LLEGÓ LA HORA DE MAS GENERALES EN EL CIBERESPACIO

"POR LA SUPERIORIDAD MULTIDOMINIO"

NOTA DEL DIRECTOR

Estimados lectores,

En un mundo donde la tecnología digital desempeña un papel cada vez más crucial en todos los aspectos de nuestra vida, la seguridad cibernética se convierte en una prioridad incuestionable. Para entender el panorama actual y el rumbo que debemos seguir en la protección de nuestras redes y sistemas, presentamos un artículo excepcional en esta edición de "CiberSíem del Mundo Cambio".

La Doctora Liliana Zambrano, una destacada experta en ciberseguridad y ciberdefensa nacional, nos brinda una visión clara sobre el tema en su artículo titulado "Llegó la Hora de Más Generales en el Ciberespacio". Con su profundo conocimiento y experiencia en la materia, la Dra. Zambrano nos guía a través de la necesidad imperante de contar con líderes militares capacitados en ciberseguridad y ciberdefensa.

En su valioso análisis, la Dra. Zambrano pone de manifiesto la importancia de esta especialidad en un mundo donde las amenazas cibernéticas evolucionan constantemente. Además, resalta ejemplos de otros países que ya han adoptado esta visión estratégica en la seguridad cibernética y cómo esto los ha posicionado a la vanguardia de la protección de sus intereses nacionales.

Este artículo es una llamada a la reflexión sobre el papel de los generales en el ciberespacio y cómo su liderazgo estratégico es esencial para abordar las amenazas digitales que enfrentamos. Ademas nos ofrece una visión profunda y convincente sobre por qué **"Llegó la Hora de Más Generales en el Ciberespacio"**.

Les invitamos a leer este artículo y a sumergirse en las ideas y perspectivas que presenta la Dra. Liliana Zambrano. La seguridad cibernética es un desafío que nos concierne a todos, y su análisis nos brinda una dirección esencial en un mundo en constante cambio.

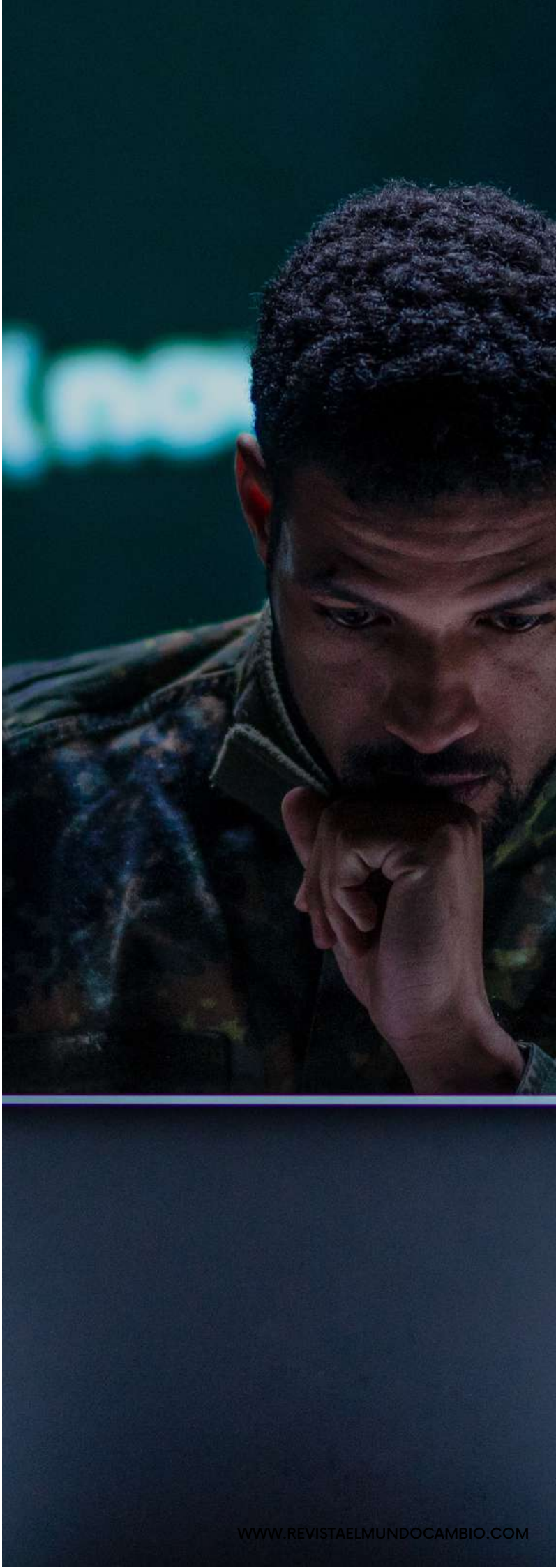
DIRECCIÓN GENERAL
Ing. Carlos A. Rojas
ASESORES CONSEJO EDITORIAL
MY (RP) Julio A. Walteros A.Ing.
Andrés Sanchez.

ASESORES DE CONTENIDO
Dra. Melissa Franco.CR. (RP) Héctor
G. González.
@Cibersiem

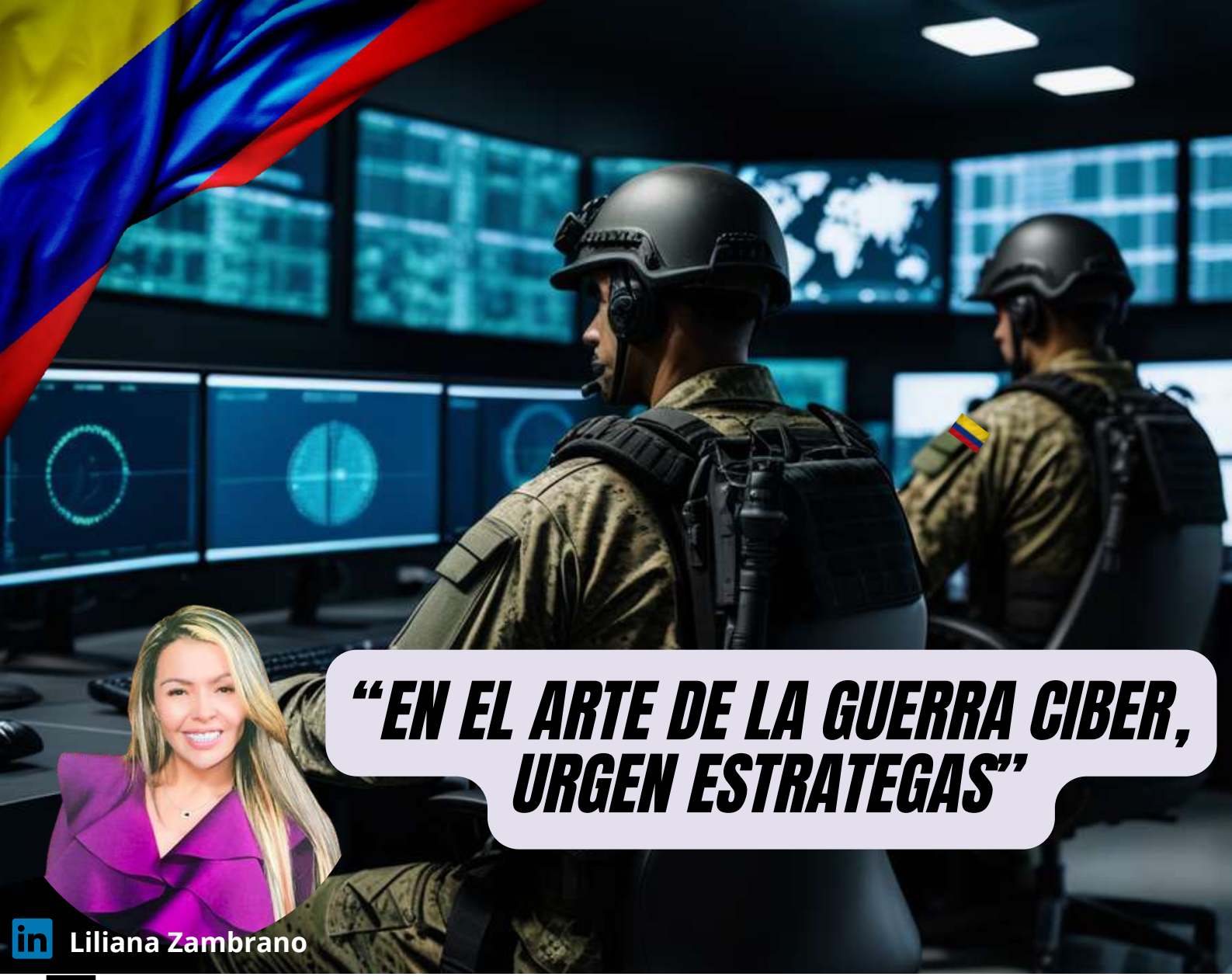
INVESTIGACIÓN DE CONTENIDO
José Albeiro Martínez.Paula Andrea
Flórez.
@Cibersiem

