Microsoft

Ciberseguridad: visión global en materia de regulación desde la perspectiva de Microsoft

Robert Ivanschitz

Director de Asuntos Jurídicos y Corporativos de Microsoft Latinoamérica

Los gobiernos juegan diferentes roles en el ciberespacio

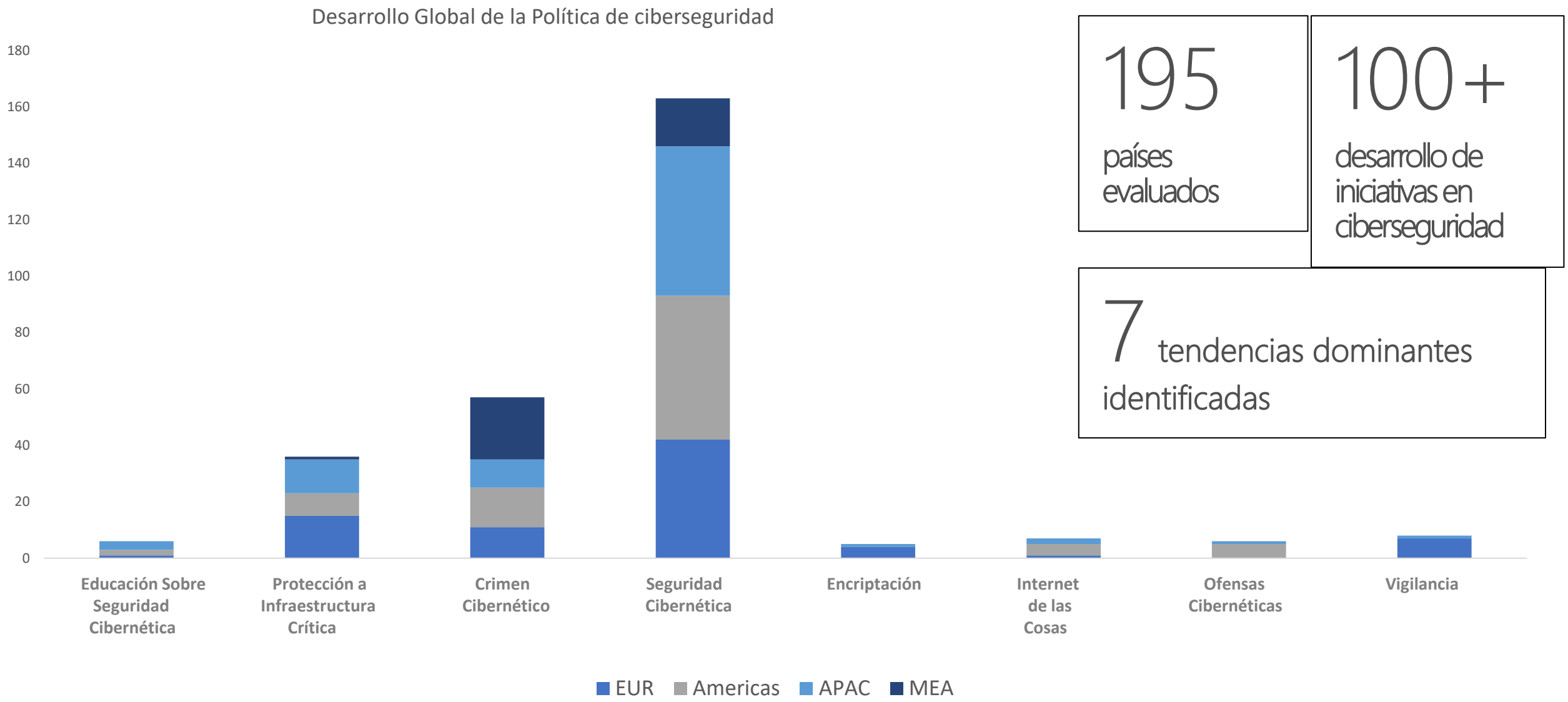
Microsoft

Esta presentación no abordará temas de:

- Privacidad
- Seguridad electoral
- Civilidad digital

Panorama cambiante en políticas de ciberseguridad

Microsoft



195 países evaluados

100+ desarrollo de iniciativas en ciberseguridad

7 tendencias dominantes identificadas

Tendencias en las políticas en ciberseguridad

Microsoft

1. Combate al crimen cibernético
2. Protección de infraestructuras críticas
3. Desarrollo de una estrategia nacional de ciberseguridad
4. Creación de una Agencia Nacional de Ciberseguridad
5. Facilitar la creación de mecanismos de prevención, reporte y defensa
6. Apoyo al desarrollo de una fuerza laboral en ciberseguridad
7. Impulso a la educación y conciencia sobre ciberseguridad en los grupos vulnerables

