ESCUELA SUPERIOR DE GUERRA
"General Rafael Reyes Prieto"
Colombia

Consideraciones Actuales del Ciberespacio y la Ciberseguridad Nacional.

Reflexiones desde la Academia

TC. Milena Elizabeth Realpe Díaz

AGENDA

1. Contextualización cibernética
2. Ciberdelitos y las Infraestructuras Críticas
3. La Ciberseguridad en Colombia
4. Reflexiones Finales

1

CONTEXTUALIZACIÓN

Reflexiones del Ciberespacio

UNIÓN, PROYECCIÓN, LIDERAZGO

Reflexión

La encuesta de percepción de riesgos globales ha respaldado el informe de riesgos globales del Foro Económico Mundial por aproximadamente dos décadas. Más de 1200 expertos.

"Una de las características de la Cuarta Revolución Industrial, es que no cambia lo que hacemos, sino lo que somos"

Klaus Schwab

Las dinámicas geopolíticas, las tecnologías emergentes y disruptivas, la falta de talento humano y de regulación representan algunos de los desafíos importantes que preocupan a los líderes actuales.

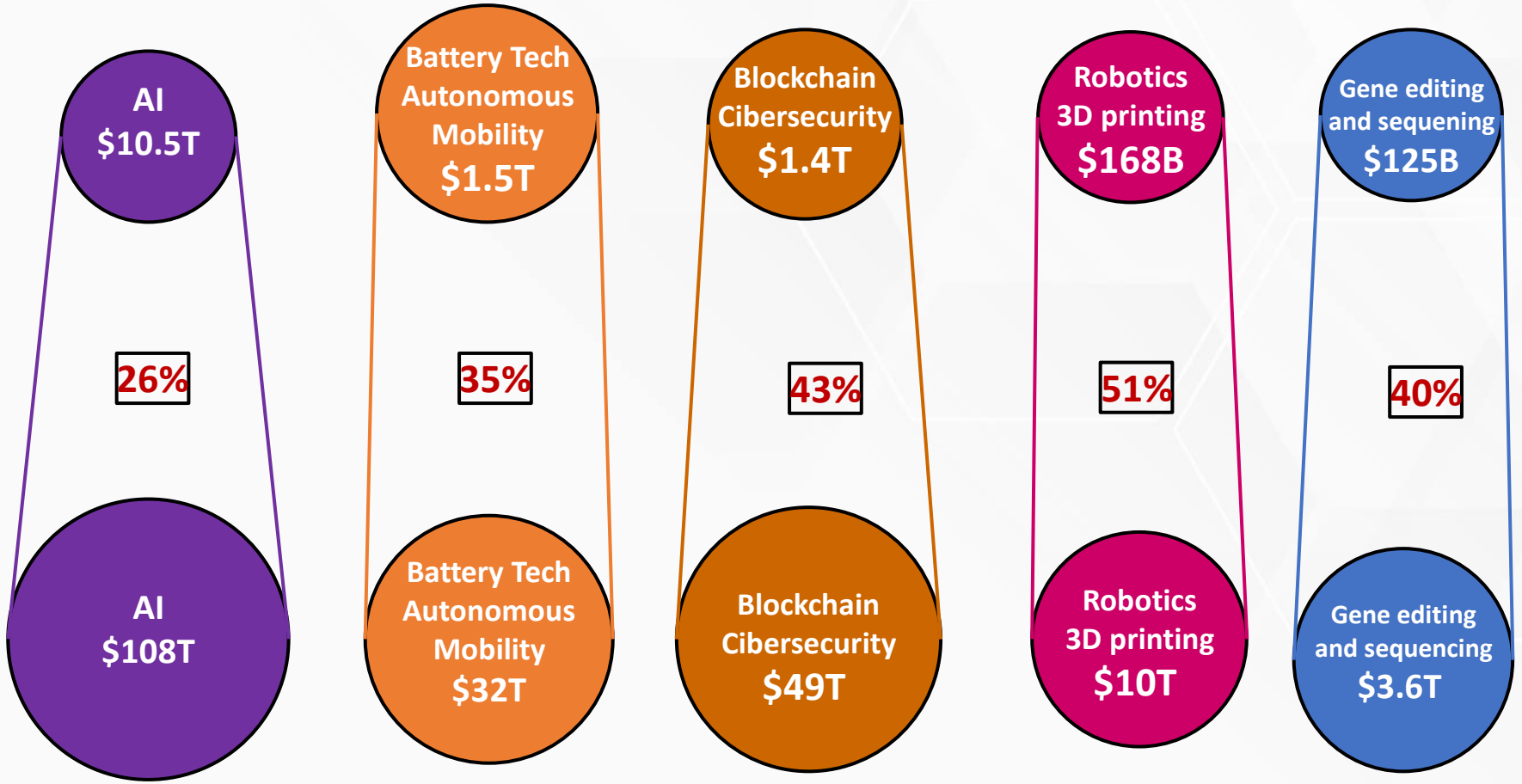
Fuente: WEF Informe Riesgos Globales 2023

NUEVAS TECNOLOGÍAS

2020
14 Trillion

CAGR
(La tasa de crecimiento anual compuesta)

