



CAEN Centro de Altos
Estudios Nacionales
ESCUELA DE POSGRADO

SEMINARIO: “AMENAZAS GLOBALES, RESILIENCIA REGIONAL Y DEFENSA DE INFRAESTRUCTURAS CRÍTICAS”

***La Ciberdefensa del Perú ante las
Amenazas Globales: "Capacidades
Militares para la Protección de
Infraestructuras Críticas y la
Resiliencia Regional"***

Acreditación



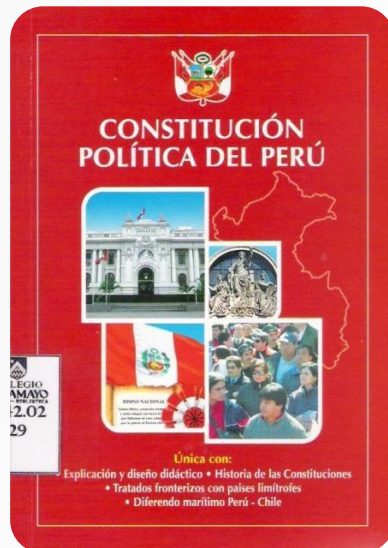
Nombre del docente:

Gral EP y Dr Ing Ernesto Castillo Fuerman

SITUACIÓN EN PERÚ DEL MARCO LEGAL EN EL CIBERESPACIO



CAPÍTULO I DEL ESTADO, LA NACIÓN Y EL TERRITORIO



Artículo 44.- Deberes del Estado

Son **deberes primordiales del Estado**: defender la **soberanía nacional**; garantizar la plena vigencia de los derechos humanos; **proteger a la población de las amenazas contra su seguridad**; y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación.

AMENAZA A LA SEGURIDAD
NACIONAL



Afectación a la seguridad
digital

MARCO LEGAL DE CIBERDEFENSA

Ley de Gobierno Digital DL 1412 (12SET18)

Marco de Seguridad Digital del
Estado Peruano

**Ley de Gobierno Digital
(12SET18)**

D.S 1412

Artículo 32.- Ámbitos

Art 30.- LA SEGURIDAD DIGITAL es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la **seguridad nacional** y los objetivos nacionales en dicho entorno

Defensa

El Ministerio de
Defensa
(MINDEF)
CIBERDEFENSA.

Inteligencia

**INTELIGENCIA,
CONTRAİNTELIGENCIA
Y SEGURIDAD DIGITAL
EN EL ÁMBITO DE ESTA
COMPETENCIA.
DIRECCIÓN DE
INTELIGENCIA
NACIONAL**

Justicia

CIBERDELINCUENCIA

Ministerio de Justicia,
Ministerio del Interior, Policía
Nacional del Perú
Art 100, DS 029-2021-PCM:
Instituto Penitenciario,
Ministerio Público, Tribunal
Constitucional, Academia de la
Magistratura, la Secretaria de
Gobierno Digital de la PCM

Institucional

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Secretaria de Gobierno y Transformación Digital

Art 3 h DU 007 2020: **CIBERSEGURIDAD**

Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país



ENE 2019 1000 Hrs



ENE 2019 1000 Hrs

ACN





ACN



ACN





1100 Hrs PROBLEMA DE DESPROGRAMACIÓN



ACN



ACN

ACN 1530 Hrs Comunicado
Problemas técnicos y esta
en etapa de contingencia

21:30 Hrs

ACN



An aerial night photograph of a city, likely Lima, Peru, showing a dense grid of buildings and streets. A prominent, bright orange-yellow light source is visible in the upper left quadrant, casting a glow over the surrounding area. The text 'ACN' is overlaid in white, sans-serif font in the center-left of the image.

ACN

0600 Hrs día
siguiente S/N

COMISIÓN DE DEFENSA NACIONAL



13 Feb, se informa
incidente ACN
CECIBER/CGE



ACN

COMISIÓN DE
DEFENSA NACIONAL



13 Feb, se informa
incidente ACN
CECIBER/CGE



LEY 30999 CIBERDEFENSA
(09AGO19)

ACN

LEY DE CIBERDEFENSA 30999

¿Qué Instituciones
trabajan en
Ciberdefensa

1. MINDEF,
MININTER,
DINI, CCFFAA
EP, MPG, FAP

Necesidad de
coordinación

3. Red Científica,
Telefónica, Claro, CISCO,
Bolsa Valores, Microsof,
AFIN, Networc Acces Point,
ASBANC, EEP

ATQ AC

07 ENE 14 ENE 18 ENE 23 ENE

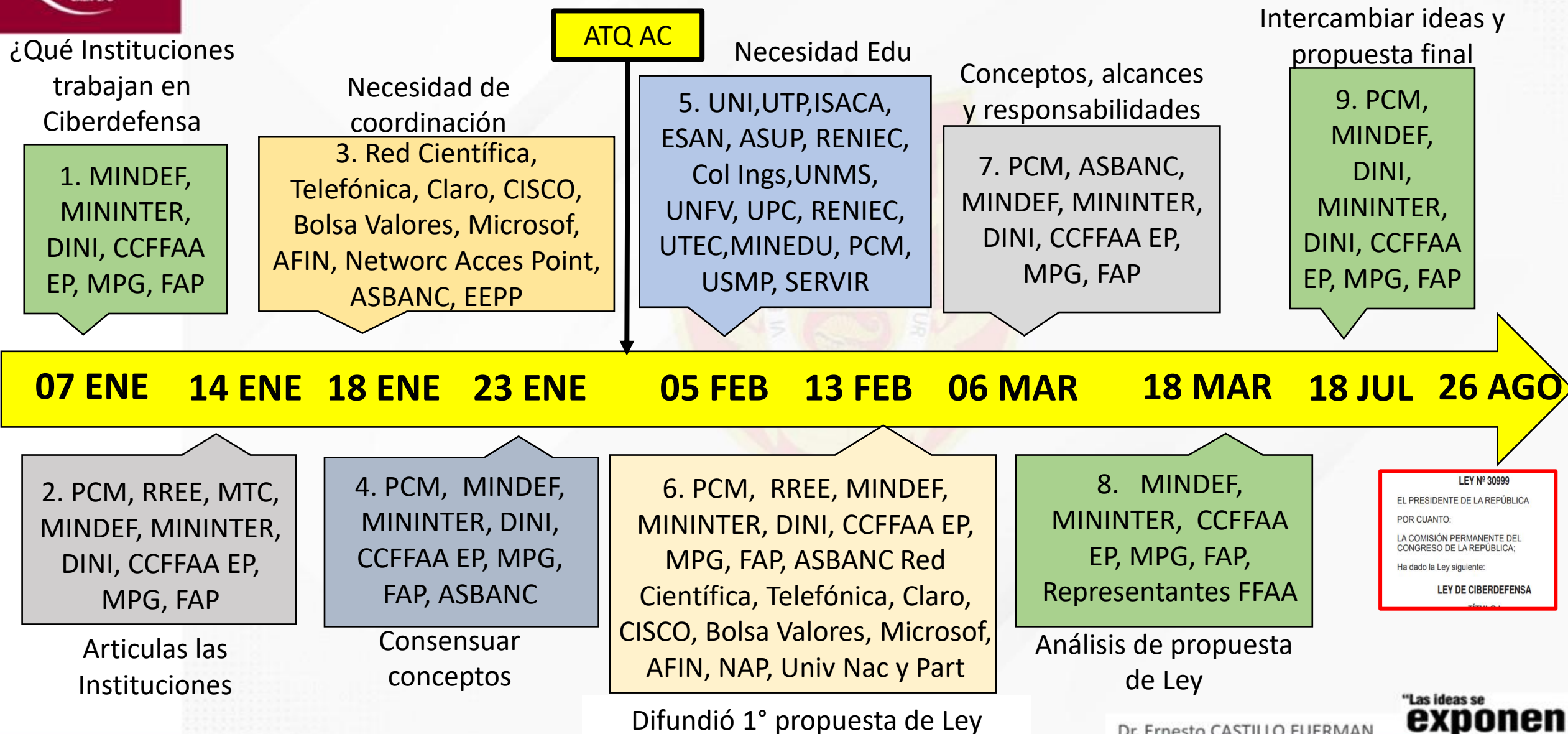
2. PCM, RREE, MTC,
MINDEF, MININTER,
DINI, CCFFAA EP,
MPG, FAP

Articulas las
Instituciones

4. PCM, MINDEF,
MININTER, DINI,
CCFFAA EP, MPG,
FAP, ASBANC

Consensuar
conceptos

LEY DE CIBERDEFENSA 30999



LEY 30999, LEY DE CIBERDEFENSA

LEY DE CIBERDEFENSA

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto

La presente ley tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley.

Artículo 2. Finalidad

Defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

Artículo 3. Ambito de aplicación

El ámbito de aplicación de la norma se circunscribe a la ejecución de operaciones de ciberdefensa en y mediante el ciberespacio frente a las amenazas o los ataques que afecten la seguridad nacional.

Artículo 4. Definición

Entiéndase por ciberdefensa a la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional.

Artículo 5. Órganos ejecutores

Las Fuerzas Armadas, que están constituidas por el Ejército, la Marina de Guerra y la Fuerza Aérea, y el Comando Conjunto de las Fuerzas Armadas son instituciones con calidad de órganos ejecutores del Ministerio de Defensa.

TÍTULO II

DE LA CIBERDEFENSA

CAPÍTULO I

LAS CAPACIDADES DE CIBERDEFENSA Y LAS OPERACIONES EN Y MEDIANTE EL CIBERESPACIO

Artículo 6. De las capacidades de ciberdefensa

Es el uso de conocimiento, habilidades y medios para realizar operaciones en y mediante el ciberespacio a fin de asegurar su empleo por las fuerzas propias.