EJECUTIVA DE CONTENIDO
Elizabeth Jaramillo Roa.

EJECUTIVA COMERCIAL
Luisa Mendoza




CYBER SECURITY
REPORTE
CIBER SIEM
Texto del prof
REPORTES DIARIOS GRATIS DE CIBERSEGURIDAD
My Channel
CLICK



“EN EL ARTE DE LA GUERRA CIBER, URGEN ESTRATEGAS”

Liliana Zambrano

En un mundo cada vez más conectado y dependiente de la tecnología, la ciberseguridad se ha convertido en un componente esencial de la defensa nacional. Colombia no es ajena a esta realidad, y en el año 2023, se plantea una necesidad apremiante: la formación y el llamado de nuevos Generales de la República especializados en ciberseguridad, ciberdefensa y tecnología . Esta medida no solo es una necesidad estratégica para proteger nuestras infraestructuras críticas y datos sensibles, sino que también nos coloca a la vanguardia en un ámbito en el que muchos países ya han avanzado significativamente. A lo largo de este artículo, exploraremos la importancia de esta iniciativa, sus beneficios y ejemplos de países que han adoptado un enfoque similar.

La Ciberseguridad como Prioridad en el Siglo XXI

En el siglo XXI, la ciberseguridad se ha erigido como un componente vital en la defensa de cualquier nación. Los ciberataques representan una amenaza constante y en rápida evolución que puede afectar no solo a la infraestructura crítica, sino también a la seguridad nacional y la economía. Los generales especializados en ciberseguridad se convierten en actores clave para mitigar estas amenazas.

II. PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Las infraestructuras críticas, como la energía, las comunicaciones, el transporte y la salud, dependen en gran medida de sistemas informáticos. Un ciberataque exitoso a cualquiera de estas áreas podría tener consecuencias devastadoras.

II. CIBERDEFENSA EN EL ÁMBITO MILITAR

La ciberdefensa es un pilar esencial de la estrategia militar moderna. Los generales de la República con conocimientos avanzados en este campo pueden liderar con eficacia las operaciones en el ciberespacio, proteger las redes de comunicación y contrarrestar las amenazas digitales, garantizando la superioridad en la guerra cibernética y la Seguridad de la infraestructura TI y TO.

LA BATALLA EN EL CIBERESPACIO ES SILENCIOSA, PERO SU IMPACTO PUEDE SER ENSORDECEDOR.

“Colombia Necesita a Gritos mas Generales en este Dominio de Guerra”

DESAFÍOS EN LA GUERRA CIBERNÉTICA: UN MUNDO SIN REGLAS PARA EL ADVERSARIO

lo cierto es, que la guerra cibernética, las reglas de juego, tal como las conocemos en contextos convencionales, **simplemente no existen.** En este escenario, no hay atribución clara, no hay reglas que los adversarios se sientan obligados a respetar. La realidad es que los ciberdelincuentes operan en un terreno donde las normas de la sociedad occidental civilizada no aplican Lo que consideramos ético y legal es, con demasiada frecuencia, ignorado por estos adversarios.

"NO EXISTE LA POSIBILIDAD DE TRATADOS O ACUERDOS DE PAZ".

Esta falta de reglas y la desproporción en la capacidad de ataque y defensa hacen que la ciberseguridad sea un desafío monumental, algo a lo que Colombia y otros países latinoamericanos no son ajenos "Es un Mal general".

Los adversarios pueden llegar a los sectores más vulnerables, donde las políticas públicas y la educación en ciberseguridad a menudo están rezagadas. La falta de conciencia y capacitación en la sociedad, junto con la escasa inversión, crea una brecha significativa en las defensas cibernéticas. Además, los adversarios cibernéticos, con frecuencia, carecen de cualquier consideración ética en sus acciones, lo que agrava aún más el desafío.

CENTRO PARA LA CIBERSEGURIDAD & INVESTIGACIÓN DEL CIBERCRIMEN

[CENTER FOR CIC]

5.476 profesionales acreditados en 71 países conocen nuestras estrategias de ciberseguridad corporativa, gracias a entrenamientos que desarrollan capacidades divergentes en un mundo cada día más interconectado.

En el Center for CIC aplicamos tecnologías avanzadas e innovación en criminología digital que nos permiten anticipar las acciones de cibercriminales y amenazas emergentes en Internet.

¿CUÁL ES EL SIGUIENTE NIVEL EN TU CIBERESTRATEGIA?

WWW.CICCONFERENCE.ORG

Enfrentando la Realidad de un Crecimiento Acelerado de los Ataques Cibernéticos

ahora bien, la realidad en el mundo actual es innegable: los ataques cibernéticos han experimentado un crecimiento acelerado de manera constante a lo largo de los años. Colombia, como muchas otras naciones, no puede ignorar los desafíos que esto presenta.

El reciente ataque a IFX Networks, que puso de manifiesto la vulnerabilidad de infraestructuras críticas de la región, es un recordatorio de que la amenaza cibernética está al acecho, siempre lista para explotar debilidades. En este contexto, las fuerzas Militares, en todos sus niveles, se enfrentan a la imperiosa necesidad de contar con comandantes dispuestos y capacitados para ejercer un mando estratégico, técnico y operacional.