1 Combate al crimen cibernético

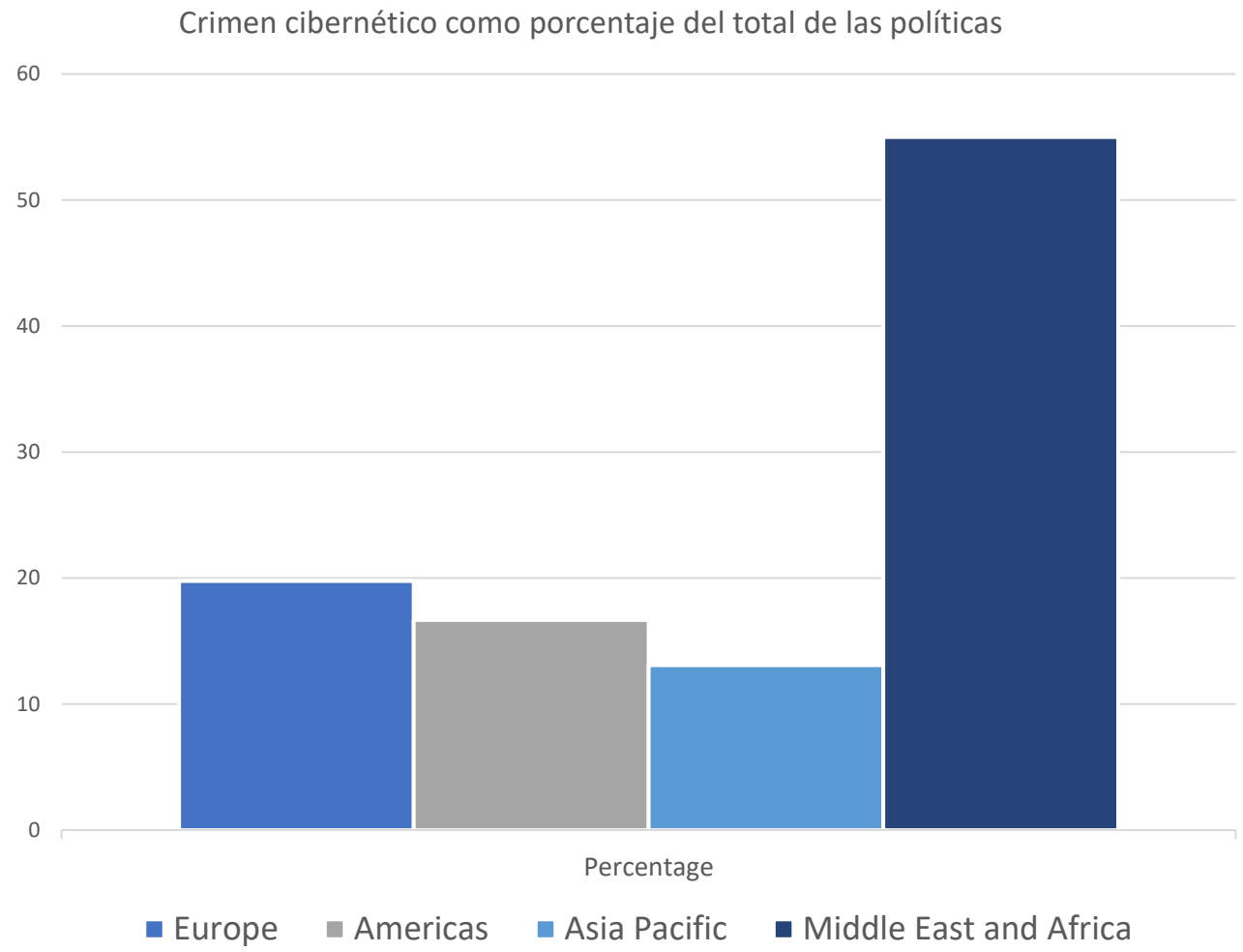
Microsoft

RETO

- ¿CÓMO LOGRAR QUE LAS LEYES AVANCEN EN LA MISMA VELOCIDAD QUE LA TECNOLOGÍA?