CAPÍTULO II

DEL USO DE LA FUERZA EN Y MEDIANTE EL CIBERESPACIO

Artículo 9. Del uso de la fuerza por las Fuerzas Armadas

El uso de la fuerza por la Fuerzas Armadas en y mediante el ciberespacio se sujeta a las disposiciones contenidas en el artículo 51 de la Carta de las Naciones Unidas y el presente dispositivo legal, y está regido por el Derecho Internacional de los Derechos Humanos y el Derecho Internacional Humanitario que

Ley Ciberdefensa 30999, Art 4:
CAPACIDAD MILITAR que permite actuar frente amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la **SEGURIDAD NACIONAL**

Legítima defensa

que en y mediante el ciberespacio o la soberanía, los intereses críticos nacionales y recursos las capacidades nacionales, da derecho de legítima defensa.

Condiciones para el ejercicio del uso de

hecho de legítima defensa en el uso de ciberdefensa está sujeto a la necesidad y oportunidad.

Realizar una operación de respuesta en el ciberespacio que contenga un ataque debe darse de acuerdo a ley.

LEY 30999, LEY DE CIBERDEFENSA

CAPITULO III

DE LA SEGURIDAD DE LOS ACTIVOS CRÍTICOS NACIONALES Y RECURSOS CLAVES

Artículo 12. Del control y de la protección de los activos críticos nacionales y recursos claves

El Comando Conjunto de las Fuerzas Armadas está a cargo de la ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores y/o del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia sea sobrepasada, a fin de mantener las capacidades nacionales, en el ámbito de la seguridad nacional.

Artículo 13. De los protocolos de escalamiento, coordinación, intercambio y activación

La Presidencia del Consejo de Ministros, en su calidad de miembro del Consejo de Seguridad y Defensa Nacional, establece los protocolos de escalamiento, coordinación, intercambio y activación para lo indicado en la presente ley.

Esta función se ejerce a través de la Secretaría de Gobierno Digital en su calidad de ente rector del Sistema Nacional de Informática y de la seguridad digital en el país, quien emite los lineamientos y las directivas correspondientes.

Artículo 14. Modificación del artículo 32 del Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital

Modifícase el artículo 32 del Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, el cual queda redactado de la siguiente manera:

“Artículo 32.- Gestión del Marco de Seguridad Digital del Estado Peruano

El Marco de Seguridad Digital del Estado Peruano tiene los siguientes ámbitos:

a. Defensa: El Ministerio de Defensa (MINDEF), en el marco de sus funciones y competencias, dirige, norma, supervisa y evalúa las normas en materia de ciberdefensa.

El Comando Conjunto de las Fuerzas Armadas está a cargo de la ciberdefensa de los **activos críticos nacionales y recursos claves**, cuando la capacidad de protección de sus operadores y/o del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia **sea sobrepasada**, a fin de mantener las capacidades nacionales, en el ámbito de la seguridad nacional.

comunicación de incidentes que pudieran afectar la capacidad de ciberdefensa nacional.

CUARTA. Desarrollo de currículos de educación superior en materia de ciberdefensa

La Presidencia del Consejo de Ministros, en su calidad de ente rector en materia de seguridad digital, coordina con el Ministerio de Defensa y el Ministerio de Educación la pertinencia del desarrollo de contenidos especializados en materia de seguridad digital, que incluye la ciberdefensa, en las instituciones de educación superior universitaria y tecnológica, a nivel de pregrado y postgrado. Para ello, establece instrumentos de cooperación interinstitucional con entidades del sector privado, la academia, la sociedad civil y la comunidad técnica.

QUINTA. Aplicación de recursos especiales

capacidades de ciberdefensa al alcance de la aplicación de Ley Legislativo 1141.

TARIA DEROGATORIA

penso, según el caso, las entarías que se opongan a ley o limiten su aplicación, presente ley.

esidente de la República

del mes de agosto de dos

MAREZ CALDERÓN
la República

Congreso de la República

TE DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

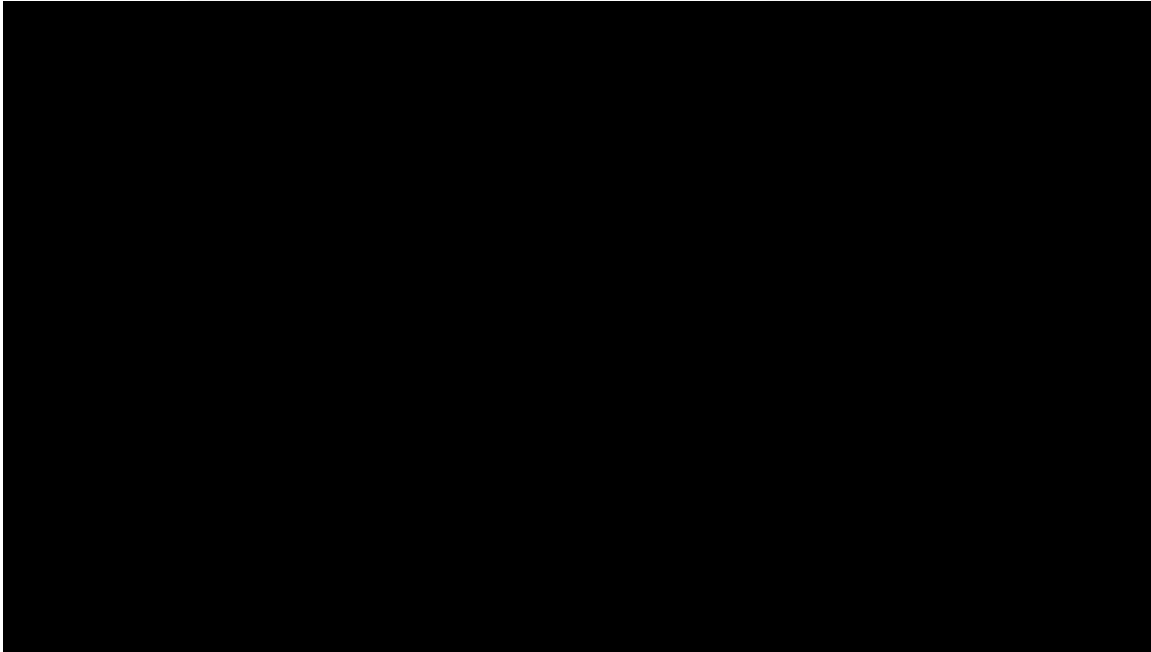
Dado en la Casa de Gobierno, en Lima, a los veintiséis días del mes de agosto del año dos mil diecinueve.

MARTÍN ALBERTO VIZCARRA CORNEJO
Presidente de la República

SALVADOR DEL SOLAR LABARTHE
Presidente del Consejo de Ministros

1801519-5

ACTIVOS CRITICOS NACIONAL



ACTIVO CRÍTICO NACIONAL: Son aquellos recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales, o que están destinados a cumplir dicho fin; y, cuya afectación, perturbación o destrucción no permite soluciones alternativas inmediatas, generando grave perjuicio a la Nación. (Art 3.4. DS 106-2017-PCM)

RECURSO CLAVE: son recursos, infraestructuras y sistemas que no califican como ACN, su destrucción o afectación origina un impacto regional y un impacto relevante a las capacidades nacionales. (Art 3.13. DS 106-2017-PCM)

CIBERDEFENSA

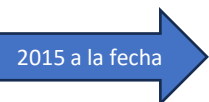
EL ÚLTIMO
BASTIÓN

Porque cuando los ACN y RECURSOS CLAVES sufren ciberataques, la CIBERDEFENSA actúa una vez que ha sido sobrepasado la capacidad de protección de sus operadores, sector responsable y/o la DINI, a fin de mantener las capacidades nacionales (Art 12 Ley 30999)