Solo de esta manera podrán estar preparados para contrarrestar las amenazas cibernéticas que, año tras año, evolucionan en complejidad y alcance y que no pararan. La inversión en líderes cibernéticos de alto rango es esencial para salvaguardar la seguridad nacional y mantener la integridad de las redes y sistemas críticos en un mundo digital en constante cambio.

LA HISTORIA DEL FUTURO SERÁ ESCRITA POR GENERALES QUE DOMINEN EL CIBERESPACIO

IV. Ejemplos de Países con Generales de la República en Ciberseguridad y Ciberdefensa.

Varios países han reconocido la importancia de contar con generales de la República especializados en ciberseguridad y han tomado medidas al respecto:

Estados Unidos: El país pionero en este campo estableció el Comando Cibernético de los Estados Unidos, que se encarga de proteger y defender las redes cibernéticas. Además, ha designado generales especializados en ciberseguridad para liderar esta iniciativa.

Israel: Conocido por su experiencia en ciberseguridad con la Dirección Cibernética Nacional de Israel (DCNI), ha desarrollado un enfoque similar. Sus generales y Comandantes cuentan con formación avanzada en ciberseguridad y desempeñan un papel crucial en la protección del país contra amenazas cibernéticas.

Reino Unido: Ha establecido una Academia Nacional y la National Cyber Force está destinado a llevar a cabo acciones contra actividades estatales hostiles, terroristas y criminales que amenacen la seguridad nacional del país.

China: Ha realizado avances significativos en el ámbito de la ciberseguridad y la ciberdefensa. El Ejército Popular de Liberación de China ha incorporado generales con experiencia en ciberseguridad para liderar sus operaciones en el ciberespacio y proteger los intereses nacionales en línea.

Estonia: Es conocida por su enfoque proactivo en ciberseguridad. Tras el ataque cibernético que sufrió en 2007, el país ha desarrollado una infraestructura de ciberdefensa sólida. Además, ha capacitado a Generales para liderar iniciativas en este campo.

Rusia: Los generales de la República rusa han sido entrenados para comprender y enfrentar las amenazas cibernéticas, lo que les permite proteger los intereses nacionales en el ciberespacio.

Francia: ha integrado la ciberseguridad en sus fuerzas armadas y cuenta con generales especializados en este ámbito. Han establecido el Comando de Ciberdefensa para supervisar y coordinar las operaciones cibernéticas en defensa de la nación.

Australia: ha invertido significativamente en ciberseguridad y ciberdefensa, y ha designado generales de alto rango para liderar estas iniciativas. La Estrategia de Ciberseguridad de Australia busca proteger sus intereses en línea y colaborar en la defensa cibernética global.

LA FORTALEZA DE UNA NACIÓN EN EL SIGLO XXI SE MIDE POR SU CAPACIDAD PARA PROTEGER SUS ACTIVOS EN EL CIBERESPACIO.

LEGALTECH

Servicio de Asesoría jurídica en Tecnología

- EMPRESAS Y STARTUPS
- DELITOS INFORMÁTICOS
- PROTECCIÓN DE DATOS
- COMPLIANCE PENAL
- MARCO LEGAL EN ESTRATEGIAS DE MARKETING
- COBRANZAS COPYRIGHT
- FAKE NEWS – CYBERBULLING – CIBERACOSO
- SISTEMAS DE GESTIÓN DE INFORMACION

WWW.LEGALTECHCOLOMBIA.COM

CLICK

Emisora Virtual

www.mundohelp.com

Música sin comerciales - Podcast sobre seguridad y riesgos

CASO DE ÉXITO: ESTADOS UNIDOS Y EL UNITED STATES CYBER COMMAND (USCYBERCOM)

Estados Unidos, como una de las potencias mundiales en ciberseguridad, es un claro ejemplo de liderazgo en la defensa cibernética.
El United States Cyber Command (USCYBERCOM), dirigido por el General Paul M. Nakasone, ha demostrado su capacidad para abordar amenazas cibernéticas complejas y sofisticadas. Un caso ejemplar de su eficacia fue la operación contra el grupo de ciberdelincuentes rusos conocido como "APT29" o "Cozy Bear", que se sospechaba de estar involucrado en ciberataques a nivel mundial.

Bajo el liderazgo del USCYBERCOM, se llevaron a cabo operaciones que desarticularon gran parte de la infraestructura de este grupo, lo que resultó en una reducción significativa de sus actividades maliciosas. Este caso ilustra la importancia de contar con un comando cibernético de alto nivel y líderes altamente capacitados que puedan coordinar respuestas efectivas en el ciberespacio, protegiendo los intereses nacionales y la seguridad de la nación. Estados Unidos sigue siendo un referente en la ciberdefensa, destacando la necesidad de preparación y liderazgo estratégico en un mundo cada vez más digitalizado.

Paul Miki Nakasone General de cuatro estrellas del ejército de los Estados Unidos que se desempeña como comandante del Comando Cibernético de los Estados Unidos .
Se desempeña simultáneamente como director de la Agencia de Seguridad Nacional y como jefe del Servicio Central de Seguridad .

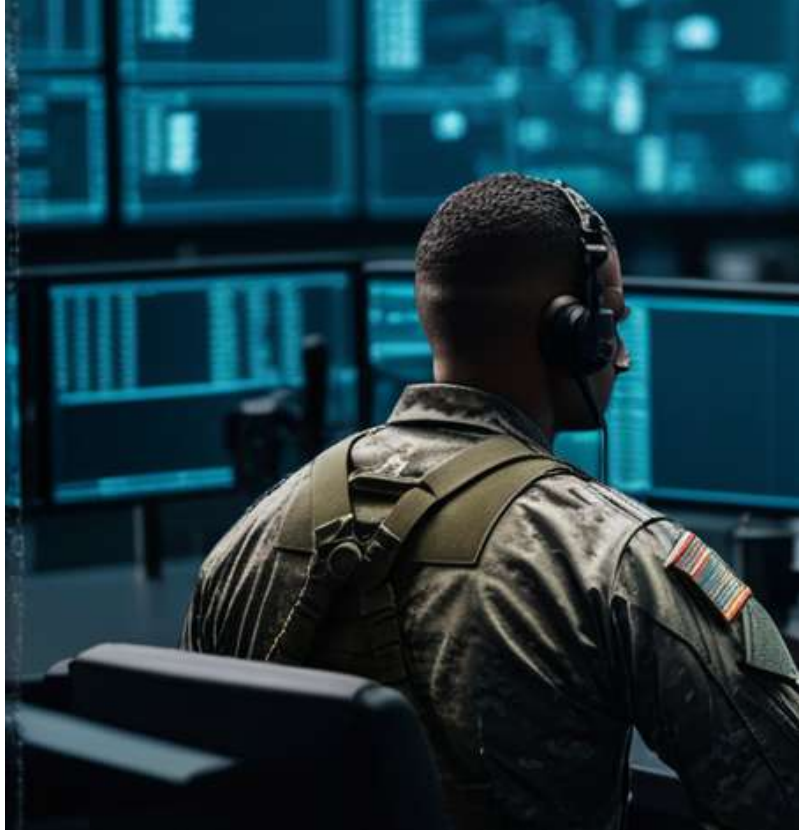
CASOS DE ÉXITO: EL EJEMPLO DE ESPAÑA

España es un claro ejemplo de cómo la capacitación de generales en ciberseguridad y ciberdefensa puede conducir a un éxito notable en la protección de intereses nacionales en el ciberespacio. En Mayo de 2020, España estableció el Mando Conjunto de Ciberdefensa (MCCE), un organismo encargado de supervisar y coordinar las operaciones cibernéticas. La creación de este mando marcó un hito significativo en el compromiso del país con la ciberseguridad.