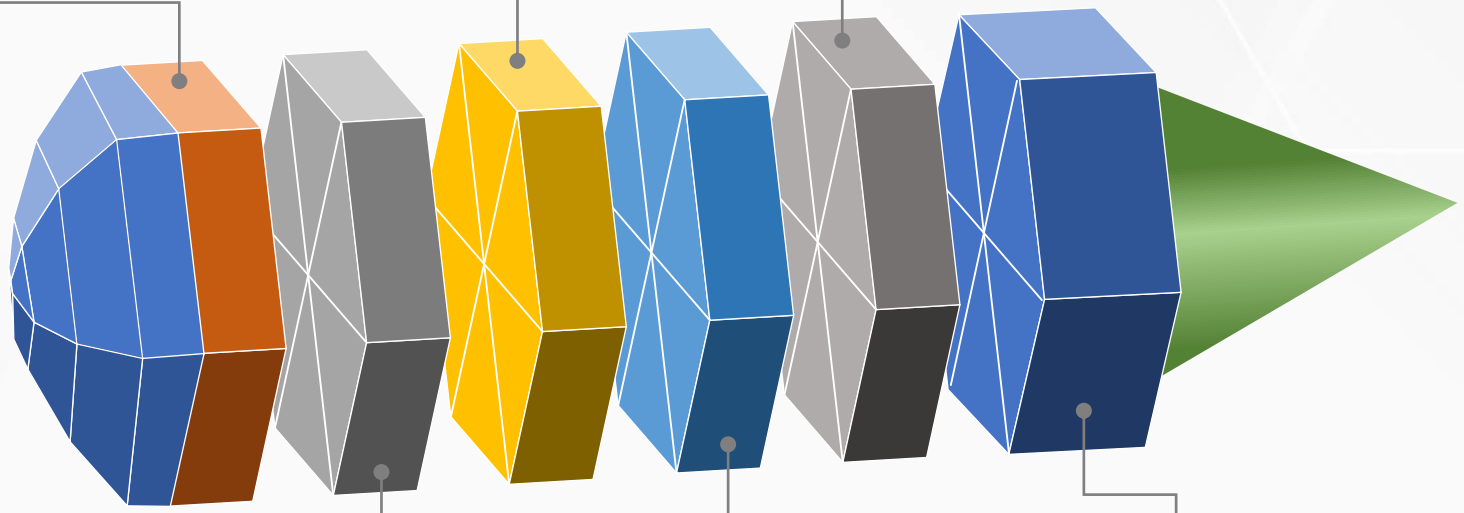
2030
210 Trillion



Representa una de las formas más precisas de calcular y determinar los rendimientos de activos individuales, carteras de inversión y cualquier cosa que pueda aumentar o disminuir su valor con el tiempo

RIESGOS GLOBALES-2023 (WEF)

Riesgo Global: Posibilidad de que ocurra un evento o condición que de ocurrir impactaría negativamente **el PIB global, la población o los recursos naturales.**



01 El costo de vida domina los riesgos globales en los próximos dos años. Crisis Global

02 La próxima década esta caracterizada por crisis ambientales y sociales impulsadas por tendencias geopolíticas y económicas.

03 La fragmentación geopolítica impulsará la guerra geoeconómica y aumentará el riesgo de conflictos multidominio

04 La tecnología exacerbará las desigualdades mientras que los riesgos de la ciberseguridad seguirán siendo una preocupación constante

05 Polarización Social: Aumento de información errónea y desinformación

06 A medida que la volatilidad en múltiples dominios crece simultáneamente el riego de una poli -crisis se acelera.

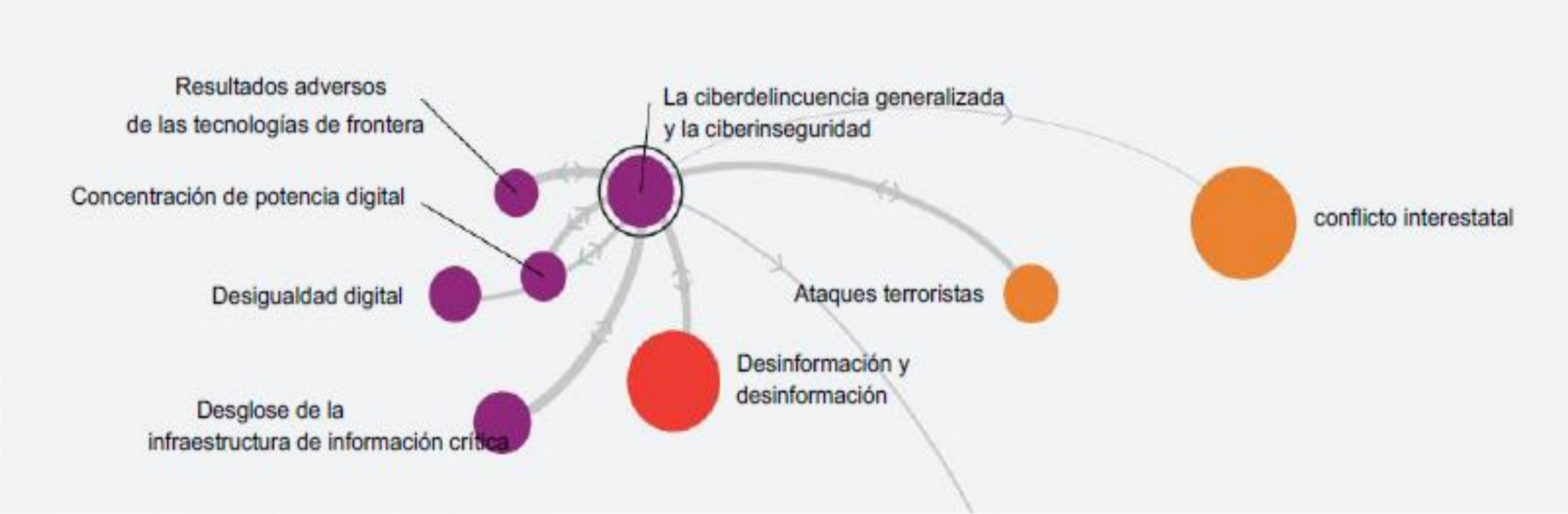
- **Aumento expectativas regulatorias.**
- **Ausencia de marcos normativos globales**

UNIÓN, PROYECCIÓN, LIDERAZGO

Fuente: WEF Informe Riesgos Globales 2023

CIBERDELINCUENCIA GENERALIZADA E INSEGURIDAD CIBERNÉTICA

- Ataques más agresivos y sofisticados que se aprovechan de una exposición más generalizada.
- Proliferación de dispositivos de recopilación de datos
- Tecnologías de IA, nuevas formas de control sobre la autonomía individual



Fuente: WEF Informe Riesgos Globales 2023. Pg. 44

Fuente: WEF Informe Riesgos Globales 2023

El Panorama en Colombia

Descubren campaña de ciber espionaje en Colombia

La acción llamada Operación Absoluta estaba enfocada a entidades gubernamentales. Fue alertada por el laboratorio de seguridad informática ESET Latinoamérica.