AVANCES DE LA CIBERDEFENSA 2018-2023



2018



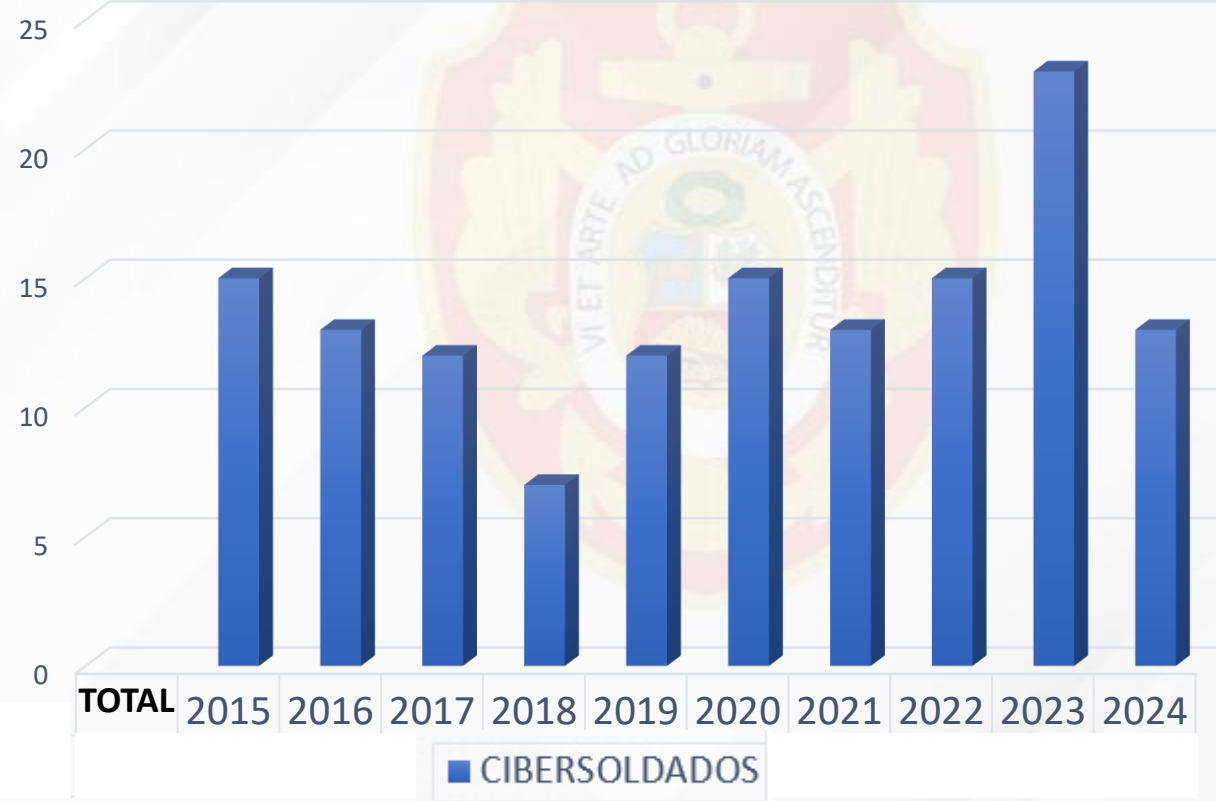
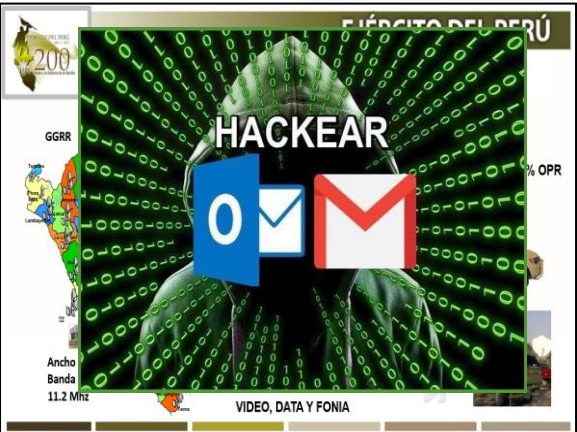
2015 a la fecha

ECOME
Curso Ons
Ciber

ESCUELA DE COMUNICACIONES DEL EJÉRCITO

PROGRAMA OPERACIONES DE CIBERDEFENSA

2010



HASTA EL 20 DE AGOSTO
PRESENTACIÓN DE SOLICITUDES

ADMISIÓN 2025
XI PROGRAMA OPERACIONES DE CIBERDEFENSA

Ser Oficial del Arma de Comunicaciones y Artillería.
Postular en el grado de Subteniente hasta el grado de Teniente en su 3er año de servicio

<https://jeduca.ejercito.mil.pe/solicitudes-ppc>

SE CAPACITA A PERSONAL DE LAS FUERZAS ARMADAS Y LA POLICIA NACIONAL

AVANCES DE LA CIBERDEFENSA 2018-2023



2018

CAEN a la
fecha D/M

2015 a la fecha

ECOME
Curso Ons
Ciber

DIPLOMADOS Y MAESTRÍAS EN EL CAEN

4 DIPLOMADOS



3 MAESTRÍAS



AVANCES DE LA CIBERDEFENSA 2018-2023

Doctrina de
Operaciones en el
Ciberespacio, se
publicó el 27MAR.



2018

CAEN a la
fecha D/M

2015 a la fecha

ECOME
Curso Ons
Ciber



DOCTRINA DE OPERACIONES EN EL CIBERESPACIO, SE PUBLICÓ EL 27 MARZO 2018



DFA-CD-03-10
MINISTERIO DE DEFENSA
CCFFAA

DOCTRINA DE OPERACIONES EN EL CIBERESPACIO

ÍNDICE

	Nº PÁRR.	Nº PÁG.
INTRODUCCIÓN		
CAPÍTULO I: GENERALIDADES		
Objeto	1.1	I - 1
Finalidad	1.2	I - 1
Alcance	1.3	I - 2
Consideraciones Básicas	1.4	I - 2
CAPÍTULO II: MARCO LEGAL Y DOCTRINARIO		
Sección I.- MARCO LEGAL		
De Carácter Internacional	2.1	II - 1
Sociedad de la Información	2.2	II - 1
Gobierno Electrónico	2.3	II - 1
Seguridad de la Información	2.4	II - 2
Sección II.- MARCO DOCTRINARIO		
Base Doctrinaria	2.5	II - 3
Entorno Jurídico Internacional	2.6	II - 3
Ciberespacio	2.7	II - 3

CAPÍTULO III: FUNDAMENTOS DEL CIBERESPACIO

Entorno Operacional	3.1	
III - 1		
Estructura de las Operaciones	3.2	
III - 1		
Operaciones en el Ciberespacio	3.3	III - 2
Desafíos de las Operaciones en el Ciberespacio	3.4	III - 6
Principios aplicables en el entorno del Ciberespacio	3.5	III - 18
Integración de las Operaciones en el Ciberespacio con los otros dominios	3.6	III - 19
CAPÍTULO IV: ORGANIZACIÓN ESTRATÉGICA OPERACIONAL		
Política relacionada al Comando y Organización de las Fuerzas del Ciberespacio	4.1	IV - 1
Relaciones de Comando	4.2	IV - 1
Organización de las Operaciones en el Ciberespacio	4.3	IV - 1
Funciones de las Organizaciones de Ciberdefensa de las Fuerzas Armadas	4.4	IV - 6
GLOSARIO DE TÉRMINOS	GT - 1	GT - 9

AVANCES DE LA CIBERDEFENSA 2018-2023

Doctrina de
Operaciones en el
Ciberespacio, se
publicó el 27MAR.

EP Y MGP crean
entidades de
Ciberdefensa
EXPERIMENTAL

2018

2018

2018

2018

CAEN a la
fecha D/M

2015 a la fecha

ECOME
Curso Ons
Ciber

Ley de Gobierno
Digital N° 1412,
13Set.

Inauguración del
Centro (Comando)
Ciberdefensa Ejército
[29Oct18](#)

INAUGURACIÓN DEL COMANDO CIBERDEFENSA EJÉRCITO

AMBITO DE RESPONSABILIDAD CIBERESPACIO QUE EMPLEA LAS FUERZAS TERRESTRES, ASÍ
COMO ACN Y RC ASIGNADOS A LA FUERZA TERRESTRE



29 OCTUBRE 2018

AVANCES DE LA CIBERDEFENSA 2018-2023



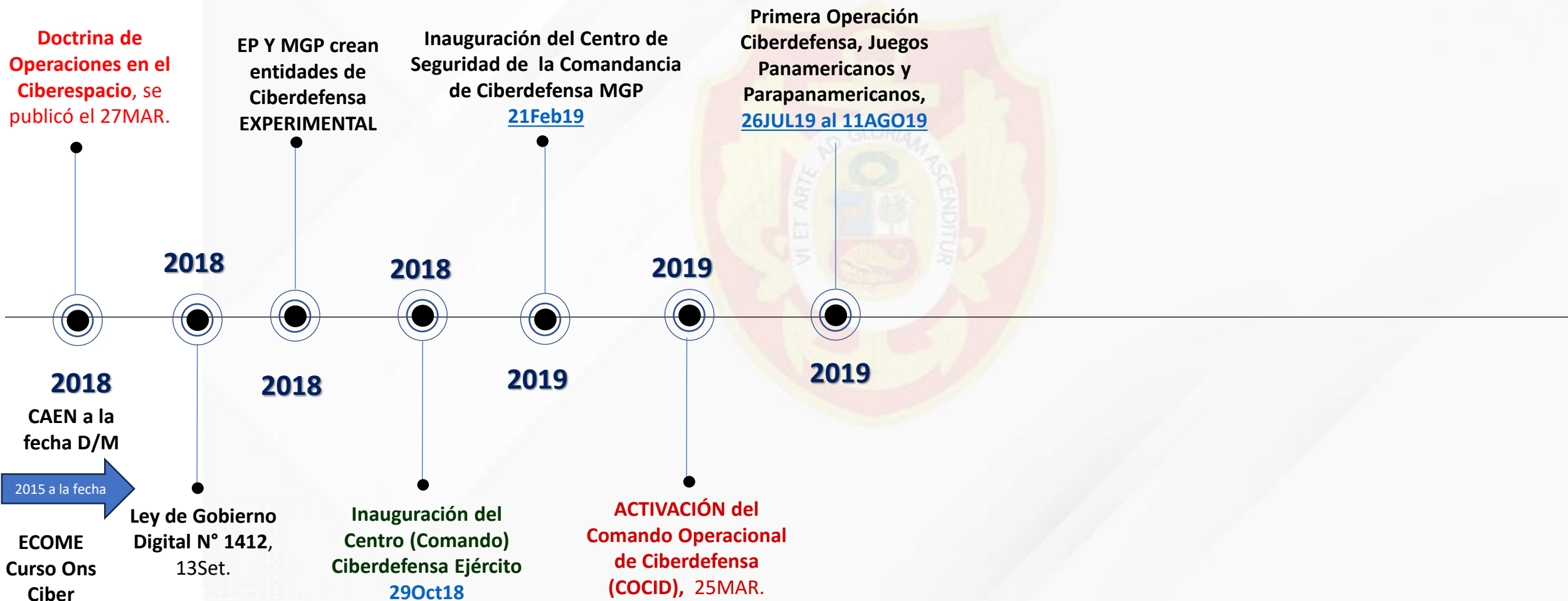
Inauguración del Centro de Seguridad de la Comandancia de Ciberdefensa MGP

AMBITO DE RESPONSABILIDAD CIBERESPACIO QUE EMPLEA LAS FUERZAS NAVALES, ASÍ
COMO ACN Y RC ASIGNADOS A LA FUERZA NAVALES



21 FEBRERO 2019

AVANCES DE LA CIBERDEFENSA 2018-2023



OPERACIONES DE CIBERDEFENSA PANAMERICANOS 2019

Comando Conjunto de las Fuerzas Armadas del Perú
1 de agosto · 🌐

El Comando Conjunto de las Fuerzas Armadas a través de su Comando Operacional de Ciberdefensa trabaja en la protección de Activos Críticos Nacionales frente a posibles amenazas en el ciberespacio, en apoyo al normal desenvolvimiento de los Juegos Panamericanos y Parapanamericanos #Lima2019.