ENFOQUE DE LA POLÍTICA

- MEJORAR EL PROCEDIMIENTO "MLAT"
- ALINEACIÓN CON LAS CONVENCIONES RECONOCIDAS INTERNACIONALMENTE



Microsoft

13 mil millones

De e-mails sospechosos o maliciosos bloqueados.

1,600 millones

de URL´s bloqueadas, que tenían el propósito de realizar ataques de Phishing.

35%

de incremento en ataques dirigidos a IoT.

90%

de las intrusiones empiezan con un ataque de phishing.

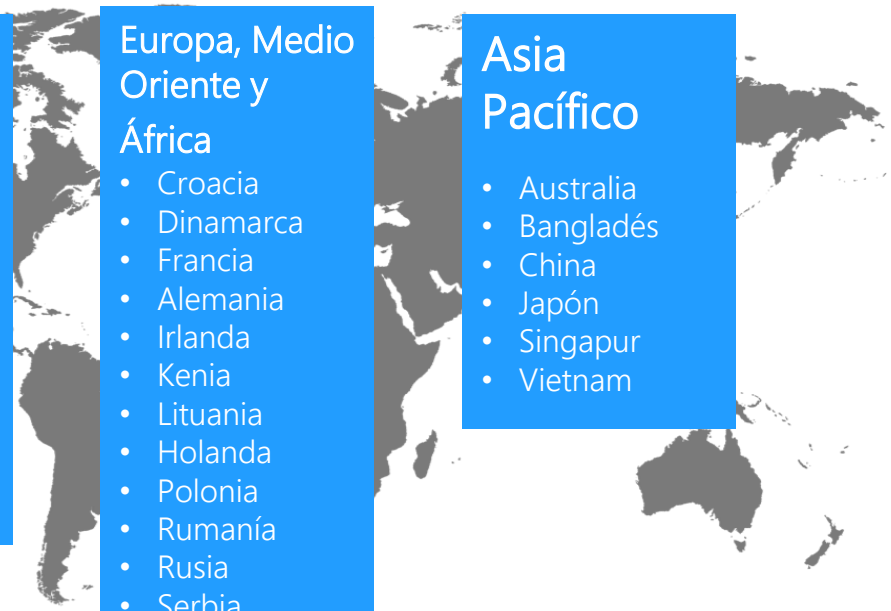
60 mil

mensajes diarios detectados con archivos o enlaces maliciosos relacionados con COVID-19.


Threats - 30 Days
Avalanche
B106
Bamital
Barium
Caphaw
Citadel
Conficker
Dorkbot
Gamarue
Gameover Zeus
Necurs
Phosphorous
Ramnit
Simda
Sirefef
Strontium
Thallium
Trickbot
Waledac
Davis Strait
GREENLAND (DEN.)
ICELAND
Hudson Bay
CANADA
Labrador Sea
SWEDEN
NORWAY
FINLAND
RUSSIA
UNITED KINGDOM
DENMARK
IRELAND
BELARUS
POLAND
UKRAINE
KAZAKHSTAN
MONGOLIA
FRANCE
AUSTRIA
ROMANIA
Black Sea
ITALY
UZBEKISTAN
SPAIN
PORTUGAL
GREECE
TURKEY
TURKMENISTAN
TAJIKISTAN
NORTH KOREA
S. KOREA
JAPAN
CHINA
Mediterranean Sea
SYRIA
IRAQ
IRAN
AFGHANISTAN
PAKISTAN
MOROCCO
ALGERIA
LIBYA
EGYPT
SAUDI ARABIA
OMAN
INDIA
MYANMAR
THAILAND
VIETNAM
PHILIPPINES
Philippine Sea
MAURITANIA
MALI
NIGER
CHAD
SUDAN
YEMEN
BURKINA FASO
GUINEA
NIGERIA
GHANA
SOUTH SUDAN
Arabian Sea
CAMEROON
SOMALIA
UGANDA
KENYA
GABON
CONGO (DRC)
TANZANIA
MALAYSIA
INDONESIA
ANGOLA
ZAMBIA
ZIMBABWE
NAMIBIA
MADAGASCAR
MOZAMBIQUE
ESWATINI
SOUTH AFRICA
Indian Ocean
AUSTRALIA
Southern Ocean
Sea of Okh
Sargasso Sea
Atlantic Ocean
Gulf of Mexico
CUBA
HAITI
PR (U.S.)
GUATEMALA
NICARAGUA
VENEZUELA
GUYANA
SURINAME
COLOMBIA
ECUADOR
PERU
BRAZIL
BOLIVIA
PARAGUAY
CHILE
URUGUAY
ARGENTINA

