

COMITÉ DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA

PLAN DE GOBIERNO DIGITAL 2025-2030

<p>Secretaria General Presidente CGD María Cecilia Chumbe Rodríguez</p>	<p>Directora General de la Oficina General de Recursos Humanos Nedy Alcántara Lino</p>
<p>Secretario Técnico Jefe de la Oficina General de Tecnologías de la Información y Estadística Ernesto Castillo Fuerman</p>	<p>Director General de Planeamiento y Presupuesto Juan Izquierdo Herrera</p>
<p>Jefe de la Oficina General de Asesoría Jurídica José Luis Rojas Alcocer</p>	<p>Jefe de la Oficina General de Gestión Documental Jorge Cardo Velit</p>
<p>Oficial de Seguridad Digital Ministerio de Defensa Pedro Benjamin Garay Campos</p>	<p>Líder de Gobierno Y Transformación Digital Miguel Balta Sevillano</p>

HOJA DE CONTROL DE CAMBIOS				
Versión	Fecha de Revisión	Responsable del cambio	Cargo responsable	Resumen
1.0	30.01.2025	Comité de Gobierno Digital	Comité de Gobierno Digital	Versión inicial

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código: Versión: Fecha: Clasificación:	PGD 2025-2030 1.0 30/01/2025 Público
--	---	---	---

TABLA DE CONTENIDO

I.	INTRODUCCIÓN	4
II.	BASE LEGAL.....	4
III.	ENFOQUE ESTRATÉGICO DE LA ENTIDAD.....	7
	3.1. POLÍTICAS.....	7
	3.2. PLAN ESTRATÉGICO SECTORIAL MULTIANUAL - PESEM 2024-2030.....	9
	3.3. PLAN ESTRATÉGICO INSTITUCIONAL 2025-2030	10
	3.4.1. OBJETIVOS ESTRATÉGICOS INSTITUCIONALES DEL SECTOR DEFENSA	10
	3.4.1.1. AEI 8.2 CIBERSEGURIDAD RESILIENTE EN EL SECTOR DEFENSA	10
	3.4.1.2. AEI 8.3 TRASFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	15
	3.4. ORGANIGRAMA INSTITUCIONAL.....	19
IV.	SITUACIÓN ACTUAL DEL GOBIERNO DIGITAL EN LA ENTIDAD.....	20
	4.1. AEI 5.3: CIBERSEGURIDAD RESILIENTE EN LAS INSTITUCIONES DEL MINISTERIO DE DEFENSA	20
	4.2. AEI 10.3: TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN IMPLEMENTADAS PARA MEJORAR LA GESTIÓN INSTITUCIONAL	23
	4.3. RELACION DE LOS PROYECTOS EN EL 2024.....	29
V.	OBJETIVOS DE GOBIERNO DIGITAL	31
	5.1. DESAFÍOS DE GOBIERNO DIGITAL.....	31
	5.2. OBJETIVO DE GOBIERNO DIGITAL	35
	5.2.1. Objetivo 01: Transformación digital implementada en el Ministerio de Defensa	35
	5.2.2. Objetivo 02: Ciberseguridad resiliente en el sector defensa.....	38
	5.3. MAPA ESTRATÉGICO DE GOBIERNO DIGITAL.....	41
VI.	PROYECTOS DE GOBIERNO DIGITAL.....	43
	6.1. LISTADO DE PROYECTO DE GOBIERNO DIGITAL.....	44
	6.1.1. Evaluación y Priorización.....	44
	6.1.2. Presupuesto Estimado	53
	6.1.3. Cronograma de la Implementación del Portafolio de Proyectos	56
	6.2. FICHAS DE PROYECTOS DE GOBIERNO DIGITAL	60

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código: Versión: Fecha: Clasificación:	PGD 2025-2030 1.0 30/01/2025 Público
---	---	---	---

I. INTRODUCCIÓN

El presente “Plan de Gobierno Digital 2025-2030” ha sido elaborado considerando la priorización de la Alta Dirección para la implementación del Gobierno y Transformación Digital en el Ministerio de Defensa; lo que ha sido gestionado mediante el Comité de Gobierno Digital cuya conformación fue actualizada con la Resolución Ministerial N° 0108-2021-DE del 08 de marzo del 2021.

El Ministerio de Defensa, creado mediante la Ley N°24654 del 01 de abril de 1987, ha elaborado su primer Plan de Gobierno Digital teniendo como alcance a la Unidad Ejecutora denominada Ministerio de Defensa (OGA) teniendo como objetivo que en esa dirección sean emitidos planes similares en todas las unidades ejecutoras del Sector Defensa en coordinación con la Oficina General de Tecnologías de Información y Estadística, Unidad Orgánica Rectora en Tecnologías de la Información del Sector Defensa.

El proceso de su formulación, ha considerado un trabajo conjunto de los miembros del Comité de Gobierno Digital, ejecutándose las sesiones de presentación de avances y aprobación de los mismos cumpliendo todas las etapas estipuladas en la Resolución de Secretaría de Gobierno Digital N° 005-2018-PCM/SEGDI “Lineamientos para la formulación del Plan de Gobierno Digital” del 13 de diciembre del 2018.

En ese marco, el presente plan se desarrolla el enfoque estratégico institucional en materia de gobierno digital, se expone la situación actual del gobierno digital, se definen objetivos de gobierno digital y finalmente, en base a ello, se define un portafolio de proyectos de gobierno digital para los próximos 6 años, abarcando desde el primer semestre del año 2025 hasta el segundo semestre del año 2025, teniendo como objetivo general “IMPULSAR LA TRANSFORMACIÓN DIGITAL SEGURA EN EL MINISTERIO DE DEFENSA”, con dos objetivos:

01. TRANSFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA
02. CIBERSEGURIDAD RESILIENTE EN EL SECTOR DEFENSA

Con la elaboración del “Plan de Gobierno Digital 2025-2030”, el Ministerio de Defensa establece una dirección estratégica en las tecnologías de la información, buscando continuar su proceso de transformación digital avanzada para la generación de servicios digitales orientados a la ciudadanía generando valor público en todos sus usuarios.

II. BASE LEGAL

- Constitución Política del Perú
- Ley N° 29158 Ley Orgánica del Poder Ejecutivo.
- Ley N° 29733 Ley de Protección de Datos Personales
- Decreto Supremo N°006-2016-DE se aprueban el Reglamento de Organización y Funciones - ROF del Ministerio de Defensa

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código: Versión: Fecha: Clasificación:	PGD 2025-2030 1.0 30/01/2025 Público
---	---	---	---

- Decreto Legislativo N° 1554, que Modifica La Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado
- Ley N° 27269, Ley de Firmas y Certificados Digitales y su Reglamento.
- Ley N°29248, Ley del Servicio Militar.
- Ley N° 27291, Ley que permite la Utilización de Medios Electrónicos para la Comunicación de la Manifestación de Voluntad y la Utilización de la Firma Electrónica.
- Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno digital y su Reglamento.
- Decreto Legislativo N° 604, Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática
- Decreto de Urgencia N° 006-2020, que Crea El Sistema Nacional de Transformación Digital y su reglamento.
- Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital.
- Decreto de Urgencia N° 026-2021, que crea la figura del trabajo remoto.
- Decreto Supremo N° 066-2003-PCM, que fusionan la Subjefatura de Informática del Instituto Nacional de Estadísticas e Informática-INEI y la Presidencia del Consejo de ministros, a través de su Secretaría de Gestión Pública.
- Decreto Supremo N° 029-2021, que aprueba el reglamento del Decreto Legislativo N° 1412, que establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Decreto Supremo N° 066-2011 PCM, que aprueba el Plan de Desarrollo de la Sociedad de la Información en el Perú-La Agenda Digital Peruana 2.0.
- Decreto Supremo N° 083-2011-PCM, que aprueba la Plataforma de Interoperabilidad del Estado Peruano – PIDE.
- Decreto Supremo N°004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
- Decreto Supremo N° 081-2013-PCM, que aprueba la Política Nacional de Gobierno Electrónico 2013-2017.
- Decreto Supremo N° 016-2017-PCM, aprueba la "Estrategia Nacional de Datos Abiertos Gubernamentales del Perú 2017-2021" y el "Modelo de Datos Abiertos Gubernamentales del Perú".
- Decreto Supremo N° 050-2018-PCM, que establece la definición de Seguridad Digital.
- Decreto Supremo N° 033-2018-PCM, que crea la Plataforma Digital Única del Estado Peruano y establece disposiciones adicionales para el desarrollo del Gobierno Digital; y su Decreto Supremo N° 119-2018-PCM, que modifica la Quinta Disposición Complementaria Final del Decreto Supremo N° 033-2018-PCM
- Resolución Ministerial N° 186-2010/DE/SG, que aprueba la Directiva General N° 005-2010-MINDEF/SG/B/01 "Normas para el proceso de Respaldo de la Información del Ministerio de Defensa".
- Resolución Ministerial N° 1018-2014, que aprueba la Directiva General N° 16-2014-MINDEF/SGB/04 denominada "Metodología de Desarrollo de Software y Estándares de Desarrollo"
- Resolución Ministerial N° 372-2014-DE/SG, que aprueba la Directiva General N° 009-2014/MINDEF/SG/B, denominada "Normas para el Mantenimiento Preventivo y Correctivo de Equipos de cómputo y Telecomunicaciones del MINDEF".

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código: Versión: Fecha: Clasificación:	PGD 2025-2030 1.0 30/01/2025 Público
---	---	---	---

- Resolución Ministerial N° 919-2015-DE/SG, que aprueba la Directiva General N° 007-2015/SG/B/04 denominada "Normas para el uso del servicio de Correo Electrónico Institucional en el Ministerio de Defensa".
- Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-SGTD/PCM que aprueba el uso obligatorio de la Norma Técnica Peruano "NTP ISO/IEC 27001".
- Resolución Ministerial N° 01193-2024-DE que aprueba el Mapa de Procesos del Ministerio de Defensa.
- Resolución Ministerial N° 041-2017-PCM, que aprueba uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2016-Ingeniería de Software y Sistemas. Procesos del ciclo de vida del software. 3a Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 035-2017-PCM, aprueba Lineamientos para la implementación del Portal de Transparencia Estándar en las entidades de la Administración Pública.
- Resolución Ministerial N°119-2018-PCM, que dispone la creación de un Comité de Gobierno digital en cada entidad de la Administración Pública.
- Resolución de Secretaría de Gobierno Digital N° 005-2018 PCM/SEGDI, que aprueba los lineamientos para la formulación del Plan de Gobierno Digital-PGD.
- Resolución de Secretaría de Gobierno Digital N° 004-2018 PCM/SEGDI, que aprueba los lineamientos del Líder de Gobierno Digital.
- Resolución de Secretaría de Gobierno Digital N° 002-2018-PCM, que aprueba los Lineamientos para la suscripción de un Acuerdo de Nivel de Servicio (ANS)
- Resolución Ministerial N° 1825-2018-DE/SG, que aprueba la Directiva General N° 017-2018/MINDEF/SG-OGGD "Directiva General de Gestión Documental".
- Directiva N° 001-2019-PCM/SEGDI, "Directiva para compartir y usar Software Público Peruano
- Resolución Ministerial N° 1961-2019-DE/SG, que aprueba la Directiva General N° 020-2019-MINDEF/SG-OGTIE "Normas para la Administración del Portal de Transparencia Estándar del Ministerio de Defensa".
- Resolución Ministerial N° 1913-2019-DE/SG, que aprueba la Directiva General N° 019-2019-MINDEF/SG-OGTIE "Normas para la administración y uso de la Intranet del Ministerio de Defensa".
- Resolución Ministerial N° 121-2020, que aprueba la modificación del Plan Estratégico Sectorial Multianual-PESEM 2017-2025.
- Resolución Ministerial N° 276-2020. Que aprueba el Plan Estratégico Institucional – PEI 2020-2025 del Ministerio de Defensa.
- Resolución Ministerial N°108-2021-DE, que designa la conformación del Comité de Gobierno Digital del Ministerio de Defensa
- Resolución Ministerial N° 109-2021-DE, que designa al Líder de Gobierno Digital
- Resolución Ministerial N° 086-2021-DE, que designa al Oficial de Seguridad Digital.
- Resolución Ministerial N° 0179-021-DE, que designa al responsable del Software Público
- Resolución Ministerial N° 355-2021-DE, que constituye el "Equipo de Respuestas ante Incidentes de Seguridad Digital del Ministerio de Defensa".
- Directiva N° 005-2016-EF/21.01 que indica que la depreciación de un equipo de cómputo es de 4 años con una tasa del 25%.

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código: Versión: Fecha: Clasificación:	PGD 2025-2030 1.0 30/01/2025 Público
--	---	---	---

III. ENFOQUE ESTRATÉGICO DE LA ENTIDAD

3.1. POLÍTICAS

Reglamento que regula las Políticas Nacionales, aprobado con D.S. N° 029-2018-PCM y su modificatoria.¹

ART 6.2 del DS N° 029-2018-PCM: “Están contenidas en el Acuerdo Nacional y se concretan en el Plan Estratégico de Desarrollo Nacional”.

3.1.1.POLÍTICAS DE ESTADO DEL ACUERDO NACIONAL OBJETIVOS DEL ACUERDO NACIONAL ²

I. Democracia y Estado de Derecho (lograr la paz y el desarrollo del país)

9. Política de Seguridad Y Defensa Nacional

“Nos comprometemos a mantener una política de seguridad nacional que garantice la independencia, soberanía, integridad territorial y la salvaguarda de los intereses nacionales. Consideramos que esta es una tarea que involucra a la sociedad en su conjunto, a los organismos de conducción del Estado, en especial a las Fuerzas Armadas, en el marco de la Constitución y las leyes. En tal sentido, nos comprometemos a prevenir y afrontar cualquier amenaza externa o interna que ponga en peligro la paz social, la seguridad integral y el bienestar general”

AMENAZA A LA SEGURIDAD NACIONAL (Plan de Inteligencia Nacional)
Afectación a la seguridad digital

IV. Estado eficiente, transparente y descentralizado

35. Política Sociedad de la Información y Sociedad del Conocimiento

Nos comprometemos a impulsar una sociedad de la información hacia una sociedad del conocimiento al desarrollo integral y sostenible, en base al ejercicio pleno de las libertades de las personas, y capaz de identificar, producir, transformar, utilizar y difundir en todas las dimensiones incluyendo la dimensión ambiental. Promovemos las Tecnologías de información y Comunicaciones (TIC) como medio para fortalecer la gobernabilidad democrática y el desarrollo sostenible, a través de un servicio moderno, transparente, eficiente, eficaz, efectivo y descentralizado al ciudadano.

Lineamiento de Política

i. Diseñara políticas y la regulación en materia de sociedad de la información y del conocimiento teniendo como base los principios de internet libre, abierto, neutro y para todos, así como el adecuado resguardo de la seguridad de la información.

3.1.2.PLAN ESTRATÉGICO DE DESARROLLO NACIONAL AL 2050 ³

- OBJETIVO NACIONAL 2

Gestionar el territorio de manera sostenible a fin de prevenir y reducir los riesgos y amenazas que afectan a las personas y sus medios de vida, con el uso intensivo del conocimiento y las comunicaciones, reconociendo la diversidad geográfica y cultural, en un contexto de cambio climático.

¹ <https://www.gob.pe/institucion/pcm/normas-legales/1933839-029-2018-pcm>

² : Acuerdo Nacional: <https://acuerdonacional.pe/politicas-de-estado-del-acuerdo-nacional/politicas-de-estado/politicas-de-estado-castellano/>

³ <https://cdn.www.gob.pe/uploads/document/file/5133337/Peru%20-%20Plan%20Estrategico%20de%20Desarrollo%20Nacional%20al%202050.pdf?v=1694719008>

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código: Versión: Fecha: Clasificación:	PGD 2025-2030 1.0 30/01/2025 Público
--	---	---	---

TEMÁTICA: SEGURIDAD NACIONAL

OE 2.8 Garantizar la defensa de los intereses nacionales destinados a la paz y seguridad internacional.

Sub temática: Seguridad y confianza digital

AE 2.8.3 Garantizar el uso, desarrollo y gestión del entorno digital o ciberespacio frente a los riesgos que afectan la seguridad y confianza de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales con énfasis en el fortalecimiento de la capacidad de coordinación de los actores competentes.

- **OBJETIVO NACIONAL 3**

Elevar los niveles de competitividad y productividad con empleo decente y en base al aprovechamiento sostenible de los recursos, el capital humano, el uso intensivo de la ciencia y tecnología, y la transformación digital del país.

TEMÁTICA: CIENCIA, TECNOLOGÍA E INNOVACIÓN Y TRANSFORMACIÓN DIGITAL

OE 3.5: Elevar la capacidad científica y de Innovación tecnológica del país, en base a la investigación, creación, adaptación y transferencia tecnológica y científica, y el impulso al proceso nacional de transformación digital; favoreciendo la articulación entre la academia, el Estado, los sectores productivos y la Sociedad Civil.

- **OBJETIVO NACIONAL 4**

Garantizar una sociedad justa, democrática, pacífica y un Estado efectivo al servicio de las personas, en base al diálogo, la concertación nacional y el fortalecimiento de las instituciones.

TEMÁTICA: EFECTIVIDAD DE LA GESTIÓN PÚBLICA

OE 4.5. Garantizar intervenciones públicas de calidad que respondan de manera oportuna a las necesidades y expectativas de las personas, tomando en cuenta la heterogeneidad territorial, social, económica, cultural e intergeneracional del país, con énfasis en el fortalecimiento de la cultura de integridad y de lucha contra la corrupción, y la transformación digital.

Sub Temática Transformación digital

AE.4.5.4. Lograr el gobierno y la transformación digital en las entidades públicas, mediante el aprovechamiento de las tecnologías digitales, el impulso del ecosistema digital, el avance de la innovación digital y ciudadana, la publicación de los datos abiertos y fortaleciendo

3.1.3.LA POLÍTICA NACIONAL MULTISECTORIAL DE SEGURIDAD Y DEFENSA NACIONAL AL 2030 (*)⁴

OE 3. Alcanzar las condiciones necesarias contribuyentes a la Seguridad Nacional

3.1. Fortalecer las capacidades y mecanismos destinados a la promoción de la igualdad de oportunidades en las aéreas críticas, zonas vulnerables y de difícil acceso.

⁴<https://cdn.www.gob.pe/uploads/document/file/3350044/RESUMEN%20EJECUTIVO%20PNMSDN%20AL%202030.pdf.pdf>

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código: Versión: Fecha: Clasificación:	PGD 2025-2030 1.0 30/01/2025 Público
--	---	---	---

- 3.2. Intensificar la construcción de infraestructura pública crítica vinculada a la Seguridad Nacional.
- 3.3. Mejorar los instrumentos y mecanismos de preservación y protección del ambiente, especialmente en la amazonia, con énfasis en la adaptación del Perú al Cambio Climático.
- 3.4. Promover el desarrollo de las actividades de la ciencia, tecnología e innovación tecnológica en función de las necesidades de la seguridad y defensa.

3.1.4.LA POLÍTICA DE TRANSFORMACIÓN DIGITAL AL 2030⁵

OBJETIVO: INCREMENTO DEL EJERCICIO DE LA CIUDADANÍA DIGITAL

- Objetivo prioritario 1: Garantizar el acceso inclusivo, seguro y de calidad al entorno digital a todas las personas.
- Objetivo prioritario 2: Vincular la economía digital a los procesos productivos sostenibles del país.
- Objetivo prioritario 3: Garantizar la disponibilidad de servicios públicos digitales inclusivos, predictivos y empáticos con la ciudadanía.
- Objetivo prioritario 4: Fortalecer el talento digital en todas las personas.
- Objetivo prioritario 5: Consolidar la seguridad y confianza digital en la sociedad
- Objetivo prioritario 6: Garantizar el uso ético y adopción de las tecnologías exponenciales y la innovación en la sociedad.

3.2. PLAN ESTRATÉGICO SECTORIAL MULTIANUAL - PESEM 2024-2030

OE 1: GARANTIZAR LA SOBERANÍA, INTEGRIDAD TERRITORIAL E INDEPENDENCIA DEL PAÍS

AE 1.2 Fortalecer la gestión del sector Defensa

Tiene como objetivo principal optimizar los procesos administrativos, operativos y estratégicos del sector Defensa para garantizar una gestión eficiente y efectiva en el cumplimiento de su misión.

El fortalecimiento de la gestión busca mejorar las capacidades organizativas, normativas y operativas de las instituciones que integran el sector Defensa, con un enfoque en la modernización, transparencia y rendición de cuentas.

⁵https://cdn.www.gob.pe/uploads/document/file/4912655/Pol%C3%ADtica%20Nacional%20de%20Transformaci%C3%B3n%20Digital%20al%202030_Resumen%20ejecutivo.pdf?v=1690558614

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código: Versión: Fecha: Clasificación:	PGD 2025-2030 1.0 30/01/2025 Público
--	---	---	---

3.3. PLAN ESTRATÉGICO INSTITUCIONAL 2025-2030

El plan estratégico institucional 2025-2030 contiene 8 objetivos estratégicos institucionales.

3.4.1. OBJETIVOS ESTRATÉGICOS INSTITUCIONALES DEL SECTOR DEFENSA

El Objetivo Estratégico Institucional que la OGTIE participa es:

OEI N°8: FORTALECER LA GESTIÓN CON INTEGRIDAD Y LUCHA CONTRA LA CORRUPCIÓN

El Objetivo de Fortalecer la gestión con integridad y lucha contra la corrupción, tiene dos actividades estratégicas que corresponden a la Oficina General de Tecnologías de la Información y Estadística; los cuales son:

- AEI 8.2 CIBERSEGURIDAD RESILIENTE EN EL SECTOR DEFENSA
- AEI 8.3 TRASFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA

A continuación, se explicará cada uno de ellos en un enfoque estratégico para la Institución:

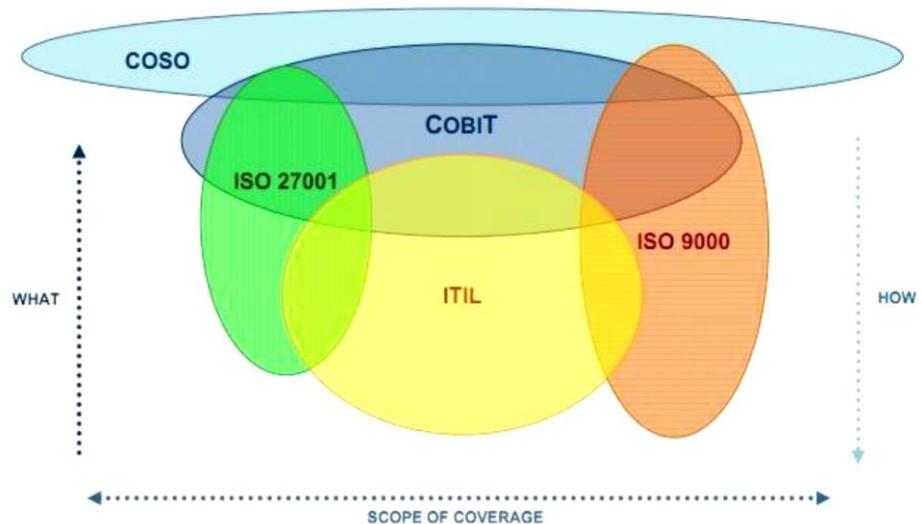
3.4.1.1. AEI 8.2 CIBERSEGURIDAD RESILIENTE EN EL SECTOR DEFENSA

Se está utilizando como INDICADOR el NIST Cybersecurity Framework 1.1. que es una guía, basada en estándares, directrices y prácticas existentes para que las organizaciones gestionen y reduzcan mejor el riesgo de ciberseguridad.

El National Institute of Standards and Technology (NIST) ofrece un marco robusto de normas y buenas prácticas que se pueden integrar de manera estratégica en un plan de gobierno digital para el Perú. Con un enfoque en la seguridad, interoperabilidad, y protección de la información, los estándares del NIST son ampliamente reconocidos y aplicados internacionalmente para fortalecer la resiliencia digital en instituciones gubernamentales. Incorporar los lineamientos del NIST permite no solo mitigar riesgos cibernéticos, sino también impulsar la confianza ciudadana en los servicios digitales.

El National Institute of Standards and Technology (NIST) proporciona un conjunto sólido de normas y buenas prácticas que resultan esenciales para el desarrollo de un plan de gobierno digital efectivo y seguro en el Perú. Reconocido a nivel internacional, el marco del NIST abarca áreas clave como la ciberseguridad, la interoperabilidad de sistemas y la protección de la información, ofreciendo una base confiable para construir servicios digitales que sean resilientes y alineados con los más altos estándares globales.

