Priva y Microsoft Foo para ayudar a proteger los datos de su empresa

Gestión de riesgos y operaciones de privacidad
Identifique y mitigue los riesgos de privacidad de manera efectiva y automatice las solicitudes de derechos de los sujetos

Microsoft Priva
Proteja los datos personales y cree un lugar de trabajo resistente a la privacidad

Defender a través de cadenas de ataque

Amenazas internas y externas

Microsoft December 2021 – https://aka.ms/MCRA

Defender for Office 365

Correo con Phishing

Abrir adjuntos

Clic en una URL

Navegar por un sitio web

Defender for IoT (& OT)

Explotación de dispositivos IoT

Interrumpir el entorno OT

Azure AD Identity Protection

Fuerza bruta a cuentas o usar credenciales de cuenta robadas

Defender for Cloud Apps

El atacante accede a datos confidenciales

Exfiltración de datos

Defender for Endpoint

Explotación e Instalación

Comando y Contro C2

Microsoft Defender for Cloud

Defender for Identity

La cuenta de usuario está comprometida

El atacante recopila datos de reconocimiento y configuración

Compromiso de Dominio

El atacante intenta el movimiento lateral

Cuenta privilegiada comprometida

AMENAZAS EXTERNAS

Microsoft Sentinel

RIESGOS INTERNOS

Indicadores Pro activos

Historial de violaciones

Distraído y descuidado

Descontento o desencantado

Sujeto a factores estresantes

Gestión de riesgos internos

Los internos tienen acceso a datos confidenciales

Actividad anómala detectada

Fuga de datos

Posible sabotaje

Microsoft

“La seguridad cibernética es la mayor amenaza para la transformación digital en la actualidad y es el riesgo número uno que enfrentan todas las empresas en el futuro."

Satya Nadella

#Bogotá territorio inteligente

Jueves 06 de octubre de 2022
9:00 a.m. a 10:30 am

ALCALDÍA MAYOR DE BOGOTÁ D.C.
ALTA CONSEJERÍA DISTRITAL DE TIC
BOGOTÁ

COMPARTIC BOGOTÁ
GOBIERNO Y SEGURIDAD DIGITAL

Sistemas de planificación de recursos empresariales (ERP)

Tema:

ERP

FECHA: octubre 06, 2022 9:00am

- **9:00 Apertura y presentación de la Alta Consejería Distrital de TIC**
  - Estrategia de la Oficina de Alta Consejería TIC
  - Objetivos de las sesiones de ComparTIC
  - Mensajes de Sistemas de planificación de recursos empresariales (ERP)
- **9:20 Presentación de Secretaría Distrital de Seguridad, Convivencia y Justicia**
  - Beneficios, recomendaciones y experiencias.
  - Mayor reto y cómo lo solucionaron.
- **10:00 Preguntas por parte de las entidades y/o asistentes**
  - Agenda de talleres de ComparTIC – Gobierno Digital 2022
- **10:29 Cierre del evento**

Tema:

ERP

FECHA: octubre 06, 2022 9:00am

Mario Ortiz Salgado
Director de Tecnologías y Sistemas de la Información
mario.ortizs@scj.gov.co

Jairo Bohórquez
Líder de infraestructura
Oscar Suárez
Líder Si Capital

Secretaría Distrital de Seguridad, Convivencia y Justicia

Oficina de Alta Consejería Distrital de TIC

Nicolás Sánchez Barrera
nsanchez@alcaldiabogota.gov.co

Jaime Leonardo Acosta Diaz
jlacosta@alcaldiabogota.gov.co

Tema:

ERP

FECHA: octubre 06, 2022 9:00am

Estrategia

Oficina de Alta Consejería Distrital de TIC

ALCALDÍA MAYOR DE BOGOTÁ D.C. | ALTA CONSEJERÍA DISTRITAL DE TIC | BOGOTÁ

Buscamos consolidar a Bogotá como un Territorio Inteligente

Se consolida a través de la implementación de un Gobierno Abierto en Bogotá

GOBIERNO ABIERTO DE BOGOTÁ

Lo hacemos a partir del aprovechamiento estratégico de tecnología, datos e innovación a través de proyectos concretos en el Distrito