2 Protección de infraestructuras críticas

Microsoft



Américas

- Austria
- Bermuda
- Canadá
- Islas Caimán
- Chile
- Colombia
- México
- Estados Unidos
- OEA

Europa, Medio Oriente y África

- Croacia
- Dinamarca
- Francia
- Alemania
- Irlanda
- Kenia
- Lituania
- Holanda
- Polonia
- Rumanía
- Rusia
- Serbia
- Eslovaquia
- Eslovenia
- Suecia

Asia Pacífico

- Australia
- Bangladés
- China
- Japón
- Singapur
- Vietnam

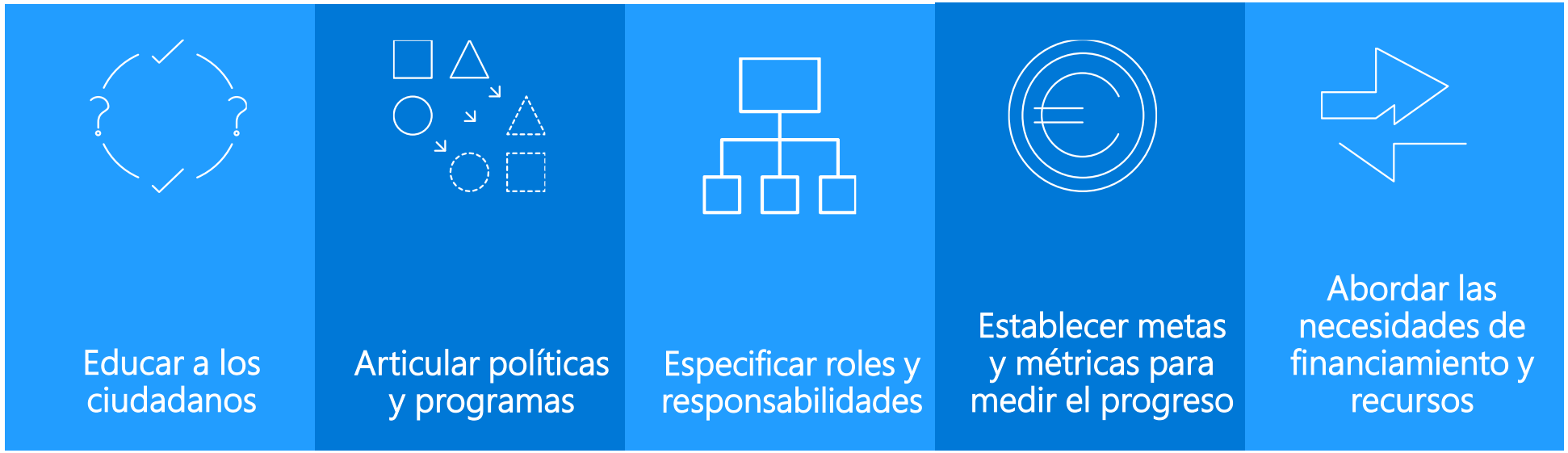
Para administrar mejor los riesgos de la ciberseguridad en infraestructura crítica, los gobiernos están introduciendo leyes o lineamientos basados principalmente en la Directiva NIS de la UE y el Marco NIST de Ciberseguridad.

Infraestructura Crítica:

"Infraestructura Crítica" significa los sistemas y activos, ya sean físicos o virtuales que son tan vitales al país, que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitador en la seguridad, la seguridad económica nacional, la salud o seguridad pública y nacional, o cualquier combinación de estos."

3 Desarrollo de una estrategia nacional de ciberseguridad

Una estrategia nacional exitosa sobre ciberseguridad es un documento "vivo", con principios claramente establecidos y adopta un acercamiento de administración de riesgos.



Más de 70 países han adoptado estrategias nacionales de ciberseguridad

4 Creación de una Agencia Nacional de Ciberseguridad

Microsoft

La ciberseguridad necesita ser coordinada por una entidad a nivel nacional

Crear una Agencia Nacional de Ciberseguridad única para evitar la duplicación y priorizar recursos limitados.

Establecer un mandato claro en el que se especifique su alcance, funciones y obligaciones.

5

Facilitar la creación de mecanismos de prevención, reporte y defensa

Microsoft

Principios

1. Compartir información sobre amenazas, incidentes, vulnerabilidades y mitigación entre autoridades, empresas de tecnología, organizaciones de industria, de la sociedad civil y víctimas con el fin de promover medidas de protección, detección y respuesta.