Ejército del Perú INICIO NOSOTROS · PRENSA · CONTRIBUCIÓN · ORGANIZACIÓN ·

Cuartel General del Ejército sede del comando de Ciberdefensa del Comando Conjunto de las Fuerzas Armadas

Escrito por [Administrador Portal Institucional](#)

tamaño de la fuente 🔍 | Imprimir | Email



Activación de protocolos de seguridad en el Ciberespacio de los activos críticos nacionales asignados a las Fuerzas Armadas en apoyo a la realización de los Juegos Panamericanos y Parapanamericanos Lima 2019, en las instalaciones del Cuartel General del Ejército, sede de puesto comando de las Fuerzas Armadas.

OPERACIONES DE CIBERDEFENSA PANAMERICANOS 2019

**PORCENTAJE DE RESPONSABILIDADES DE RESGUARDO DEL CIBERESPACIO QUE
EMPLEAN LOS ACTIVOS CRITICOS NACIONALES Y SEDES DEPORTIVAS**

**16 %
3 ACN**



COMPONENTE NAVAL

**79 %
15 ACN**

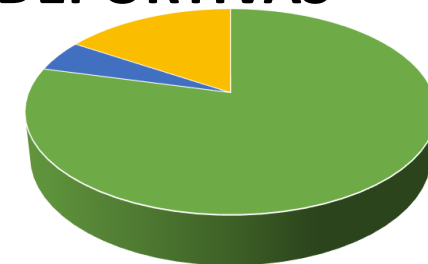


COMPONENTE TERRESTRE

**5 %
1 ACN**



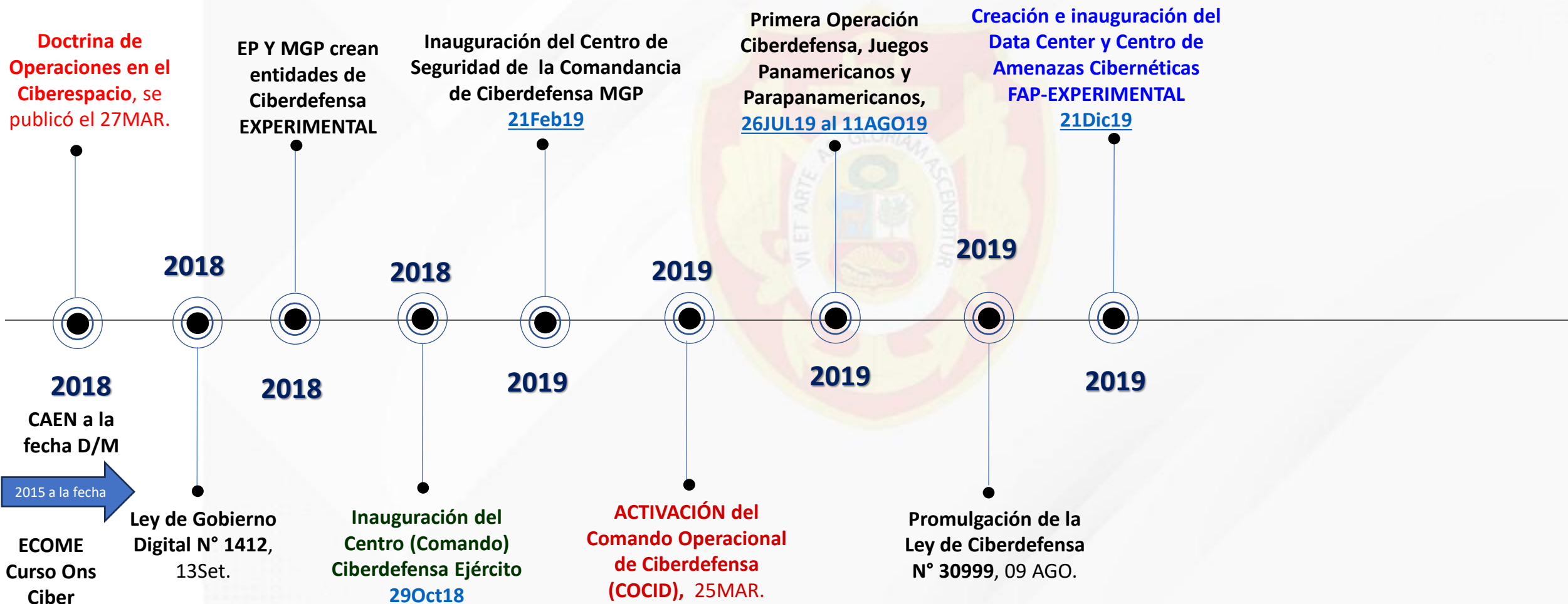
COMPONENTE AEREO



■ EJERCITO ■ FUERZA AEREA ■ MARINA

**%
ACN**

AVANCES DE LA CIBERDEFENSA 2018-2023



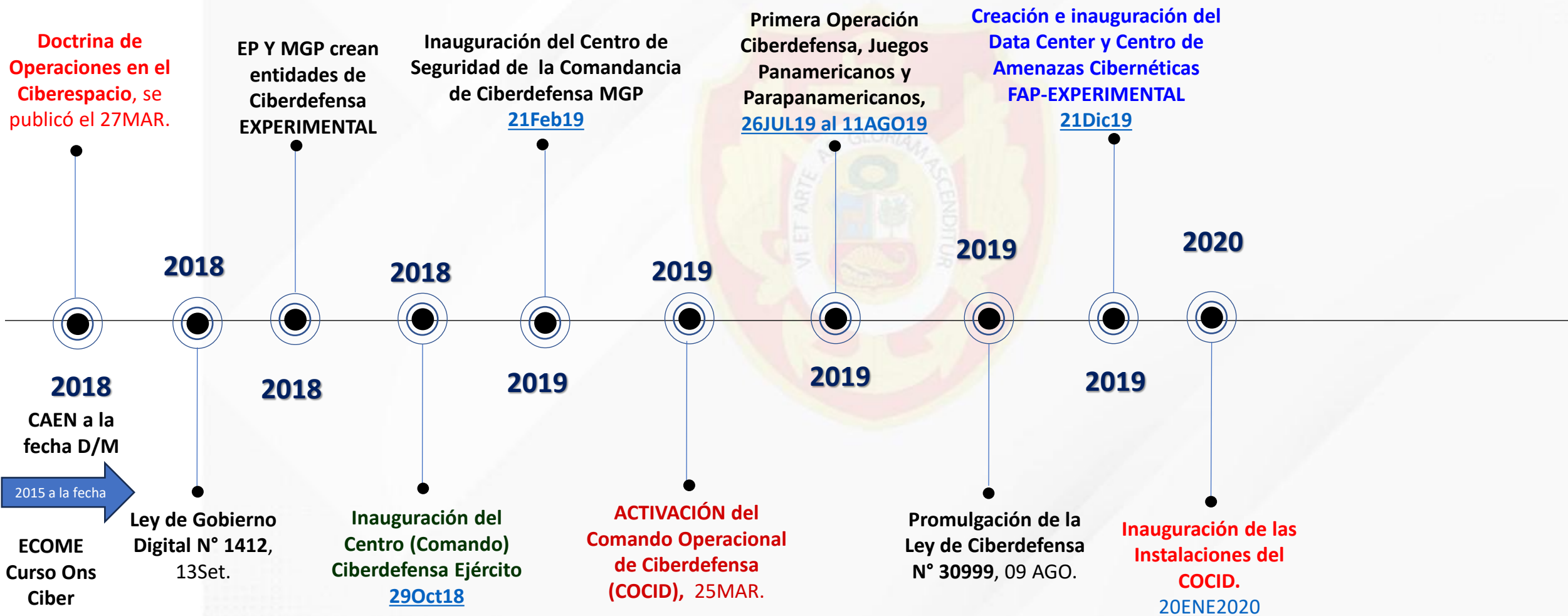
CREACIÓN E INAUGURACIÓN DEL DATA CENTER Y CENTRO DE AMENAZAS CIBERNÉTICAS FAP

AMBITO DE RESPONSABILIDAD CIBERESPACIO QUE EMPLEA LAS FUERZA AÉREA, ASÍ COMO
ACN Y RC ASIGNADOS A LA FUERZA AÉREA



21 DICIEMBRE 2019

AVANCES DE LA CIBERDEFENSA 2018-2023