En un mundo cada vez más digitalizado, donde la tecnología permea todos los aspectos de la vida, contar con un marco de referencia sólido y confiable para la implementación de iniciativas de gobierno digital es esencial. El Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) de los Estados Unidos, reconocido mundialmente por su liderazgo en el desarrollo de estándares y guías en materia de ciberseguridad y tecnología, ofrece un conjunto de herramientas y metodologías invaluable para asegurar la eficacia, seguridad y confiabilidad de los sistemas de información gubernamentales.



El NIST como Pilar Fundamental para la Transformación Digital en Perú

En el contexto peruano, la adopción de estos estándares es clave para fortalecer la transformación digital bajo principios de transparencia y accesibilidad, además de facilitar la armonización con otras normativas globales.

Integrar las pautas del NIST en el contexto peruano representa un paso estratégico para fortalecer la transformación digital del Estado, promoviendo un entorno digital seguro, accesible y transparente para los ciudadanos. Además, esta adopción facilita la armonización con normativas internacionales y aumenta la confianza pública en los servicios digitales gubernamentales, estableciendo una base sólida para un crecimiento digital sostenible y una mayor eficiencia en los servicios del Estado.

¿Por qué el NIST es relevante para Perú?

- **Universalidad:** Los estándares del NIST son aplicables a cualquier organización, independientemente de su tamaño o sector.
- **Flexibilidad:** Los estándares del NIST ofrecen un marco general que puede adaptarse a las necesidades específicas de cada organización.
- **Reconocimiento internacional:** El NIST es una autoridad mundial en materia de estándares, lo que otorga a las organizaciones que los adoptan un mayor prestigio y credibilidad.
- **Soporte técnico:** El NIST ofrece una amplia gama de recursos y herramientas para ayudar a las organizaciones a implementar sus estándares.

Aspectos clave del NIST a considerar en el plan de gobierno digital de Perú:

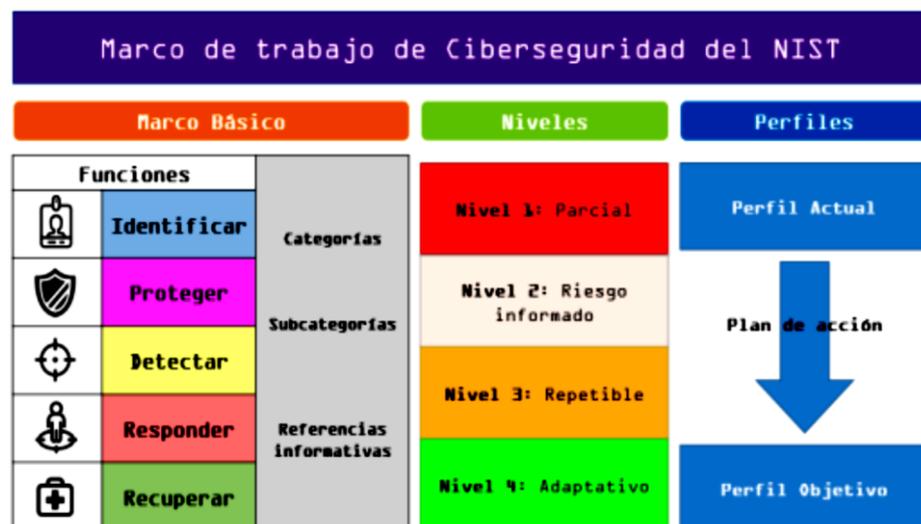
- **Cyberseguridad:** El NIST ofrece un amplio catálogo de publicaciones y marcos de trabajo para la gestión de riesgos cibernéticos, la protección de la infraestructura crítica y la respuesta a incidentes.
- **Interoperabilidad:** Los estándares del NIST promueven la interoperabilidad de los sistemas de información, lo que facilita la integración de datos y la colaboración entre diferentes agencias gubernamentales.

- **Cloud Computing:** El NIST ha desarrollado estándares y guías para la adopción segura y eficiente de servicios en la nube.
- **Internet de las Cosas (IoT):** El NIST ofrece recomendaciones para asegurar la privacidad, seguridad y confiabilidad de los dispositivos IoT.
- **Inteligencia Artificial:** El NIST está trabajando en el desarrollo de estándares para la ética en la inteligencia artificial y la gestión de riesgos asociados a esta tecnología.

La incorporación de los estándares y prácticas del NIST en el plan de gobierno digital de MINDEF representa un paso estratégico hacia la construcción de una administración pública moderna, eficiente y resiliente. Al adoptar estos estándares, el país no solo se alinea con las mejores prácticas internacionales, sino que también fortalece su capacidad para:

- **Proteger la información gubernamental:** Los estándares del NIST proporcionan un conjunto de controles de seguridad robustos para proteger la confidencialidad, integridad y disponibilidad de los datos gubernamentales, mitigando el riesgo de ciberataques y otras amenazas.
- **Mejorar la interoperabilidad de los sistemas:** Al establecer estándares comunes para la interoperabilidad, se facilita la integración de diferentes sistemas y aplicaciones gubernamentales, lo que a su vez agiliza los procesos y reduce costos.
- **Aumentar la confianza de los ciudadanos:** La implementación de estándares internacionales reconocidos, como los del NIST, genera confianza en la ciudadanía al garantizar que la información gubernamental se maneja de manera segura y transparente.
- **Fomentar la innovación:** Los estándares del NIST promueven la innovación al proporcionar un marco de referencia sólido para el desarrollo de nuevas tecnologías y soluciones.

La incorporación de los estándares y prácticas del NIST en el plan de gobierno digital de MINDEF es una inversión estratégica que permitirá al país avanzar hacia una administración pública más moderna, eficiente y segura.



APLICACIÓN DEL NIST EN EL MINISTERIO DE DEFENSA DEL PERÚ

El Instituto Nacional de Estándares y Tecnología (NIST) ofrece un marco de referencia invaluable para el Ministerio de Defensa del Perú, especialmente en lo que respecta a la ciberseguridad y la gestión de riesgos. Dada la naturaleza crítica de las operaciones militares y la creciente dependencia de sistemas informáticos, la implementación de los estándares NIST resulta esencial para garantizar la seguridad nacional y la protección de activos estratégicos.

¿Por qué el NIST es relevante para el Ministerio de Defensa del Perú?

- **Ciberseguridad:** El sector defensa es un objetivo constante de ataques cibernéticos. Los estándares NIST proporcionan un conjunto de prácticas y controles de seguridad que ayudan a proteger sistemas de armas, comunicaciones, inteligencia y otros sistemas críticos.
- **Gestión de riesgos:** El NIST ofrece un enfoque sistemático para identificar, evaluar y mitigar los riesgos cibernéticos, permitiendo a las Fuerzas Armadas tomar decisiones informadas sobre la asignación de recursos y la inversión en seguridad.
- **Interoperabilidad:** Los estándares NIST promueven la interoperabilidad entre diferentes sistemas y plataformas, facilitando la colaboración entre diferentes unidades y ramas de las Fuerzas Armadas.
- **Resiliencia:** Al adoptar los estándares NIST, las Fuerzas Armadas pueden mejorar su capacidad para recuperarse de incidentes cibernéticos y garantizar la continuidad de las operaciones

Tabla 1: Identificadores únicos de función y categoría

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR.AC	Gestión de identidad y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de seguridad
		DE.DP	Procesos de detección
RS	Responder	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código: Versión: Fecha: Clasificación:	PGD 2025-2030 1.0 30/01/2025 Público
--	---	---	---

ÁREAS ESPECÍFICAS DE APLICACIÓN:

- **Protección de la infraestructura crítica:** Los sistemas de defensa, como bases militares, sistemas de comando y control, y redes de comunicaciones, son considerados infraestructura crítica. Los estándares NIST proporcionan un conjunto de controles de seguridad para proteger estos activos.
- **Seguridad de la información clasificada:** El manejo de información clasificada es fundamental para la seguridad nacional. Los estándares NIST ofrecen pautas para proteger la confidencialidad, integridad y disponibilidad de esta información.
- **Ciberdefensa:** Los estándares NIST pueden ser utilizados para desarrollar capacidades de ciberdefensa, incluyendo la detección de amenazas, la respuesta a incidentes y la recuperación.
- **Adquisición de tecnología:** Al establecer requisitos de seguridad basados en los estándares NIST, el Ministerio de Defensa puede garantizar que los sistemas y equipos adquiridos cumplan con los más altos estándares de seguridad.

BENEFICIOS PARA EL MINISTERIO DE DEFENSA DEL PERÚ:

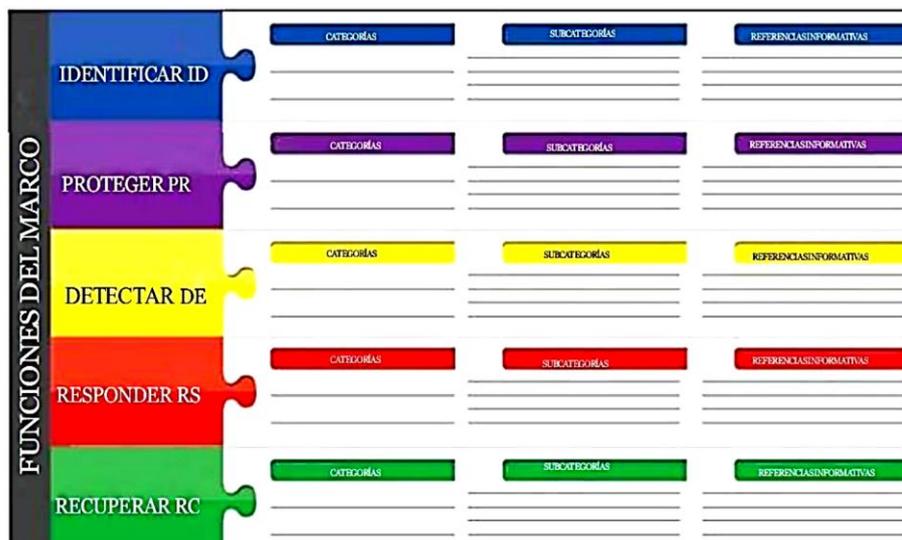
- **Mayor seguridad:** La implementación de los estándares NIST reduce el riesgo de sufrir ataques cibernéticos y la pérdida de información confidencial.
- **Mejor toma de decisiones:** Los estándares NIST proporcionan una base sólida para la toma de decisiones estratégicas en materia de ciberseguridad.
- **Aumento de la confianza:** La adopción de estándares internacionales reconocidos, como los del NIST, aumenta la confianza de los aliados y socios internacionales.
- **Mayor eficiencia:** Al mejorar la seguridad y la interoperabilidad de los sistemas, los estándares NIST pueden contribuir a aumentar la eficiencia de las operaciones militares.

IMPLEMENTACIÓN EXITOSA:

Para implementar con éxito los estándares NIST en el Ministerio de Defensa del Perú, se requiere un enfoque integral que incluya:

- **Evaluación de la situación actual:** Identificar las brechas de seguridad existentes y los riesgos más importantes.
- **Desarrollo de una estrategia:** Elaborar un plan detallado para la implementación de los estándares NIST, incluyendo la asignación de recursos y responsabilidades.
- **Capacitación del personal:** Proporcionar la capacitación necesaria al personal para que comprenda y aplique los estándares NIST.
- **Monitoreo y evaluación:** Implementar un sistema de monitoreo continuo para evaluar la efectividad de las medidas de seguridad y realizar ajustes según sea necesario.

En resumen, la adopción de los estándares NIST es una inversión estratégica para el Ministerio de Defensa del Perú. Al proporcionar un marco de referencia sólido y confiable, los estándares NIST pueden ayudar a garantizar la seguridad nacional y proteger los intereses del país.



3.4.1.2. AEI 8. 3 TRANSFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA

TRANSFORMACION DIGITAL EN EL PERU

El Decreto de Urgencia N°06- 2020-PCM, en el artículo 3 define la Transformación Digital como el proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intensivo de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas. La Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros (PCM) lidera la articulación, implementación y evaluación de la Política Nacional de Transformación Digital y su estrategia, así como las políticas nacionales, planes nacionales, normas, lineamientos, proyectos y plataformas para tal fin.

NIVELES DE TRANSFORMACIÓN DIGITAL

1. Nivel Inicial (Digitalización Básica)

En este nivel, las organizaciones están comenzando su camino hacia la transformación digital. Las iniciativas tecnológicas suelen ser aisladas y no forman parte de una estrategia clara. Los procesos son manuales o semiautomáticos, con una dependencia significativa del papel y métodos tradicionales. No hay una visión unificada sobre la digitalización, y las inversiones en tecnología son limitadas y reactivas, enfocadas en solucionar problemas específicos.

2. Nivel Intermedio (Digitalización Localizada)

En este nivel, las organizaciones comienzan a implementar tecnologías digitales en áreas específicas o departamentos. La digitalización es más sistemática, pero aún falta integración y colaboración entre las diferentes áreas. Las tecnologías como automatización de procesos, gestión documental digital y herramientas colaborativas empiezan a adoptarse, aunque no hay un enfoque holístico. Las decisiones sobre tecnología son más estratégicas, pero aún fragmentadas.

3. Nivel Avanzado (Digitalización Integrada)

Aquí, las organizaciones han integrado la tecnología en la mayor parte de sus operaciones y procesos. La estrategia digital está alineada con los objetivos de negocio, y se observa una colaboración transversal entre los departamentos mediante plataformas digitales compartidas. Se utiliza big

data, analítica avanzada y automatización inteligente para optimizar procesos y tomar decisiones basadas en datos. Las organizaciones están en una fase donde la innovación digital es parte de su ADN y se enfoca en la mejora continua.

4. Nivel Madurez Completa (Transformación Digital Total)

En este nivel, la organización ha alcanzado la madurez digital plena. La tecnología no solo soporta las operaciones, sino que también impulsa la innovación y la creación de nuevos modelos de negocio. Existe una cultura digital fuerte, con empleados y líderes capacitados para adaptarse rápidamente a nuevas tecnologías. Tecnologías avanzadas como inteligencia artificial, blockchain y machine learning están profundamente integradas. La organización está en un estado de agilidad digital, donde puede responder de manera proactiva y flexible a los cambios del mercado y las expectativas del cliente.

ÍNDICE DE MADUREZ DE GOBTEC



El Índice de Madurez Gobtec (GTMI) es una herramienta fundamental para medir el nivel de desarrollo y sofisticación en el uso de tecnologías digitales dentro de una administración pública. Desarrollado por el Banco Mundial, el GTMI evalúa el progreso de los países en la transformación digital de sus gobiernos y proporciona una visión comparativa de su desempeño.

El Índice de Madurez de Gobtec (GTMI, por sus siglas en inglés) se desarrolló como parte de la Iniciativa Gobtec para introducir una medida de la madurez de Gobtec en cuatro áreas de enfoque (apoyar los sistemas Institucionales centrales, mejorar la prestación de servicios, incorporar la participación ciudadana y fomentar los facilitadores de Gobtec) y para ayudar a los profesionales en el diseño de nuevos proyectos de transformación digital. El GTMI, elaborado para 198 economías, es la medida más completa de la transformación digital en el Sector Defensa. El GTMI no tiene como objetivo crear una clasificación ni evaluar la preparación de un país para la implementación de Gobtec o su desempeño; más bien, tiene como objetivo complementar las herramientas y los diagnósticos existentes al proporcionar una línea de base y un punto de referencia para la madurez de Gobtec e identificar áreas de mejora.



COMPONENTES DEL MARCO DE GOBERNANZA PARA GOBTEC

1. **SISTEMAS INSTITUCIONALES BASICOS:** Compuesto de 17 indicadores, los cuales mide la capacidad de la Institución de adoptar tecnologías digitales como infraestructura para crear soluciones innovadoras, como plataformas de datos abiertos, identificación digital y servicios de interoperabilidad.
EQUIPOS DE TRABAJO DE LA OGTIE: Innovación, Gobierno, infraestructura y estadística

2. **SERVICIOS PUBLICOS DIGITALES:** Compuesto de 9 indicadores, los cuales mide la madurez de los portales de servicios públicos en línea, con un enfoque en el diseño centrado en el ciudadano y la accesibilidad universal. Evalúa cómo la Institución utilizan tecnologías para mejorar la eficiencia y accesibilidad de los servicios públicos, facilitando la interacción digital entre la Institución y los ciudadanos.
EQUIPOS DE TRABAJO DE LA OGTIE: Innovación, Gobierno y estadística.

3. **PARTICIPACION CIUDADANA DIGITAL:** Compuesto de 6 indicadores, los cuales mide aspectos de las plataformas de participación pública, los mecanismos de retroalimentación ciudadana, los datos abiertos y los portales de la Institución abiertos al ciudadano. Son las herramientas y plataformas que permiten a los ciudadanos participar activamente en los procesos de toma de decisiones y en la cocreación de soluciones Institucionales.
EQUIPOS DE TRABAJO DE LA OGTIE: Innovación, Gobierno y estadística.

4. **SOPORTE PARA EL ECOSISTEMA GOBTEC:** Compuesto de 13 indicadores, los cuales captura la estrategia, las instituciones, las leyes y las regulaciones, así como las habilidades digitales y las políticas y programas de innovación para fomentar la Gobtec. Evalúa la existencia de políticas, marcos regulatorios y financiamiento para apoyar a startups y empresas tecnológicas que trabajen en soluciones para el Sector Defensa.
EQUIPOS DE TRABAJO DE LA OGTIE: Innovación, Gobierno, infraestructura.



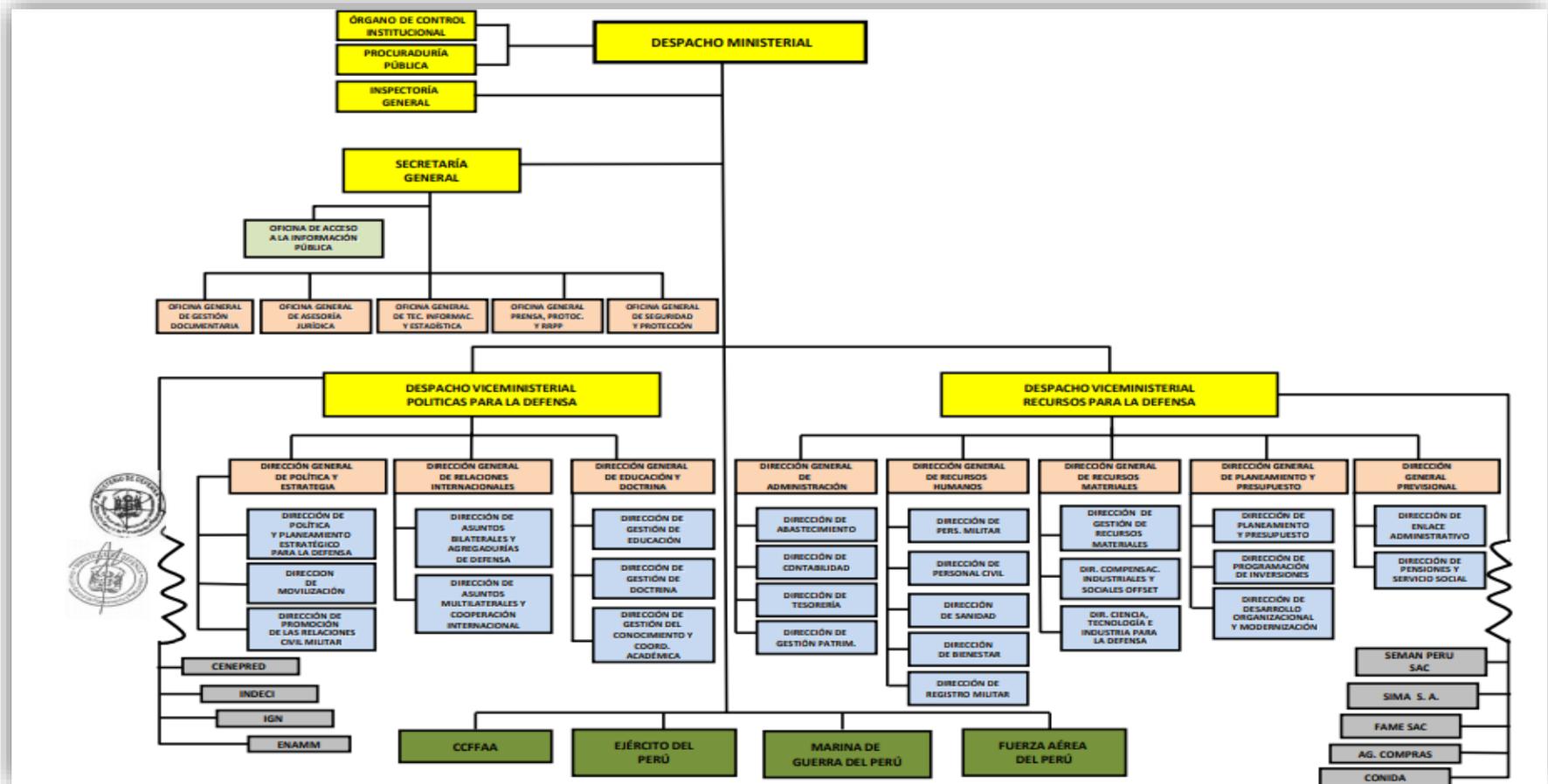
MARCO DE GOBERNANZA DEL GOBTEC COMPONENTES E INDICADORES DEL MINDEF

COMPONENTES SIGLAS	COMPONENTES	Identificador único del Indicador	INDICADORES
SIB	SISTEMAS INSTITUCIONALES BÁSICOS	SIB1.AIP	Accesibilidad de Información Pública
		SIB2.TGF	Transparencia en la Gestión Financiera
		SIB3.APA	Automatización de Procesos Administrativos
		SIB4.RC	Registro de Servidores
		SIB5.SID	Seguridad de la Información Digital
		SIB6.CI	Capacidad de Interoperabilidad
		SIB7.CRA	Capacidades de Reporte y Análisis
		SIB8.GPS	Gestión de Proyectos Sectoriales
		SIB9.SAC	Sistema de Atención al Servidor
		SIB10.SECI	Sistema de Evaluación y Control Interno
		SIB11.SGCP	Sistema de Gestión de Contrataciones Públicas
		SIB12.SGC	Sistema de Gestión de Crisis
		SIB13.SGD	Sistema de Gestión de Documentos
		SIB14.SGRH	Sistema de Gestión de Recursos Humanos
		SIB15.SGSP	Sistema de Gestión de Servicios Públicos
		SIB16.SPS	Sistema de Participación de Servidores
		SIB17.SRR	Sistema de Recursos Recaudados
SPD	SERVICIOS PÚBLICOS DIGITALES	SPD.1.ASD	Accesibilidad de Servicios Digitales
		SPD.2.DCU	Diseño Centrado en el Usuario
		SPD.3.ICD	Integración de Canales Digitales
		SPD.4.STP	Simplificación de Trámites y Procedimientos
		SPD.5.PSP	Personalización de Servicios Públicos
		SPD.6.PSPL	Pago de Servicios Públicos en Línea
		SPD.7.EU	Experiencia del Usuario
		SPD.8.IGV	Inclusión de Grupos Vulnerables
		SPD.9.TPS	Transparencia en la Prestación de Servicios
PCD	PARTICIPACIÓN CIUDADANA DIGITAL	PCD.1.AUPP	Acceso y Usabilidad de Plataformas de Participación
		PCD.2.DCPD	Diversidad de Canales de Participación Digital
		PCD.3.TR	Transparencia y Retroalimentación
		PCD.4.IP	Inclusión y Representatividad
		PCD.5.CIR	Capacidad de Impacto Real
		PCD.6.ECP	Educación y Capacitación para la Participación
SEG	SOPORTE PARA EL ECOSISTEMA GOVTECH	SEG.1.ANT	Adopción de nuevas tecnologías
		SEG.2.APPT	Alianzas Público-Privadas en Tecnología
		SEG.3.CGD	Capacitación en Gobierno Digital
		SEG.4.CDNP	Centros de Datos y Nubes Privadas
		SEG.5.CIBA	Cobertura de Internet de Banda Ancha
		SEG.6.EGD	Estrategia de Gobierno Digital
		SEG.7.FI	Financiamiento para Innovación
		SEG.8.ID	Identidad Digital (e-ID)
		SEG.9.ITI	Infraestructura de TI
		SEG.10.IESP	Innovación y Emprendimiento en el Sector Público
		SEG.11.PI	Plataforma de Interoperabilidad
		SEG.12.SM	Servicios Móviles
		SEG.13.UN	Unidad de Innovación

TOTAL DE INDICADORES:	45
TOTAL DE SUB INDICADORES:	135

3.4. ORGANIGRAMA INSTITUCIONAL

Mediante el Decreto Supremo N°006-2016-DE se aprueban el Reglamento de Organización y Funciones -ROF del Ministerio de Defensa, teniendo como finalidad definir y delimitar facultades, funciones y atribuciones de los órganos que conforman el Ministerio de Defensa, así como definir su estructura orgánica hasta el tercer nivel organizacional.