El MCCCE no solo se ha centrado en la defensa de infraestructuras críticas, sino que también ha llevado a cabo operaciones de ciberseguridad en apoyo de las misiones militares españolas en el extranjero. Esto ha permitido la protección efectiva de las comunicaciones y la información sensible en contextos de alta tensión, fortaleciendo la seguridad y la capacidad de respuesta del país.

Además, España ha promovido la formación avanzada de sus generales en ciberseguridad, lo que ha resultado en un liderazgo experto en esta área. Este enfoque proactivo ha sido crucial para asegurar que España esté preparada para enfrentar las amenazas cibernéticas en constante evolución y para mantener una ventaja estratégica en el ciberespacio.

El éxito de España en el campo de la ciberseguridad y ciberdefensa demuestra que la inversión en la formación de generales especializados en esta área y la creación de estructuras organizativas dedicadas pueden llevar a una protección más sólida y una posición de liderazgo en la era digital.



Nombre: Rafael García Hernández.
Empleo: General de División.
Cargo: COMANDANTE DEL MCCE.
MANDO CONJUNTO DEL CIBERESPACIO (MCCE)

CASO DE ÉXITO: EL CIBEREJÉRCITO DE ISRAEL

Israel ha sido un ejemplo de liderazgo en el ámbito de la ciberseguridad y la ciberdefensa.

Su CiberEjército, dirigido por Generales expertos en seguridad cibernética, ha demostrado su efectividad en la protección de las redes y sistemas críticos del país. Un logro particularmente notable fue la operación "Operación Pilar Defensivo" en 2012, en respuesta a una oleada de ataques con cohetes desde Gaza y la Hoy reciente guerra. Utilizando sus capacidades cibernéticas, Israel fue y es capaz de desactivar infraestructuras clave de grupos terroristas y frenar los ataques, minimizando así la amenaza para la población civil.

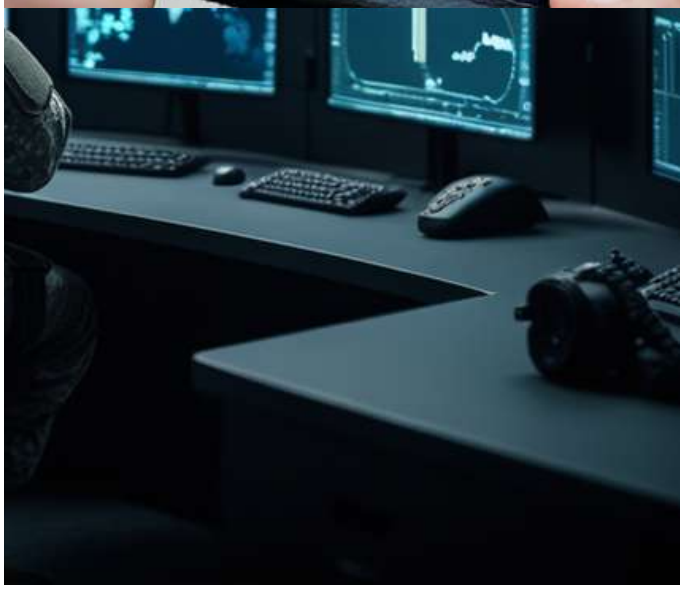
Israel sigue siendo un referente en la defensa cibernética, demostrando que un enfoque proactivo en el ciberespacio es esencial en la era digital actual.

Segun el General Ludwig Leinhos:
El área organizativa del espacio cibernético y de la información incluye actualmente alrededor de **13.500 puestos**. El personal asociado proviene principalmente de la base de las fuerzas armadas y fue puesto bajo nuestro control el 1 de julio de 2017.

Para 2021, nuestra área creció aproximadamente 15 000 puestos y alcanzará la plena preparación operativa y la gama completa de capacidades.

Los especialistas en TI que necesitamos para ello también son muy solicitados en el mercado civil. Para atraer a este personal altamente cualificado a la Bundeswehr, **nos posicionamos cada vez más como un empleador atractivo en el mercado laboral del sector de TI.** Al hacerlo, nos centramos principalmente en la relevancia del área organizativa del espacio cibernético y de la información para la sociedad en su conjunto. Al mismo tiempo, fomentamos un trabajo muy significativo y cualificado en la Bundeswehr y ofrecemos puestos de trabajo modernos y flexibles en un entorno laboral innovador y orientado al futuro.

CASO DE ÉXITO: ALEMANIA Y SU CENTRO DE CIBERDEFENSA



Alemania ha sobresalido en la esfera de la ciberseguridad con la creación del Centro de Ciberdefensa (KdoCIR). Este centro ha demostrado ser un pilar fundamental en la protección de sus sistemas y redes críticas.

Un ejemplo destacado fue su capacidad para abordar y mitigar un ataque cibernético a gran escala que afectó a instituciones gubernamentales y empresas en 2015. El KdoCIR actuó con rapidez y eficacia, coordinando la respuesta a nivel nacional y colaborando estrechamente con organizaciones del sector privado. Este caso subraya la importancia de contar con una estructura dedicada a la ciberdefensa y líderes altamente capacitados. Alemania, al poner énfasis en la ciberseguridad, ha demostrado ser un referente en la protección contra las amenazas digitales y un modelo a seguir para otros países en la lucha contra los ataques cibernéticos.

Basada en Bonn, esta unidad especial(Comando Ciberespacio e Información) inició en acción con un número inicial de **260 personas**, aunque tiene previsto aumentar sus efectivos hasta alcanzar 13.500, militares y civiles en los próximos meses, según explicó recientemente la ministra de Defensa alemana Ursula von der Leyen en 2017.

REVISTA

GEODESE

GEOPOLÍTICA, DEFENSA Y SEGURIDAD.