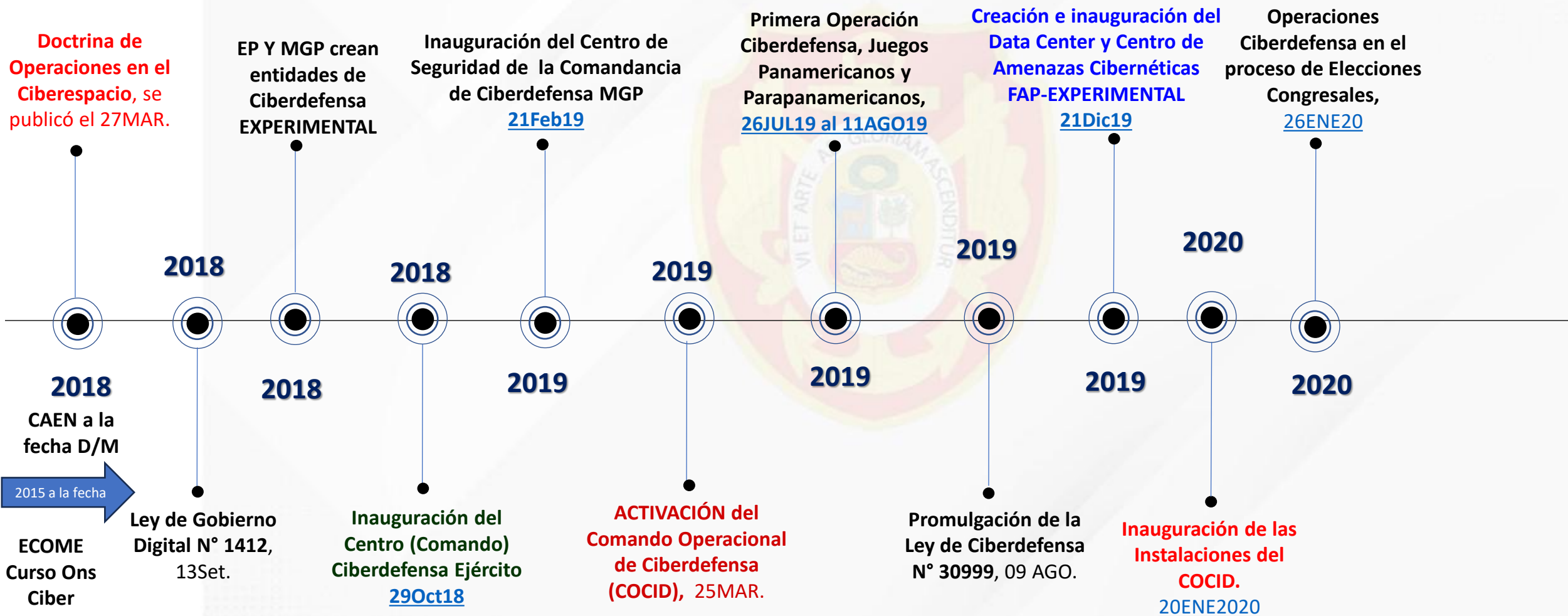
INAUGURACIÓN DE LAS INSTALACIONES DEL COCID

AMBITO DE RESPONSABILIDAD CIBERESPACIO QUE EMPLEA LAS FUERZAS CONJUNTAS, ASÍ
COMO ACN Y RC ASIGNADOS A LA FUERZAS CONJUNTAS



20 ENERO 2020

AVANCES DE LA CIBERDEFENSA 2018-2023



OPERACIONES DE CIBERDEFENSA ELECCIONES CONGRESALES



- Reunión del 26 de noviembre del 2019, donde se recomienda la activación de un **“Centro de Respuesta ante Incidentes Informático Electoral”** formado por la **ONPE, RENIEC y JNE**, así como el **apoyo por parte de las FFAA** a las Elecciones Congresales Excepcionales 2020 de **acuerdo a ley**.

OPERACIONES DE CIBERDEFENSA ELECCIONES CONGRESALES

“Centro de Respuesta ante Incidentes Informático Electoral”

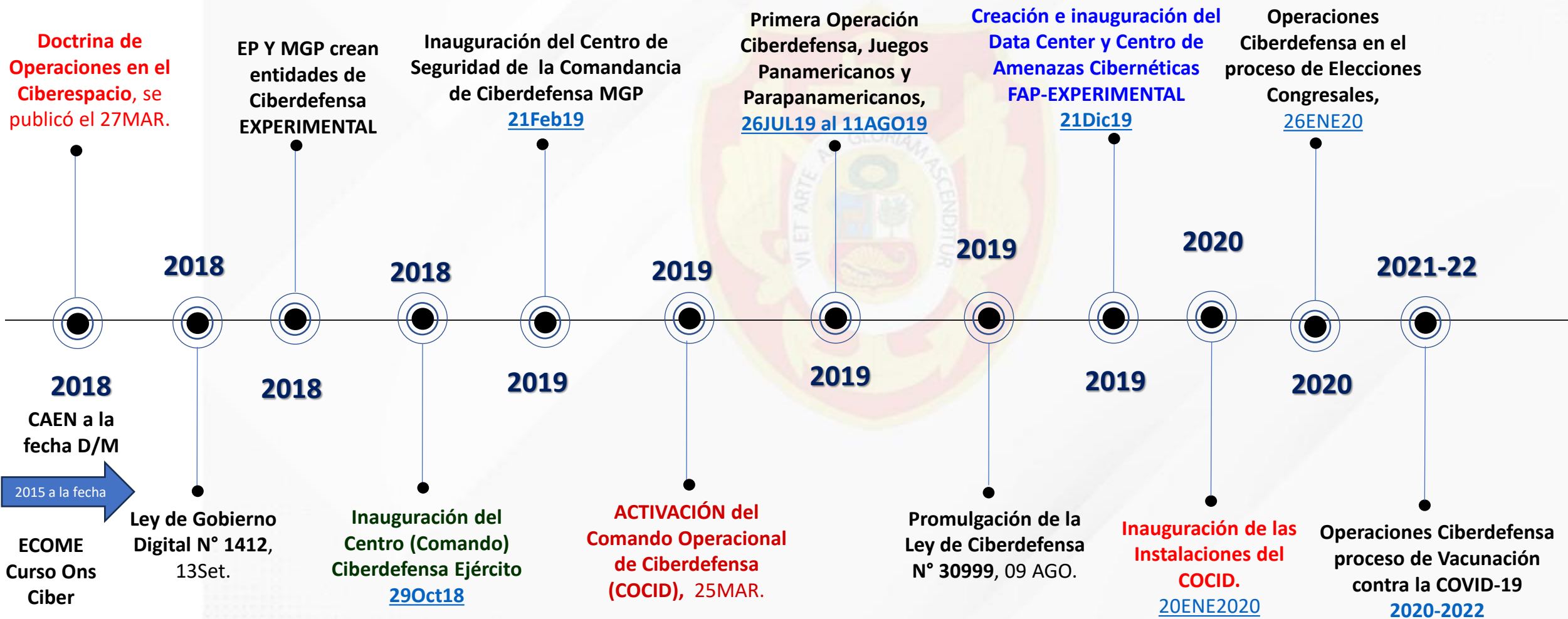


- Apoyo realizado mediante el **monitoreo** de 55 activos público de la ONPE, RENIEC y JNE del 23 al 27 de enero verificando su **disponibilidad y concurrencia las 24 horas de día** y utilización de la plataforma **MISP**=Malware Information Sharing Platform, para realizar para una mejor colaboración interinstitucional.

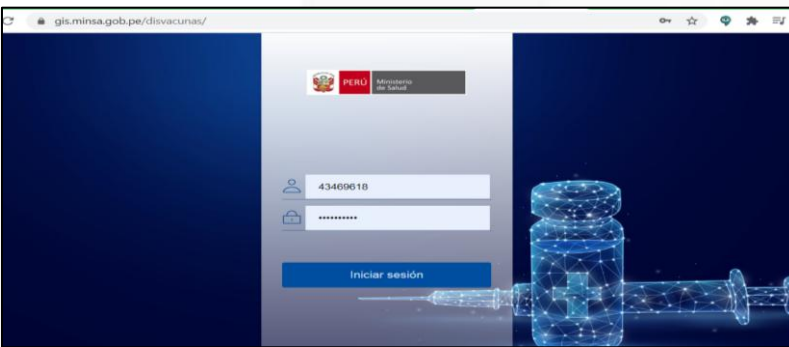
PLATAFORMA DE CONECTIVIDAD



AVANCES DE LA CIBERDEFENSA 2018-2023



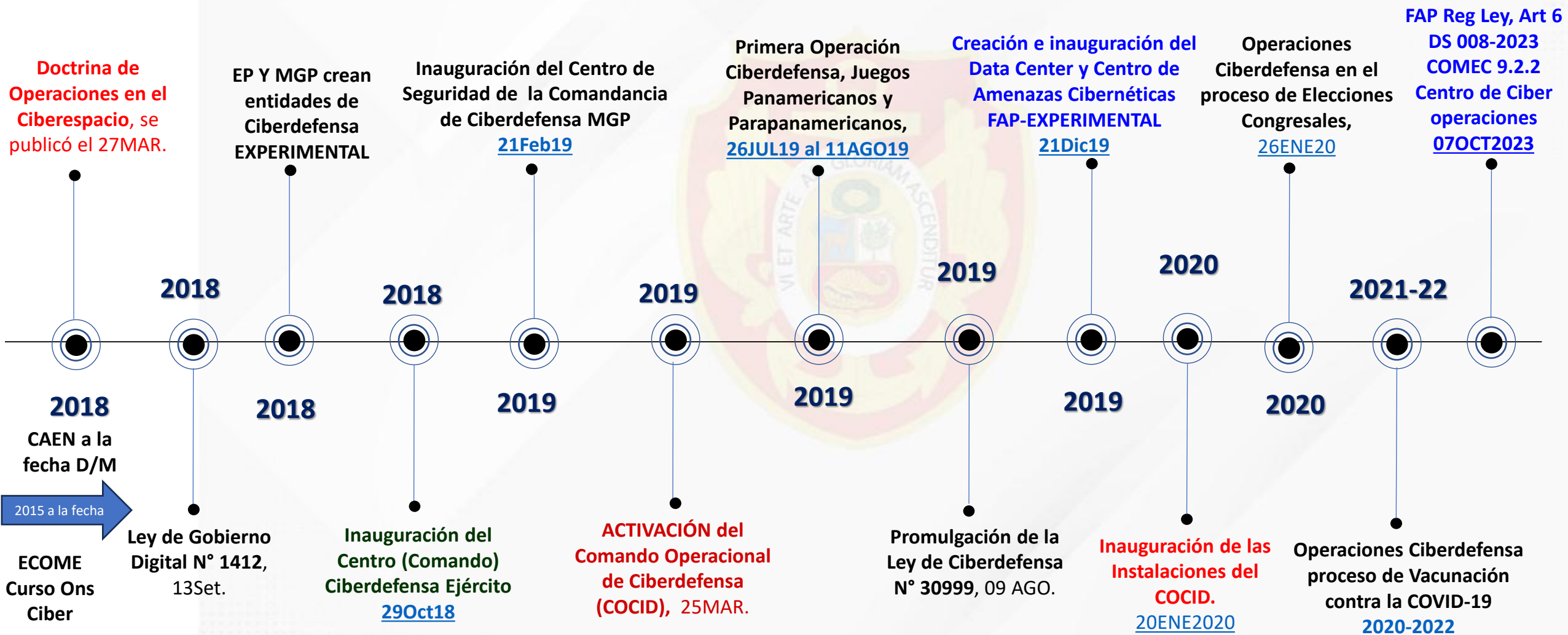
OPERACIONES DE CIBERDEFENSA “VACUNACIÓN COVID 19-2021-22”