 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código: Versión: Fecha: Clasificación:	PGD 2025-2030 1.0 30/01/2025 Público
--	---	---	---

IV. SITUACIÓN ACTUAL DEL GOBIERNO DIGITAL EN LA ENTIDAD

La situación actual de los proyectos del portafolio del Plan del Gobierno Digital se está articulando o alineado al Plan Estratégico Institucional 2020-2027 ampliado, de los cuales se cumple con los siguientes objetivos estratégicos institucionales del sector defensa:

- Objetivo N° 5: Desarrollar la Ciberdefensa institucional
 - Acción Estratégica Institucional 5.3: Ciberseguridad resiliente en las instituciones del Ministerio de Defensa
- Objetivo N° 10: Fortalecer la gestión institucional
 - Acción Estratégica Institucional 10.3: Tecnologías de la información y comunicación implementadas para mejorar la gestión institucional

La Oficina General de Tecnologías de la Información y Estadística (OGTIE), a principios del segundo trimestre del año 2024, por indicaciones de la Jefatura; establecidos objetivos alineados a las actividades estratégicas institucionales que se encuentran en el Plan Estratégico Institucional 2025-2030 las cuales son:

4.1. AEI 5.3: CIBERSEGURIDAD RESILIENTE EN LAS INSTITUCIONES DEL MINISTERIO DE DEFENSA

La situación actual del Plan de Gobierno Digital en el Ministerio de Defensa del Perú desde la perspectiva del framework NIST, podemos centrarnos en las áreas clave que evalúan el índice de resiliencia en ciberseguridad. Este enfoque permite organizar el análisis alrededor de las cinco funciones para identificar fortalezas y oportunidades de mejora.

CIBERSEGURIDAD RESILIENTE EN EL MINDEF SEGÚN NIST 1.1

Con respecto a la Acción Estratégica Institucional 5.3: Ciberseguridad resiliente en las instituciones del Ministerio de Defensa; se utiliza el índice de resiliencia que cumple con el NIST 1.1 Framework. Este último es la guía basada en estándares, pautas y prácticas existentes, en la cual una organización puede administrar y reducir el riesgo de ciberseguridad. Asimismo, fomentar la comunicación de gestión de riesgos y ciberseguridad entre todas las partes interesadas de la organización (internas y externas).

La versión 1.1 del NIST Framework permite evaluar cada una de las cinco funciones que se encuentran definidas en la misma:

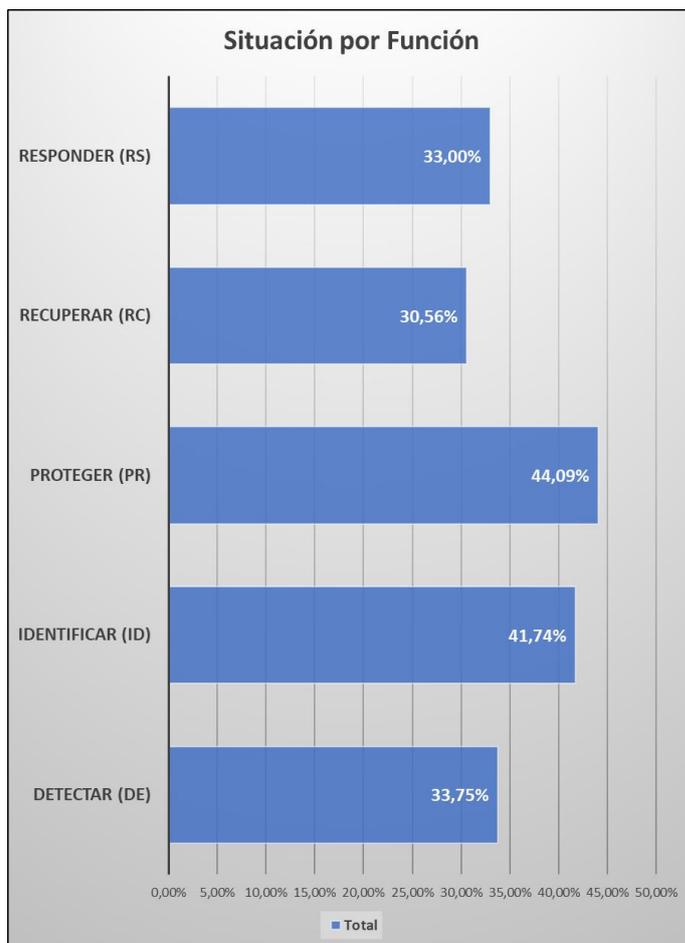
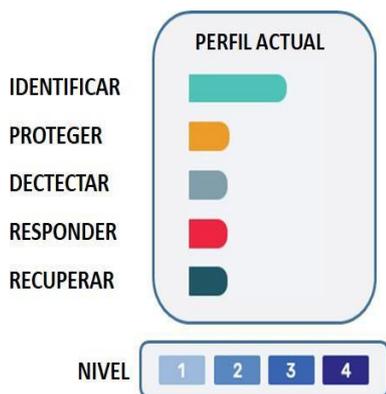
- IDENTIFICAR (ID)
- PROTEGER (PR)
- DETECTAR (DE)
- RESPONDER (RS)
- RECUPERAR (RC)

Utilizando las cinco funciones, se estableció la situación actual de la ciberseguridad en el MINDEF, tal y como se puede apreciar a continuación:

LOGRO EN EL 2024: 37.72%



MATRIZ DE LAS FUNCIONES DEL NIST 1.1



 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código: Versión: Fecha: Clasificación:	PGD 2025-2030 1.0 30/01/2025 Público
--	---	---	---

4.1.1.IDENTIFICACIÓN (IDENTIFY)

- **Activos y Servicios Críticos:** Identificación de activos de TI y sistemas críticos para la misión del Ministerio de Defensa.
- **Riesgos y Vulnerabilidades:** Análisis de riesgos actuales, amenazas específicas para el sector de defensa, y vulnerabilidades de los sistemas existentes.
- **Entorno y Ecosistema de TI:** Evaluación de cómo el Ministerio interactúa con otros actores gubernamentales y privados en términos de interoperabilidad y seguridad.

4.1.2.PROTECCIÓN (PROTECT)

- **Medidas de Seguridad y Control de Acceso:** Descripción de las políticas de acceso, autenticación, y protección de datos implementadas.
- **Concientización y Capacitación:** Evaluación de la capacitación en ciberseguridad para el personal, con enfoque en el manejo seguro de la información.
- **Protección de Datos y Continuidad del Servicio:** Revisión de las estrategias para asegurar la continuidad operativa de los sistemas en caso de incidentes.

4.1.3.DETECCIÓN (DETECT)

- **Capacidades de Detección de Incidentes:** Estado actual de las herramientas y prácticas de monitoreo para la detección de amenazas y anomalías.
- **Alertas y Comunicación de Incidentes:** Evaluación de la infraestructura y protocolos para la gestión de alertas y respuestas tempranas.
- **Evaluación de la Eficacia de Detección:** Análisis de la capacidad del Ministerio para detectar y reportar incidentes en tiempo real.

4.1.4.RESPUESTA (RESPOND)

- **Planificación de Respuesta a Incidentes:** Estado de los planes y protocolos de respuesta a incidentes cibernéticos o tecnológicos.
- **Comunicación y Coordinación:** Descripción de los procedimientos para la comunicación de incidentes entre las entidades relevantes y dentro del Ministerio.
- **Mejora Continua:** Evaluación de los procesos para aprender de los incidentes y mejorar la postura de seguridad.

4.1.5.RECUPERACIÓN (RECOVER)

- **Planificación de Recuperación y Resiliencia:** Análisis de los planes de recuperación de TI y su capacidad para restaurar operaciones después de un incidente.
- **Evaluación de Recursos para la Recuperación:** Revisión de los recursos humanos y tecnológicos destinados a la recuperación de sistemas críticos.
- **Lecciones Aprendidas y Revisión Post-Incidente:** Proceso de documentación y aprendizaje tras cada incidente para mejorar el plan de recuperación.

4.2. AEI 10.3: TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN IMPLEMENTADAS PARA MEJORAR LA GESTIÓN INSTITUCIONAL

La situación actual del Plan de Gobierno Digital en el Ministerio de Defensa del Perú desde la perspectiva del marco Gobtec, podemos centrarnos en las áreas clave que evalúa el índice de madurez Gobtec (GTMI). Este enfoque permite organizar el análisis alrededor de las cuatro áreas de madurez (Apoyo Institucional, Regulación, Gobierno Digital y Capacidades de Innovación Digital) para identificar fortalezas y oportunidades de mejora.

MARCO GOBTEC Y SU RELEVANCIA EN LA TRANSFORMACIÓN DIGITAL EN EL CONTEXTO GUBERNAMENTAL

Con respecto a la Acción Estratégica Institucional 10.3: Tecnologías de la información y comunicación implementadas para mejorar la gestión institucional; se utiliza el El Índice de Madurez Gobtec. Es una herramienta fundamental para medir el nivel de desarrollo y sofisticación en el uso de tecnologías digitales dentro de una administración pública. Desarrollado por el Banco Mundial, el GTMI evalúa el progreso de los países en la transformación digital de sus gobiernos y proporciona una visión comparativa de su desempeño

El Índice de Madurez de Gobtec (GTMI, por sus siglas en inglés) se desarrolló como parte de la Iniciativa Gobtec para introducir una medida de la madurez de Gobtec en cuatro áreas de enfoque (apoyar los sistemas Institucionales centrales, mejorar la prestación de servicios, incorporar la participación ciudadana y fomentar los facilitadores de Gobtec) y para ayudar a los profesionales en el diseño de nuevos proyectos de transformación digital. El GTMI, elaborado para 198 economías, es la medida más completa de la transformación digital en el Sector Defensa. El GTMI no tiene como objetivo crear una clasificación ni evaluar la preparación de un país para la implementación de Gobtec o su desempeño; más bien, tiene como objetivo complementar las herramientas y los diagnósticos existentes al proporcionar una línea de base y un punto de referencia para la madurez de Gobtec e identificar áreas de mejora.

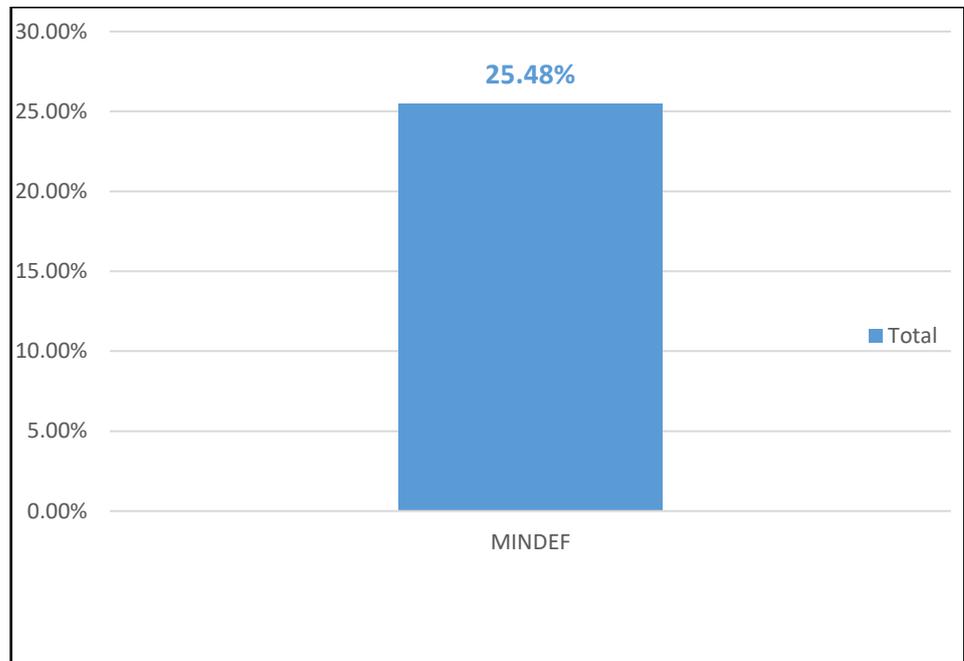
La versión 2022 del GTMI es el promedio simple de los puntajes normalizados de cuatro componentes:

1. SISTEMAS INSTITUCIONALES BÁSICOS (SIB)
2. SERVICIOS PÚBLICOS DIGITALES (SPD)
3. PARTICIPACIÓN CIUDADANA DIGITAL (PCD)
4. SOPORTE PARA EL ECOSISTEMA GOBTEC (SEG)

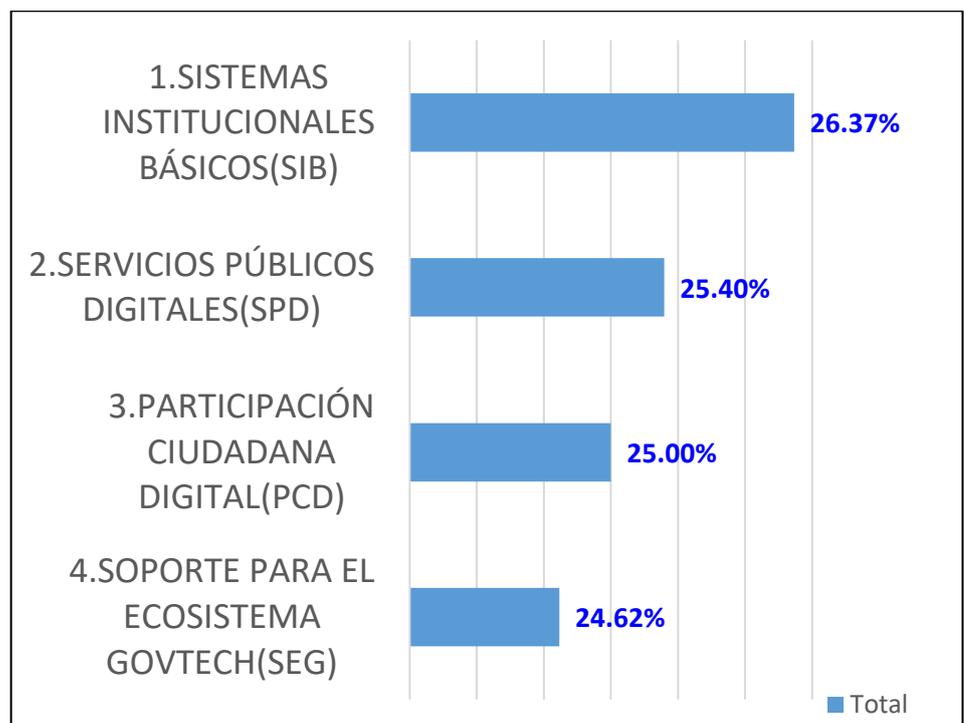


Utilizando los cuatro componentes, se estableció la situación actual de la transformación digital en el MINDEF el cual es:

LOGROS DEL MINDEF EN EL 2024: 25.48%



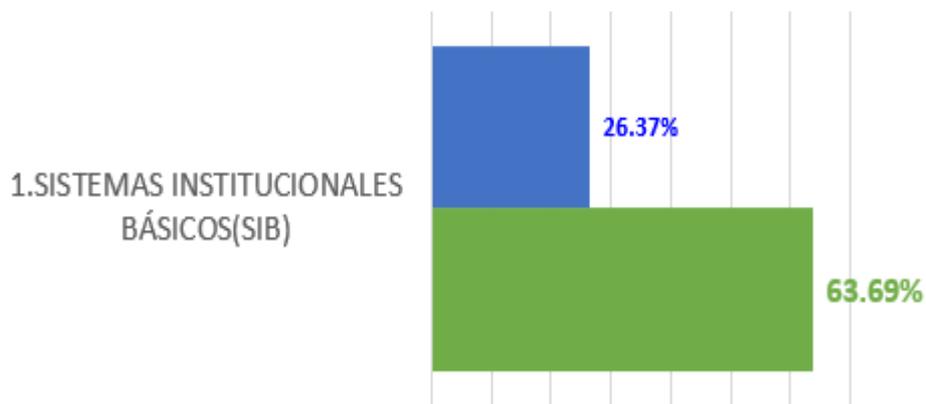
LOGROS POR COMPONENTES DEL GOBTEC



Utilizando el marco de GOBTEC para medir la transformación digital implementada en el MINDEF, el resultado se muestra según los cuatro componentes:

4.2.1. SISTEMAS INSTITUCIONALES BÁSICOS

LOGRO 2024: 26.37%
OBJETIVO AL 2030: 63.69%



Estado Actual de los Sistemas Institucionales en el MINDEF:

- **Infraestructura Tecnológica:** Descripción de la infraestructura tecnológica actual en el MDP, incluyendo servidores, redes, sistemas de comunicación y almacenamiento de datos. Evaluación de su capacidad y nivel de modernización.
- **Sistemas de Gestión Interna:** Análisis de los sistemas actuales que apoyan la gestión interna del MDP, como los sistemas de recursos humanos, logística, adquisiciones, gestión de activos y otros procesos administrativos.
- **Interoperabilidad:** Evaluación de la interoperabilidad de los sistemas con otras instituciones del gobierno peruano, como el Ministerio del Interior, el Ministerio de Economía y Finanzas, y otros actores internacionales en el ámbito de defensa.

Desafíos Identificados:

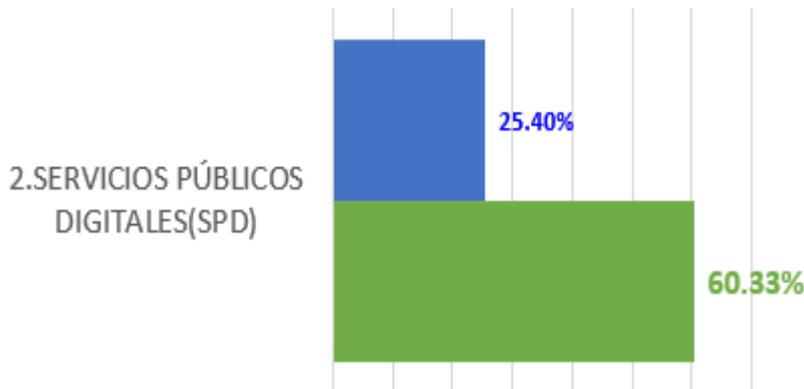
- **Obsolescencia de los sistemas:** Identificación de sistemas antiguos que no cumplen con los estándares actuales o que están desactualizados en términos de ciberseguridad y eficiencia.
- **Limitaciones en la infraestructura de TI:** Evaluación de los problemas relacionados con la capacidad de los sistemas tecnológicos para adaptarse a nuevas demandas o a tecnologías emergentes.

Oportunidades de Mejora:

- Implementación de sistemas integrados y plataformas de gestión empresarial (ERP) que optimicen los procesos administrativos y logísticos.
- Modernización de la infraestructura tecnológica, migración a la nube y uso de tecnologías como la inteligencia artificial (IA) y big data para mejorar la toma de decisiones estratégicas.

4.2.2.SERVICIOS PÚBLICOS DIGITALES

LOGRO 2024: 25.40%
OBJETIVO AL 2030: 63.33%



Servicios Internos y Externos del MINDEF:

- Servicios Internos: Análisis de los servicios digitales utilizados dentro del MDP, como la gestión de personal, la capacitación en línea, la coordinación interinstitucional digital y el manejo de recursos.
- Servicios Externos: Evaluación de los servicios digitales ofrecidos al público, como el acceso a información sobre defensa, informes de transparencia, solicitudes y trámites públicos.

Estado Actual de los Servicios Públicos Digitales:

- Portal de Transparencia y Acceso a Información: Evaluación de los esfuerzos del MDP para digitalizar la información relevante sobre presupuestos, adquisiciones y operaciones.
- Interacción con la Sociedad Civil: Evaluación de la interacción y los canales digitales de comunicación con la ciudadanía, como plataformas para la presentación de quejas o solicitudes de información.

Desafíos en los Servicios Públicos Digitales:

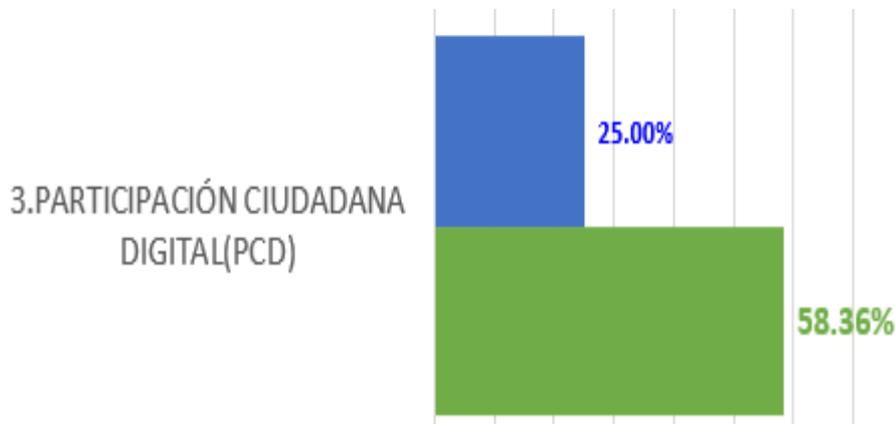
- Falta de Servicios Digitales Integrados: Muchos servicios aún se prestan en formato físico o con procesos manuales, lo que reduce la eficiencia.
- Limitada disponibilidad de plataformas de acceso público: Las plataformas en línea no están completamente disponibles o no son fáciles de usar para la ciudadanía.

Oportunidades de Mejora:

- Desarrollar plataformas de servicios en línea más accesibles y fáciles de usar que permitan a los ciudadanos acceder a la información de defensa, realizar trámites y tener acceso a servicios de forma digital.
- Implementar sistemas de solicitudes y consultas en línea para mejorar la eficiencia de los trámites administrativos.
- Mejorar la interoperabilidad de los sistemas con otros ministerios y organismos para facilitar la gestión de servicios.

4.2.3. PARTICIPACIÓN CIUDADANA DIGITAL

LOGRO 2024: 25.00%
OBJETIVO AL 2030: 58.36%



Estado Actual de la Participación Ciudadana en el MINDEF:

- Plataformas de Participación Digital: Evaluación de las iniciativas existentes para fomentar la participación de los ciudadanos en la toma de decisiones o en la supervisión de la gestión pública relacionada con la defensa, como encuestas, foros de debate, y consultas públicas.
- Accesibilidad y Transparencia: Evaluación de la accesibilidad de la información del MDP para la ciudadanía, especialmente en temas de seguridad y defensa nacional. Análisis de las barreras tecnológicas o sociales que limitan la participación.

Desafíos en la Participación Ciudadana:

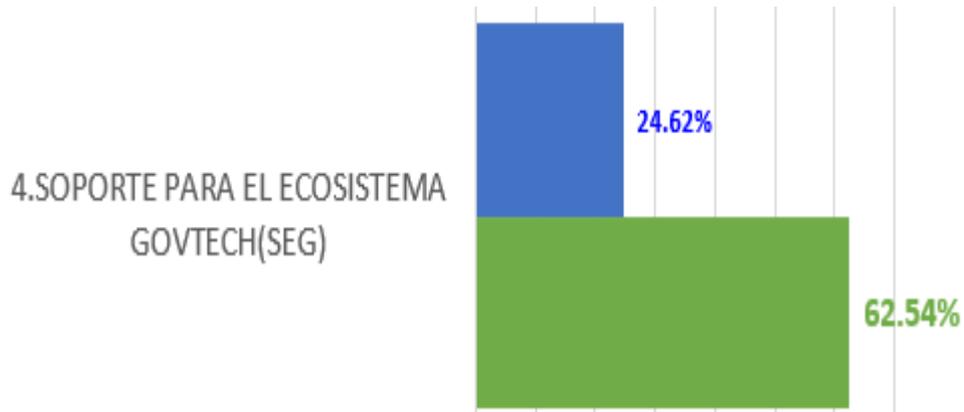
- Desconfianza o desconocimiento sobre los procesos digitales: Muchos ciudadanos pueden ser reacios a utilizar plataformas digitales para interactuar con el gobierno, especialmente en temas sensibles como la defensa.
- Limitación en la retroalimentación efectiva: Falta de mecanismos eficientes para recibir y procesar la participación ciudadana a través de plataformas digitales.

Oportunidades de Mejora:

- Crear canales de comunicación más accesibles y transparentes para que la ciudadanía pueda participar activamente en debates sobre seguridad y política de defensa.
- Implementar plataformas de consulta y participación en tiempo real donde los ciudadanos puedan presentar propuestas, comentarios y preocupaciones sobre políticas de defensa.
- Fomentar la educación digital sobre temas de seguridad cibernética y defensa para aumentar la confianza en las plataformas de participación.