2. Privilegiar la creación de mecanismos de reporte efectivos y modernos.

6 Apoyo al desarrollo de una fuerza laboral en ciberseguridad

Microsoft

IMPULSORES

PAÍSES EN VÍAS DE DESARROLLO EN PROCESO DE ADOPCIÓN DE TECNOLOGÍAS

INCREMENTO MASIVO DE DISPOSITIVOS CONECTADOS

BRECHA EN LAS HABILIDADES EN MATERIA DE CIBERSEGURIDAD

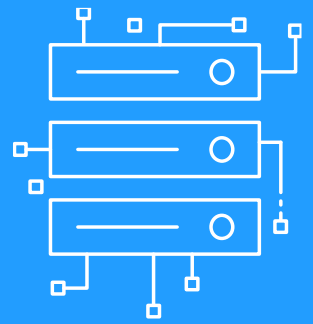
ENFOQUE DE LA POLÍTICA

PROGRAMAS PARA EL DESARROLLO DE FUERZA LABORAL

7 Impulso a la educación y conciencia sobre ciberseguridad en los grupos vulnerables

Microsoft

CULTURA DE LA CIBERSEGURIDAD

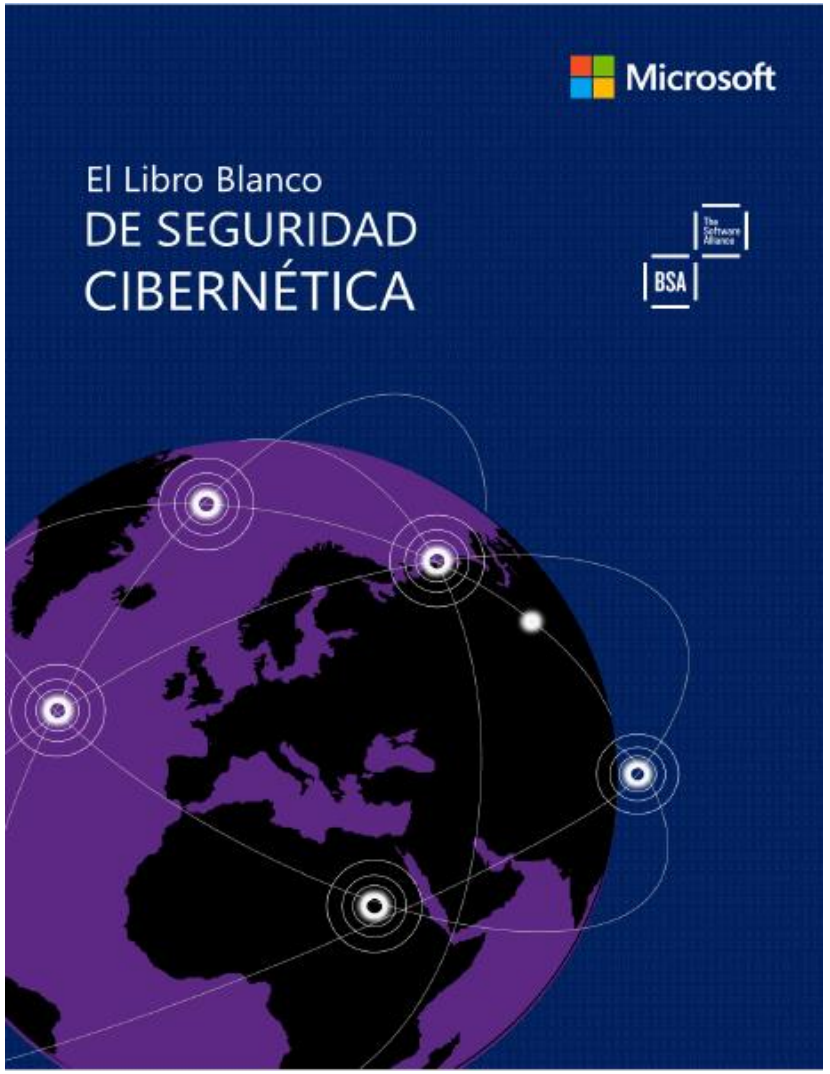


EDUCACIÓN Y CAPACITACIÓN

CONCIENCIA PÚBLICA

*El **elemento humano** es esencial para mejorar la ciberseguridad (educación seguridad digital)* →

RECURSOS ADICIONALES



Muchas gracias