En coordinación con la SEGDI se realiza el Monitoreo de los Activos Públicos involucrados en el **Proceso de vacunación contra la COVID-19, (05 activos públicos de información)** entregados al **Comando Operacional de Ciberdefensa.**



AVANCES DE LA CIBERDEFENSA 2018-2023



COMEC-CENTRO DE OPERACIONES CIBERESPACIALES-FAP

Ley de la Fuerza Aérea del Perú

DECRETO LEGISLATIVO N° 1139

TÍTULO III

ORGANIZACIÓN

CAPÍTULO I

ESTRUCTURA ORGÁNICA

Artículo 5°.-Estructura Orgánica Básica

La FAP está compuesta por los siguientes órganos y sus funciones y atribuciones se establecen en el reglamento de la presente norma:

7) Órganos de Línea

Los Órganos de Línea son aquellos entes operacionales de la institución, y están integrados por los Comandos de Fuerza.

Artículo 16°.- Comandos de Fuerza

La FAP cuenta con Comandos de Fuerza, como órganos encargados de cumplir las funciones sustantivas de la institución, mediante la preparación y entrenamiento operativo orientado a realizar operaciones que contribuyan con la Seguridad y Defensa Nacional, el Orden Interno en los estados de excepción, el desarrollo económico y social del país y la Defensa Civil.

Cada Comando de Fuerza estará al mando de un Oficial General. Su organización interna, conformación y funciones se establecen en el reglamento de la presente norma.

FUENTE: Perú. Ministerio de Defensa. (2025, 4 de abril). *Decreto Legislativo N.º 1139 – Ley de la Fuerza Aérea del Perú*. <https://cdn.www.gob.pe/uploads/document/file/7878148/6637359-ley-de-la-fuerza-aerea-del-peru-decreto-legislativo-n-1139.pdf?v=1743781244>

REGLAMENTO DEL DECRETO LEGISLATIVO N° 1139, LEY DE LA FUERZA AÉREA DEL PERÚ

DS 008-2023

Artículo 107.- Comando Espacial y Ciberespacial de la Fuerza Aérea del Perú

El Comando Espacial y Ciberespacial de la Fuerza Aérea del Perú es el órgano dependiente de la Comandancia General, responsable de planear y conducir las operaciones en el dominio espacial y en el dominio ciberespacial en el ámbito de su competencia, que contribuyan con la seguridad y defensa nacional, al control del orden interno en los estados de excepción, al desarrollo económico y social, a la gestión del riesgo de desastres y a la política exterior del país.

Está al mando de un Oficial General, del grado de Teniente General FAP.

Artículo 108.- Funciones específicas

Son funciones específicas del Comando Espacial y Ciberespacial de la Fuerza Aérea del Perú las siguientes:

108.1 Administrar los Sistemas de Control Espacial y Control Ciberespacial de la Fuerza Aérea del Perú, así como supervisar los subsistemas y procesos en el ámbito de su competencia.

108.2 Asegurar el empleo de las capacidades espaciales y ciberespaciales en el ámbito de su competencia.

108.3 Coordinar con las entidades nacionales e internacionales correspondientes, la operación, control y explotación de los medios en el espacio.

108.4 Realizar la preparación y desarrollo de la fuerza asignada para el cumplimiento de las funciones de la Fuerza Aérea del Perú en el ámbito espacial y ciberespacial.

108.5 Planear, conducir y supervisar las actividades de entrenamiento operativo.

108.6 Conducir la investigación de fenómenos espaciales anómalos, así como el procesamiento y explotación de la información espacial con los medios disponibles.

108.7 Planear, organizar, dirigir y conducir operaciones con el fin de evitar amenazas a través del ciberespacio que afecten la seguridad digital de las redes y sistemas de información de la Fuerza Aérea del Perú.

108.8 Planear, organizar, dirigir y conducir las operaciones con el fin de evitar amenazas en el ámbito espacial que afecten los intereses nacionales.

Artículo 112.- Centro de Operaciones Ciberespaciales

El Centro de Operaciones Ciberespaciales es la unidad dependiente del Comando Espacial y Ciberespacial de la Fuerza Aérea del Perú, encargada de realizar las operaciones de defensa, explotación y respuesta en el ciberespacio, a fin de asegurar su empleo por las fuerzas propias.

Artículo 113.- Funciones específicas

Son funciones específicas del Centro de Operaciones Ciberespaciales:

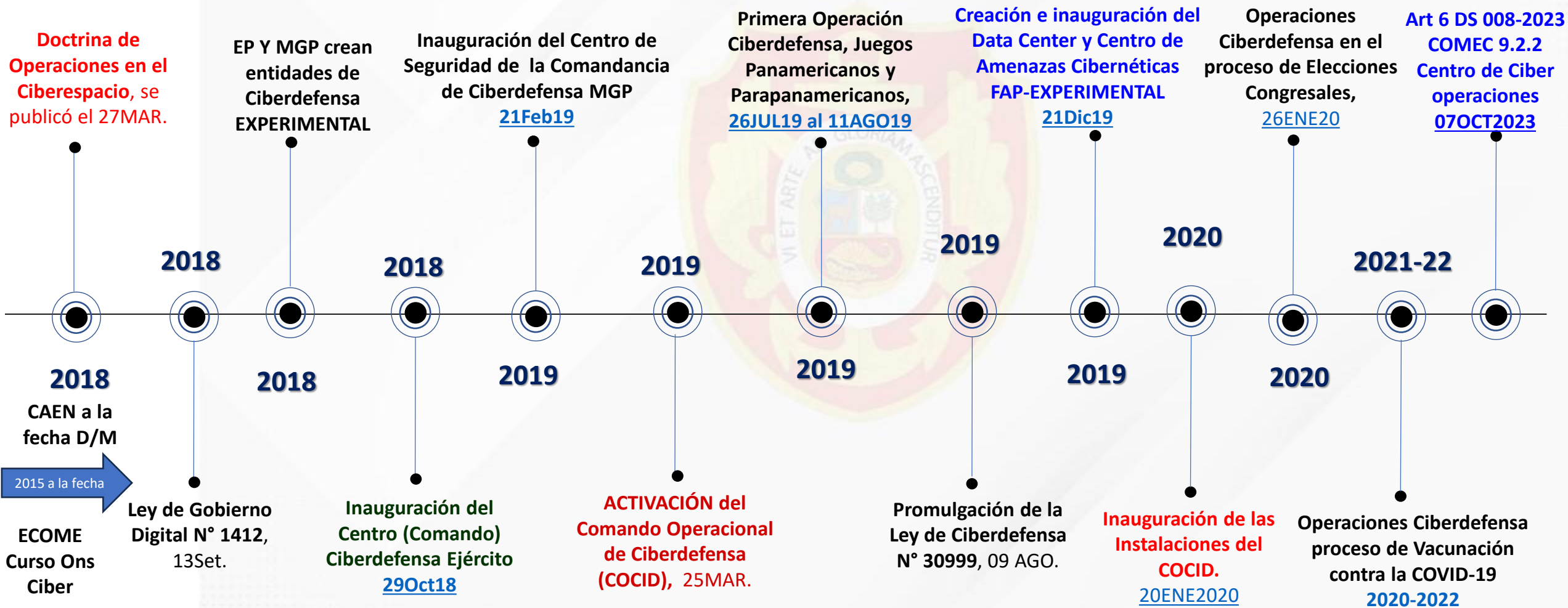
113.1 Ejecutar el entrenamiento operativo del personal calificado en operaciones de ciberdefensa.

113.2 Realizar operaciones defensivas, mediante el monitoreo permanente del ciberespacio, a fin de prevenir, detectar, evaluar, analizar y gestionar eficientemente los incidentes de seguridad digital a través de la aplicación de medidas proactivas, reactivas y la coordinación de medidas pasivas y de recuperación con las unidades correspondientes en la Institución.

113.3 Realizar operaciones de explotación mediante la búsqueda, detección e identificación de amenazas y vulnerabilidades a la seguridad del Estado en el ciberespacio, para el adecuado planeamiento de las operaciones defensivas y de respuesta, en los niveles estratégico, operacional y táctico.