TECNOLOGÍA
Mar 06, 2023

Por:

Redacción Sociedad

TEMAS TRATADOS:

- Ciber espionaje
- Seguridad
- ciberseguridad
- malware
- Operación absoluta

TEMAS DEL DÍA | ACTIVIDAD NEVADO DEL RUIZ: EN VIVO | MILLONARIOS EN COPA SUDAMERICANA | CRÉDITOS ICETEX | PRESIDENTE PETRO Y JOE BIDEN | LEY CERO CACHOS | MINSALUD | CRIMEN DE N

EL TIEMPO

TECNOLOGÍA | NOVEDADES APPS DISPOSITIVOS TUTORIALES VIDEOJUEGOS

Compartir

Colombia, el segundo país de América Latina con más ciberataques en 2022

De acuerdo con la OEA, la mayoría de los países no tiene recursos ante delitos cibernéticos. FOTO: iStock

Según IBM , el comercio minorista y mayorista son los sectores más extorsionados en Latinoamérica.

RELACIONADOS: COLOMBIA | EMPRESAS | COMERCIO | IBM | CIBERSGURIDAD

TECNOLOGÍA

Ataques cibernéticos han crecido 30% y EPM y Sanitas son dos de miles

miércoles, 14 de diciembre de 2022

GUARDAR

LR MÁS

Colombia ocupó el tercer puesto en recibir ciberataques en Latinoamérica durante el primer semestre del año, con un total de 6.300 millones

TECNOLOGÍA · 7 Febrero 2023

Por qué están aumentando los ciberataques en Colombia y qué hacer

Los ataques cibernéticos cada vez se hacen más frecuentes. No solo a personas, sino a grandes compañías y a entidades estatales. El más reciente caso parece haber ocurrido en la Alcaldía de Medellín.

Los ataques cibernéticos se volvieron constantes durante los últimos meses. El robo de la información a grandes compañías y a entidades estatales ha sido noticia en Colombia. **Con este panorama, según un experto en el tema, el país no cuenta con un responsable en ciberseguridad.**

COMPARTIR

Recomendados

TECNOLOGÍA

Nequi suspenderá el servic de su app el 23 de abril

PRINCIPALES AMENAZAS DE CIBERSEGURIDAD A 2030 - ENISA

1 Supply chain compromise of software dependencies

More integrated components and services from third party suppliers and partners could lead to novel and unforeseen vulnerabilities with compromises on the supplier and customer side.

2 Advanced disinformation campaigns

Deepfake attacks can manipulate communities for (geo)political reasons and for monetary gain.

3 Rise of digital surveillance authoritarianism/ loss of privacy

Facial recognition, digital surveillance on internet platforms or digital identities data stores may become a target for criminal groups

4 Human error and exploited legacy systems within cyber-physical ecosystems

The fast adoption of IoT, the need to retrofit legacy systems and the ongoing skill shortage could lead to a lack of knowledge, training and understanding of the cyber-physical ecosystem, which can lead to security issues.

5 Targeted attacks enhanced by smart device data

Through data obtained from internet-connected smart devices, attackers can access information for tailored and more sophisticated attacks.

6 Lack of analysis and control of space-based infrastructure and objects

Due to the intersections between private and public infrastructure in space, the security of these new infrastructures and technologies need to be investigated as a lack of understanding, analysis and control of space-based infrastructure can make it vulnerable to attacks and outages.

7 Rise of advanced hybrid threats

Physical or offline attacks are evolving and becoming often combined with cyberattacks due to the increase of smart devices, cloud usage, online identities and social platforms.

8 Skill shortage

Lack of capacities and competencies could see cybercriminal groups target organisations with the largest skills gap and the least maturity.

9 Cross border ICT service providers as a single point of failure

ICT sector connecting critical services such as transport, electric grids and industry that provide services across borders are likely be to targeted by techniques such as backdoors, physical manipulation, and denials of service and weaponised during a future potential conflict.

10 Artificial Intelligence Abuse

Manipulation of AI algorithms and training data can be used to enhance nefarious activities such as the creation of disinformation and fake content, bias exploitation, collecting biometrics and other sensitive data, military robots and data poisoning.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Fuente: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

2

CIBERDELITOS E INFRAESTRUCTURAS CRÍTICAS

Informe Anual de Ciberseguridad-CCIT

UNIÓN, PROYECCIÓN, LIDERAZGO

Sectores Estratégicos en Colombia

- Electricidad
- Financiero
- Gobierno
- Defensa
- Tecnologías de la Información y Comunicaciones
- Medio Ambiente (Recursos Naturales)
- Minero-Energético (Hidrocarburos, minas y gas)
- Agua
- Trasportes
- Educación
- Comercio, Industria y Turismo
- Alimentación
- Salud y Protección Social

10 reconocidas instituciones de Colombia hackeadas en el 2022

CARACOL TELEVISIÓN

invima
Instituto Nacional de Vigilancia de Medicamentos y Alimentos.