ALTA CONSEJERÍA DISTRITAL DE TIC | BOGOTÁ

Tema:

ERP

FECHA: octubre 06, 2022 9:00am

ALCALDÍA MAYOR DE BOGOTÁ D.C. | ALTA CONSEJERÍA DISTRITAL DE TIC | BOGOTÁ

ComparTIC

Conocer **cómo hacen otras** entidades **para mejorar la calidad** de vida de los ciudadanos

Aprender a utilizar la tecnología como un medio para facilitar el día a día de las ciudadanas y los ciudadanos

Implementar los lineamientos no es el objetivo final. Debemos **aprender a generar valor a partir de su implementación**

Primer jueves de cada mes
9:00 am a 10:30 am
Gobierno Digital
nsanchez@alcaldiabogota.gov.co

Último Jueves de cada mes
10:00 am a 11:30 am
Seguridad Digital
jcmancipe@alcaldiabogota.gov.co

Tema:

ERP

FECHA: octubre 06, 2022 9:00am

Sistemas de planificación de recursos empresariales (ERP)

ALCALDÍA MAYOR DE BOGOTÁ D.C. | ALTA CONSEJERÍA DISTRITAL DE TIC | BOGOTÁ

ALCALDÍA MAYOR DE BOGOTÁ D.C. | SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA | BOGOTÁ

Mensajes

1. Las entidades deben realizar diagnósticos y análisis que permitan identificar las oportunidades de mejora en sus procesos de apoyo para soportar la adquisición de sistemas de información de tipo (ERP)

2. Los ERP que adquieran las entidades deben interoperar con otras plataformas de manera fácil y segura; principalmente se debe buscar la generación de la información solicitada el sistema BogData.

3. Las entidades deben realizar los ajustes necesarios en sus ERP para utilizar la información que genera BogData en sus procesos internos.

Tema:

ERP

FECHA: octubre 06, 2022 9:00am

PREGUNTAS DE ENTIDADES Y ASISTENTES

Tema:

ERP

FECHA: octubre 06, 2022 9:00am

ComparTIC Bogotá: Gobierno Digital

primer jueves del mes de 9:00 a.m. a 10:30 a.m., de la siguiente manera:

- **22 de febrero:** Acuerdo Marco de Precios Nube Pública IV
- **22 de marzo:** Accesibilidad, Usabilidad y Transparencia
- **05 de mayo:** Arquitectura Empresarial
- **02 de junio:** Desarrollo de software DevOps
- **07 de julio:** Desarrollo de Software
- **04 de agosto:** Planeación estratégica de Tecnologías de la Información y las Comunicaciones
- **01 de septiembre:** Internet de las cosas (IoT)
- **06 de octubre: Sistemas de planificación de recursos empresariales (ERP)**
- **03 de noviembre:** Servicios centrados en el usuario
- **01 de diciembre:** Analítica

ComparTIC Bogotá: Seguridad Digital

Último jueves del mes de 10:00 a.m. a 11:30 a.m., con los siguientes temas:

- **24 de febrero:** Seguridad Digital – Modelo de Seguridad y Privacidad de la Información
- **24 de marzo:** Plan Distrital de Protección de Datos Personales
- **28 de abril:** Riesgos de seguridad digital
- **26 de mayo:** Seguridad en el teletrabajo o trabajo en casa
- **30 de junio:** Taller de buenas prácticas en seguridad de sitios Web
- **28 de julio:** Plan Estratégico de Seguridad de la Información - PESI
- **25 de agosto:** Riesgos de ciberseguridad en IoT
- **29 de septiembre:** Taller de Hacking ético e Ingeniería Social
- **27 de octubre:** Gestión de incidentes de seguridad de la información
- **24 de noviembre:** Servicios seguros en continuidad del

2022

Alta Consejería Distrital de TIC
Secretaría General - Alcaldía Mayor de Bogotá
Tel: 601 3813000, ext. 2001
Bogotá, Colombia: Carrera 8 # 10 – 65
tic.bogota.gov.co

@ConsejeriaTIC

ALCALDÍA MAYOR DE BOGOTÁ D.C.
ALTA CONSEJERÍA DISTRITAL DE TIC
BOGOTÁ