FUENTE: Perú. Ministerio de Defensa. (2023, 7 de octubre). *Decreto Supremo N.º 008-2023-DE: Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N.º 1139, Ley de la Fuerza Aérea del Perú* [Texto legal]. <https://img.lpderecho.pe/wp-content/uploads/2023/10/Decreto-Supremo-008-2023-DE-LPDerecho.pdf>

AVANCES DE LA CIBERDEFENSA 2018-2023



REGLAMENTO DE LA LEY DE CIBERDEFENSA

13 FEB 2024 SE APRUEBA

PODER EJECUTIVO

PRESIDENCIA DEL CONSEJO DE MINISTROS

**Decreto Supremo que aprueba el
Reglamento de la Ley N° 30999, Ley de
Ciberdefensa**

**DECRETO SUPREMO
N° 017-2024-PCM**



El Ministerio de Defensa, es la entidad encargada de gestionar la ciberdefensa. Asimismo, dicta **políticas y lineamientos para el planeamiento y conducción de operaciones militares en y mediante el ciberespacio** conforme a la Política de Seguridad y Defensa Nacional aprobada por el Consejo de Seguridad y Defensa Nacional

OPERACIONES MILITARES: COCID

ESPACIAL

CIBERESPACIO

LEY 30999: CAPACIDAD MILITAR DE CIBERDEFENSA

CIBERESPACIO

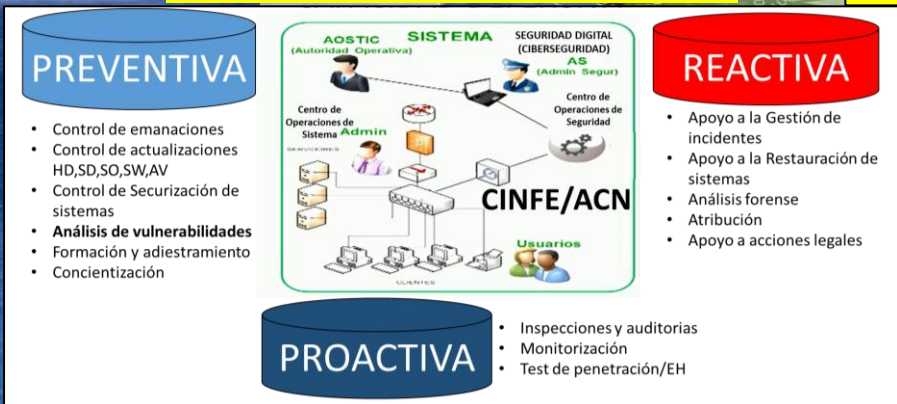
CAPÍTULO III
DE LA SEGURIDAD DE LOS ACTIVOS CRÍTICOS NACIONALES Y RECURSOS CLAVES
Artículo 12. Del control y de la protección de los activos críticos nacionales y recursos claves
El Comando Conjunto de las Fuerzas Armadas está a cargo de la ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores y/o del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia sea sobrepasada, a fin de mantener las capacidades nacionales, en el ámbito de la seguridad nacional.

Artículo 11. Requisitos para el ejercicio del uso de la fuerza
El ejercicio del derecho de legítima defensa en el contexto de las operaciones de ciberdefensa está sujeto a los principios de legalidad, necesidad y oportunidad.
En el caso de conducir una operación de respuesta en y mediante el ciberespacio que contenga un ataque deliberado, debe realizarse de acuerdo a ley.

OPERACIONES DEFENSIVAS

OPERACIONES DE EXPLOTACIÓN

OPERACIONES OFENSIVAS



Consiste en la búsqueda, identificación, reconocimiento, vigilancia y seguimiento de cibramenazas en y mediante el ciberespacio; recurriendo a medidas pasivas y activas (Art 6.b, DS° 017-PCM 2024)



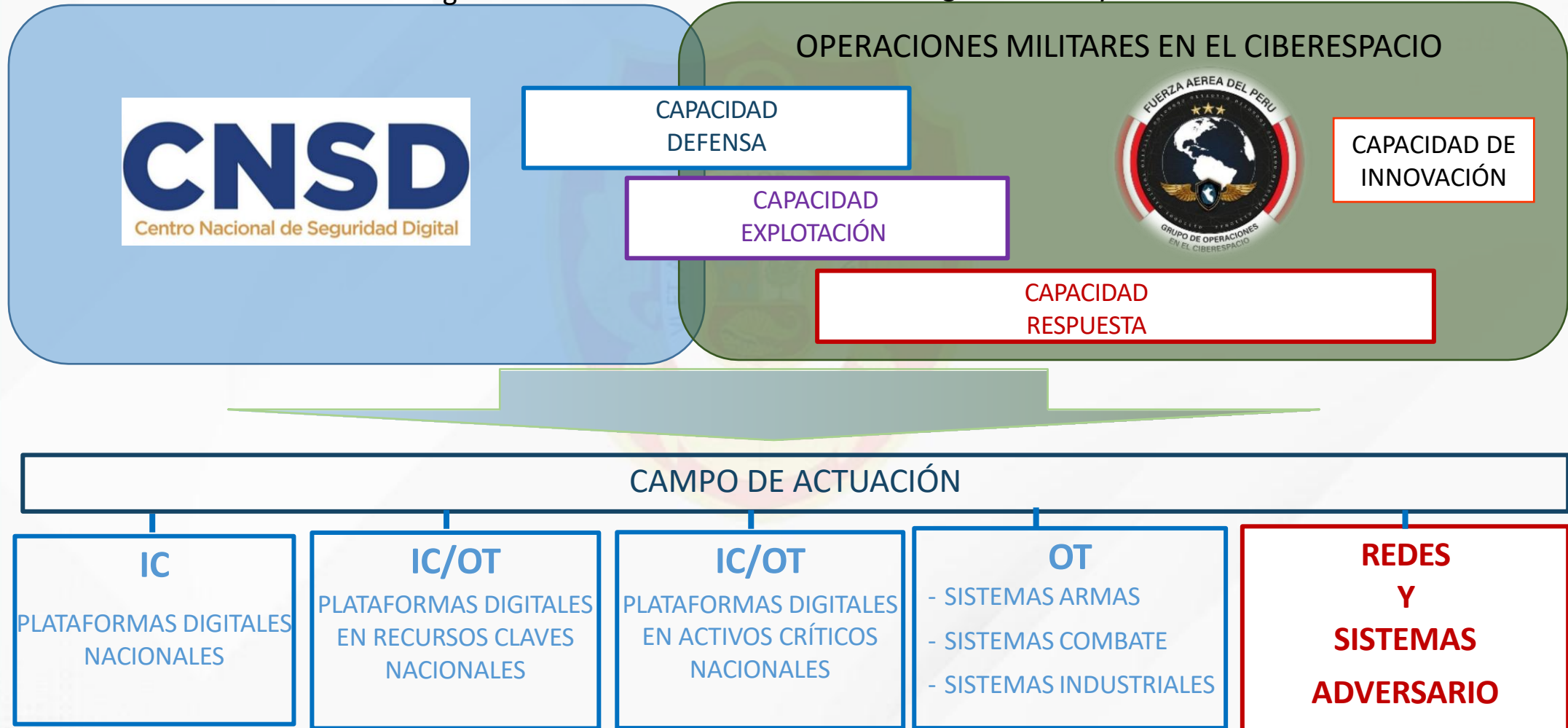
Consiste en la prevención, protección y resiliencia de las diferentes plataformas tecnológicas o sistemas de información ante amenazas cibernéticas, actos hostiles u otros incidentes de seguridad digital; recurriendo a medidas pasivas y activas (Art 6.a, DS° 017-PCM 2024)

Consiste en limitar o negar, temporal o permanentemente, el uso del ciberespacio del objetivo militar mediante la degradación o neutralización de sus sistemas, impactando en sus capacidades; recurriendo a medidas activas (Art 6.c, DS° 017-PCM 2024)

MARCO LEGAL EN EL CIBERESPACIO

DECRETO URGENCIA N° 007-2020-PCM
Marco de Confianza Digital

DECRETO SUPREMO N° 17-2024-PCM
Reglamento Ley Ciberdefensa



En ABRL 2024 EL MINDEF SOLICITA FACULTADES LEGISLATIVAS: ADECUACIÓN LEY 30999 DE NORMAS FFAA

LEY 30999, LEY DE CIBERDEFENSA

SEGUNDA. Modificaciones a normas de las FFAA en materia de ciberdefensa

Presenta las **modificaciones, derogaciones e incorporaciones** a las normas correspondientes a las Fuerzas Armadas en materia de la presente ley.