vivaair.com

Claro

SaludTotal EPS-S

Pontificia Universidad JAVERIANA Colombia

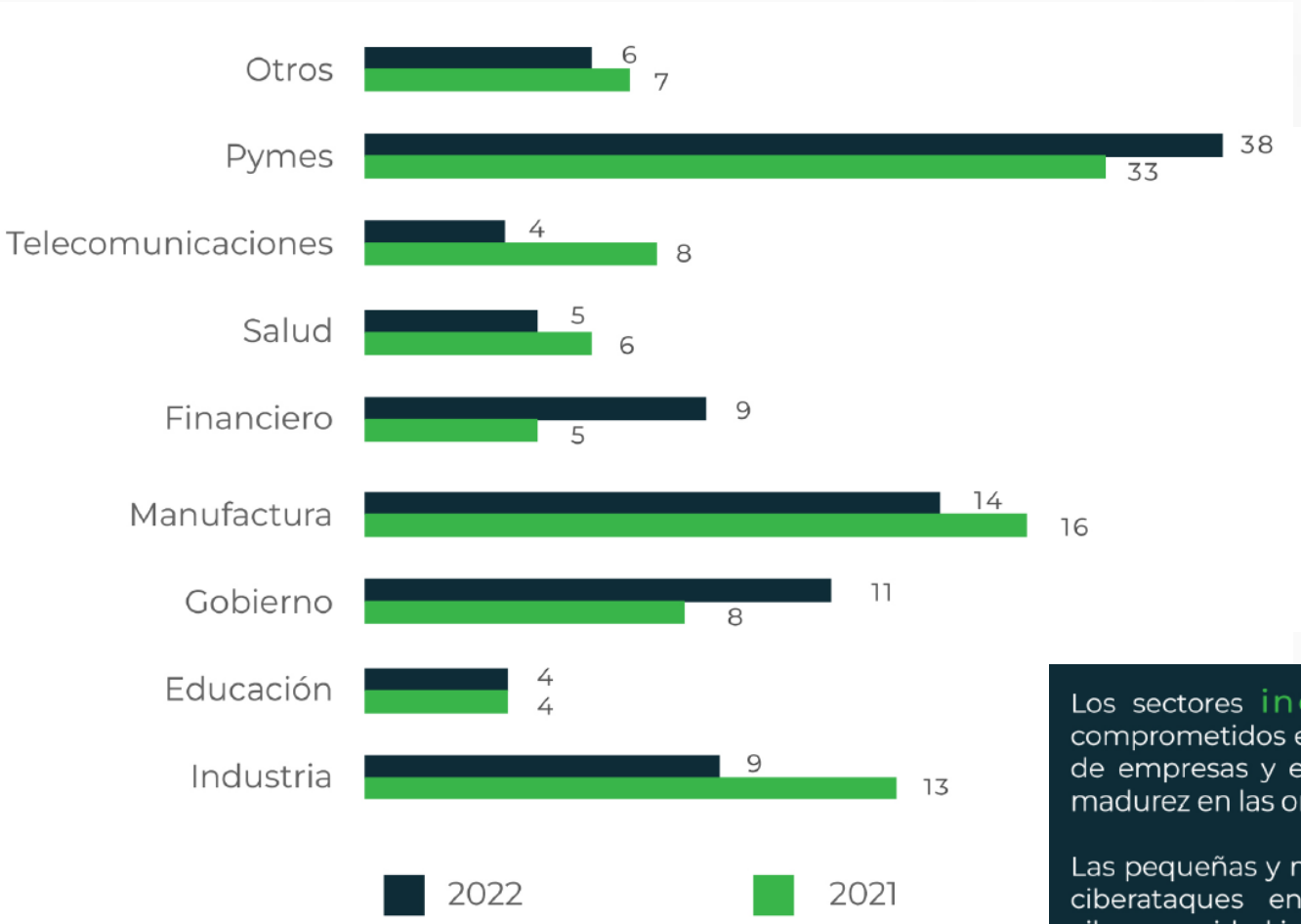
FISCALIA GENERAL DE LA NACION

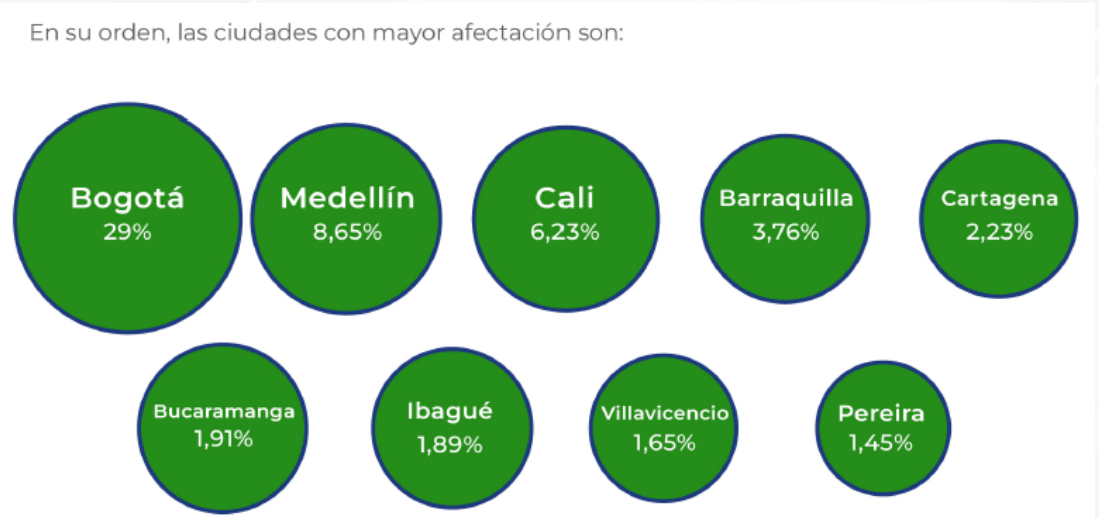
EPS Sanitas

FONDO NACIONAL DE PENSIONES DE LAS ENTIDADES TERRITORIALES -FONPET-

epm

Comportamiento de las Cifras del Ciberdelito





Los sectores **industriales, gobierno, educación y salud,** fueron los más comprometidos en ataques durante el 2022, un 67% del total de denuncias se registran por parte de empresas y entidades del sector público y privado. La anterior cifra señala un proceso de madurez en las organizaciones respecto al deber de denuncia.

Las pequeñas y medianas industrias (Sector PYME) siguen siendo el sector más afectado por los ciberataques en Colombia. Esto, obedece principalmente a las débiles estrategias de ciberseguridad implantadas por los responsables de estas organizaciones, bien sea, porque no se identifica dentro de la cadena productiva la necesidad de incorporar a los costos de la operación de los negocios la ciberseguridad como un factor estratégico, o por desconocimiento de las amenazas por parte de quienes realizan la gestión operativa de los negocios.