4.2.4.SOPORTE PARA EL ECOSISTEMA GOBTEC

LOGRO 2024: 24.62%
OBJETIVO AL 2030: 62.54%



Ecosistema Gobtec en el Perú:

- Colaboración con Startups y Empresas de Tecnología: Evaluación del nivel de cooperación entre el MDP y el ecosistema de Gobtec en Perú. ¿Está el Ministerio aprovechando las oportunidades de colaboración con startups tecnológicas para modernizar sus sistemas?
- Iniciativas del Gobierno para Impulsar Gobtec: Descripción de las políticas y programas nacionales que impulsan el desarrollo de Gobtec en Perú, como la estrategia nacional de digitalización o proyectos conjuntos entre el sector público y privado.

Desafíos en el Ecosistema Gobtec:

- Falta de una estrategia coherente para involucrar a actores del ecosistema tecnológico en los proyectos de defensa.
- Restricciones presupuestarias y recursos limitados para financiar la integración de soluciones tecnológicas avanzadas dentro del MDP.

Oportunidades de Mejora:

- Fortalecer las alianzas público-privadas con empresas tecnológicas especializadas en seguridad, big data, y análisis predictivo para innovar en los procesos internos del MDP.
- Promover la investigación y el desarrollo (I+D) en el sector Gobtec para crear soluciones específicas que respondan a las necesidades de defensa y seguridad nacional.
- Fomentar la creación de un ecosistema colaborativo Gobtec dentro del gobierno y en colaboración con universidades y centros de investigación tecnológica.

4.3. RELACION DE LOS PROYECTOS EN EL 2024

La relación de los proyectos del portafolio del Plan de Gobierno Digital según la situación en el año 2024 es:

Nº	PROYECTO EN EL 2024	SITUACION
1	Sistema de Casillas Electrónicas	CULMINADO
2	Incorporación en la Plataforma de Datos Abiertos y Plataforma de Datos Georreferenciados	ANALISIS
3	Aula Virtual del Sector Defensa	DESESTIMADO
4	Portal de cursos de aprendizaje del Sector Defensa	DESESTIMADO
5	Gestión de la implementación de los Proyectos del Plan de Gobierno Digital	DESESTIMADO
6	Implementación del Sistema de Gestión de Seguridad de la Información	CULMINADO
7	Implementación de sistemas de seguridad informática	CULMINADO
8	Atenciones de seguridad informática	CULMINADO
9	Implementación de equipamiento de infraestructura tecnológica	PGD 2025-2030
10	Implementación de equipamiento de cómputo	PGD 2025-2030
11	Atenciones de soporte técnico a los usuarios	PGD 2025-2030
12	Mantenimiento de Sistemas de Información	PGD 2025-2030
13	Sistema de Gestión Vehicular	PGD 2025-2030
14	Sistema Centralizado de Legajos del Sector – Datos Personales	DESESTIMADO
15	Sistema Centralizado de los Recursos Materiales del Sector – Recursos Principales	ANALISIS
16	Sistema Centralizado de Legajos del Sector – Datos Académicos	DESESTIMADO
17	Sistema Centralizado de los Recursos Materiales del Sector – Recursos Secundarios	ANALISIS
18	Sistema Centralizado de Legajos del Sector – Datos de Proyectos.	PGD 2025-2030

Nº	PROYECTO EN EL 2024	SITUACION
19	Sistema de planificación, registro y seguimiento de acciones cívicas del Sector.	PGD 2025-2030
20	Sistema Centralizado de Legajos del Sector – Datos Atención Medicas	DESESTIMADO
21	Sistema de Gestión de Relaciones Internacionales	ANALISIS
22	Sistema de Trámite Documentario 2.0. – Maestras	DESESTIMADO
23	Sistema de consulta de Políticas y Estrategias del Sector	PGD 2025-2030
24	Sistema de Trámite Documentario 2.0. – Mesa de Partes	DESESTIMADO
25	Sistema de Programación de Inversiones	PGD 2025-2030
26	Sistema de Trámite Documentario 2.0. – Bandejas	DESESTIMADO
27	Intranet 2.0.	CULMINADO
28	Sistema de Trámite Documentario 2.0. – Consultas y Reportes	DESESTIMADO
29	Implementación de productos estadísticos	CULMINADO

RESUMEN:

SITUACION	CANT.
CULMINADOS	06
ANALISIS	03
DESESTIMADO	10
PGD 2025-2030	09

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código: Versión: Fecha: Clasificación:	PGD 2025-2030 1.0 30/01/2025 Público
---	---	---	---

V. OBJETIVOS DE GOBIERNO DIGITAL

Para establecer los objetivos, se inicia en análisis de los desafíos de Gobierno Digital, luego se establece los objetivos y finalmente se elabora un Mapa Estratégico de Gobierno Digital.

5.1. DESAFÍOS DE GOBIERNO DIGITAL

5.1.1. Desafío 01: Transformación digital implementada en el Ministerio de Defensa

La Transformación Digital en el Ministerio de Defensa (MINDEF) del Perú presenta desafíos significativos, ya que implica una evolución integral hacia un modelo en el que la tecnología se convierte en el eje de la modernización de sus procesos, sistemas y servicios. Esto no solo abarca la digitalización de procesos existentes, sino también una transformación cultural, organizacional y estratégica. A continuación, se detallan los principales desafíos asociados:

I. Infraestructura tecnológica obsoleta: Muchas de las infraestructuras de TI del MINDEF y sus instituciones vinculadas (Fuerzas Armadas) se encuentran desactualizadas, limitando la capacidad de implementar soluciones avanzadas de transformación digital.

Implicaciones:

- Brechas en interoperabilidad entre sistemas.
- Falta de capacidad para gestionar grandes volúmenes de datos.
- Dificultades para implementar plataformas en la nube y tecnologías emergentes.

II. Resistencia al cambio cultural: La transformación digital no solo implica tecnología, sino también un cambio cultural en la forma de trabajar y en la adopción de nuevas herramientas y procesos.

Implicaciones:

- Reticencia del personal militar y civil a modificar prácticas tradicionales.
- Dificultades para fomentar una mentalidad de innovación y aprendizaje continuo.
- Riesgo de subutilización de las herramientas digitales disponibles.

III. Capacitación del talento humano: Existe una brecha significativa en las competencias digitales del personal, tanto civil como militar, lo que limita la adopción efectiva de nuevas tecnologías.

Implicaciones:

- Insuficiente conocimiento sobre ciberseguridad, análisis de datos y tecnologías emergentes.
- Baja capacidad para desarrollar e implementar soluciones digitales.
- Necesidad de programas de formación continua.

IV. Gestión de la ciberseguridad: El sector Defensa maneja información crítica y sensible, lo que lo convierte en un objetivo atractivo para ciberataques.

Implicaciones:

- Incremento en el riesgo de brechas de seguridad.
- Necesidad de fortalecer protocolos y estrategias de ciberseguridad.
- Limitaciones en la capacidad para responder a incidentes cibernéticos.

V. Limitaciones presupuestales: La asignación de recursos financieros para proyectos de transformación digital puede competir con otras prioridades del sector Defensa.

Implicaciones:

- Retrasos en la implementación de proyectos tecnológicos.
- Dependencia de financiamiento externo o alianzas público-privadas.
- Necesidad de optimizar los recursos disponibles mediante un enfoque estratégico.

VI. Gobernanza digital: La falta de un marco claro de gobernanza digital dificulta la coordinación entre las distintas entidades del sector Defensa.

Implicaciones:

- Duplicación de esfuerzos en proyectos digitales.
- Dificultades para alinear iniciativas digitales con objetivos estratégicos.
- Falta de estándares comunes para la interoperabilidad de sistemas.

VII. Interoperabilidad entre sistemas: El sector Defensa incluye múltiples organismos y unidades, cada uno con sus propios sistemas y procesos.

Implicaciones:

- Fragmentación de la información y procesos.
- Baja capacidad para compartir y analizar datos en tiempo real.
- Necesidad de implementar plataformas integradoras.

VIII. Marco normativo y regulaciones: La transformación digital requiere actualizar el marco normativo y las directivas del sector Defensa para incluir aspectos de tecnología, datos y seguridad digital.

Implicaciones:

- Retrasos en la implementación de proyectos por falta de claridad normativa.
- Dificultades para incorporar tecnologías emergentes debido a vacíos regulatorios.
- Necesidad de garantizar el cumplimiento de estándares internacionales.

IX. Enfoque en servicios al ciudadano: Existe un reto en la orientación de la transformación digital hacia servicios que beneficien directamente a los ciudadanos y otras entidades gubernamentales.

Implicaciones:

- Baja percepción del impacto de la digitalización en la población.
- Dificultades para implementar plataformas accesibles y usables.
- Necesidad de priorizar la transparencia y la rendición de cuentas a través de herramientas digitales.

Es un desafío importante, ya que involucra no solo la modernización tecnológica de la institución, sino también un enfoque integral en torno a la eficiencia, seguridad y accesibilidad de los servicios públicos digitales. Considerando la particularidad de la seguridad nacional y la confidencialidad que requiere este sector, lo que puede influir tanto en la adopción de nuevas tecnologías como en la formulación de políticas públicas. La modernización debe hacerse de manera gradual y teniendo en cuenta la resistencia al cambio, el marco normativo y las limitaciones presupuestarias.

ESTRATEGIAS PARA SUPERAR LOS DESAFÍOS

- Modernización de la infraestructura tecnológica: Implementar tecnologías en la nube, fortalecer redes de datos y adoptar estándares internacionales de TI.
- Formación y sensibilización del personal: Diseñar programas de capacitación específicos y promover el cambio cultural hacia la innovación.
- Fortalecimiento de la ciberseguridad: Establecer estrategias integrales y protocolos robustos para proteger activos digitales.
- Optimización de recursos: Priorizar proyectos digitales mediante un enfoque de valor público y resultados estratégicos.
- Marco normativo actualizado: Desarrollar normativas que fomenten la transformación digital y faciliten la adopción de nuevas tecnologías.
- Gobernanza digital integrada: Crear un modelo de gobernanza que asegure la coordinación y alineación de todas las entidades del sector.

5.1.2. Desafío 02: Ciberseguridad resiliente en el sector defensa

La ciberseguridad resiliente en el sector defensa enfrenta desafíos únicos debido a la naturaleza crítica y sensible de las operaciones y datos manejados. Garantizar la resiliencia en ciberseguridad implica no solo proteger los sistemas y redes de ataques, sino también asegurar la continuidad de las operaciones frente a incidentes, minimizando los impactos y recuperándose rápidamente.

Los principales desafíos de la ciberseguridad resiliente en el sector defensa son:

- I. Naturaleza avanzada de las amenazas cibernéticas: Los actores maliciosos (naciones, grupos organizados y hackers) emplean técnicas avanzadas, como ataques dirigidos, ransomware y ciberespionaje.

Implicaciones:

- Alta probabilidad de ataques sofisticados y persistentes (APT, por sus siglas en inglés).
- Necesidad de monitoreo continuo y detección proactiva de amenazas.
- Complejidad para identificar actores detrás de los ataques y responder de manera efectiva.

- II. Protección de infraestructuras críticas: El sector defensa depende de infraestructuras críticas como redes de comunicación, sistemas de control de armas, bases de datos estratégicas y sistemas logísticos.

Implicaciones:

- Incremento en la vulnerabilidad ante ataques cibernéticos dirigidos a deshabilitar infraestructuras esenciales.
- Necesidad de segmentar y proteger sistemas de control industrial (OT) y tecnologías de la información (TI).
- Riesgo de interrupción de operaciones militares o estratégicas.

- III. Gestión de riesgos en la cadena de suministro: La adquisición de tecnologías y servicios externos introduce riesgos relacionados con hardware y software comprometido.

Implicaciones:

- Posibilidad de puertas traseras y componentes comprometidos en sistemas críticos.
- Dificultades para auditar y certificar la seguridad de todos los proveedores.
- Necesidad de normativas estrictas y controles para la adquisición de tecnologías.

- IV. Interoperabilidad segura: Las fuerzas armadas y entidades de defensa trabajan con aliados internacionales y agencias gubernamentales, requiriendo sistemas interoperables.

Implicaciones:

- Incremento en los puntos de acceso que pueden ser explotados por atacantes.
- Dificultades para alinear estándares de ciberseguridad entre múltiples actores.
- Necesidad de compartir información sensible de manera segura y confiable.

- V. Talento humano especializado: Existe una escasez global de profesionales en ciberseguridad, lo cual también afecta al sector defensa.

Implicaciones:

- Dificultad para reclutar y retener personal calificado.
- Brechas en competencias específicas, como ciberinteligencia, análisis forense y respuesta a incidentes.
- Necesidad de programas internos de capacitación y desarrollo.

- VI. Cultura de seguridad: El personal militar y administrativo puede ser un punto débil si no está capacitado en buenas prácticas de ciberseguridad.

Implicaciones:

- Mayor vulnerabilidad a ataques de ingeniería social, como phishing.
- Baja conciencia sobre la importancia de la seguridad en sistemas cotidianos.
- Necesidad de fomentar una cultura organizacional orientada a la seguridad.

VII. Adaptación a tecnologías emergentes: La adopción de tecnologías como inteligencia artificial, IoT, blockchain y 5G introduce nuevos riesgos.

Implicaciones:

- Exposición a vectores de ataque desconocidos.
- Incremento en la complejidad de proteger ecosistemas tecnológicos integrados.
- Necesidad de evaluar constantemente las vulnerabilidades de estas tecnologías.

VIII. Normativas y estándares: La ciberseguridad resiliente requiere un marco regulatorio sólido y actualizado.

Implicaciones:

- Desafíos para cumplir con estándares internacionales y locales.
- Falta de normativas específicas para nuevas amenazas y tecnologías.
- Necesidad de coordinación con organismos nacionales e internacionales.

IX. Resiliencia operativa: La capacidad de mantener operaciones críticas durante un ciberataque es esencial.

Implicaciones:

- Necesidad de planes de continuidad del negocio y recuperación ante desastres (BCP/DRP).
- Dificultad para simular escenarios de ataque complejos para pruebas.
- Requerimiento de redundancias tecnológicas y protocolos claros.

ESTRATEGIAS PARA ABORDAR LOS DESAFÍOS

- Fortalecer las capacidades de ciberdefensa:
 - Implementar centros de operaciones de seguridad (SOC) especializados.
 - Desarrollar capacidades de ciberinteligencia para anticipar amenazas.
- Protección de infraestructuras críticas:
 - Adoptar marcos de referencia como el NIST Cybersecurity Framework.
 - Implementar segmentación y controles avanzados en sistemas críticos.
- Gestión de talento:
 - Crear programas de formación en ciberseguridad para personal militar y civil.
 - Promover alianzas con universidades y centros de investigación.
- Cultura de ciberseguridad:
 - Realizar campañas internas de sensibilización y simulacros de ciberataques.
 - Establecer políticas claras de manejo seguro de datos y acceso a sistemas.
- Normativas y cooperación internacional:
 - Colaborar con aliados estratégicos para compartir información y mejores prácticas.
 - Actualizar regulaciones nacionales para abordar nuevos riesgos.
- Resiliencia operativa:
 - Diseñar e implementar planes de continuidad y recuperación.
 - Realizar simulacros periódicos de ataques cibernéticos.

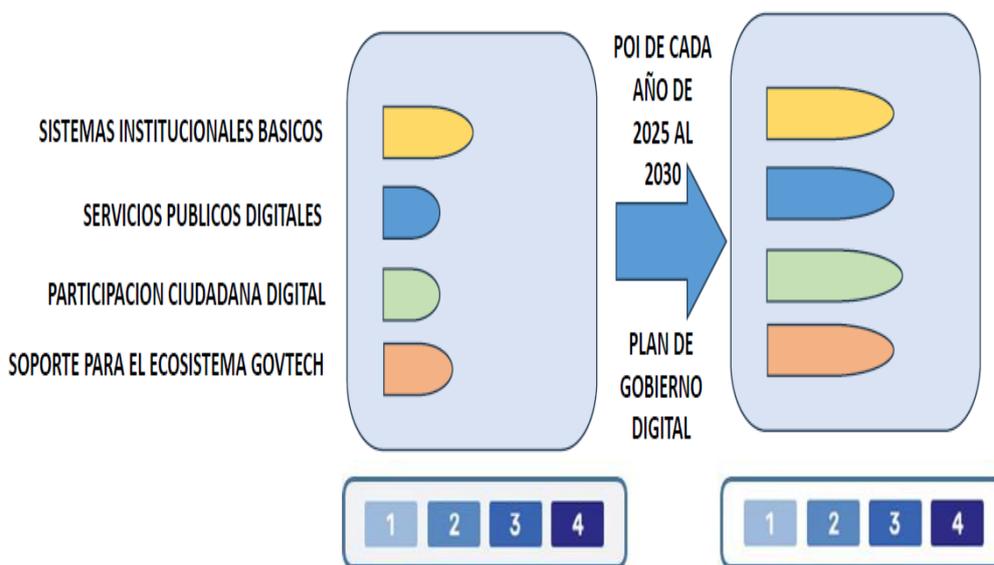
5.2. OBJETIVO DE GOBIERNO DIGITAL

Para el Sector Defensa se establece como objetivo general “IMPULSAR LA TRANSFORMACIÓN DIGITAL SEGURA EN EL MINISTERIO DE DEFENSA”, con dos objetivos, los cuales son:

5.2.1. Objetivo 01: Transformación digital implementada en el Ministerio de Defensa

Es un objetivo estratégico clave que tiene un impacto significativo en las capacidades operativas, la eficiencia administrativa y la seguridad del sector Defensa en el Perú

Utilizando los cuatros componentes del Gobtec, el logro que se espera es:



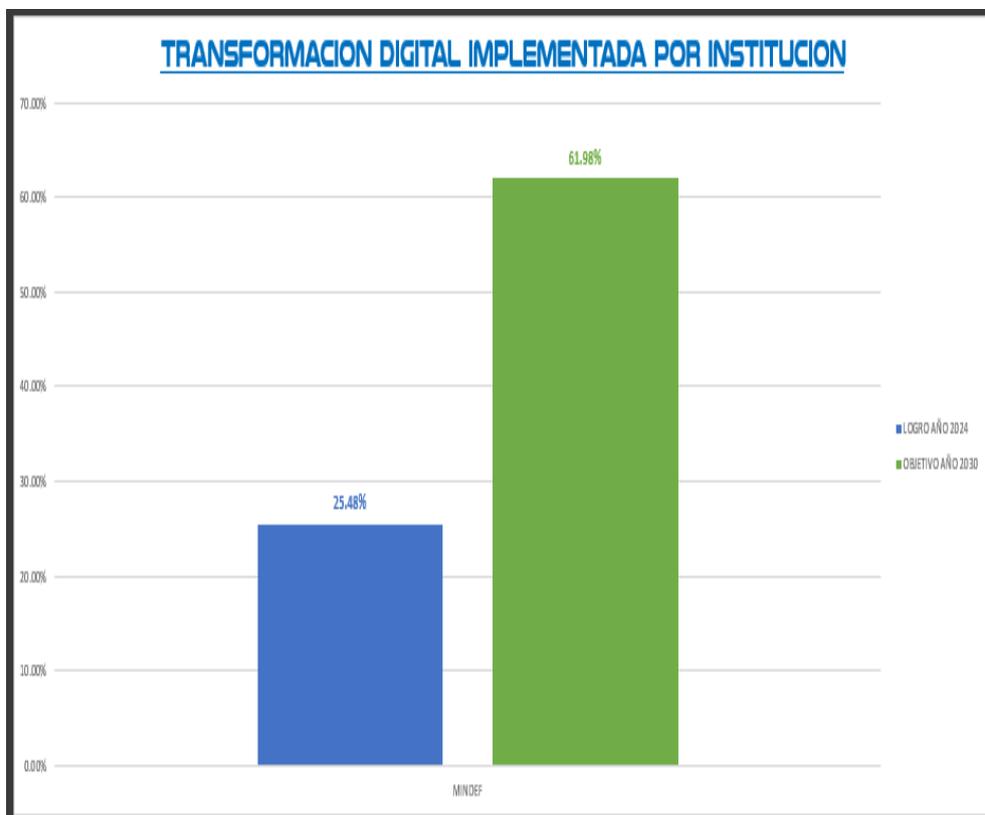
La ficha del Plan Estratégico Institucional del 2025 al 2030 tiene como objetivo Estratégico Institucional de Fortalecer la Gestión de la Integridad y lucha contra la corrupción.

Como una Acción Estratégica Institucional y el nombre del indicador es:

Acción Estratégica Institucional:	Trasformación Digital implementada en el Sector Defensa
Nombre del indicador:	Porcentaje de la trasformación digital implementada en el Sector Defensa
Justificación:	Este indicador permite metodológicamente evaluar la transformación digital implementada en el Sector Defensa según la guía el GOBTEC, para la evaluación de la transformación digital y poder integrar tecnologías de información emergentes en su gestión y así brindar servicios digitales eficientes en las unidades ejecutoras del Ministerio de Defensa.

La transformación digital implementada en el MINDEF y el sector defensa se espera los siguientes logros:

Fuente y bases de datos:	Fuente: CCFFAA, EP, MGP, FAP, CONIDA, ENAMM y DGPREV. Base de datos: Plataforma Digital "Trasformación Digital implementada en el Sector Defensa" y registros administrativos que sustentan la información registrada.						
	Línea de base	Logros esperados					
Año	2024	2025	2026	2027	2028	2029	2030
Valor en absoluto	32%	37%	43%	49%	55%	61%	67%
Valor en relativo <u>MINDEF</u>	25%	31%	37%	43%	49%	55%	63%
CCFFAA	33%	38%	43%	47%	52%	57%	62%
EP	36%	40%	45%	49%	53%	58%	62%
MGP	48%	52%	57%	61%	66%	70%	75%
FAP	33%	37%	43%	50%	57%	66%	75%
CONIDA	28%	30%	34%	39%	43%	48%	53%
ENAMM	28%	36%	43%	51%	59%	67%	75%
OPREFA	25%	34%	42%	50%	58%	66%	75%





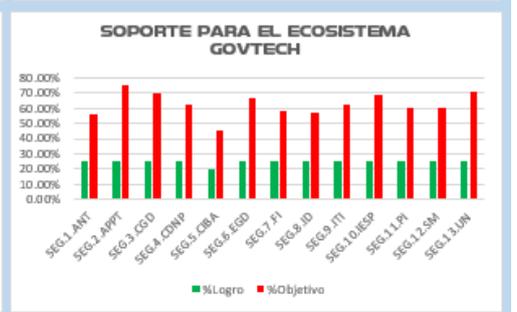
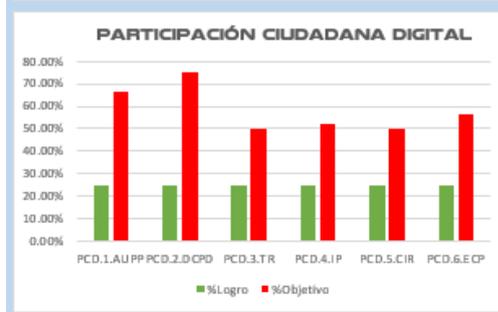
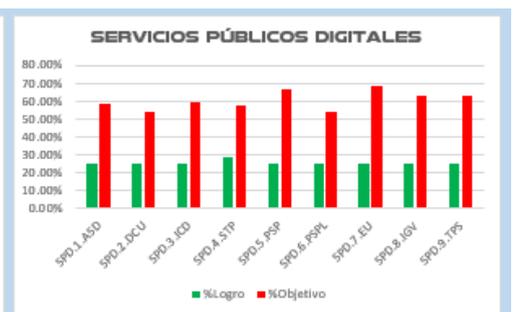
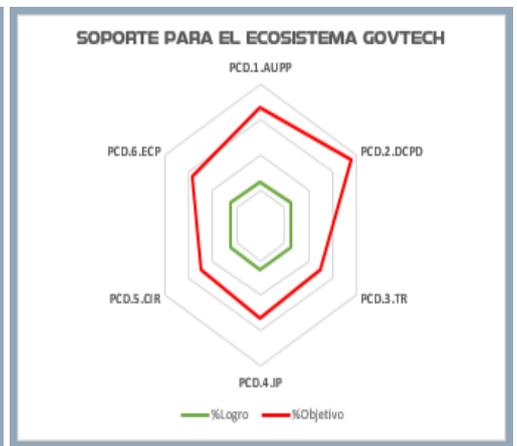
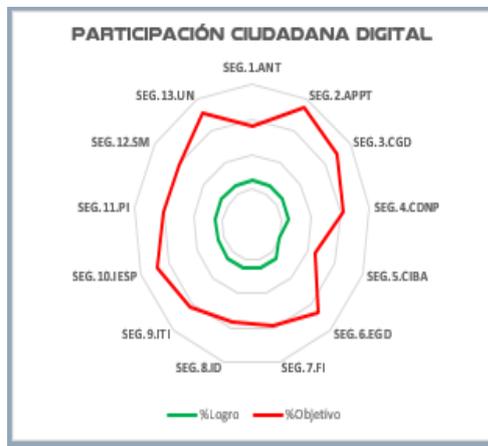
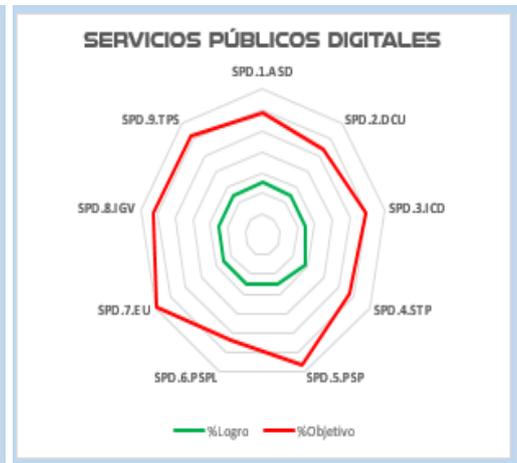
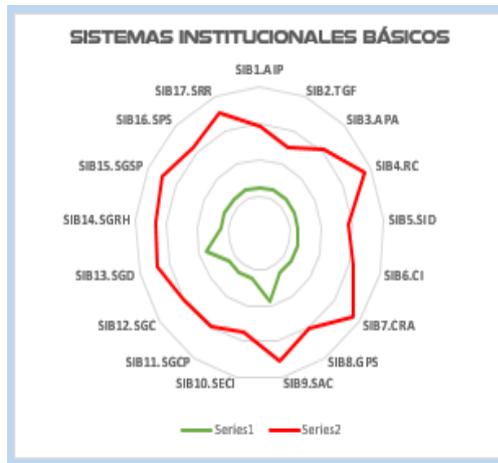
PERÚ

Ministerio de Defensa

PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030

Código: PGD 2025-2030
 Versión: 1.0
 Fecha: 30/01/2025
 Clasificación: Público

CUADRO DE MANDO: TRANSFORMACION DIGITAL IMPLEMENTADA EN EL MINDEF



Las acciones estratégicas para el primer objetivo del Gobierno Digital con respecto a la Transformación digital implementada en el Ministerio de Defensa son:

CODIGO	OBJETIVO/ACCIÓN ESTRÁTEGICA	INDICADOR OE/AE
AE.01.01	Mejorar los sistemas institucionales digitales del sector defensa	Índice del componente SISTEMAS INSTITUCIONALES DIGITALES del sector defensa
AE.01.02	Implementar los servicios públicos digitales del ministerio de defensa	Índice del componente SERVICIOS PÚBLICOS DIGITALES del Ministerio de Defensa
AE.01.03	Asegurar la participación ciudadana digital en el sector defensa	Índice del componente PARTICIPACIÓN CIUDADANA DIGITAL del Sector Defensa
AE.01.04	Fomentar el soporte del ecosistema gobierno de tecnologías en el sector defensa	Índice del componente SOPORTE DEL ECOSISTEMA DE GOBIERNO DIGITAL del Sector Defensa

5.2.2. Objetivo 02: Ciberseguridad resiliente en el sector defensa

Este objetivo es de vital importancia para garantizar la continuidad operativa, la protección de información clasificada y la integridad de las infraestructuras tecnológicas críticas del sector defensa.