Modificar las leyes de las Fuerzas Armadas con el objeto de **incorporar** la competencia en CIBERDEFENSA, así como precisar la ubicación del órgano de línea en la estructura organizacional de cada una de ellas, teniendo la urgencia por el principio de **legalidad**

EXISTEN
DESDE:

COMANDANCIA DE CIBERDEFENSA DE LA
MARINA DE GUERRA DEL PERÚ
(RESOLUCIÓN CMDTE GRAL)



21 Feb 2019



CITELE-CENTRO DE CIBERDEFENSA DEL
EJÉRCITO DEL PERÚ
(RESOLUCIÓN CMDTE GRAL)



29 Oct 2018

COMANDO OPERACIONAL DE
CIBERDEFENSA-COCID
20 ene 2020
(Ámbito de competencia, funciones)

COMEC-CENTRO DE OPERACIONES
CIBERESPACIALES DE LA FUERZA AÉREA DEL PERÚ
DL 1139 Y DS 008-2023, 07 Oct 2023



21 Dic 2019

LEYES DE LAS FFAA: DL 1136, DL 1137, DL 1138

MODIFICACIONES

ARTICULO 3. Ámbito de competencia

ARTÍCULO 4. Funciones

ARTICULO 5. Organización básica (EP,MGP)

ARTÍCULO 7. Funciones CG

INCLUSIÓN

ARTÍCULO XX. Desarrollar función del órgano de línea. (EP,MGP)

ARTÍCULO XX. APLICACIÓN DE RECURSOS ESPECIALES. Procesos de capacidades de CIBERDEFENSA

CUMPLIR LA MISIÓN DEL COCID, IMPACTANDO EN LA PROTECCIÓN EN EL CIBERESPACIO DE LOS ACN (56% Alta incidencia digital) Y RC MANTENIENDO LAS CAPACIDADES NACIONALES

EL 2024 EL MINDEF SOLICITA FACULTADES LEGISLATIVAS: ADECUACIÓN LEY 30999 DE NORMAS FFAA

El 28 de mayo 2024 el Ministro de
Defensa sustenta adecuación de las
normas de las FFAA a la Ley 30999

Aprobado en el Pleno del Congreso el
14 de junio 2024 en 1ra votación, el
01 julio en 2da votación y el 4 de julio
se público en el Peruano Ley 32089



CONGRESO
TV DIGITAL

SESIÓN ORDINARIA

VIVO

COMISIÓN DE CONSTITUCIÓN Y REGLAMENTO

f CongresoPeru | @congresodelperu | x congresoperu | congresoperu | congresodelperu | congresodelarepublicadelperu

LEY QUE DELEGA EN EL PODER EJECUTIVO LA FACULTAD DE
LEGISLAR EN MATERIAS DE REACTIVACIÓN ECONÓMICA,
SIMPLIFICACIÓN Y CALIDAD REGULATORIA, ACTIVIDAD EMPRESARIAL
DEL ESTADO, SEGURIDAD CIUDADANA Y DEFENSA NACIONAL

2.10. Seguridad y defensa nacional en el ámbito de inteligencia,
contrainteligencia y seguridad digital

2.10.3. Modificar el Decreto Legislativo 1136, Decreto Legislativo del
Comando Conjunto de las Fuerzas Armadas; el Decreto Legislativo
1137, Ley del Ejército del Perú; y el Decreto Legislativo 1138, Ley de
la Marina de Guerra del Perú, con el objeto de incluir en cada una la
competencia en ciberdefensa, así como precisar la ubicación del
órgano de línea en la estructura organizacional de cada institución
militar.

EN OCTUBRE 2024 PRESENTACIÓN DE EN EL CONSEJO DE MINISTROS DE PROYECTOS DE DECRETOS LEGISLATIVOS QUE MODIFICAN LAS LEYES DEL CCFFAA,EP Y MGP



- D.L. N° 1136, Decreto Legislativo del CCFFAA
- D.L. N° 1137, Ley del Ejército del Perú
- D.L. N° 1138, Ley de la Marina de Guerra del Perú

PUBLICACIÓN EN EL DIARIO EL PERUANO 03 SET 2024

DECRETO LEGISLATIVO Nº 1639

DECRETO LEGISLATIVO QUE MODIFICA EL
DECRETO LEGISLATIVO Nº 1136,
DECRETO LEGISLATIVO DEL COMANDO
CONJUNTO DE LAS FUERZAS ARMADAS

**Competencia y funciones de
ciberdefensa**

DECRETO LEGISLATIVO Nº 1640

DECRETO LEGISLATIVO QUE MODIFICA EL
DECRETO LEGISLATIVO Nº 1137,
LEY DEL EJÉRCITO DEL PERÚ

**Comando de Operaciones
Cibernéticas**

DECRETO LEGISLATIVO Nº 1641

DECRETO LEGISLATIVO QUE MODIFICA EL
DECRETO LEGISLATIVO Nº 1138,
LEY DE LA MARINA DE GUERRA DEL PERÚ

**Comandancia de
Ciberdefensa**

CON RM N.º 00571-2025-DE 15 MAY 2025 SE CREO FUNCIONALMENTE LA DIRECCIÓN DEL
CIBERESPACIO Y TECNOLOGIAS EMERGENTES EN DIGEPE/VPD/MINDEF

PUBLICACIÓN EN EL DIARIO EL PERUANO 05 JUL 2025

DECRETO SUPREMO N° 004-2025-DE
MODIFICA EL REG DE LEY CCFFAA

DECRETO SUPREMO N° 005-2025-DE
MODIFICA EL REG DE LEY EP

DECRETO SUPREMO N° 006-2025-DE
MODIFICA EL REG DE LEY MAGP

El espacio cibernético, una dimensión de los conflictos del siglo XXI, Universidad Internacional de La Rioja (UNIR)- 28 ABR 2023



Rafael García Hernández, comandante del Mando Conjunto de Ciberespacio del Estado Mayor de la Defensa de España, habló en una sesión organizada por la Universidad Internacional de La Rioja. (28 ABR 2023)

“Cada vez va a ser más importante tener fuerzas de ciberdefensa, eso va a ser absolutamente crucial en tiempos de conflicto pero también en tiempos de paz. Es un arma barata, con una capacidad de disuasión importante, capaz de inutilizar servicios críticos de un país y disuadirlo de no llegar o avanzar en un conflicto”, concluyó.

FUENTE: Universidad Internacional de La Rioja (UNIR). (2024, 16 de julio). El máximo responsable de la ciberseguridad en el Estado Mayor de la Defensa de España, en UNIR: “Habíamos sobrevalorado las capacidades de Rusia en el ciberespacio”. UNIR. <https://www.unir.net/actualidad/vida-academica/el-maximo-responsable-de-la-ciberseguridad-en-el-estado-mayor-de-la-defensa-de-espana-en-unir-habiamos-sobrevalorado-las-capacidades-de-rusia-en-el-ciberespacio/>

**Rusia hackeó una compañía
satelital estadounidense una
hora antes de la invasión de
Ucrania**



FUENTE: DW Español. (2023, 9 de abril). *Archivos Vulkan: detalles inéditos de una ciberguerra global* [Video]. YouTube. <https://www.youtube.com/watch?v=ZAR2Ywq0YG4>

≡ **EL PAÍS**

ANUAL, US\$ 9



GUERRA DE RUSIA EN UCRANIA >

E La guerra cibernética entre Ucrania y Rusia se intensifica en paralelo al conflicto militar

El Registro Civil de Kiev colapsó el 19 de diciembre por uno de los pirateos informáticos más graves desde el inicio de la invasión, un tipo de acciones que aumentó en 2024 casi un 70%

LOLA HIERRO (ENVIADA ESPECIAL)

Kiev - 18 ENE 2025 - 23:40 PET

Martínez, A. (2025, 19 de enero). *La guerra cibernética entre Ucrania y Rusia se intensifica en paralelo al conflicto militar*. El País. <https://elpais.com/internacional/2025-01-19/la-guerra-cibernetica-entre-ucrania-y-rusia-se-intensifica-en-paralelo-al-conflicto-militar.html>

Departures

CHECK-IN GATE

DESTINATION

FLIGHT

TIME DELAY



Reportan retrasos y cancelaciones en decenas de vuelos **CIBERATAQUES A AEROPUERTOS DE EUROPA**

FUENTE: FRANCE 24 Español. (20 SET 2025). Ciberataque desata caos y molestias entre pasajeros en aeropuertos europeos [Video]. YouTube. https://www.youtube.com/watch?v=0tbFerWH_6U

REFLEXIONES FINALES

La realidad de hoy es que la tecnología es cada vez más sofisticada, y los ciberatacantes encontrarán cada vez más formas de lograr su objetivo. Por eso, **para evitar el peor de los escenarios, como que los ciberataques paralicen todo un país**, los gobiernos deben atacar el problema de raíz:

Activos Críticos Nacionales y Recursos Claves deben estar protegidos con plataformas informáticas de la última generación e **invertir en la Capacidad de Ciberseguridad y las Fuerzas Armadas deben contar con capacidades de Ciberdefensa a fin de poder ser EL ÚLTIMO BASTIÓN DEL CIBERESPACIO;**

y quizás lo más importante, las entidades y los países deben **también invertir en al formación de una nueva generación de expertos** en, lo cual requerirá tiempo, dinero y compromiso político.

Estas acciones deben tomarse, pues **la amenaza de los ciberataques sea por razones económicas, culturales o políticas ha llegado para quedarse.**

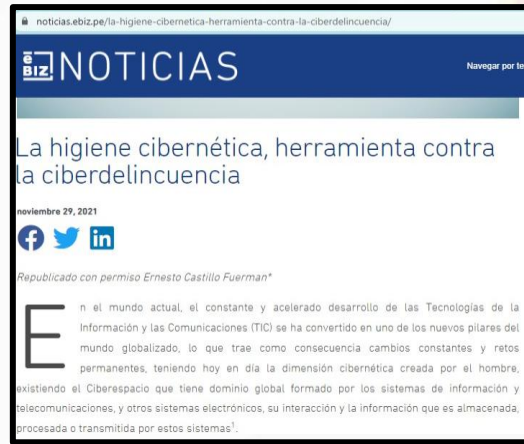
<https://ceep.mil.pe/2021/11/18/politica-sectorial-de-ciberdefensa-una-necesidad-impostergable/>

<https://noticias.ebiz.pe/la-higiene-cibernetica-herramienta-contr-la-ciberdelincuencia/>

<https://noticias.ebiz.pe/la-ciberdefensa-en-el-desarrollo-y-la-seguridad-nacional/>

<https://ebiz.pe/noticias/especial-rgto-ley-de-ciberdefensa-ernesto-castillo/>

<https://ebiz.pe/noticias/estrategia-nacional-de-ciberseguridad-del-peru-2026-2028-analisis-critico-y-propuestas-de-fortalecimiento/>



TRANSFORMACIÓN DIGITAL SIN SEGURIDAD: **AMENAZA**
TRANSFORMACIÓN DIGITAL CON SEGURIDAD: **DESARROLLO**