Fuente: Informe Anual de Ciberseguridad-CCIT

CERT-CSIRT-SOC

colCERT
Grupo de Respuesta a Emergencias Cibernéticas de Colombia

VenCERT
Sistema Nacional de Gestión de Incidentes Telemáticos

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

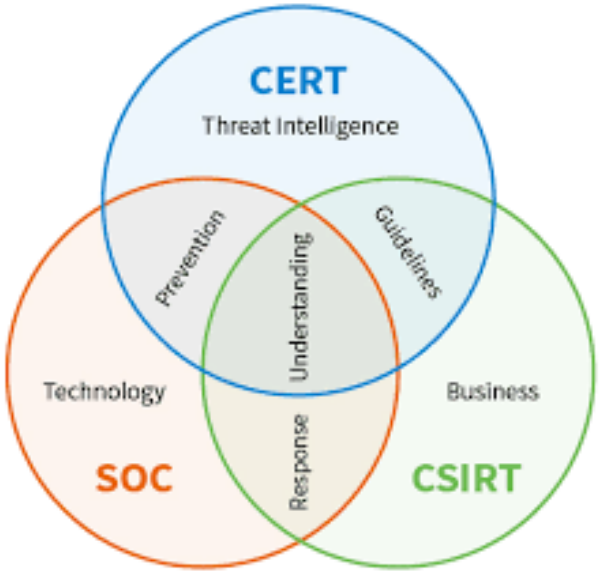


Figure 2: Understand the primary roles and characteristics of a CERT, CSIRT, and SOC.

CSIRT FINANCIERO

GUÍA PRÁCTICA PARA CSIRTs

Fuente: Organización de Estados Americanos, 2023.

https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20ESP%20Digital.pdf

CSIRT COMO MODELO DE NEGOCIO

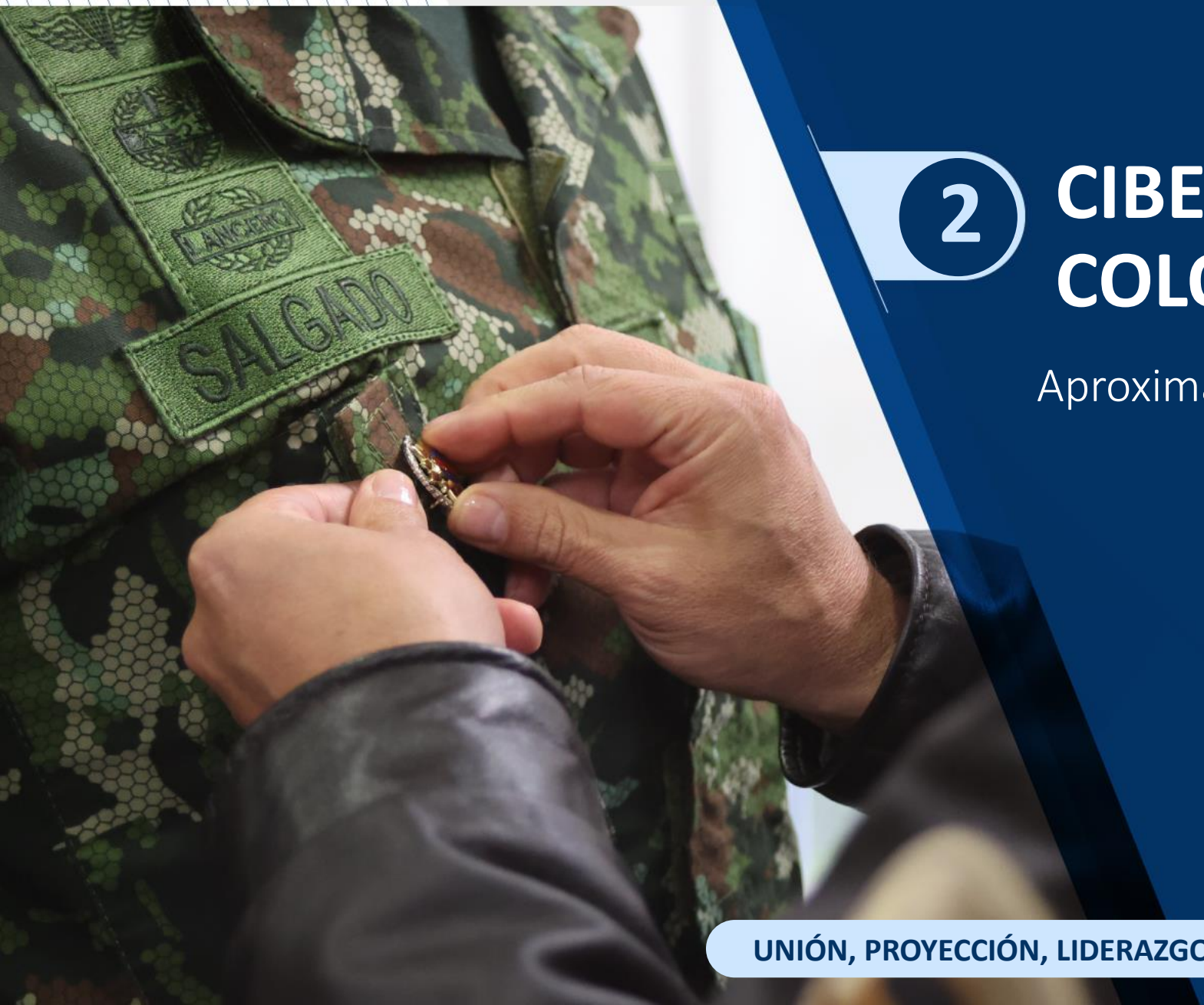
Planear y diseñar con una visión de largo plazo y crecimiento sostenido.

GUÍA PRÁCTICA PARA CSIRTs

- Gestión de incidentes de ciberseguridad.
- Gestión de vulnerabilidades.
- Concientización.
- Transferencia de conocimientos.
- Gestión de eventos de ciberseguridad.

Formarlo como un modelo de negocio ajustado a las oportunidades y limitaciones cambiantes, teniendo presente que no necesariamente va a generar rentabilidad monetaria, pero sí será un diferenciador al contribuir a tener sistemas más seguros, mayor confianza de la ciudadanía y minimización de impactos de gravedad ante incidentes cibernéticos.

Fuente: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20ESP%20Digital.pdf



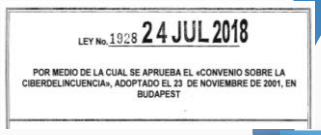
2

CIBERSEGURIDAD EN COLOMBIA

Aproximaciones desde la Academia

UNIÓN, PROYECCIÓN, LIDERAZGO

POLÍTICA EN MATERIA CIBERNÉTICA NACIONAL



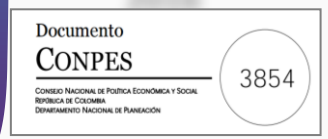
2018

Ley 1928 aprueba **Convenio sobre la Ciberdelincuencia**

2011

Institucionalidad
Educación
Legislación

2016

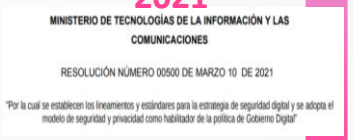


Gestión Riesgos
Economía Digital
Educación
Leyes

Directiva Presidencial. Política Pública de seguridad digital

2022

2021



Resolución 500
Lineamientos para la estrategia de seguridad digital.