EN ESTA SEGUNDA EDICIÓN: SUPLEMENTO SOBRE DEFENSA

WWW.GEODESE.COM

WWW.GEODESE.COM

El Rol Crucial de los Generales en la Guerra Cibernética

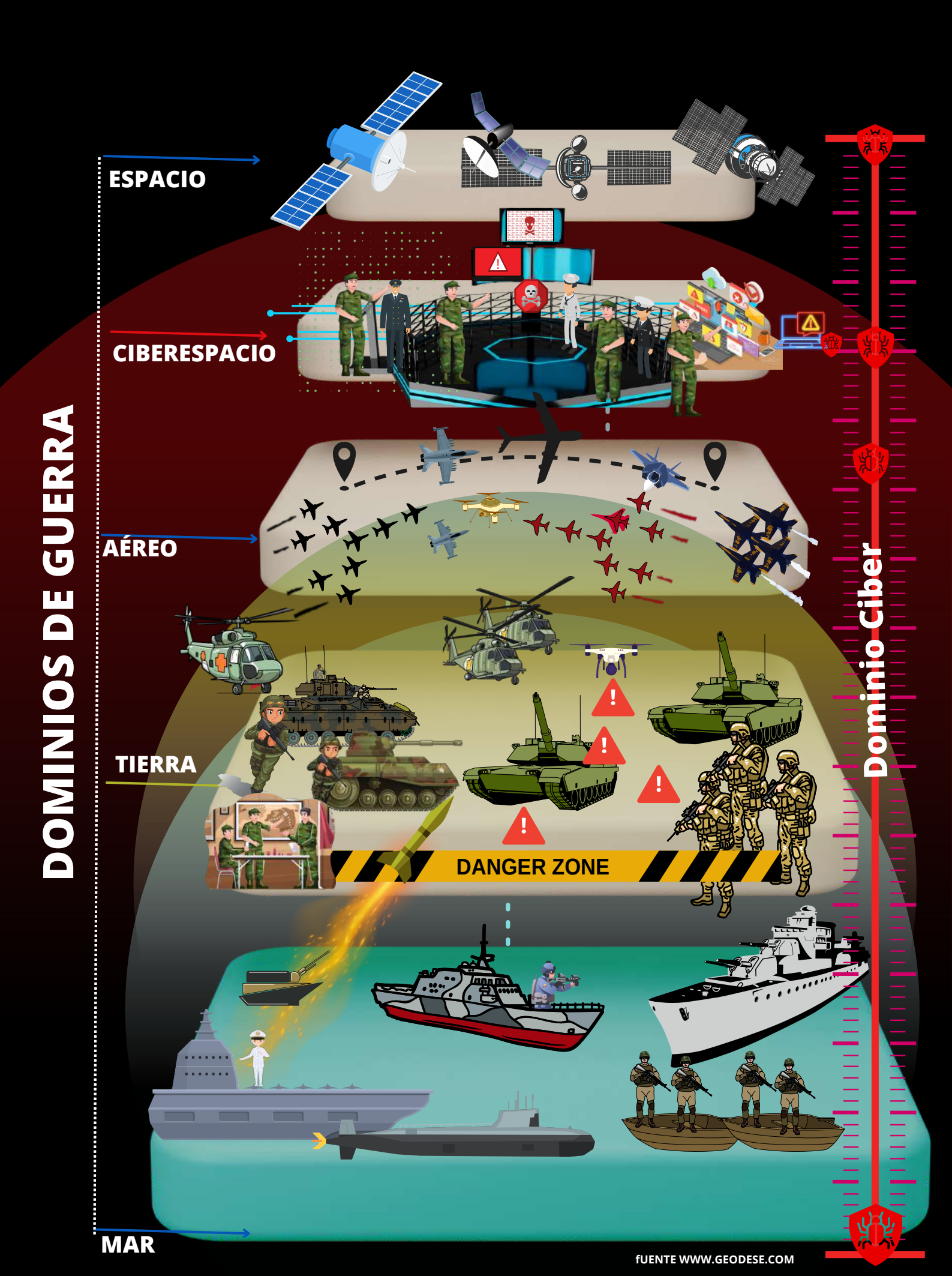
El entorno de la guerra cibernética es único y desafiante, donde las amenazas se propagan a la velocidad de la luz y las consecuencias pueden ser catastróficas. En este contexto, el papel de los generales de la República en la ciberseguridad y ciberdefensa se torna esencial. Su capacidad para ejercer un pensamiento estratégico, producto de años de preparación, conocimiento y experiencia técnica, táctica y operacional, es un activo crítico en la protección de los intereses nacionales en el ciberespacio.

Un general cibernético no solo es un líder militar con un profundo entendimiento de la ciberseguridad, sino también un estratega que puede anticipar y planificar enfoques efectivos para enfrentar las amenazas digitales. Su habilidad para decidir y aplicar las condiciones y acciones necesarias en respuesta a los ciberataques es comparable a la toma de decisiones en el campo de batalla convencional.

La formación y la experiencia acumulada a lo largo de sus carreras permiten a los coroneles de este dominio con miras a la posibilidad de ser generales, comprender las implicaciones estratégicas de los ciberataques y las tácticas necesarias para contrarrestarlos. Además, pueden coordinar de manera efectiva con otros sectores de la sociedad, incluyendo el gobierno, la industria y la academia, para garantizar una respuesta integral ante amenazas cibernéticas**. En un entorno donde la adaptabilidad y la rapidez son cruciales.**

No podemos olvidar que al igual que en otros dominios, el paisaje de la ciberdefensa y la ciberseguridad se ha vuelto increíblemente complejo y trascendental. En la era digital actual, las guerras ya no se limitan a los campos de batalla físicos; se extienden profundamente en las redes y sistemas digitales. Estas "guerras cibernéticas" implican amenazas sofisticadas y en constante evolución que pueden desmantelar infraestructuras críticas, comprometer datos sensibles y desestabilizar naciones. Por esta razón, es esencial contar con estrategas de ciberdefensa y ciberseguridad. Estos expertos no solo deben tener un sólido conocimiento técnico, sino que también necesitan habilidades estratégicas para anticipar, prevenir y responder a estos ataques. Su papel es crítico para navegar por este tablero de ajedrez digital en constante cambio e incertidumbre.

EL DOMINIO CIBER YA EXIGE QUE VENGAN PREPARADOS


DOMINIOS DE GUERRA
ESPACIO
CIBERESPACIO
AÉREO
TIERRA
MAR
Dominio Ciber
DANGER ZONE
fUENTE WWW.GEODESE.COM

COMANDANTES MULTIDOMINIO

La imagen previa destaca la capacidad del ciberespacio para trascender los demás dominios de guerra. En este punto, se hace evidente la necesidad de un Comandante Multidominio, el que debe poseer la habilidad de conectar y liderar de manera integral las características de los dominios, junto con las capacidades de los componentes de las Fuerzas Militares.

Esto se vuelve esencial para plantear de manera eficaz y acertada la toma de decisiones a nivel estratégico.

El ciberespacio no opera en aislamiento, sino que se entrelaza con tierra, mar, aire y espacio. **Un líder multidominio debe ser capaz de comprender y aprovechar esta interconexión e hiperconexion para garantizar la eficacia en la conducción de operaciones militares.**

La explotación del Ciberespacio se convierte en un elemento crucial para el éxito estratégico.

La realidad es que el desconocimiento del quinto dominio, el ciberespacio, ha sido un obstáculo para aprovechar plenamente todas las capacidades que ofrece. En un mundo cada vez más digital, la ciberinteligencia por ejemplo, se convierte en un recurso fundamental para anticipar amenazas y tomar decisiones estratégicas informadas. La convergencia de capacidades entre dominios, como tierra, mar, aire, espacio y ciberespacio, es esencial para lograr la superioridad y anticipación. Sin embargo, este potencial no se ha explotado completamente debido a la falta de comprensión y conciencia.