La ficha del Plan Estratégico Institucional del 2025 al 2030 tiene como objetivo Fortalecer la Gestión de la Integridad y lucha contra la corrupción.

Como una Acción Estratégica Institucional y el nombre del indicador es:

Acción Estratégica Institucional:	Ciberseguridad Resiliente en el Sector Defensa
Nombre del indicador:	Índice de resiliencia en ciberseguridad que cumple con el NIST Cybersecurity Framework 1.1
Justificación:	Este indicador permite metodológicamente evaluar la resiliencia en ciberseguridad, según la guía NIST Framework Cybersecurity Framework 1.1, lo cual aportará con la gestión y minimización de riesgos que puedan afectar la información digital, en las unidades ejecutoras del Ministerio de Defensa.

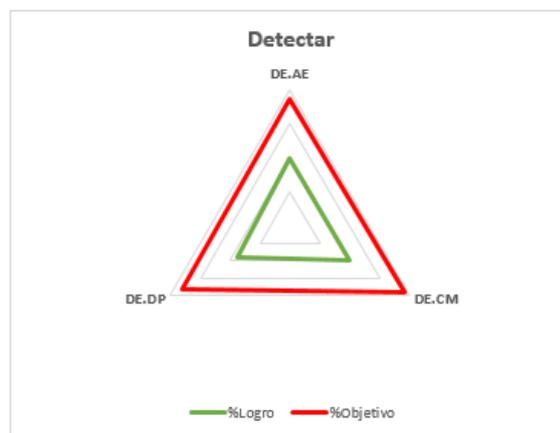
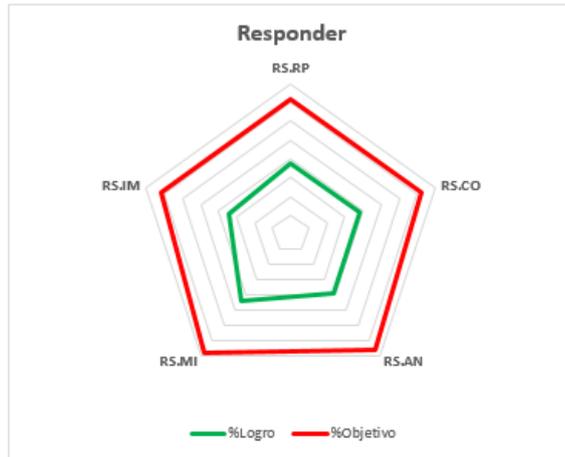
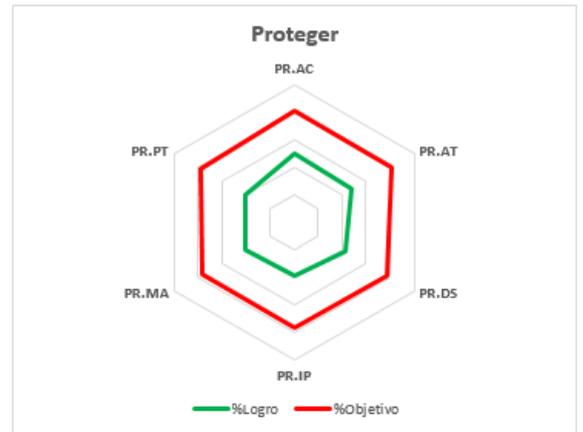
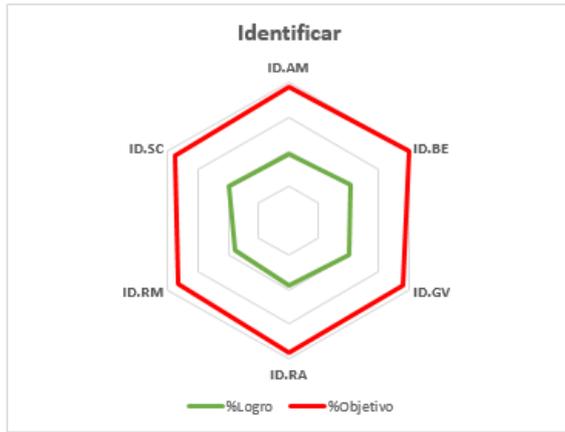
La ciberseguridad resiliente en el MINDEF y el sector defensa se espera los siguientes logros:

Fuente y bases de datos:		Fuente: CCFFAA, EP, MGP, FAP, CONIDA, ENAMM y DGPREV. Base de datos: Plataforma Digital y registros administrativos que sustentan la información registrada.					
	Línea de base	Logros esperados					
Año	2024	2025	2026	2027	2028	2029	2030
Valor en absoluto	39%	46%	52%	58%	64%	71%	77%
Valor en relativo							
MINDEF	37%	45%	53%	61%	68%	77%	82%
CCFFAA	41%	47%	54%	60%	66%	73%	79%
EP	39%	45%	52%	58%	64%	71%	77%
MGP	46%	55%	60%	65%	70%	80%	90%
FAP	69%	73%	77%	81%	85%	89%	94%
CONIDA	29%	34%	39%	44%	49%	54%	59%
ENAMM	27%	32%	37%	43%	48%	53%	59%
OPREFA	26%	34%	43%	51%	59%	68%	76%





CUADRO DE MANDO: CIBERSEGURIDAD RESILIENTE EN EL MINDEF



Las acciones estratégicas para el segundo objetivo son:

CODIGO	OBJETIVO/ACCIÓN ESTRATÉGICA	INDICADOR 0E/AE
AE.02.01	Identificar las amenazas y vulnerabilidades cibernéticas de los sistemas de información y la infraestructura tecnológica del Ministerio de Defensa	Índice de la función IDENTIFICAR del NIST del Ministerio de Defensa
AE.02.02	Proteger los activos digitales de los sistemas de información del Ministerio de Defensa.	Índice de la función PROTEGER del NIST del Ministerio de Defensa
AE.02.03	Detectar actividades anómalas y potenciales incidentes de seguridad digital en la infraestructura tecnológica del Ministerio de Defensa.	Índice de la función DETECTAR del NIST del Ministerio de Defensa
AE.02.04	Responder de manera efectiva a incidentes de seguridad digital en el Ministerio de Defensa.	Índice de la función RESPONDER del NIST del Ministerio de Defensa
AE.02.05	Recuperar la continuidad operativa de los sistemas digitales del Ministerio de Defensa.	Índice de la función RECUPERAR del NIST del Ministerio de Defensa

5.3. MAPA ESTRATÉGICO DE GOBIERNO DIGITAL

El índice de madurez Gobtec (GTMI) divide las capacidades digitales en cuatro componentes fundamentales:

- I. SISTEMAS INSTITUCIONALES BÁSICOS (SIB)
- II. SERVICIOS PÚBLICOS DIGITALES (SPD)
- III. PARTICIPACIÓN CIUDADANA DIGITAL (PCD)
- IV. SOPORTE PARA EL ECOSISTEMA GOBTEC (SEG)

A partir de estos pilares, integramos los dos objetivos de transformación digital y ciberseguridad resiliente del MINDEF en un Mapa Estratégico.

5.3.1. Dimensión Tecnológica:

Objetivo 1: Transformación Digital.

Acciones: "Mejorar sistemas institucionales digitales" y "Fomentar el ecosistema gobierno de tecnologías".

Objetivo 2: Ciberseguridad Resiliente.

Acciones: "Identificar amenazas y vulnerabilidades" y "Proteger activos digitales".

5.3.2. Dimensión de Servicios Digitales:

Objetivo 1: Transformación Digital.

Acciones: "Implementar servicios públicos digitales".

Objetivo 2: Ciberseguridad Resiliente.

Acciones: "Detectar actividades anómalas y potenciales incidentes".

5.3.3. Dimensión de Participación Ciudadana:

Objetivo 1: Transformación Digital.

Acciones: "Asegurar participación ciudadana digital".

Objetivo 2: No aplica directamente.

5.3.4. Dimensión de Gobernanza y Seguridad:

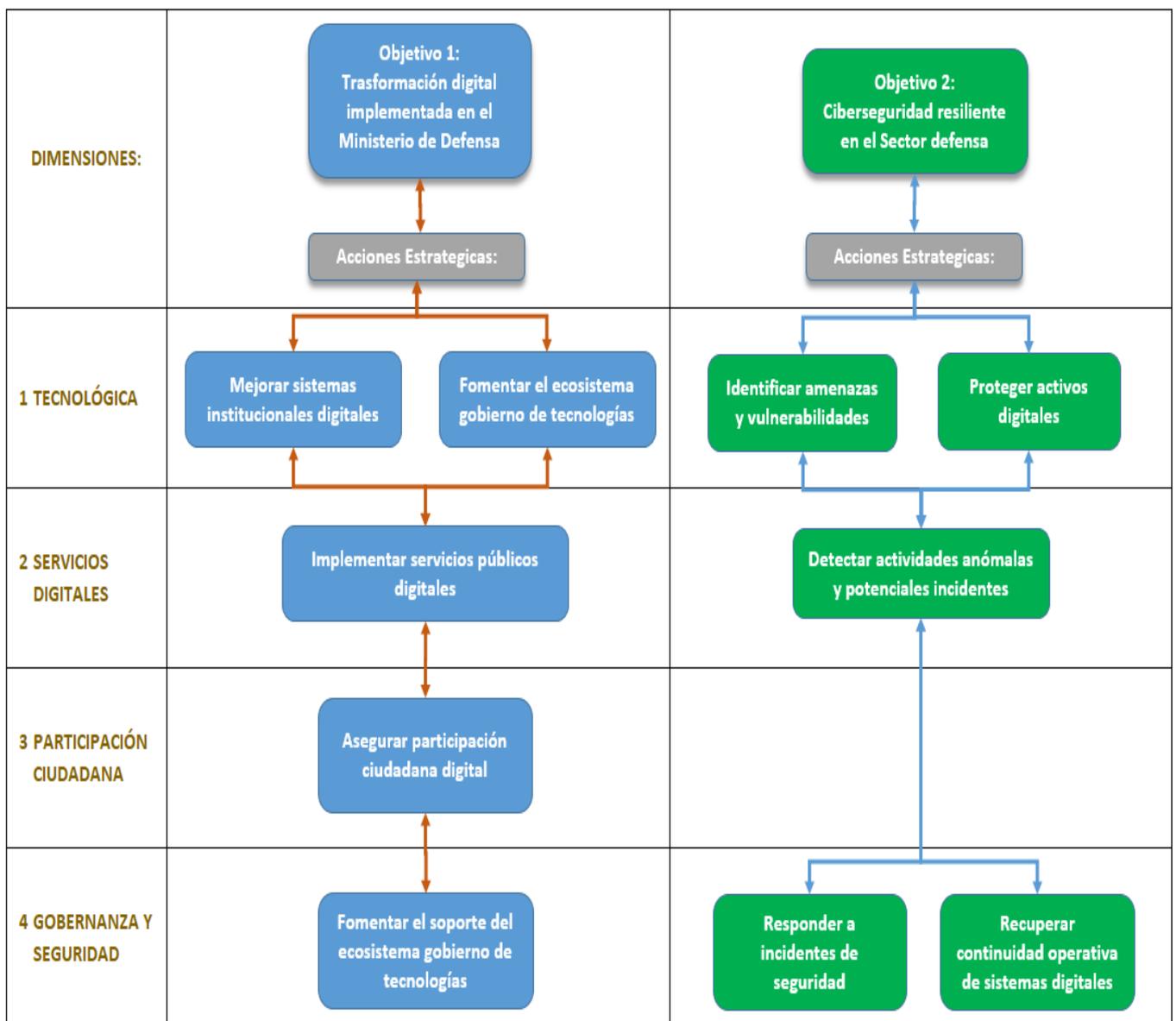
Objetivo 1: Transformación Digital.

Acciones: "Fomentar el soporte del ecosistema gobierno de tecnologías".

Objetivo 2: Ciberseguridad Resiliente.

Acciones: "Responder a incidentes de seguridad" y "Recuperar continuidad operativa".

MAPA ESTRATEGICO DE GOBIERNO DIGITAL DEL MINDEF



VI. PROYECTOS DE GOBIERNO DIGITAL

A continuación, se detallan los proyectos de gobierno digital que han sido definidos para alcanzar los objetivos de gobierno digital trazados:

- El objetivo Transformación Digital implementada en el Ministerio de Defensa, tiene 14 proyectos los cuales son:

NRO.	PROYECTO
1	IMPLEMENTACION Y SOSTENIBILIDAD DE SISTEMAS DE GESTIÓN EN EL MINDEF
2	IMPLEMENTACIÓN DE TRANSFORMACIÓN DIGITAL PARA UNA GOBERNANZA TECNOLÓGICA SOSTENIBLE
3	FORMULACIÓN Y DIFUSIÓN DEL ANUARIO ESTADISTICO DEL SECTOR DEFENSA
4	LEVANTAMIENTO Y PRODUCCIÓN DE INFORMACIÓN ESTADÍSTICA DE LA SEDE CENTRAL DEL MINDEF
5	IMPLEMENTACIÓN DEL SIESDEF II EN LAS ENTIDADES DEL SECTOR DEFENSA
6	ACTUALIZAR EL MARCO LEGAL Y NORMATIVO DEL SISTEMA ESTADÍSTICO DEL SECTOR DEFENSA
7	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA TECNOLOGICA
8	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA DE COMUNICACIONES
9	IMPLEMENTACION DE PROYECTOS RELACIONADOS A LA ADMINISTRACION DE BASE DE DATOS
10	IMPLEMENTACION DE PROYECTOS DE SOPORTE TÉCNICO ESPECIALIZADO Y ATENCION A LOS USUARIOS
11	SISTEMAS BÁSICOS INSTITUCIONALES
12	SISTEMAS PARA LA PRESTACIÓN DE SERVICIOS
13	SISTEMAS PARA LA PARTICIPACIÓN DIGITAL DEL SECTOR
14	SOPORTE Y MANTENIMIENTO DE LOS SISTEMAS DIGITALES DEL MINDEF

- El objetivo Ciberseguridad resiliente en el Sector Defensa, tiene 5 proyectos los cuales son:

NRO.	PROYECTO
15	FORTALECIMIENTO DE LA IDENTIFICACIÓN DE ACTIVOS DIGITALES EN EL MINDEF
16	PROTECCIÓN DE LA INFORMACIÓN DIGITAL DEL MINDEF
17	DETECCIÓN PROACTIVA DE AMENAZAS CIBERNÉTICAS EN LA INFRAESTRUCTURA DIGITAL DE MINDEF
18	RESPUESTA RÁPIDA Y COORDINADA ANTE CIBERATAQUES EN EL MINDEF
19	RESILIENCIA DIGITAL PARA LA RECUPERACIÓN DE LOS SISTEMAS EN EL MINDEF

6.1. LISTADO DE PROYECTO DE GOBIERNO DIGITAL

6.1.1. Evaluación y Priorización

6.1.1.1. Proyectos de Cara al Ciudadano

NRO.	NOMBRE DEL PROYECTO	CATEGORIA	FINANCIAMIENTO AO POI 2025-2030	POLITICO	LEGAL	TIEMPO	ALINEAMIENTO CON LOS OGD	PRIORIDAD
12	SISTEMAS PARA LA PRESTACIÓN DE SERVICIOS	Cumplimiento Normativo	Planificado en el POI con la AO 06 IMPLEMENTACION DE SISTEMAS DE INFORMACION DE CARA AL CIUDADANO	Se requiere coordinar con las Entidades que conforman el Sector Defensa (Principalmente con el CCFFAA, EP, MGP y FAP); además de coordinar con el Instituto Nacional de Estadística e Informática y la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.	Decreto Supremo N° 006-2016-DE Aprueban el Reglamento de Organización y Funciones (ROF) del Ministerio de Defensa. Artículo N° 34.- Funciones de la Oficina General de Tecnologías de la Información y Estadística. Inc. K).- Centralizar y mantener actualizada la Estadística Sectorial, desarrollando los Indicadores correspondientes.	6 AÑOS	TRANSFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	1

6.1.1.2. Proyectos de Gestión Interna

NRO.	NOMBRE DEL PROYECTO	CATEGORIA	FINANCIAMIENTO AO POI 2025-2030	POLITICO	LEGAL	TIEMPO	ALINEAMIENTO CON LOS OGD	PRIORIDAD
1	IMPLEMENTACION Y SOSTENIBILIDAD DE SISTEMAS DE GESTIÓN EN EL MINDEF	Sistema de Información	Planificado en el POI con la AO 03 GESTION DE LA SEGURIDAD DE LA INFORMACIÓN	Se requiere coordinar con las dependencias del Sector, entre ellas las Instituciones Armadas, además de coordinar con la secretaria de Gobierno Digital.	-Decreto Supremo N° 029-2021-PCM que aprueba el Reglamento de Ley de Gobierno Digital sobre la prestación de servicios digitales. -Resolución Ministerial 003-2023-SGTD/PCM Implementar SGTI según la norma NTP ISO 27001.	6 AÑOS	TRASFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	1
2	IMPLEMENTACIÓN DE TRANSFORMACIÓN DIGITAL PARA UNA GOBERNANZA TECNOLÓGICA SOSTENIBLE	Cumplimiento Normativo	Planificado en el POI con la AO 02 GESTION DE GOBIERNO DE TECNOLOGIAS DE LA INFORMACION	Se requiere coordinar con las dependencias del Sector, entre ellas las Instituciones Armadas, además de coordinar con la secretaria de Gobierno Digital.	Decreto Supremo N° 029-2021-PCM que aprueba el Reglamento de Ley de Gobierno Digital sobre la prestación de servicios digitales.	6 AÑOS	TRASFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	1
3	FORMULAR Y DIFUNDIR EL ANUARIO ESTADISTICO DEL SECTOR DEFENSA	Cumplimiento Normativo	Planificado en el POI con la AO 04 GESTIÓN ESTADÍSTICA	Se requiere permanente coordinación con las Entidades que Conforman el Sector Defensa.	Decreto Supremo N° 006-2016 - Aprobado el 06 junio 2016 - Reglamento de la Ley de Organización y Funciones del MINDEF	6 AÑOS	TRASFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	1



NRO.	NOMBRE DEL PROYECTO	CATEGORIA	FINANCIAMIENTO AO POI 2025-2030	POLITICO	LEGAL	TIEMPO	ALINEAMIENTO CON LOS OGD	PRIORIDAD
4	PRODUCIR Y DIFUNDIR INFORMACIÓN ESTADÍSTICA DE LA SEDE CENTRAL DEL MINDEF	Sistema de Información	Planificado en el POI con la AO 04 GESTIÓN ESTADÍSTICA	Se requiere permanente coordinación con las Entidades que Conforman el Sector Defensa.	Decreto Supremo N° 006-2016 - Aprobado el 06 junio 2016 - Reglamento de la Ley de Organización y Funciones del MINDEF	6 AÑOS	TRASFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	1
5	IMPLEMENTAR EL SISTEMA DE INFORMACIÓN ESTADÍSTICA - SIESDEF II - EN EL SECTOR DEFENSA	Sistema de Información	Planificado en el POI con la AO 04 GESTIÓN ESTADÍSTICA	Se requiere permanente coordinación con las Entidades que Conforman el Sector Defensa.	Decreto Supremo N° 006-2016 - Aprobado el 06 junio 2016 - Reglamento de la Ley de Organización y Funciones del MINDEF	6 AÑOS	TRASFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	1
6	ACTUALIZAR EL MARCO LEGAL Y NORMATIVO DEL SISTEMA ESTADÍSTICO DEL SECTOR DEFENSA	Cumplimiento Normativo	Planificado en el POI con la AO 04 GESTIÓN ESTADÍSTICA	Se requiere permanente coordinación con las Entidades que Conforman el Sector Defensa y el Órgano Rector del Sistema Estadístico Nacional (INEI).	Decreto Legislativo N° 604 (Aprobado el 30 abril 1990) - Ley de Organización y Funciones del Instituto Nacional de Estadística. Organismo Central y Rector del Sistema Nacional de Estadística, responsable de normar, planear, dirigir, coordinar y supervisar las actividades estadísticas oficiales del país	6 AÑOS	TRASFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	1



NRO.	NOMBRE DEL PROYECTO	CATEGORIA	FINANCIAMIENTO AO POI 2025-2030	POLITICO	LEGAL	TIEMPO	ALINEAMIENTO CON LOS OGD	PRIORIDAD
7	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA TECNOLÓGICA	Cumplimiento Normativo	Planificado en el POI con la AO 08 IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA TECNOLÓGICA	De acuerdo a los lineamientos para formular el Plan de Gobierno Digital, se considera la evaluación política a la revisión de si el proyecto requiere la participación de diversos sectores o entidades que pudieran no estar de acuerdo.	Decreto Supremo N° 029-2021-PCM que aprueba el Reglamento de Ley de Gobierno Digital sobre la prestación de servicios digitales.	6 AÑOS	TRANSFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	1
8	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA DE COMUNICACIONES	Adquisiciones Informáticas	Planificado en el POI con la AO 09 IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA DE COMUNICACIONES		Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento Resolución Ministerial N°355-2021-DE que constituye el "Equipo de Respuestas ante Incidentes de Seguridad Digital del Ministerio de Defensa" Decreto de Urgencia N° 026-2020 que crea la figura del trabajo remoto	6 AÑOS	CIBERSEGURIDAD RESILIENTE EN EL SECTOR DEFENSA	1