2022-2026

Agencia Nacional Ciberseguridad

Gobernanza de la Seguridad Digital

2022

2020

Seguridad Digital
Confianza Ciudadana
Educación

UNIÓN, PROYECCIÓN, LIDERAZGO

(Realpe, 2023)

DECRETO 338 -2022

"TITULO 21

LINEANIIENTOS GENERALES PARA FORTALECER LA GOBERNANZA DE LA SEGURIDAD DIGITAL, LA IDENTIFICACIÓN DE INFRAESTRUCTURAS CRÍTICAS CIBERNÉTICAS Y SERVICIOS ESENCIALES, LA GESTIÓN DE RIESGOS Y LA RESPUESTA A INCIDENTES DE SEGURIDAD DIGITAL

ARTÍCULO 2.2.21.1.1.1. *Objeto.* El presente título tiene por objeto reglamentar parcialmente los artículos 64 de la Ley 1437 de 2011, 147 de la Ley 1955 de 2019 y 230 de la Ley 1450 de 2011, modificado por el artículo 148 de la Ley 1955 de 2019, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras criticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital.

ARTÍCULO 2.2.21.1.1.2. *Ámbito de aplicación.* Los sujetos obligados a las disposiciones contenidas en el presente título serán las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones públicas o administrativas. Para los efectos del presente se les dará el nombre de autoridades.

PARÁGRAFO 1. La implementación del presente decreto en las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113, 209 de la Constitución Política, y demás normas concordantes.

PARÁGRAFO 2. Las personas jurídicas de derecho privado que tengan a su cargo la prestación de servicios y que administren y gestionen infraestructuras críticas cibernéticas o presten servicios esenciales, podrán aplicar las disposiciones contenidas en este decreto, siempre que no resulten contrarias a su naturaleza y a las disposiciones que regulan su actividad o servicio. En cualquier caso, las personas jurídicas de derecho privado sujetarán sus actuaciones a las disposiciones especiales que regulen su actividad o servicio.

PARÁGRAFO 3. Las entidades de regulación, en el marco de sus competencias, evaluarán la necesidad de expedir normas para la protección de las infraestructuras criticas cibernéticas o de los servicios esenciales de su sector. Las entidades de supervisión, en el marco de sus competencias, evaluarán la necesidad de proferir instrucciones a sus vigiladas para el mismo fin.

Agencia Nacional de Ciberseguridad

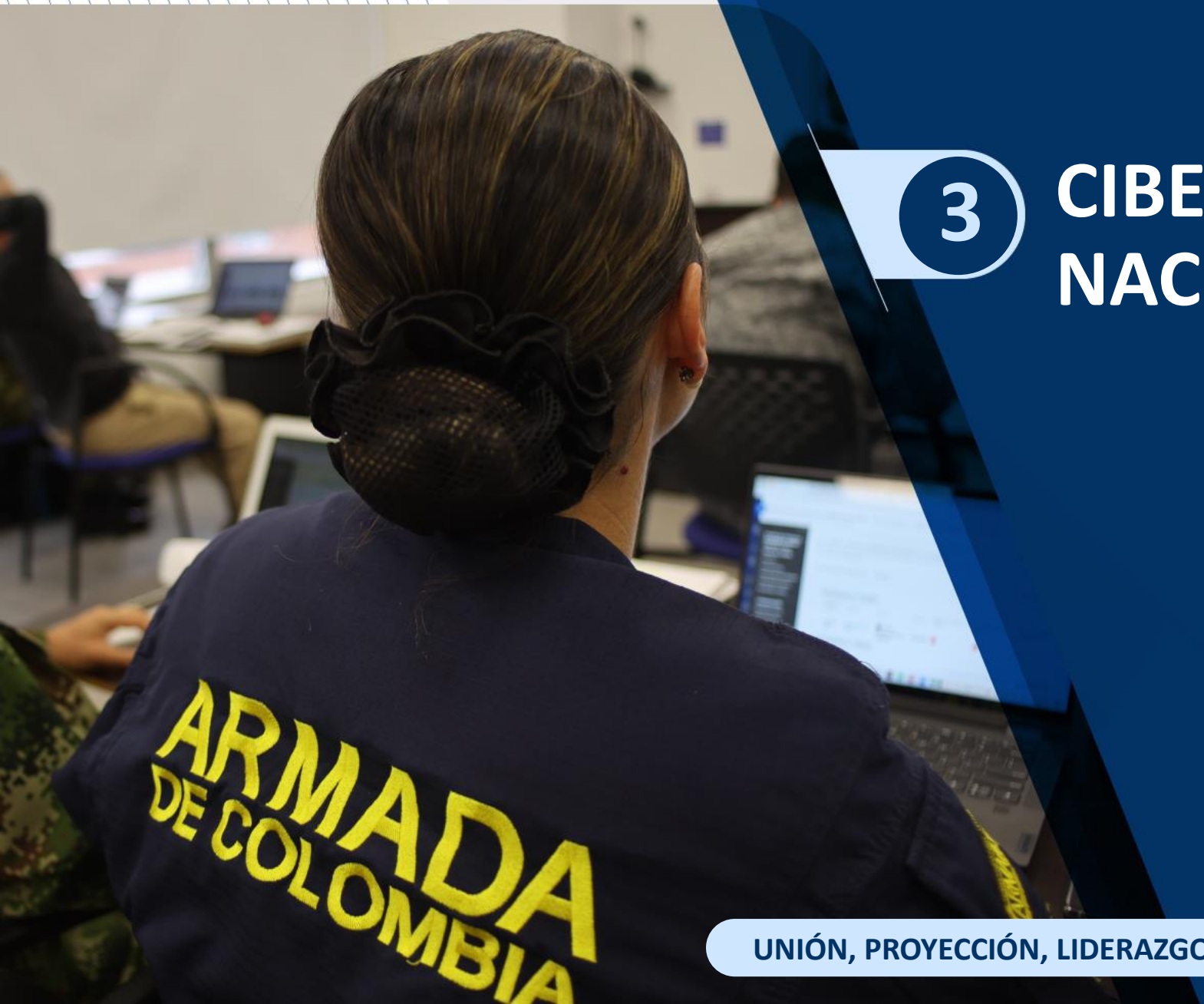
1. ***Seguridad Digital:*** *Atender y* ***dar respuesta*** *a los ataques cibernéticos*