Recomendado CIBERSIEM MEXICO

FORO INTERNACIONAL DE CIBERSEGURIDAD E INTELIGENCIA

RETOS DE LAS ORGANIZACIONES MODERNAS

VIERNES 27 DE OCTUBRE

HORARIO:
Registro 8:00 am
Fin del evento 16:00 pm

UBICACIÓN
FACDYC Loma Larga - Edificio FACDYC
UANL, Loma Redonda 1515, Loma
Larga, 64710 Monterrey, N.L.

UANL FACDYC AMESP

Comandante en la Guerra Cibernética

América del Norte:

País	Unidad Militar y Comando Militar	Comandante de Ciberoperaciones
Estados Unidos	United States Cyber Command (USCYBERCOM)	General Paul M. Nakasone
Canadá	Agencia de Seguridad de las Comunicaciones (CSE)	No Disponible

América Latina y Centroamérica:

País	Unidad Militar y Comando Militar	Comandante de Ciberoperaciones
Brasil	Comando de Defensa Cibernética (CDCiber)	General Guido Amin Naves
México	Unidad de Ciberseguridad Nacional (UCSN)	General José Arturo Trejo
Colombia	Comando Conjunto Cibernético	General Juan Diego Sepulveda
Argentina	Unidad de Ciberdefensa (Ejército)	General Gustavo Adolfo Luis
Chile	Batallon de Ciberdefensa depende del Regimiento Inteligencias N°2 Llaitún de la Briga de inteligencias del Ejército (Binte)	General Ricado Martinez
Ecuador	Comando Conjunto de Ciberdefensa	
Perú	Comando de Ciberdefensa del Ejército	Coronel Ernesto Castillo Fuerman
Bolivia	Departamento de Ciberdefensa	
Venezuela	Dirección conjunta de seguridad informática (DICOCEI)	
República Dominicana	Comando Conjunto de las Fuerzas Armadas de la República Dominicana C51	Vicealmirante Luis Rafael Lee Ballester, ARD
Nicaragua	No disponible	
Panamá	No disponible	
Guatemala	Comando de Informática y Tecnología del Ejército	
Honduras	No disponible	
Costa Rica	Agencia de Seguridad de la Información y Ministerio de Seguridad Pública de Costa Rica	

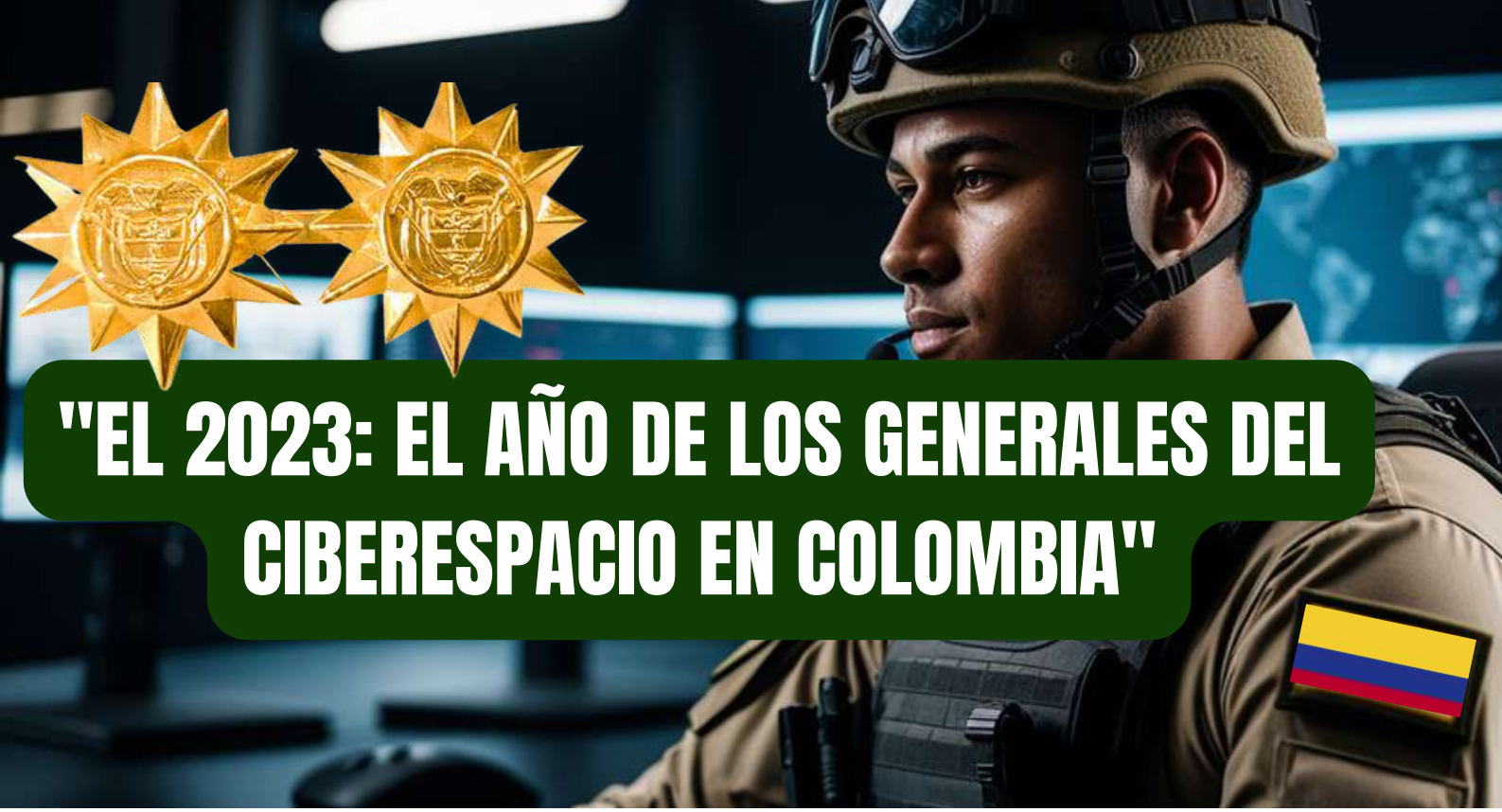
Europa:

País	Unidad Militar y Comando Militar	Comandante de Ciberoperaciones
Alemania	Centro de Ciberdefensa (KdoCIR)	General Ludwig Leinhos
Francia	Comando de Ciberdefensa (COMCYBER)	General Didier Tisseyre
Estonia	Unidad de Ciberdefensa (Kaitseväe Küberkaitsekeskus)	Coronel Jaak Tarien
Noruega	Unidad de Ciberdefensa (Forsvarets Cyber Defence)	Coronel Per-Ole Værnes
Portugal	Centro de Ciberdefensa (CCD)	General Rui Oliveira
Italia	Comando Interfuerzas de Ciberdefensa (CIDC)	General Guglielmo Luigi Miglietta
Suiza	Unidad de Ciberdefensa (Unité de Cyberdéfense)	General Walter Knutti
Bélgica	Unidad de Seguridad Cibernética (Cyber Security Unit)	General-mayor Philippe Boucké
Hungría	Unidad de Ciberdefensa del Ejército Húngaro	General László Tari
Japón	Unidad de Seguridad Cibernética (Cyber Security Unit)	Teniente General Hidehiro Ikematsu
Singapur	División de Ciberdefensa en la Fuerza de Defensa de Singapur	No Disponible
España	MANDO CONJUNTO DEL CIBERESPACIO (MCCE)	General Rafael García Hernández.