NRO.	NOMBRE DEL PROYECTO	CATEGORIA	FINANCIAMIENTO AO POI 2025-2030	POLITICO	LEGAL	TIEMPO	ALINEAMIENTO CON LOS OGD	PRIORIDAD
9	IMPLEMENTACION DE PROYECTOS RELACIONADOS A LA ADMINISTRACION DE BASE DE DATOS	Atenciones Informáticas	Planificado en el POI con la AO 10 IMPLEMENTACION DE PROYECTOS RELACIONADOS A LA ADMINISTRACION DE BASE DE DATOS		Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento Resolución Ministerial N°355-2021-DE que constituye el "Equipo de Respuestas ante Incidentes de Seguridad Digital del Ministerio de Defensa" Decreto de Urgencia N° 026-2020 que crea la figura del trabajo remoto	6 AÑOS	CIBERSEGURIDAD RESILIENTE EN EL SECTOR DEFENSA	1
10	IMPLEMENTACION DE PROYECTOS DE SOPORTE TÉCNICO ESPECIALIZADO Y ATENCION A LOS USUARIOS	Cumplimiento Normativo	Planificado en el POI con la AO 11 IMPLEMENTACION DE PROYECTOS DE SOPORTE TÉCNICO ESPECIALIZADO Y ATENCION A LOS USUARIOS	Se requiere coordinar con las Entidades que conforman el Sector Defensa (CCFFAA, EP, MGP y FAP); además de coordinar con el Instituto Nacional de Estadística e Informática y la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.	Decreto Supremo N° 006-2016-DE Aprueban el Reglamento de Organización y Funciones (ROF) del Ministerio de Defensa. Artículo N° 34.- Funciones de la Oficina General de Tecnologías de la Información y Estadística. Inc. K).- Centralizar y mantener actualizada la Estadística Sectorial, desarrollando los Indicadores correspondientes.	6 AÑOS	TRASFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	1



NRO.	NOMBRE DEL PROYECTO	CATEGORIA	FINANCIAMIENTO AO POI 2025-2030	POLITICO	LEGAL	TIEMPO	ALINEAMIENTO CON LOS OGD	PRIORIDAD
11	SISTEMAS BÁSICOS INSTITUCIONALES	Cumplimiento Normativo	Planificado en el POI con la AO 05 IMPLEMENTACION DE SISTEMAS DE INFORMACION DE GESTION INTERNA	Se requiere coordinar con las Entidades que conforman el Sector Defensa (Principalmente con el CCFFAA, EP, MGP y FAP); además de coordinar con el Instituto Nacional de Estadística e Informática y la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.	Decreto Supremo N° 006-2016-DE Aprueban el Reglamento de Organización y Funciones (ROF) del Ministerio de Defensa. Artículo N° 34.- Funciones de la Oficina General de Tecnologías de la Información y Estadística. Inc. K).- Centralizar y mantener actualizada la Estadística Sectorial, desarrollando los Indicadores correspondientes.	6 AÑOS	TRANSFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	1
13	SISTEMAS PARA LA PARTICIPACIÓN DIGITAL DEL SECTOR	Cumplimiento Normativo	Planificado en el POI con la AO 06 IMPLEMENTACION DE SISTEMAS DE INFORMACION DE CARA AL CIUDADANO	Se requiere coordinar con las Entidades que conforman el Sector Defensa (CCFFAA, EP, MGP y FAP); además de coordinar con el INEI y la Secretaría de Gobierno y Transformación Digital de la PCM.	Decreto Supremo N° 006-2016-DE Aprueban el Reglamento de Organización y Funciones (ROF) del Ministerio de Defensa. Artículo N° 34.- Funciones de la Oficina General de Tecnologías de la Información y Estadística. Inc. K).- Centralizar y mantener actualizada la Estadística Sectorial, desarrollando los Indicadores correspondientes.	6 AÑOS	TRANSFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	1

NRO.	NOMBRE DEL PROYECTO	CATEGORIA	FINANCIAMIENTO AO POI 2025-2030	POLITICO	LEGAL	TIEMPO	ALINEAMIENTO CON LOS OGD	PRIORIDAD
14	SOPORTE Y MANTENIMIENTO DE LOS SISTEMAS DIGITALES DEL MINDEF	Atenciones Informáticas	Planificado en el POI con la AO 07 MANTENIMIENTO DE SISTEMAS DE INFORMACION	Se requiere coordinar con las diferentes dependencias del MINDEF.	Decreto Supremo N° 029-2021-PCM que aprueba el Reglamento de Ley de Gobierno Digital sobre la prestación de servicios digitales.	CADA AÑO	TRASFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	1
15	FORTALECIMIENTO DE LA IDENTIFICACIÓN DE ACTIVOS DIGITALES EN EL MINDEF	Adquisiciones Informáticas	Planificado en el POI con la AO.1 IMPLEMENTACION DE PROYECTOS DE SEGURIDAD INFORMATICA		Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento Resolución Ministerial N°355-2021-DE que constituye el "Equipo de Respuestas ante Incidentes de Seguridad Digital del Ministerio de Defensa" Decreto de Urgencia N° 026-2020 que crea la figura del trabajo remoto	CADA AÑO	CIBERSEGURIDAD RESILIENTE EN EL SECTOR DEFENSA	1



NRO.	NOMBRE DEL PROYECTO	CATEGORIA	FINANCIAMIENTO AO POI 2025-2030	POLITICO	LEGAL	TIEMPO	ALINEAMIENTO CON LOS OGD	PRIORIDAD
16	PROTECCIÓN DE LA INFORMACIÓN DIGITAL DEL MINDEF	Adquisiciones Informáticas	Planificado en el POI con la AO.1 IMPLEMENTACION DE PROYECTOS DE SEGURIDAD INFORMATICA		Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento Resolución Ministerial N°355-2021-DE que constituye el “Equipo de Respuestas ante Incidentes de Seguridad Digital del Ministerio de Defensa” Decreto de Urgencia N° 026-2020 que crea la figura del trabajo remoto	CADA AÑO	CIBERSEGURIDAD RESILIENTE EN EL SECTOR DEFENSA	1
17	DETECCIÓN PROACTIVA DE AMENAZAS CIBERNÉTICAS EN LA INFRAESTRUCTURA DIGITAL DE MINDEF	Adquisiciones Informáticas	Planificado en el POI con la AO.1 IMPLEMENTACION DE PROYECTOS DE SEGURIDAD INFORMATICA		Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento Resolución Ministerial N°355-2021-DE que constituye el “Equipo de Respuestas ante Incidentes de Seguridad Digital del Ministerio de Defensa” Decreto de Urgencia N° 026-2020 que crea la figura del trabajo remoto	CADA AÑO	CIBERSEGURIDAD RESILIENTE EN EL SECTOR DEFENSA	1



NRO.	NOMBRE DEL PROYECTO	CATEGORIA	FINANCIAMIENTO AO POI 2025-2030	POLITICO	LEGAL	TIEMPO	ALINEAMIENTO CON LOS OGD	PRIORIDAD
18	RESPUESTA RÁPIDA Y COORDINADA ANTE CIBERATAQUES EN EL MINDEF	Adquisiciones Informáticas	Planificado en el POI con la AO.1 IMPLEMENTACION DE PROYECTOS DE SEGURIDAD INFORMATICA		Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento Resolución Ministerial N°355-2021-DE que constituye el “Equipo de Respuestas ante Incidentes de Seguridad Digital del Ministerio de Defensa” Decreto de Urgencia N° 026-2020 que crea la figura del trabajo remoto	CADA AÑO	CIBERSEGURIDAD RESILIENTE EN EL SECTOR DEFENSA	1
19	RESILIENCIA DIGITAL PARA LA RECUPERACIÓN DE LOS SISTEMAS EN EL MINDEF	Adquisiciones Informáticas	Planificado en el POI con la AO.1 IMPLEMENTACION DE PROYECTOS DE SEGURIDAD INFORMATICA		Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento Resolución Ministerial N°355-2021-DE que constituye el “Equipo de Respuestas ante Incidentes de Seguridad Digital del Ministerio de Defensa” Decreto de Urgencia N° 026-2020 que crea la figura del trabajo remoto	CADA AÑO	CIBERSEGURIDAD RESILIENTE EN EL SECTOR DEFENSA	1

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030		Código:	PGD 2025-2030
			Versión:	1.0
			Fecha:	30/01/2025
			Clasificación:	Público

6.1.2. Presupuesto Estimado

El presupuesto estimado desde el año 2025 hasta el año 2030 son:

AÑO 2025	AÑO 2026	AÑO 2027	AÑO 2028	AÑO 2029	AÑO 2030
8,622,969.52	6,037,320.03	10,126,806.69	7,844,296.68	6,720,447.00	7,851,980.33

6.1.2.1. Proyectos de Cara al Ciudadano

NRO.	NOMBRE DEL PROYECTO	AÑO 2025	AÑO 2026	AÑO 2027	AÑO 2028	AÑO 2029	AÑO 2030
12	SISTEMAS PARA LA PRESTACIÓN DE SERVICIOS	33,000.00	21,000.00	21,000.00		18,000.00	
TOTAL GENERAL		33,000.00	21,000.00	21,000.00	0.00	18,000.00	0.00

6.1.2.2. Proyectos de Gestión Interna

NRO.	NOMBRE DEL PROYECTO	AÑO 2025	AÑO 2026	AÑO 2027	AÑO 2028	AÑO 2029	AÑO 2030
1	IMPLEMENTACION Y SOSTENIBILIDAD DE SISTEMAS DE GESTIÓN EN EL MINDEF	346,000.00	322,000.00	304,000.00	304,000.00	346,000.00	304,000.00
2	IMPLEMENTACIÓN DE TRANSFORMACIÓN DIGITAL PARA UNA GOBERNANZA TECNOLÓGICA SOSTENIBLE	342,480.00	342,480.00	347,480.00	347,480.00	347,480.00	347,480.00
3	FORMULACIÓN Y DIFUSIÓN DEL ANUARIO ESTADISTICO DEL SECTOR DEFENSA	73,500.00	73,500.00	73,500.00	73,500.00	73,500.00	73,500.00
4	LEVANTAMIENTO Y PRODUCCIÓN DE INFORMACIÓN ESTADÍSTICA DE LA SEDE CENTRAL DEL MINDEF	36,000.00	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00



NRO.	NOMBRE DEL PROYECTO	AÑO 2025	AÑO 2026	AÑO 2027	AÑO 2028	AÑO 2029	AÑO 2030
5	IMPLEMENTACIÓN DEL SIESDEF II EN LAS ENTIDADES DEL SECTOR DEFENSA	36,000.00	36,000.00	36,000.00	36,000.00	36,000.00	36,000.00
6	ACTUALIZAR EL MARCO LEGAL Y NORMATIVO DEL SISTEMA ESTADÍSTICO DEL SECTOR DEFENSA	36,000.00	36,000.00	36,000.00	36,000.00	36,000.00	36,000.00
7	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA TECNOLÓGICA	1,450,931.00	578,867.00	1,105,467.00	1,065,867.00	1,937,667.00	1,319,867.00
8	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA DE COMUNICACIONES	764,000.00	170,800.00	2,319,800.00	170,800.00	119,800.00	170,800.00
9	IMPLEMENTACION DE PROYECTOS RELACIONADOS A LA ADMINISTRACION DE BASE DE DATOS	430,233.00	430,233.00	430,233.00	430,233.00	90,000.00	90,000.00
10	IMPLEMENTACION DE PROYECTOS DE SOPORTE TÉCNICO ESPECIALIZADO Y ATENCION A LOS USUARIOS	590,000.00	590,000.00	590,000.00	590,000.00	581,000.00	581,000.00
11	SISTEMAS BÁSICOS INSTITUCIONALES	150,000.00	198,000.00	198,000.00	258,000.00	78,000.00	108,000.00
13	SISTEMAS PARA LA PARTICIPACIÓN DIGITAL DEL SECTOR	210,000.00	240,000.00	60,000.00	120,000.00	60,000.00	
14	SOPORTE Y MANTENIMIENTO DE LOS SISTEMAS DIGITALES DEL MINDEF	81,000.00	240,000.00	240,000.00	240,000.00	240,000.00	240,000.00



NRO.	NOMBRE DEL PROYECTO	AÑO 2025	AÑO 2026	AÑO 2027	AÑO 2028	AÑO 2029	AÑO 2030
15	FORTALECIMIENTO DE LA IDENTIFICACIÓN DE ACTIVOS DIGITALES EN EL MINDEF	260,000.00	260,000.00	260,000.00	260,000.00	260,000.00	260,000.00
16	PROTECCIÓN DE LA INFORMACIÓN DIGITAL DEL MINDEF	3,675,825.52	1,299,773.36	784,993.36	2,937,916.68	1,400,000.00	1,490,000.00
17	DETECCIÓN PROACTIVA DE AMENAZAS CIBERNÉTICAS EN LA INFRAESTRUCTURA DIGITAL DE MINDEF			2,875,000.00	50,000.00	50,000.00	2,275,000.00
18	RESPUESTA RÁPIDA Y COORDINADA ANTE CIBERATAQUES EN EL MINDEF	108,000.00	874,666.67	121,333.33	600,500.00	723,000.00	196,333.33
19	RESILIENCIA DIGITAL PARA LA RECUPERACIÓN DE LOS SISTEMAS EN EL MINDEF		252,000.00	252,000.00	252,000.00	252,000.00	252,000.00
TOTAL GENERAL		8,589,969.52	6,016,320.03	10,105,806.69	7,844,296.68	6,702,447.00	7,851,980.33

6.1.3. Cronograma de la Implementación del Portafolio de Proyectos

6.1.3.1. Proyectos de Cara al Ciudadano

NRO.	PROYECTO	PERIODO AÑO 2025				PERIODO AÑO 2026				PERIODO AÑO 2027				PERIODO AÑO 2028				PERIODO AÑO 2029				PERIODO AÑO 2030			
		1T	2T	3T	4T																				
12	SISTEMAS PARA LA PRESTACIÓN DE SERVICIOS	■		■	■			■	■			■	■					■	■						

6.1.3.2. Proyectos de Gestión Interna

NRO.	PROYECTO	PERIODO AÑO 2025				PERIODO AÑO 2026				PERIODO AÑO 2027				PERIODO AÑO 2028				PERIODO AÑO 2029				PERIODO AÑO 2030			
		1T	2T	3T	4T																				
1	IMPLEMENTACION Y SOSTENIBILIDAD DE SISTEMAS DE GESTIÓN EN EL MINDEF		■		■		■		■		■		■		■		■		■		■		■		■
2	IMPLEMENTACIÓN DE TRANSFORMACIÓN DIGITAL PARA UNA GOBERNANZA TECNOLÓGICA SOSTENIBLE		■		■		■		■		■		■		■		■		■		■		■		■
3	FORMULAR Y DIFUNDIR EL ANUARIO ESTADISTICO DEL SECTOR DEFENSA	■		■		■		■		■		■		■		■		■		■		■		■	

NRO.	PROYECTO	PERIODO AÑO 2025				PERIODO AÑO 2026				PERIODO AÑO 2027				PERIODO AÑO 2028				PERIODO AÑO 2029				PERIODO AÑO 2030			
		1T	2T	3T	4T																				
4	PRODUCIR Y DIFUNDIR INFORMACIÓN ESTADÍSTICA DE LA SEDE CENTRAL DEL MINDEF				■				■				■				■				■				■
5	IMPLEMENTAR EL SISTEMA DE INFORMACIÓN ESTADÍSTICA - SIESDEF II - EN EL SECTOR DEFENSA				■				■				■				■				■				■
6	ACTUALIZAR EL MARCO LEGAL Y NORMATIVO DEL SISTEMA ESTADÍSTICO DEL SECTOR DEFENSA	■	■	■	■				■				■				■				■				■
7	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA TECNOLÓGICA	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
8	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA DE COMUNICACIONES			■				■				■				■				■				■	
9	IMPLEMENTACION DE PROYECTOS RELACIONADOS A LA ADMINISTRACION DE BASE DE DATOS	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



Ministerio de Defensa

PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030

Código: PGD 2025-2030
Versión: 1.0
Fecha: 30/01/2025
Clasificación: Público

Table with 25 columns (NRO., PROYECTO, and quarterly periods from 2025 to 2030) and 7 rows of project data. Projects include 'IMPLEMENTACION DE PROYECTOS DE SOPORTE TÉCNICO ESPECIALIZADO...', 'SISTEMAS BÁSICOS INSTITUCIONALES', 'SISTEMAS PARA LA PARTICIPACIÓN DIGITAL DEL SECTOR', 'SOPORTE Y MANTENIMIENTO DE LOS SISTEMAS DIGITALES DEL MINDEF', 'FORTALECIMIENTO DE LA IDENTIFICACIÓN DE ACTIVOS DIGITALES EN EL MINDEF', and 'PROTECCIÓN DE LA INFORMACIÓN DIGITAL DEL MINDEF'.

NRO.	PROYECTO	PERIODO AÑO 2025				PERIODO AÑO 2026				PERIODO AÑO 2027				PERIODO AÑO 2028				PERIODO AÑO 2029				PERIODO AÑO 2030							
		1T	2T	3T	4T																								
17	DETECCIÓN PROACTIVA DE AMENAZAS CIBERNÉTICAS EN LA INFRAESTRUCTURA DIGITAL DE MINDEF																												
18	RESPUESTA RÁPIDA Y COORDINADA ANTE CIBERATAQUES EN EL MINDEF																												
19	RESILIENCIA DIGITAL PARA LA RECUPERACIÓN DE LOS SISTEMAS EN EL MINDEF																												

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030		Código: PGD 2025-2030 Versión: 1.0 Fecha: 30/01/2025 Clasificación: Público

6.2. FICHAS DE PROYECTOS DE GOBIERNO DIGITAL

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 01		
NOMBRE DEL PROYECTO	IMPLEMENTACION Y SOSTENIBILIDAD DE SISTEMAS DE GESTIÓN EN EL MINDEF			
ALCANCE	Proyecto que busca implementar una estrategia integral para el desarrollo y fortalecimiento de los Sistemas de Gestión para la transformación digital del Sector Defensa. Esto incluye la planificación, diseño, ejecución, monitoreo y mejora continua de los Sistemas de Gestión adaptados a las necesidades específicas del Sector, dando cumplimiento a las disposiciones de la Presidencia del Consejo de Ministros.			
TIEMPO O PLAZO ESTIMADO	<p>En el segundo trimestre, se informará el avance del progreso de los planes vigentes de los Sistemas de Gestión del Sector Defensa.</p> <p>En el cuarto trimestre, se informará el avance del progreso de los planes vigentes de los Sistemas de Gestión del Sector Defensa.</p>			
COSTO ESTIMADO	- Año 2025: S/346,000.00 - Año 2028: S/304,000.00 - Año 2026: S/322,000.00 - Año 2029: S/346,000.00 - Año 2027: S/304,000.00 - Año 2030: S/304,000.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”			
BENEFICIARIOS (INTERNO O EXTERNO)	Las entidades del Sector Defensa y los ciudadanos.			
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO	
	GOBIERNO TI	PEDRO BENJAMIN GARAY CAMPOS	OFICIAL DE SEGURIDAD DIGITAL	
ANALISIS COSTO-BENEFICIO	-Reduce el impacto negativo que podría ocurrir debido a los ciberataques efectuados por los delincuentes cibernéticos y los hacktivistas en contra de las entidades del Sector Defensa. -El retorno de la inversión en el equipamiento de las plataformas de ciberseguridad resulta positivo, debido a la efectividad de los Sistemas de Gestión.			
TIPO DE PROYECTO	Proyecto de gestión interna			

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 02		
NOMBRE DEL PROYECTO	IMPLEMENTACIÓN DE TRANSFORMACIÓN DIGITAL PARA UNA GOBERNANZA TECNOLÓGICA SOSTENIBLE			
ALCANCE	El proyecto tiene como objetivo principal la modernización y transformación digital del Ministerio de Defensa, orientado a optimizar la gestión tecnológica y mejorar la gobernanza mediante el uso eficiente de las tecnologías de la información.			
TIEMPO O PLAZO ESTIMADO	Durante el segundo trimestre, se llevarán a cabo las actividades iniciales esenciales para establecer una base sólida para la transformación digital. En el cuarto trimestre, se enfocarán esfuerzos en la implementación de las soluciones tecnológicas y la priorización de las tareas clave para asegurar el cumplimiento de los objetivos del proyecto dentro de los plazos establecidos.			
COSTO ESTIMADO	- Año 2025: S/342,480.00 - Año 2028: S/347,480.00 - Año 2026: S/342,480.00 - Año 2029: S/347,480.00 - Año 2027: S/347,480.00 - Año 2030: S/347,480.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”			
BENEFICIARIOS(INTERNO O EXTERNO)	Los trabajadores del Ministerio de Defensa, los ciudadanos.			
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO	
	GOBIERNO TI	MARTA MARIA VERA GUERRERO	COORDINADORA	
ANALISIS COSTO-BENEFICIO	El análisis costo-beneficio del proyecto muestra que la modernización de sistemas optimizará recursos y reducirá costos operativos. Mejorará la gobernanza tecnológica, aumentando la transparencia, seguridad y toma de decisiones. A largo plazo, fortalecerá la eficiencia en los servicios, beneficiando directamente al ciudadano con una atención más ágil y eficaz.			
TIPO DE PROYECTO	Proyecto de gestión interna			

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 03		
NOMBRE DEL PROYECTO	FORMULACIÓN Y DIFUSIÓN DEL ANUARIO ESTADISTICO DEL SECTOR DEFENSA			
ALCANCE	A todas las Entidades que conforman el Sector Defensa			
TIEMPO O PLAZO ESTIMADO	Actividad permanente durante todo el Año			
COSTO ESTIMADO	Año 2025 S/. 73,500.00 Año 2026 S/. 73,500.00 Año 2027 S/. 73,500.00 Año 2028 S/. 73,500.00 Año 2029 S/. 73,500.00 Año 2030 S/. 73,500.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”			
BENEFICIARIOS(INTERNO O EXTERNO)	A Nivel Nacional, Regional, Local y Sectorial; en especial las Entidades que conforman el Sector Defensa.			
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO	
	ESTADISTICA	OSCAR ALFREDO GALARZA MEZA	COORDINADOR	
ANALISIS COSTO-BENEFICIO	Contar en tiempo real con información estadística confiable y oportuna que permita satisfacer las necesidades de información estadística que demandan los procesos de planificación, administración en general y la toma de decisiones de la Alta Dirección del MINDEF y de las Entidades que conforman el Sector Defensa.			
TIPO DE PROYECTO	Proyecto de gestión interna			

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código:	PGD 2025-2030
		Versión:	1.0
		Fecha:	30/01/2025
		Clasificación:	Público

 PERÚ Ministerio de Defensa	FICHA DE PROYECTO N° 04		
NOMBRE DEL PROYECTO	LEVANTAMIENTO Y PRODUCCIÓN DE INFORMACIÓN ESTADÍSTICA DE LA SEDE CENTRAL DEL MINDEF		
ALCANCE	A todas las Entidades que conforman el Sector Defensa		
TIEMPO O PLAZO ESTIMADO	Actividad permanente durante todo el Año		
COSTO ESTIMADO	Año 2025 S/. 36,000.00 Año 2026 S/. 72,000.00 Año 2027 S/. 72,000.00 Año 2028 S/. 72,000.00 Año 2029 S/. 72,000.00 Año 2030 S/. 72,000.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”		
BENEFICIARIOS(INTERNO O EXTERNO)	A Nivel Nacional, Regional, Local y Sectorial; en especial las Entidades que conforman el Sector Defensa.		
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO
	ESTADISTICA	OSCAR ALFREDO GALARZA MEZA	COORDINADOR
ANALISIS COSTO-BENEFICIO	Contar en tiempo real con información estadística confiable y oportuna que permita satisfacer las necesidades de información estadística que demandan los procesos de planificación, administración en general y la toma de decisiones de la Alta Dirección del MINDEF y de las Entidades que conforman el Sector Defensa.		
TIPO DE PROYECTO	Proyecto de gestión interna		

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 05		
NOMBRE DEL PROYECTO	IMPLEMENTACIÓN DEL SIESDEF II EN LAS ENTIDADES DEL SECTOR DEFENSA			
ALCANCE	A todas las Entidades que conforman el Sector Defensa			
TIEMPO O PLAZO ESTIMADO	Actividad permanente durante todo el Año			
COSTO ESTIMADO	Año 2025 S/. 36,000.00 Año 2026 S/. 36,000.00 Año 2027 S/. 36,000.00 Año 2028 S/. 36,000.00 Año 2029 S/. 36,000.00 Año 2030 S/. 36,000.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”			
BENEFICIARIOS(INTERNO O EXTERNO)	A Nivel Nacional, Regional, Local y Sectorial; en especial las Entidades que conforman el Sector Defensa.			
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO	
	ESTADISTICA	OSCAR ALFREDO GALARZA MEZA	COORDINADOR	
ANALISIS COSTO-BENEFICIO	Contar en tiempo real con información estadística confiable y oportuna que permita satisfacer las necesidades de información estadística que demandan los procesos de planificación, administración en general y la toma de decisiones de la Alta Dirección del MINDEF y de las Entidades que conforman el Sector Defensa.			
TIPO DE PROYECTO	Proyecto de gestión interna			