2. ***Desarrollo Aeroespacial****: Programa satelital.*

3. ***Estimular la Educación****: a todo nivel para tener las capacidades*

Agencia tendrá la responsabilidad de Articular *esfuerzos para educación, empleo, seguridad en estas áreas.*

Mesa técnica a través de las comisiones segundas de la cámara y senado acompañarán la estructuración de la agencia de ciberseguridad y aeroespacial.



3

CIBERDEFENSA NACIONAL

UNIÓN, PROYECCIÓN, LIDERAZGO

Conflictos en el Ciberespacio

El conflicto cibernético adolece de una **falta de claridad conceptual y una falta de consenso entre los actores** internacionales clave sobre cómo interpretarlo.

Durante años, los académicos se han esforzado por dar cuenta de las potencialidades y los efectos de las tecnologías digitales **en la dinámica de los conflictos.**

El debate se ha centrado en **la inclusión del ciberconflicto en la conceptualización Clausewitziana de la guerra**

(Rid,2012; Piedra, 2013).

Cibeconfrontación

Las especificidades de la ciberconfrontación han buscado explicar las brechas entre expectativas y comportamientos, ya sea en términos de **atribución** (Rid & Buchanan,2015), **disuasión** (Fischerkeller & Harknett,2017; Libicki,2009; nye,2016/ 2017), **dinámica de escalada** (Lin,2012; Valeriano, Jensen y Maness,2018), **coerción** (Borghard & Lonergan,2017; Gartzke y Lindsay,2016; Afilado,2017), y **el carácter ofensivo-dominante del conflicto** en el ciberespacio (Gartzke & Lindsay,2015).

(Rid,2012; Piedra, 2013).

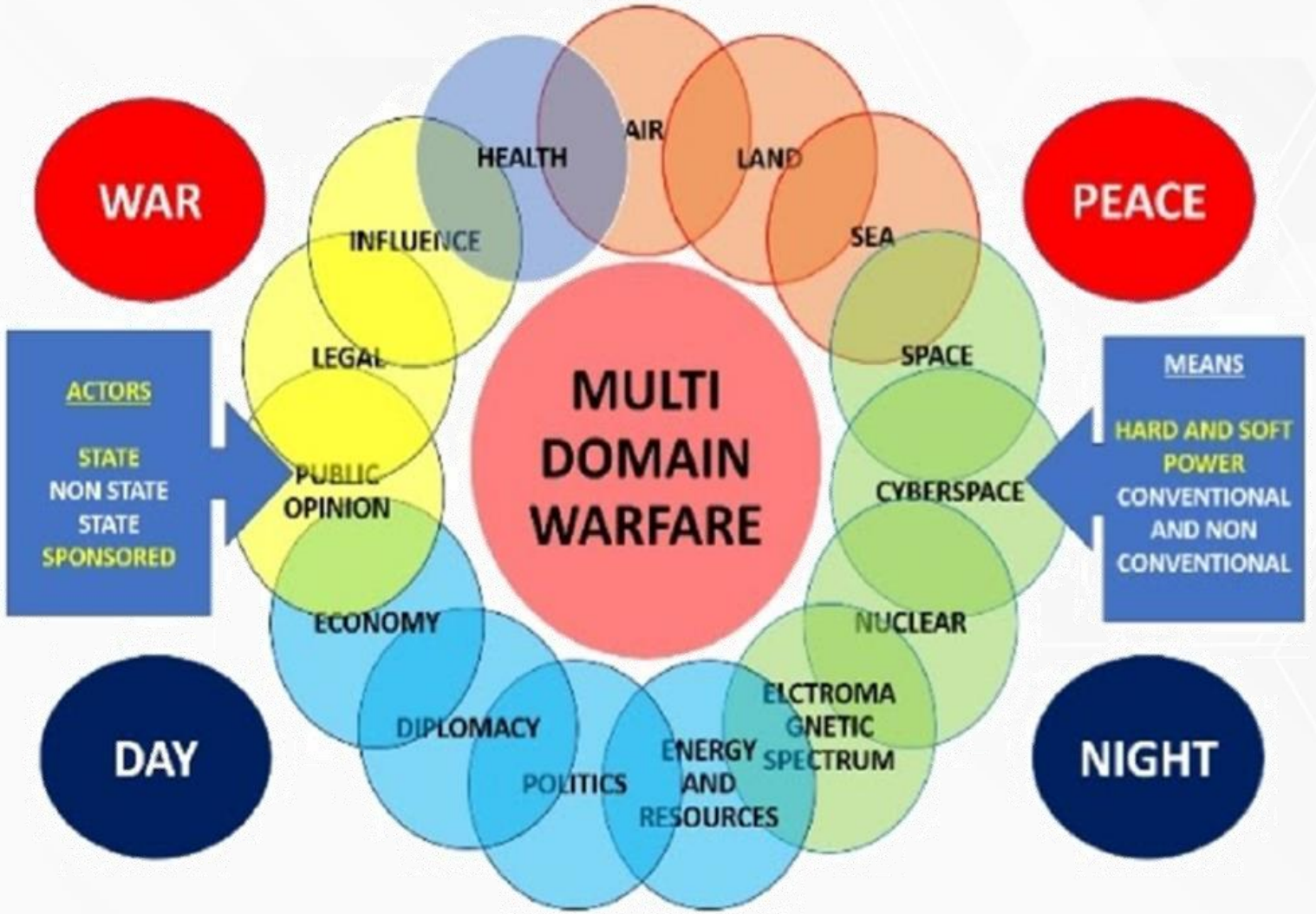
Ciberguerra, Guerra de Información, Guerra Hibrida o Zona Gris

El general Joseph L. Votel en 2019.