África, Asia y Oriente Medio:		
País	Unidad Militar y Comando Militar	Comandante de Ciberoperaciones
China	Unidad de Ciberespionaje del EPL	General Tan Rui
Rusia	Fuerzas Cibernéticas de Rusia	General Sergey Mayev
Israel	Unidad 8200 (IDF)	General Tamir Hayman
India	Fuerza de Tareas de Respuesta Cibernética	No Disponible
Corea del Sur	Agencia de Seguridad de Internet y de Seguridad de Corea (KISA)	No Disponible
Irán	Organización de Seguridad Cibernética (FATA)	Brigadier General Gholamreza Jalali
Taiwán	Agencia Nacional de Seguridad Cibernética (NCSA)	No Disponible
Nepal, Afganistán, Líbano, Catar, Emiratos Árabes y Siria	No Disponible	

Nota Importante: Acerca de la Información de Unidades Militares y Comandantes de Ciberseguridad

La información proporcionada anteriormente sobre las unidades militares y comandantes de ciberseguridad en varios países se basa en fuentes abiertas y accesibles al público. Es importante destacar que, en el ámbito militar, la información puede estar sujeta a cambios, incluyendo la rotación de comandantes y la actualización de estructuras organizativas.



"EL 2023: EL AÑO DE LOS GENERALES DEL CIBERESPACIO EN COLOMBIA"

El 2023 se presenta como un año crucial para la ciberseguridad y la defensa de Colombia. En un contexto donde las amenazas cibernéticas evolucionan constantemente, la elección de nuevos generales para liderar la guerra cibernética y la administración de las redes de tecnología de la información se convierte en una prioridad incuestionable. No es simplemente una cuestión de elegir uno, sino de reconocer que el desafío es multidimensional y requiere una respuesta en consecuencia. Para cumplir con la política de seguridad y defensa del Estado, es esencial contar con al menos dos vacantes para Colombia. Esta acción no solo fortalecerá nuestras capacidades en la protección de las redes y sistemas críticos, sino que también nos permitirá estar a la altura de las demandas del ciberespacio en constante cambio. En este momento crítico, elegir nuevos candidatos a generales es un paso esencial para garantizar la seguridad y defensa de nuestro país en la era digital actual.

Estamos en camino hacia la paz en Colombia, con acuerdos históricos como el cese de hostilidades con grupos como el ELN, que representan un anhelo fundamental para el presidente y el país. Sin embargo, mientras buscamos la armonía en nuestro país, debemos reconocer que el ciberespacio es otro campo de batalla crucial que no puede pasarse por alto.

En este terreno, no hay treguas ni asientos en la mesa de negociaciones. Los ciberatacantes no están dispuestos a detenerse ni a ser llamados a la mesa de diálogo.

Es aquí donde el Mando Político, Militar y Policial de Colombia deben liderar con visión estratégica y asegurarse que el ciberespacio sea un dominio que nuestras fuerzas militares dominen por completo. La ciberseguridad se convierte en un componente esencial para garantizar la estabilidad y la seguridad de nuestro país en una era donde la tecnología digital es una parte integral de nuestras vidas.

¿Pero, Qué Perfil Necesitamos?

En el juego actual del ciberespacio, es evidente que se necesitan líderes con un perfil específico y sólido.

Y hoy en el juego existen varios coroneles o contados mas bien, con una experiencia inquebrantable en este campo, es hora de reconocer que Colombia requiere un escalón más alto en la jerarquía acompañando al actual Comandante del Comando Conjunto Cibernético garantizando el relevo generacional y ampliando de manera holistica la toma decisiones en este dominio.

El ciberespacio es un terreno complejo que abarca tanto operaciones cibernéticas como la gestión de la infraestructura de tecnología de la información. En mi opinión personal, el momento ha llegado para que Colombia cuente con no uno sino dos o mas de ser posible, nuevos generales capaces de liderar operaciones cibernéticas desde el campo de batalla, asegurando nuestra superioridad en el ciberespacio. y otro experto en el área de tecnología de la información, lo que permitirá a las Fuerzas Militares mantener la integridad y la ventaja en su infraestructura tecnológica y operaciones.

Así que, en este nuevo panorama, le llegó la hora a los comandantes formados y preparados operacionalmente para Ciberseguridad, Ciberdefensa y Seguridad de las redes, que sé están hoy a la espera de la próxima Honorable Junta Asesora 2023. Esta áreas exigen un liderazgo especializado y capacitado para enfrentar los desafíos del mundo digital actual.

UN LLAMADO A LA EVALUACIÓN Y LA INNOVACIÓN

Este es un llamado urgente a los actuales generales y almirantes de nuestras Fuerzas Militares de todos los Dominios. Es hora de que evaluemos y promovamos un pensamiento estratégico innovador, especialmente en el marco del nuevo panorama de confrontación global.

Los desafíos en el ciberespacio demandan líderes con visión y la capacidad de adaptarse a un entorno en constante cambio. La ciberseguridad y la ciberdefensa son componentes cruciales para garantizar la seguridad de Colombia en el quinto dominio de la guerra, el ciberespacio.

Por tanto, es imperativo que consideren la necesidad de liderar en este campo y contribuir al desarrollo del plan de carrera cibernético, que preserve al personal que se ha formado en este ámbito, desarrollado capacidades, siendo útil para el cumplimiento de la Misión .

Colombia clama por una estrategia cibernética integral que garantice nuestra superioridad en un terreno donde la destreza y la preparación son fundamentales.

Los Futuros relatos de los conflictos contaran de batallas en el ciberespacio.

Consciente de que se avecina la próxima Junta Asesora de Generales, donde se tomarán decisiones cruciales para el liderazgo las Operaciones Militares, es la razón por la cual exploro a detalle y muestro con argumentos por que se *"llegó la Hora de mas Generales en el Ciberespacio" en pocas palabras* ***MAS CIBERGENERALES.*** Sin embargo, este artículo no se limita únicamente a nuestro país. La realidad es que la ciberseguridad y la ciberdefensa son desafíos que trascienden fronteras, y la cooperación en el ciberespacio ante amenazas persistentes es una necesidad compartida en todas las Naciones. Cada ejército de la región se enfrenta a desafíos similares en la era digital. Este llamado a fortalecerse en el dominio cibernético no solo es para Colombia, sino para todos los ejércitos que buscan proteger sus intereses nacionales en el ciberespacio.