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 06		
NOMBRE DEL PROYECTO	ACTUALIZAR EL MARCO LEGAL Y NORMATIVO DEL SISTEMA ESTADÍSTICO DEL SECTOR DEFENSA			
ALCANCE	A todas las Entidades que conforman el Sector Defensa			
TIEMPO O PLAZO ESTIMADO	Actividad permanente durante todo el Año			
COSTO ESTIMADO	Año 2025 S/. 36,000.00 Año 2026 S/. 36,000.00 Año 2027 S/. 36,000.00 Año 2028 S/. 36,000.00 Año 2029 S/. 36,000.00 Año 2030 S/. 36,000.00 Ver detalle en el punto 6.1.2 "Presupuesto Estimado de Proyectos de Gobierno Digital"			
BENEFICIARIOS(INTERNO O EXTERNO)	A Nivel Nacional, Regional, Local y Sectorial; en especial las Entidades que conforman el Sector Defensa.			
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO	
	ESTADISTICA	OSCAR ALFREDO GALARZA MEZA	COORDINADOR	
ANALISIS COSTO-BENEFICIO	Contar en tiempo real con información estadística confiable y oportuna que permita satisfacer las necesidades de información estadística que demandan los procesos de planificación, administración en general y la toma de decisiones de la Alta Dirección del MINDEF y de las Entidades que conforman el Sector Defensa.			
TIPO DE PROYECTO	Proyecto de gestión interna			

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código:	PGD 2025-2030
		Versión:	1.0
		Fecha:	30/01/2025
		Clasificación:	Público

 PERÚ Ministerio de Defensa	FICHA DE PROYECTO N° 07		
NOMBRE DEL PROYECTO	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA TECNOLOGICA		
ALCANCE	Proyecto considerado para la gestión de todos los proyectos de gobierno digital y estadística implicando además la supervisión y participación en las tareas de trabajo operativo informático diario; mediante coordinaciones con las distintas dependencias y supervisión del cumplimiento de todas las tareas técnicas.		
TIEMPO O PLAZO ESTIMADO	Anual (Debe garantizarse la actualización a través de nuevas adquisiciones o asegurar soporte técnico y cobertura de garantías). 6.1.3 “Cronograma de implementación de Proyectos de Gobierno Digital”		
COSTO ESTIMADO	- Año 2025: S/1,450,931.00 - Año 2027: S/1,105,467.00 - Año 2029: S/1,937,667.00 - Año 2026: S/ 578,867.00 - Año 2028: S/1,065,867.00 - Año 2030: S/1,319,867.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”		
BENEFICIARIOS(INTERNO O EXTERNO)	Los usuarios finales que utilizan los servicios tecnológicos del Ministerio de Defensa		
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO
	INFRAESTRUCTURA	JORGE GUILLERMO PINEDA BECERRA	COORDINADOR
ANALISIS COSTO-BENEFICIO	<ul style="list-style-type: none"> -Mantener la infraestructura tecnológica del Ministerio de Defensa incorporación de equipos de última generación. -Reducir los tiempos de inactividad, mejorar la escalabilidad y garantizar mayor seguridad. -Implementar soluciones informáticas que optimicen el desarrollo de las actividades y aseguren la continuidad operativa. -Garantizar el mantenimiento integral de los equipos actuales del Ministerio de Defensa para preservar su funcionalidad. -Fomentar una gestión moderna y eficiente, basada en tecnología avanzada que permita integrar las comunicaciones en un sistema centralizado y unificado, asegurando resultados de alta calidad. -Asegurar el resguardo de la información Institucional más importante ante desastres. 		
TIPO DE PROYECTO	Proyecto de gestión interna		

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 08		
NOMBRE DEL PROYECTO	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA DE COMUNICACIONES			
ALCANCE	Implementar proyectos de comunicación seguras y capaces de garantizar la operatividad existente.			
TIEMPO O PLAZO ESTIMADO	Anual (Debe garantizarse la actualización a través de nuevas adquisiciones o asegurar soporte técnico y cobertura de garantías). 6.1.3 “Cronograma de implementación de Proyectos de Gobierno Digital”			
COSTO ESTIMADO	- Año 2025: S/764,000.00 - Año 2026: S/170,800.00 - Año 2027: S/2,319,800.00 - Año 2028: S/170,800.00 - Año 2029: S/119,800.00 - Año 2030: S/170,800.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”			
BENEFICIARIOS(INTERNO O EXTERNO)	Los usuarios finales que utilizan los servicios tecnológicos del Ministerio de Defensa			
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO	
	INFRAESTRUCTURA	JORGE GUILLERMO PINEDA BECERRA	COORDINADOR	
ANALISIS COSTO-BENEFICIO	-Mantener la infraestructura tecnológica de comunicaciones operativa y funcional del Ministerio de Defensa. -Reducir los tiempos de incidencias de fallas en las comunicaciones incorporando tecnología vigente y soporte técnico. -Garantizar el mantenimiento integral de los equipos de comunicaciones del Ministerio de Defensa para preservar su operatividad.			
TIPO DE PROYECTO	Proyecto de gestión interna			

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 09		
NOMBRE DEL PROYECTO	IMPLEMENTACION DE PROYECTOS RELACIONADOS A LA ADMINISTRACION DE BASE DE DATOS			
ALCANCE	Implementar proyectos relacionados a la administración de bases que sean escalables y segura para optimizar el manejo, almacenamiento y acceso a datos críticos de una organización, mejorando la eficiencia operativa en la toma de decisiones.			
TIEMPO O PLAZO ESTIMADO	Trimestral (Debe garantizarse la actualización a través de nuevas adquisiciones o asegurar soporte técnico y cobertura de garantías). 6.1.3 “Cronograma de implementación de Proyectos de Gobierno Digital”			
COSTO ESTIMADO	- Año 2025: S/430,233.00 - Año 2028: S/430,233.00 - Año 2026: S/430,233.00 - Año 2029: S/ 90,000.00 - Año 2027: S/430,233.00 - Año 2030: S/ 90,000.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”			
BENEFICIARIOS (INTERNO O EXTERNO)	Los usuarios finales que utilizan los servicios tecnológicos del Ministerio de Defensa			
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO	
	INFRAESTRUCTURA	JORGE GUILLERMO PINEDA BECERRA	COORDINADOR	
ANALISIS COSTO-BENEFICIO	-Mantener la infraestructura tecnológica relacionada a la administración de base de datos del Ministerio de Defensa. -Mantener operativo el sistema de almacenamiento y procesamiento principal del Ministerio de Defensa -Implementar soluciones de base de datos que optimicen el desarrollo de las actividades y aseguren la continuidad operativa. -Garantizar el mantenimiento integral del motor de base de datos principal del Ministerio de Defensa. -Optimización de tiempos de procesamiento de datos.			
TIPO DE PROYECTO	Proyecto de gestión interna			

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 10		
NOMBRE DEL PROYECTO	IMPLEMENTACION DE PROYECTOS DE SOPORTE TÉCNICO ESPECIALIZADO Y ATENCION A LOS USUARIOS			
ALCANCE	Proyecto que busca implementar un soporte técnico especializado y eficiente para garantizar la continuidad operativa, mejorar la experiencia de los usuarios y optimizar la resolución de problemas técnicos en el Ministerio de Defensa.			
TIEMPO O PLAZO ESTIMADO	Anual (Debe garantizarse la actualización a través de nuevas adquisiciones o asegurar soporte técnico y cobertura de garantías). 6.1.3 “Cronograma de implementación de Proyectos de Gobierno Digital”			
COSTO ESTIMADO	- Año 2025: S/590,000.00 - Año 2026: S/590,000.00 - Año 2027: S/590,000.00 - Año 2028: S/590,000.00 - Año 2029: S/581,000.00 - Año 2030: S/581,000.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”			
BENEFICIARIOS(INTERNO O EXTERNO)	Los usuarios finales que utilizan los servicios tecnológicos del Ministerio de Defensa			
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO	
	INFRAESTRUCTURA	JORGE GUILLERMO PINEDA BECERRA	COORDINADOR	
ANALISIS COSTO-BENEFICIO	-Resolución rápida de incidentes críticos. -Reducción en tiempos de espera y resolución de problemas técnicos, incrementando la productividad general -Implementación de monitoreo proactivo, actividades programadas. -Incremento en la satisfacción de los usuarios. -Seguimiento de las actividades.			
TIPO DE PROYECTO	Proyecto de gestión interna			

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 11		
NOMBRE DEL PROYECTO	SISTEMAS BÁSICOS INSTITUCIONALES			
ALCANCE	Proyecto considerado a fin de desarrollar e implementar sistemas de información para los usuarios internos del ministerio en base a nuestros estándares de desarrollo institucionales.			
TIEMPO O PLAZO ESTIMADO	Anual.			
COSTO ESTIMADO	- Año 2025: S/ 150,000.00 - Año 2026: S/ 198,000.00 - Año 2027: S/ 198,000.00 - Año 2028: S/ 258,000.00 - Año 2029: S/ 78,000.00 - Año 2030: S/ 180,000.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”			
BENEFICIARIOS(INTERNO O EXTERNO)	IIAA y Ministerio de Defensa			
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO	
	INNOVACION	HERNAN VARGAS PEREYRA	COORDINADOR	
ANALISIS COSTO-BENEFICIO	-Coadyuvar al uso eficiente de las tecnologías digitales dentro de la entidad, destacando su rol habilitador y facilitador para el cumplimiento de su misión, objetivos estratégicos institucionales, entre otros. -Contar con Sistema actualizado que permita cumplir los lineamientos de desarrollo de sistemas de la OGTIE, digitalización de servicios, procesos e información, así como la transformación digital de la entidad.			
TIPO DE PROYECTO	Proyecto de gestión Interna			

	PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030	Código: Versión: Fecha: Clasificación:	PGD 2025-2030 1.0 30/01/2025 Público
--	-----------------------------------	--	---	---

	FICHA DE PROYECTO N° 12		
NOMBRE DEL PROYECTO	SISTEMAS PARA LA PARTICIPACIÓN DIGITAL DEL SECTOR		
ALCANCE	Proyecto considerado a fin de desarrollar e implementar sistemas de información para los usuarios internos y externos del ministerio en base a nuestros estándares de desarrollo institucionales.		
TIEMPO O PLAZO ESTIMADO	Anual.		
COSTO ESTIMADO	- Año 2025: S/ 33,000.00 - Año 2026: S/ 21,000.00 - Año 2027: S/ 21,000.00 - Año 2028: S/ 0.00 - Año 2029: S/ 18,000.00 - Año 2030: S/ 0.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”		
BENEFICIARIOS(INTERNO O EXTERNO)	IIAA y Ministerio de Defensa		
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO
	INNOVACION	HERNAN VARGAS PEREYRA	COORDINADOR
ANALISIS COSTO-BENEFICIO	-Coadyuvar al uso eficiente de las tecnologías digitales dentro de la entidad, destacando su rol habilitador y facilitador para el cumplimiento de su misión, objetivos estratégicos institucionales, entre otros. -Contar con Sistema actualizado que permita cumplir los lineamientos de desarrollo de sistemas de la OGTIE, digitalización de servicios, procesos e información, así como la transformación digital de la entidad		
TIPO DE PROYECTO	Proyectos de Cara al Ciudadano		

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 13		
NOMBRE DEL PROYECTO	SISTEMAS PARA LA PRESTACIÓN DE SERVICIOS			
ALCANCE	Proyecto considerado a fin de desarrollar e implementar sistemas de información para los usuarios internos y externos del ministerio en base a nuestros estándares de desarrollo institucionales con participación digital.			
TIEMPO O PLAZO ESTIMADO	Anual.			
COSTO ESTIMADO	- Año 2025: S/ 210,000.00 - Año 2026: S/ 240,000.00 - Año 2027: S/ 60,000.00 - Año 2028: S/ 120,000.00 - Año 2029: S/ 60,000.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”			
BENEFICIARIOS(INTERNO O EXTERNO)	IIAA y Ministerio de Defensa			
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO	
	INNOVACION	HERNAN VARGAS PEREYRA	COORDINADOR	
ANALISIS COSTO-BENEFICIO	-Coadyuvar al uso eficiente de las tecnologías digitales dentro de la entidad, destacando su rol habilitador y facilitador para el cumplimiento de su misión, objetivos estratégicos institucionales, entre otros. -Contar con Sistema actualizado que permita cumplir los lineamientos de desarrollo de sistemas de la OGTIE, digitalización de servicios, procesos e información, así como la transformación digital de la entidad			
TIPO DE PROYECTO	Proyectos de Cara al Ciudadano			

 PERÚ Ministerio de Defensa	PLAN DE GOBIERNO DIGITAL DEL MINISTERIO DE DEFENSA 2025-2030		Código:	PGD 2025-2030
			Versión:	1.0
			Fecha:	30/01/2025
			Clasificación:	Público

 PERÚ Ministerio de Defensa	FICHA DE PROYECTO N° 14		
	NOMBRE DEL PROYECTO	SISTEMAS PARA LA PRESTACIÓN DE SERVICIOS	
ALCANCE	Proyecto considerado a fin de desarrollar e implementar sistemas de información para los usuarios internos y externos del ministerio en base a nuestros estándares de desarrollo institucionales con participación digital.		
TIEMPO O PLAZO ESTIMADO	Anual.		
COSTO ESTIMADO	- Año 2025: S/ 81,000.00 - Año 2026: S/ 240,000.00 - Año 2027: S/ 240,000.00 - Año 2028: S/ 240,000.00 - Año 2029: S/ 240,000.00 - Año 2030: S/ 240,000.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”		
BENEFICIARIOS(INTERNO O EXTERNO)	IIAA y Ministerio de Defensa		
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO
	INNOVACION	HERNAN VARGAS PEREYRA	COORDINADOR
ANALISIS COSTO-BENEFICIO	-Coadyuvar al uso eficiente de las tecnologías digitales dentro de la entidad, destacando su rol habilitador y facilitador para el cumplimiento de su misión, objetivos estratégicos institucionales, entre otros. -Contar con Sistema actualizado que permita cumplir los lineamientos de desarrollo de sistemas de la OGTIE, digitalización de servicios, procesos e información, así como la transformación digital de la entidad		
TIPO DE PROYECTO	Proyecto de gestión Interna		

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 15																																						
NOMBRE DEL PROYECTO	FORTALECIMIENTO DE LA IDENTIFICACIÓN DE ACTIVOS DIGITALES EN EL MINDEF																																							
ALCANCE	<p>Proyecto considerado dada la relevancia de la seguridad informática institucional; se desarrollarán actividades de identificación de activos y evaluación de vulnerabilidades tecnológicas, complementadas con la participación en eventos y capacitaciones especializadas en ciberseguridad.</p> <p>El alcance del proyecto considera la ejecución de la siguiente cantidad de actividades:</p> <table border="1" style="width: 100%; text-align: center;"> <thead> <tr> <th>ACTIVIDADES</th> <th>I TRIMESTRE</th> <th>II TRIMESTRE</th> <th>III TRIMESTRE</th> <th>IV TRIMESTRE</th> </tr> </thead> <tbody> <tr> <td>2025</td> <td>6</td> <td>6</td> <td>8</td> <td>8</td> </tr> <tr> <td>2026</td> <td>6</td> <td>6</td> <td>8</td> <td>8</td> </tr> <tr> <td>2027</td> <td>6</td> <td>6</td> <td>8</td> <td>8</td> </tr> <tr> <td>2028</td> <td>6</td> <td>6</td> <td>8</td> <td>8</td> </tr> <tr> <td>2029</td> <td>6</td> <td>6</td> <td>8</td> <td>8</td> </tr> <tr> <td>2030</td> <td>6</td> <td>6</td> <td>8</td> <td>8</td> </tr> </tbody> </table>					ACTIVIDADES	I TRIMESTRE	II TRIMESTRE	III TRIMESTRE	IV TRIMESTRE	2025	6	6	8	8	2026	6	6	8	8	2027	6	6	8	8	2028	6	6	8	8	2029	6	6	8	8	2030	6	6	8	8
ACTIVIDADES	I TRIMESTRE	II TRIMESTRE	III TRIMESTRE	IV TRIMESTRE																																				
2025	6	6	8	8																																				
2026	6	6	8	8																																				
2027	6	6	8	8																																				
2028	6	6	8	8																																				
2029	6	6	8	8																																				
2030	6	6	8	8																																				
TIEMPO O PLAZO ESTIMADO	Anual (Cada año, de manera mensual). Ver detalle en el punto “Cronograma de implementación de Proyectos de Seguridad Informática”.																																							
COSTO ESTIMADO	<ul style="list-style-type: none"> - Año 2025: S/ 260,000.00 - Año 2026: S/ 260,000.00 - Año 2027: S/ 260,000.00 - Año 2028: S/ 260,000.00 - Año 2029: S/ 260,000.00 - Año 2030: S/ 260,000.00 Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”																																							

BENEFICIARIOS (INTERNO O EXTERNO)	<ul style="list-style-type: none"> - Usuarios internos, quienes contarán con una plataforma segura para el cumplimiento de sus funciones. - Usuarios externos, quienes contarán con servicios digitales seguros. 		
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO
	CIBERSEGURIDAD	JAVIER FRANCISCO CASTILLO YARLEQUE	COORDINADOR
ANALISIS COSTO-BENEFICIO	<p>Reducción de riesgos por falta de control sobre activos digitales, optimización de la gestión de recursos tecnológicos, cumplimiento normativo, reducción de costos por incidentes de seguridad y mejora en la toma de decisiones estratégicas. Además, el proyecto permitirá la identificación precisa de activos críticos, facilitando una mejor planificación y asignación de recursos, así como la implementación de controles de seguridad más efectivos.</p>		
TIPO DE PROYECTO	Proyecto de gestión interna		

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 16																																						
NOMBRE DEL PROYECTO	PROTECCIÓN DE LA INFORMACIÓN DIGITAL DEL MINDEF																																							
ALCANCE	<p>Proyecto considerado dada la relevancia de la seguridad informática institucional; se llevarán a cabo actividades de gestión de la protección digital, garantizando el soporte y mantenimiento de los sistemas de seguridad informática existentes, así como su actualización y la incorporación de nuevas soluciones para reforzar la infraestructura tecnológica actual.</p> <p>El alcance del proyecto considera la ejecución de la siguiente cantidad de actividades:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>ACTIVIDADES</th> <th>I TRIMESTRE</th> <th>II TRIMESTRE</th> <th>III TRIMESTRE</th> <th>IV TRIMESTRE</th> </tr> </thead> <tbody> <tr> <td>2025</td> <td style="text-align: center;">7</td> <td style="text-align: center;">11</td> <td style="text-align: center;">3</td> <td style="text-align: center;">10</td> </tr> <tr> <td>2026</td> <td style="text-align: center;">3</td> <td style="text-align: center;">11</td> <td style="text-align: center;">3</td> <td style="text-align: center;">12</td> </tr> <tr> <td>2027</td> <td style="text-align: center;">3</td> <td style="text-align: center;">11</td> <td style="text-align: center;">3</td> <td style="text-align: center;">12</td> </tr> <tr> <td>2028</td> <td style="text-align: center;">3</td> <td style="text-align: center;">16</td> <td style="text-align: center;">3</td> <td style="text-align: center;">11</td> </tr> <tr> <td>2029</td> <td style="text-align: center;">3</td> <td style="text-align: center;">12</td> <td style="text-align: center;">3</td> <td style="text-align: center;">12</td> </tr> <tr> <td>2030</td> <td style="text-align: center;">3</td> <td style="text-align: center;">11</td> <td style="text-align: center;">3</td> <td style="text-align: center;">12</td> </tr> </tbody> </table>					ACTIVIDADES	I TRIMESTRE	II TRIMESTRE	III TRIMESTRE	IV TRIMESTRE	2025	7	11	3	10	2026	3	11	3	12	2027	3	11	3	12	2028	3	16	3	11	2029	3	12	3	12	2030	3	11	3	12
ACTIVIDADES	I TRIMESTRE	II TRIMESTRE	III TRIMESTRE	IV TRIMESTRE																																				
2025	7	11	3	10																																				
2026	3	11	3	12																																				
2027	3	11	3	12																																				
2028	3	16	3	11																																				
2029	3	12	3	12																																				
2030	3	11	3	12																																				
TIEMPO O PLAZO ESTIMADO	Anual (Cada año, de manera mensual). Ver detalle en el punto “Cronograma de implementación de Proyectos de Seguridad Informática”.																																							

COSTO ESTIMADO	<ul style="list-style-type: none"> - Año 2025: S/ 3,675,825.52 - Año 2026: S/ 1,299,773.36 - Año 2027: S/ 784,993.36 - Año 2028: S/ 2,937,916.68 - Año 2029: S/ 1,400,000.00 - Año 2030: S/ 1,490,000.00 <p>Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”</p>		
BENEFICIARIOS (INTERNO O EXTERNO)	<ul style="list-style-type: none"> - Usuarios internos, quienes contarán con una plataforma segura para el cumplimiento de sus funciones. - Usuarios externos, quienes contarán con servicios digitales seguros. 		
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO
	CIBERSEGURIDAD	JAVIER FRANCISCO CASTILLO YARLEQUE	COORDINADOR
ANALISIS COSTO-BENEFICIO	<ul style="list-style-type: none"> - Prever, asegurar y autenticar un alto nivel de seguridad, sobre los diversos servicios publicados en internet para el funcionamiento de la plataforma de servidores, los cuales garantizarán autenticación, integridad y confidencialidad de la información del Ministerio de Defensa. - Navegación segura en Internet de los usuarios finales del MINDEF, evitando el acceso a páginas no permitidas, inseguras o infectadas, las cuales pueden contener software malicioso. - Protección de manera proactiva a la infraestructura tecnológica del MINDEF contra amenazas latentes (por ejemplo: infección por virus, malware, entre otros). - Protección de los equipos de cómputo (computadoras personales y servidores), a través de una base de datos contenida en un antivirus que, a su vez, realiza el análisis de software malicioso, minimizando los riesgos que puedan afectar la disponibilidad, integridad y confidencialidad de la información digital del MINDEF. 		
TIPO DE PROYECTO	Proyecto de gestión interna		

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 17																																						
NOMBRE DEL PROYECTO	DETECCIÓN PROACTIVA DE AMENAZAS CIBERNÉTICAS EN LA INFRAESTRUCTURA DIGITAL DE MINDEF																																							
ALCANCE	<p>Proyecto considerado dada la relevancia de la seguridad informática institucional; se realizarán actividades para la adquisición, implementación y mantenimiento de una solución de seguridad que garantice capacidades robustas de detección, asegurando su óptimo funcionamiento con actualizaciones periódicas alineadas con las amenazas emergentes.</p> <p>El alcance del proyecto considera la ejecución de la siguiente cantidad de actividades:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>ACTIVIDADES</th> <th>I TRIMESTRE</th> <th>II TRIMESTRE</th> <th>III TRIMESTRE</th> <th>IV TRIMESTRE</th> </tr> </thead> <tbody> <tr> <td>2025</td> <td style="text-align: center;">0</td> <td style="text-align: center;">0</td> <td style="text-align: center;">0</td> <td style="text-align: center;">0</td> </tr> <tr> <td>2026</td> <td style="text-align: center;">0</td> <td style="text-align: center;">0</td> <td style="text-align: center;">0</td> <td style="text-align: center;">0</td> </tr> <tr> <td>2027</td> <td style="text-align: center;">0</td> <td style="text-align: center;">1</td> <td style="text-align: center;">0</td> <td style="text-align: center;">1</td> </tr> <tr> <td>2028</td> <td style="text-align: center;">0</td> <td style="text-align: center;">1</td> <td style="text-align: center;">0</td> <td style="text-align: center;">1</td> </tr> <tr> <td>2029</td> <td style="text-align: center;">0</td> <td style="text-align: center;">1</td> <td style="text-align: center;">0</td> <td style="text-align: center;">1</td> </tr> <tr> <td>2030</td> <td style="text-align: center;">0</td> <td style="text-align: center;">2</td> <td style="text-align: center;">0</td> <td style="text-align: center;">1</td> </tr> </tbody> </table>					ACTIVIDADES	I TRIMESTRE	II TRIMESTRE	III TRIMESTRE	IV TRIMESTRE	2025	0	0	0	0	2026	0	0	0	0	2027	0	1	0	1	2028	0	1	0	1	2029	0	1	0	1	2030	0	2	0	1
ACTIVIDADES	I TRIMESTRE	II TRIMESTRE	III TRIMESTRE	IV TRIMESTRE																																				
2025	0	0	0	0																																				
2026	0	0	0	0																																				
2027	0	1	0	1																																				
2028	0	1	0	1																																				
2029	0	1	0	1																																				
2030	0	2	0	1																																				
TIEMPO O PLAZO ESTIMADO	Anual (Cada año, de manera semestral). Ver detalle en el punto “Cronograma de implementación de Proyectos de Seguridad Informática”.																																							