Nuestro éxito en este entorno será determinado por nuestra habilidad para ***navegar adecuadamente conflictos que caen fuera del tradicional constructo de guerra o paz" .***

La **"zona gris"** supone que **"nos enfrentamos con la ambigüedad de la naturaleza del conflicto, las partes implicadas y la validez de las reclamaciones legales y políticas en juego".**

https://emad.defensa.gob.es/Galerias/CCDC/files/OPERACIONES_MULTI-DOMINIO.PDF



4 REFLEXIÓN FINAL

UNIÓN, PROYECCIÓN, LIDERAZGO

PUNTOS DE INTERÉS COMÚN

Construir sobre lo Construido

Cultura Ciberseguridad
Alfabetización Digital

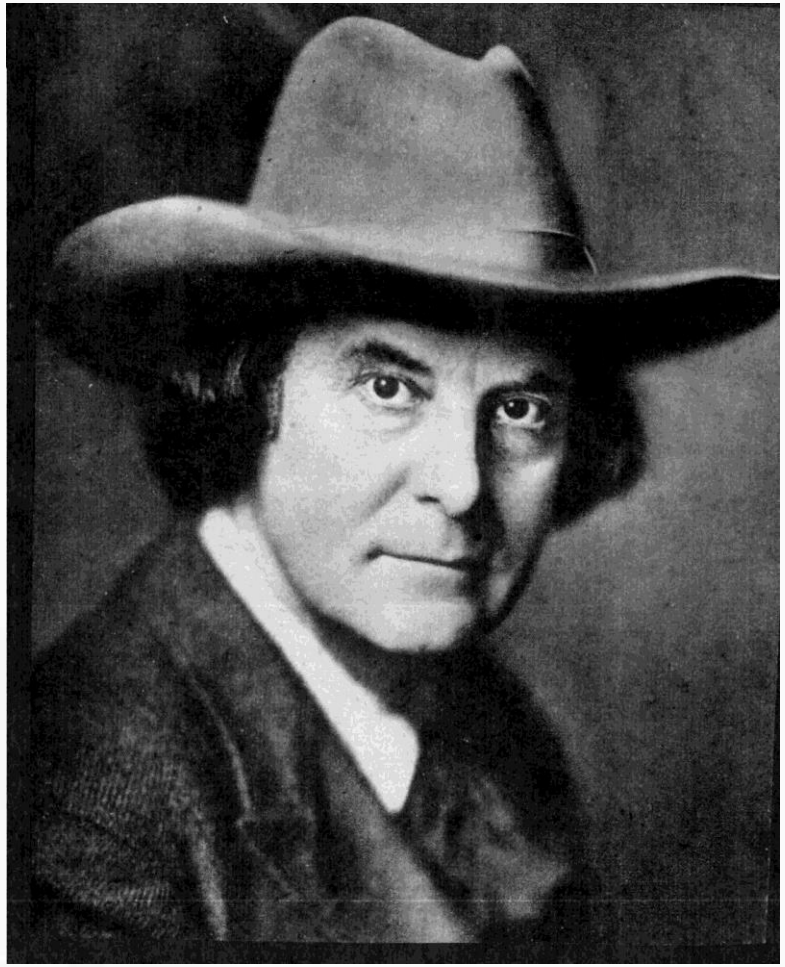
Estrategia Preventiva y NO Reactiva
Trabajo colaborativo Múltiples Partes Interesadas

Marco Normativo y Regulatorio

Ecosistema de Seguridad Digital
Gobernanza Ciberseguridad

Fortalecimiento Capacidades
Autonomía Tecnológica Nacional

Infraestructuras Criticas
De Gobierno y Privadas



Elbert Hubbard 1856-1915
Escritor, editor, artista y filósofo estadounidense

“Una máquina puede hacer el trabajo de cincuenta hombres ordinarios, pero ninguna máquina puede hacer el trabajo de un hombre extraordinario”.

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

Preguntas

UNIÓN, PROYECCIÓN, LIDERAZGO

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

BIENVENIDOS

INSCRIPCIONES ABIERTAS 2023-2

Doctorado
13 de febrero al 06 de junio

Maestrías
01 de marzo al 06 de julio

UNIÓN, PROYECCIÓN, LIDERAZGO

INFORMACIÓN GENERAL

Maestría en Seguridad y Defensa Nacionales

Registro Calificado Res. 007084 del 11 de mayo de 2020, por 7 años.
Cód. SNIES 16196

Matrícula : 8.462.000
Horario: Martes a Jueves 18:00 a 21:00

Más Información: ELIZABETH TRIANA RIOS
elizabeth.trianar@esdeg.edu.co

Maestría en Derechos Humanos y Derecho Internacional de los Conflictos Armados

Registro Calificado Res. MEN 20521 de octubre de 2017. Cód. SNIES 90906

Matrícula : 8.869.000
Horario: Viernes 14:00 a 18:00
Sábado 07:00 a 13:00

Más Información: DAYANNE MORENO CÁRDENAS
Cel: (+57) 310 219 2615
correo-maedh@esdeg.edu.co

Maestría en Estrategia y Geopolítica

Registro Calificado Res. MEN 022523 del 28 de noviembre de 2022.
Cód. SNIES 16196

Matrícula : 8.462.000
Horario: Viernes 14:00 a 18:30
Sábado 08:00 a 12:30

Más Información: MIGUEL ÁNGEL BURGOS GIRALDO
Cel: (+57) 323 248 7758
miguel.burgos@esdeg.edu.co

Maestría en Ciberseguridad y Ciberdefensa

Registro Calificado Res. 001140 del 03 febrero de 2022, por 7 años.
Cód. SNIES 104695

Matrícula : 8.613.000
Horario: Viernes 14:00 a 18:30
Sábado 07:00 a 12:30/ 14:00 a 18:30 (ocasionalmente)

Más Información: ANGIE GARCIA
Cel: (+57) 310 219 2729
maestriaciber@esdeg.edu.co

Gracias

UNIÓN, PROYECCIÓN, LIDERAZGO

Escuela Superior de Guerra

@EsdegCol

Escuela Superior de Guerra

Escuela Superior de Guerra

esdeguecol