Recuerden que la independencia tecnológica de las fuerzas militares es inminente. A la fecha, no existe un ámbito dentro de la defensa que no esté influenciado por la tecnología. Armamento, aviones, buques, sistemas de comunicación, drones, sistemas de artillería, helicópteros, radares etc; todos han evolucionado en el mundo digital. Es evidente que en no más de ocho años, en el 2030, no habrá ejército que no cuente con un ecosistema digital robusto en su operación. Por tanto, se debe iniciar sin demora la creación de su escenario operacional multidominio para mantenerse a la vanguardia en esta nueva era de la defensa

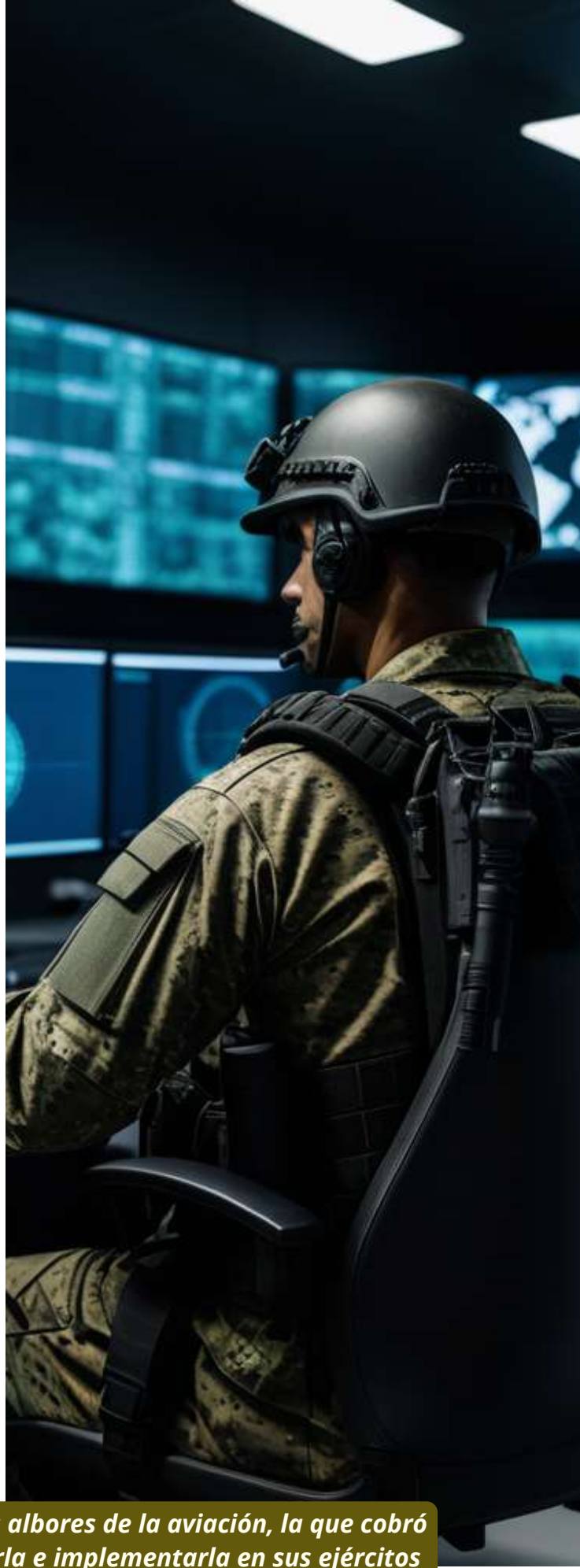
La historia nos ha enseñado que resistirse al cambio tecnológico solo conduce a la desventaja y a pagar un alto precio en términos de seguridad.

Para Colombia y para los países de la Región, la independencia tecnológica en defensa no es una opción, sino una necesidad apremiante. Nuestra visión debe ser clara: estar a la vanguardia en la era digital. Comenzar a crear nuestro escenario operacional multidominio es el primer paso para lograrlo.

La independencia tecnológica no es un lujo, es un imperativo, y Colombia está llamada a liderar en este nuevo paradigma de la defensa.

Nuestro enfoque debe estar en el futuro y en la adaptación constante a un entorno en constante cambio. Esto implica no solo la adquisición de tecnología de vanguardia, sino también la capacitación y el desarrollo propio de talento humano altamente calificado en ciberseguridad y ciberdefensa. La inversión estratégica en investigación y desarrollo tecnológico es clave para garantizar que las Fuerzas Militares estén a la altura de los desafíos del ciberespacio y otros dominios de guerra. La independencia tecnológica no es un mero objetivo; es un imperativo que garantiza la seguridad y la soberanía de Colombia en una era donde la defensa y la seguridad están intrínsecamente ligadas a la tecnología. Es hora de liderar en este nuevo paradigma de la defensa, y el momento para comenzar es ahora.".

Solo queda decir:



"Aun Hoy el Ciberespacio es visto, como los albores de la aviación, la que cobró tributo aquellos que se resistieron aceptarla e implementarla en sus ejércitos negándose a la superioridad. Recordaremos esta lección de la Historia. Esperemos que no se repita"

Liliana Zambrano

IT-SF

IT SECURITY FORENSIC

En IT -SF , nos enorgullece ofrecer servicios de ciberseguridad de primer nivel. Nuestras metodologías eficientes garantizan los mejores resultados en pruebas de seguridad. Desde la detección y solución de vulnerabilidades hasta la adopción de IPv6 y la informática forense, nuestro equipo de expertos lo respalda en cada paso del camino.

SERVICIOS

- Análisis Forense Informático
- Etical Hacking
- Detección, análisis y remediación de vulnerabilidades.
- Diseño e implementación del protocolo IPv6 y servicios asociados
- Sistemas de Gestión de la Información
- Capacitación en Ciberseguridad

CONTACTO
3163500451

WWW.IT-SF.COM.CO

PPH

Compañía de Vigilancia

Su seguridad
nuestra meta,
su tranquilidad
nuestro compromiso.

www.pph.com.co
info@pph.com.co

Bogotá- Colombia
Calle 143 #46-09
Barrio Prado Pinzón

coinsa
s.a.s

- Soluciones de Infraestructura.
- Desaster Recovery: DRP - Centro Alterno.
- Servicios Gestionados de Seguridad: CoinSOC / NOC.
- Ciberseguridad y BCP.
- Outsourcing de IT.
- Nubes Públicas y Privadas.

coinsoc

TU EMPRESA LA LLEVAMOS HASTA TUS CLIENTES DE TECNOLOGÍA

CONTACTO +57 3009590045

CLICK

REPORTE CIBER SIEM

DIOS Y PATRIA
Es un honor ser Policía

¡NO DEJES QUE TE ENGAÑEN!

Juntos **prevenimos** el delito

CUELGA y marca 165

YO NO PAGO DENUNCIO 165

GAULA POLICÍA NACIONAL

EL MUNDO CAMBIÓ

@REVISTADIGITALELMUNDOCAMBIO

El Mundo Cambió

Escanea el código QR para seguir esta cuenta

TikTok

Revista Digital El Mundo Cambió