COSTO ESTIMADO	<ul style="list-style-type: none"> - Año 2025: S/ 0.00 - Año 2026: S/ 0.00 - Año 2027: S/ 2,875,000.00 - Año 2028: S/ 50,000.00 - Año 2029: S/ 50,000.00 - Año 2030: S/ 2,275,000.00 <p>Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”</p>		
BENEFICIARIOS (INTERNO O EXTERNO)	<ul style="list-style-type: none"> - Usuarios internos, quienes contarán con una plataforma segura para el cumplimiento de sus funciones. - Usuarios externos, quienes contarán con servicios digitales seguros. 		
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO
	CIBERSEGURIDAD	JAVIER FRANCISCO CASTILLO YARLEQUE	COORDINADOR
ANALISIS COSTO-BENEFICIO	<p>Reducción del tiempo de detección de amenazas, minimización de impactos en la operatividad, optimización de los recursos de seguridad, prevención proactiva de incidentes y alineación con estándares internacionales. Adicionalmente, se incrementará la visibilidad sobre las amenazas emergentes, mejorando la capacidad de respuesta del equipo de ciberseguridad y permitiendo una mejor priorización de riesgos.</p>		
TIPO DE PROYECTO	Proyecto de gestión interna		

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 18																																						
NOMBRE DEL PROYECTO	RESPUESTA RÁPIDA Y COORDINADA ANTE CIBERATAQUES EN EL MINDEF																																							
ALCANCE	<p>Proyecto considerado dada la relevancia de la seguridad informática institucional; se desarrollarán actividades para fortalecer la gestión de respuesta ante incidentes y se implementarán nuevas soluciones de seguridad para optimizar la capacidad de reacción. También se contemplan acciones de mantenimiento y renovación de estos sistemas para asegurar su rendimiento continuo.</p> <p>El alcance del proyecto considera la ejecución de la siguiente cantidad de actividades:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>ACTIVIDADES</th> <th>I TRIMESTRE</th> <th>II TRIMESTRE</th> <th>III TRIMESTRE</th> <th>IV TRIMESTRE</th> </tr> </thead> <tbody> <tr> <td>2025</td> <td style="text-align: center;">3</td> <td style="text-align: center;">3</td> <td style="text-align: center;">3</td> <td style="text-align: center;">3</td> </tr> <tr> <td>2026</td> <td style="text-align: center;">3</td> <td style="text-align: center;">4</td> <td style="text-align: center;">3</td> <td style="text-align: center;">4</td> </tr> <tr> <td>2027</td> <td style="text-align: center;">3</td> <td style="text-align: center;">4</td> <td style="text-align: center;">3</td> <td style="text-align: center;">4</td> </tr> <tr> <td>2028</td> <td style="text-align: center;">3</td> <td style="text-align: center;">5</td> <td style="text-align: center;">3</td> <td style="text-align: center;">5</td> </tr> <tr> <td>2029</td> <td style="text-align: center;">3</td> <td style="text-align: center;">6</td> <td style="text-align: center;">3</td> <td style="text-align: center;">5</td> </tr> <tr> <td>2030</td> <td style="text-align: center;">3</td> <td style="text-align: center;">5</td> <td style="text-align: center;">3</td> <td style="text-align: center;">5</td> </tr> </tbody> </table>					ACTIVIDADES	I TRIMESTRE	II TRIMESTRE	III TRIMESTRE	IV TRIMESTRE	2025	3	3	3	3	2026	3	4	3	4	2027	3	4	3	4	2028	3	5	3	5	2029	3	6	3	5	2030	3	5	3	5
ACTIVIDADES	I TRIMESTRE	II TRIMESTRE	III TRIMESTRE	IV TRIMESTRE																																				
2025	3	3	3	3																																				
2026	3	4	3	4																																				
2027	3	4	3	4																																				
2028	3	5	3	5																																				
2029	3	6	3	5																																				
2030	3	5	3	5																																				
TIEMPO O PLAZO ESTIMADO	Anual (Cada año, de manera mensual). Ver detalle en el punto “Cronograma de implementación de Proyectos de Seguridad Informática”.																																							

COSTO ESTIMADO	<ul style="list-style-type: none"> - Año 2025: S/ 108,000.00 - Año 2026: S/ 874,666.67 - Año 2027: S/ 121,333.33 - Año 2028: S/ 600,500.00 - Año 2029: S/ 723,000.00 - Año 2030: S/ 196,333.33 <p>Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”</p>		
BENEFICIARIOS (INTERNO O EXTERNO)	<ul style="list-style-type: none"> - Usuarios internos, quienes contarán con una plataforma segura para el cumplimiento de sus funciones. - Usuarios externos, quienes contarán con servicios digitales seguros. 		
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO
	CIBERSEGURIDAD	JAVIER FRANCISCO CASTILLO YARLEQUE	COORDINADOR
ANALISIS COSTO-BENEFICIO	<p>Reducción de tiempos de respuesta ante incidentes, mejora en la coordinación interinstitucional, optimización de recursos mediante la automatización de procesos y fortalecimiento de la confianza en las operaciones digitales. Además, permite una mejor visibilidad de los incidentes, minimización del impacto operacional y cumplimiento de normativas vigentes en ciberseguridad.</p>		
TIPO DE PROYECTO	Proyecto de gestión interna		

 PERÚ Ministerio de Defensa		FICHA DE PROYECTO N° 19																																						
NOMBRE DEL PROYECTO	RESILIENCIA DIGITAL PARA LA RECUPERACIÓN DE LOS SISTEMAS EN EL MINDEF																																							
ALCANCE	<p>Proyecto considerado dada la relevancia de la seguridad informática institucional; se llevarán a cabo actividades enfocadas en la gestión de acciones de recuperación, implementación de estrategias ante incidentes y análisis post-incidente, con el objetivo de optimizar procesos y minimizar el tiempo de inactividad.</p> <p>El alcance del proyecto considera la ejecución de la siguiente cantidad de actividades:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>ACTIVIDADES</th> <th>I TRIMESTRE</th> <th>II TRIMESTRE</th> <th>III TRIMESTRE</th> <th>IV TRIMESTRE</th> </tr> </thead> <tbody> <tr> <td>2025</td> <td style="text-align: center;">0</td> <td style="text-align: center;">0</td> <td style="text-align: center;">0</td> <td style="text-align: center;">0</td> </tr> <tr> <td>2026</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> </tr> <tr> <td>2027</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> </tr> <tr> <td>2028</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> </tr> <tr> <td>2029</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> </tr> <tr> <td>2030</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> <td style="text-align: center;">9</td> </tr> </tbody> </table>					ACTIVIDADES	I TRIMESTRE	II TRIMESTRE	III TRIMESTRE	IV TRIMESTRE	2025	0	0	0	0	2026	9	9	9	9	2027	9	9	9	9	2028	9	9	9	9	2029	9	9	9	9	2030	9	9	9	9
ACTIVIDADES	I TRIMESTRE	II TRIMESTRE	III TRIMESTRE	IV TRIMESTRE																																				
2025	0	0	0	0																																				
2026	9	9	9	9																																				
2027	9	9	9	9																																				
2028	9	9	9	9																																				
2029	9	9	9	9																																				
2030	9	9	9	9																																				
TIEMPO O PLAZO ESTIMADO	<p>Anual (Cada año, de manera mensual). Ver detalle en el punto “Cronograma de implementación de Proyectos de Seguridad Informática”.</p>																																							

COSTO ESTIMADO	<ul style="list-style-type: none"> - Año 2025: S/ 0.00 - Año 2026: S/ 252,000.00 - Año 2027: S/ 252,000.00 - Año 2028: S/ 252,000.00 - Año 2029: S/ 252,000.00 - Año 2030: S/ 252,000.00 <p>Ver detalle en el punto 6.1.2 “Presupuesto Estimado de Proyectos de Gobierno Digital”</p>		
BENEFICIARIOS (INTERNO O EXTERNO)	<ul style="list-style-type: none"> - Usuarios internos, quienes contarán con una plataforma segura para el cumplimiento de sus funciones. - Usuarios externos, quienes contarán con servicios digitales seguros. 		
RESPONSABLE DEL PROYECTO	EQUIPO DE TRABAJO	NOMBRE	CARGO
	CIBERSEGURIDAD	JAVIER FRANCISCO CASTILLO YARLEQUE	COORDINADOR
ANALISIS COSTO-BENEFICIO	<p>Minimización de pérdidas operativas ante incidentes, mejora en la capacidad de respuesta, reducción del tiempo de inactividad y optimización del uso de recursos tecnológicos. Asimismo, permitirá establecer planes de recuperación efectivos, reducir costos operativos asociados a la recuperación de datos y mejorar la resiliencia organizacional frente a amenazas cibernéticas.</p>		
TIPO DE PROYECTO	Proyecto de gestión interna		

PROYECTOS Y ACTIVIDADES DEL PORTAFOLIO DEL PLAN DE GOBIERNO DIGITAL 2025-2030 DEL MINISTERIO DE DEFENSA

OBJETIVOS DEL GOBIERNO DIGITAL	NRO.	PROYECTO	AÑO 2025	AÑO 2026	AÑO 2027	AÑO 2028	AÑO 2029	AÑO 2030
01. TRANSFORMACIÓN DIGITAL IMPLEMENTADA EN EL MINISTERIO DE DEFENSA	1	IMPLEMENTACION Y SOSTENIBILIDAD DE SISTEMAS DE GESTIÓN EN EL MINDEF	346,000.00	322,000.00	304,000.00	304,000.00	346,000.00	304,000.00
	2	IMPLEMENTACIÓN DE TRANSFORMACIÓN DIGITAL PARA UNA GOBERNANZA TECNOLÓGICA SOSTENIBLE	342,480.00	342,480.00	347,480.00	347,480.00	347,480.00	347,480.00
	3	FORMULACIÓN Y DIFUSIÓN DEL ANUARIO ESTADISTICO DEL SECTOR DEFENSA	73,500.00	73,500.00	73,500.00	73,500.00	73,500.00	73,500.00
	4	LEVANTAMIENTO Y PRODUCCIÓN DE INFORMACIÓN ESTADÍSTICA DE LA SEDE CENTRAL DEL MINDEF	36,000.00	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00
	5	IMPLEMENTACIÓN DEL SIESDEF II EN LAS ENTIDADES DEL SECTOR DEFENSA	36,000.00	36,000.00	36,000.00	36,000.00	36,000.00	36,000.00
	6	ACTUALIZAR EL MARCO LEGAL Y NORMATIVO DEL SISTEMA ESTADÍSTICO DEL SECTOR DEFENSA	36,000.00	36,000.00	36,000.00	36,000.00	36,000.00	36,000.00
	7	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA TECNOLÓGICA	1,450,931.00	578,867.00	1,105,467.00	1,065,867.00	1,937,667.00	1,319,867.00
	8	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA DE COMUNICACIONES	764,000.00	170,800.00	2,319,800.00	170,800.00	119,800.00	170,800.00
	9	IMPLEMENTACION DE PROYECTOS RELACIONADOS A LA ADMINISTRACION DE BASE DE DATOS	430,233.00	430,233.00	430,233.00	430,233.00	90,000.00	90,000.00
	10	IMPLEMENTACION DE PROYECTOS DE SOPORTE TÉCNICO ESPECIALIZADO Y ATENCION A LOS USUARIOS	590,000.00	590,000.00	590,000.00	590,000.00	581,000.00	581,000.00
	11	SISTEMAS BÁSICOS INSTITUCIONALES	150,000.00	198,000.00	198,000.00	258,000.00	78,000.00	108,000.00
	12	SISTEMAS PARA LA PRESTACIÓN DE SERVICIOS	33,000.00	21,000.00	21,000.00		18,000.00	
	13	SISTEMAS PARA LA PARTICIPACIÓN DIGITAL DEL SECTOR	210,000.00	240,000.00	60,000.00	120,000.00	60,000.00	
	14	SOPORTE Y MANTENIMIENTO DE LOS SISTEMAS DIGITALES DEL MINDEF	81,000.00	240,000.00	240,000.00	240,000.00	240,000.00	240,000.00
SUB TOTAL 01			4,579,144.00	3,350,880.00	5,833,480.00	3,743,880.00	4,035,447.00	3,378,647.00
02. CIBERSEGURIDAD RESILIENTE EN EL SECTOR DEFENSA	15	FORTALECIMIENTO DE LA IDENTIFICACIÓN DE ACTIVOS DIGITALES EN EL MINDEF	260,000.00	260,000.00	260,000.00	260,000.00	260,000.00	260,000.00
	16	PROTECCIÓN DE LA INFORMACIÓN DIGITAL DEL MINDEF	3,675,825.52	1,299,773.36	784,993.36	2,937,916.68	1,400,000.00	1,490,000.00
	17	DETECCIÓN PROACTIVA DE AMENAZAS CIBERNÉTICAS EN LA INFRAESTRUCTURA DIGITAL DE MINDEF			2,875,000.00	50,000.00	50,000.00	2,275,000.00
	18	RESPUESTA RÁPIDA Y COORDINADA ANTE CIBERATAQUES EN EL MINDEF	108,000.00	874,666.67	121,333.33	600,500.00	723,000.00	196,333.33
	19	RESILIENCIA DIGITAL PARA LA RECUPERACIÓN DE LOS SISTEMAS EN EL MINDEF		252,000.00	252,000.00	252,000.00	252,000.00	252,000.00
SUB TOTAL 02			4,043,825.52	2,686,440.03	4,293,326.69	4,100,416.68	2,685,000.00	4,473,333.33
TOTALES			8,622,969.52	6,037,320.03	10,126,806.69	7,844,296.68	6,720,447.00	7,851,980.33

PROYECTOS Y ACTIVIDADES DEL PORTAFOLIO DEL PLAN DE GOBIERNO DIGITAL 2025-2030

NRO.	PROYECTO	ACTIVIDADES DE LOS PROYECTOS	2025	2026	2027	2028	2029	2030	TOTAL
1	IMPLEMENTACION Y SOSTENIBILIDAD DE SISTEMAS DE GESTIÓN EN EL MINDEF	Asegurar el funcionamiento del SGSI en el MINDEF y el SECTOR	120,000.00	120,000.00	120,000.00	120,000.00	120,000.00	120,000.00	720,000.00
		Auditoría externa del Sistema de Gestión de Seguridad de la Información ISO 27001:2022	42,000.00				42,000.00		84,000.00
		Auditoría interna del Sistema de Gestión de Seguridad de la Información ISO 27001:2022	10,000.00	10,000.00	10,000.00	10,000.00	10,000.00	10,000.00	60,000.00
		Auditoría interna de la Evaluación de cumplimiento del Ciclo de vida del software según ISO 12207	10,000.00	10,000.00	10,000.00	10,000.00	10,000.00	10,000.00	60,000.00
		Apoyo en la actualización del SGSI v.2022 en el MINDEF	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	432,000.00
		Apoyo en la implementación de SGSI en el SECTOR	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	432,000.00
		Apoyo en la elaboración de Directivas de seguridad y cumplimiento del SECTOR		18,000.00					18,000.00
		Evaluación de la gestión de la calidad en el proceso Mesa de Ayuda según ISO 9001	10,000.00						10,000.00
		Evaluación de la continuidad operativa del Centro de Datos del MINDEF según ISO 22301		10,000.00	10,000.00	10,000.00	10,000.00	10,000.00	50,000.00
		Evaluación de la exposición de contraseñas del MINDEF en Internet	10,000.00	10,000.00	10,000.00	10,000.00	10,000.00	10,000.00	60,000.00
TOTALES			346,000.00	322,000.00	304,000.00	304,000.00	346,000.00	304,000.00	1,926,000.00

PROYECTOS Y ACTIVIDADES DEL PORTAFOLIO DEL PLAN DE GOBIERNO DIGITAL 2025-2030

NRO.	PROYECTO	ACTIVIDADES DE LOS PROYECTOS	2025	2026	2027	2028	2029	2030	TOTAL
2	IMPLEMENTACIÓN DE TRANSFORMACIÓN DIGITAL PARA UNA GOBERNANZA TECNOLÓGICA SOSTENIBLE	Supervisión, control, monitoreo y emisión de los Documentos de Gestión de la OGTIE	54,000.00	54,000.00	54,000.00	54,000.00	54,000.00	54,000.00	324,000.00
		Atención de los requerimientos de información Internos y Externos solicitados de competencia a Gobernanza de TI							
		Seguimiento a la documentación por la contratación de los servicios especializados de la OGTIE							
		Monitoreo de las actividades de tecnologías de la información y estadística							
		Seguimiento continuo de la ejecución presupuestal de la OGTIE							
		Elaboración de los formatos para la planificación y ejecución presupuestal del PMBSO							
		Asegurar la plena ejecución del presupuesto en su totalidad							
		Elaboración de los formatos estratégicos de planificación (PEI-POI)	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	432,000.00
		Realizar la evaluación de los formatos estratégicos de planificación (PEI-POI)							
		Registrar en el SISPLAN la elaboración y evaluación del POI de la OGTIE							
		Elaboración de matriz de programación de gastos de la OGTIE							
		Monitorear los contratos vigentes de los servicios informáticos a cargo de la OGTIE							
		Elaboración de informes sobre el cumplimiento de los acuerdos establecidos en las reuniones del CGD							
		Monitorear y elaborar el avance de la programación del portafolio del PGD del MINDEF							
		Actualización del Portafolio del PGD del MINDEF							
		Control de calidad de sistemas básicos institucionales	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	432,000.00
		Control de calidad de sistemas para la prestación de servicios							
		control de calidad de sistemas para la participación digital del sector							
		control de calidad de para soporte y mantenimiento de los sistemas digitales del mindef	480.00	480.00	480.00	480.00	480.00	480.00	2,880.00
		Elaboración un plan de capacitación anual en habilidades digitales del MINDEF	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	432,000.00
		Monitoreo y seguimiento de la implementación del plan de capacitación en habilidades digitales del MINDEF			5,000.00	5,000.00	5,000.00	5,000.00	20,000.00
		Elaborar las políticas de transformación digital alineadas a las normativas vigentes							
		Promover la colaboración interinstitucional para la formulación de propuestas de estrategias digitales							
		Fomentar la interoperabilidad entre instituciones para optimizar los procesos digitales							
		Promover la mejora continua en la calidad de los servicios brindados a la ciudadanía							
		Elaborar las políticas de transformación digital alineadas a las normativas vigentes	18,000.00	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	378,000.00
		Asegurar la colaboración interinstitucional en la implementación de estrategias digitales							
Impulsar la interoperabilidad entre instituciones para optimizar los procesos digitales	54,000.00						54,000.00		
Garantizar la mejora continua en la calidad de los servicios brindados a la ciudadanía									
TOTALES			342,480.00	342,480.00	347,480.00	347,480.00	347,480.00	347,480.00	2,074,880.00

PROYECTOS Y ACTIVIDADES DEL PORTAFOLIO DEL PLAN DE GOBIERNO DIGITAL 2025-2030

NRO.	PROYECTO	ACTIVIDADES DE LOS PROYECTOS	2025	2026	2027	2028	2029	2030	TOTAL	
7	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA TECNOLÓGICA	Coordinador de Infraestructura tecnológica de la OGTIE	90,000.00	90,000.00	90,000.00	90,000.00	90,000.00	90,000.00	540,000.00	
		Gestión de documentos para la continuidad de los servicios de la Infraestructura tecnológica de la OGTIE								
		Gestión de la continuidad de la plataforma principal de almacenamiento y procesamiento								
		Gestión para administración de los servicios tecnológicos del Datacenter								
		Participar en comités de licitaciones (adquisiciones del estado)								
		Analizar, evaluar e informar los asuntos correspondientes a la infraestructura tecnológica y presentar las recomendaciones del caso.								
		Gestión de eventos e incidentes								
		Servicio de mantenimiento preventivo del sistema interrumpido de energía UPS principal piso 11 equipo nuevo	6,667.00	6,667.00	6,667.00	6,667.00	6,667.00	6,667.00	6,667.00	40,002.00
		Servicio de Protección dispositivos finales antivirus, DLP vence agosto 2025	16,464.00							16,464.00
		Adquisición de Herramientas y materiales de Soporte Técnico	4,000.00		4,000.00	4,000.00	4,000.00	4,000.00	4,000.00	20,000.00
		Servicio de mantenimiento preventivo y correctivo de impresoras multifuncionales de la sede central	60,000.00	60,000.00	60,000.00	60,000.00	60,000.00	60,000.00	60,000.00	360,000.00
		Renovación del servicio de soporte y mantenimiento de Certificados Digitales SSL vence nov 2025-POR 2 AÑOS	22,000.00		22,000.00			22,000.00		66,000.00
		Servicio de mantenimiento preventivo del sistema interrumpido de energía UPS principal piso 1 edificio quiñones		10,000.00	10,000.00					20,000.00
		Servicio Mantenimiento del Sistema Ininterrumpido de energía UPS Casa Odría	10,000.00							10,000.00
		Servicio de mantenimiento preventivo del sistema de aire acondicionado sede Casa Odría	7,000.00							7,000.00
		Reposición de sistema de aire acondicionado Casa Odría		30,000.00						30,000.00
		Renovación del Servicio de mantenimiento preventivo del sistema de aire acondicionado de precisión – Centro de Datos principal vence dic 2024	31,800.00		31,800.00					63,600.00
		Servicio configuración de sitio de contingencia de nube Oracle		317,000.00						317,000.00
		Servicio de implementación publicación de servicios de capa de nube Oracle			120,000.00					120,000.00
		Servicio de soporte para la solución de problemas de alta complejidad del sistema de Virtualización Principal Oracle	20,000.00	20,000.00	20,000.00	20,000.00	20,000.00	20,000.00	20,000.00	120,000.00
		Renovación de Licencias para el Servicio de Protección dispositivos finales antivirus, DLP vence agosto 2025	55,000.00	15,000.00	15,000.00	55,000.00	15,000.00	15,000.00	15,000.00	170,000.00
		Servicio de mantenimiento preventivo y correctivo del sistema contra incendios del centro de datos		24,200.00			24,200.00			72,600.00
		Servicio de soporte y actualización, relacionado al software de monitoreo de servicios de la infraestructura tecnológica del ministerio de defensa	20,000.00		20,000.00			20,000.00		60,000.00
		Servicio de soporte y mantenimiento de los productos MICROSOFT			700,000.00					700,000.00
		Servicio de mantenimiento de la solución de backup EMC NETWORKER	9,000.00							9,000.00
		Suscripción de licencia para la herramienta de monitoreo: Log de eventos y Usuarios Privilegiados	25,000.00							25,000.00
		Suscripción de licencia para la herramienta de Diagnóstico y Administración de Active Directory 400 usuarios)	24,000.00							24,000.00
IOARR Reposición de Backup Institucional Ministerio de Defensa	650,000.00	6,000.00	6,000.00	6,000.00				668,000.00		
IOARR Reposición del Centro de datos principal del Ministerio de Defensa						1,700,000.00		1,700,000.00		
IOARR Adquisición de infraestructura de procesamiento, almacenamiento y virtualización PCA del Ministerio de Defensa					800,000.00			800,000.00		
IOARR Adquisición de Hardware General y Software(Computadoras, Switchs, impresoras, laptops, software-POR 5 AÑOS)	400,000.00						400,000.00	800,000.00		
TOTALES			1,450,931.00	578,867.00	1,105,467.00	1,065,867.00	1,937,667.00	1,319,867.00	7,458,666.00	

PROYECTOS Y ACTIVIDADES DEL PORTAFOLIO DEL PLAN DE GOBIERNO DIGITAL 2025-2030

NRO.	PROYECTO	ACTIVIDADES DE LOS PROYECTOS	2025	2026	2027	2028	2029	2030	TOTAL
8	IMPLEMENTACION DE PROYECTOS DE INFRAESTRUCTURA DE COMUNICACIONES	Elaboración de documentos para la continuidad de servicios de comunicaciones del MINDEF	54,000.00	54,000.00	54,000.00	54,000.00	54,000.00	54,000.00	324,000.00
		Elaboración de documentos sobre la administración de los servicios de los dispositivos de comunicaciones							
		Elaboración de documentos sobre el estado situacional de los dispositivos de comunicaciones							
		Atención a la Central telefónica del MINDEF	42,000.00	42,000.00	42,000.00	42,000.00	42,000.00	42,000.00	252,000.00
		Atención a los ticket del sistema de mesa de ayuda del MINDEF							
		Atención a incidencias de servicios que brinda la Oficina de Telecomunicaciones (IT)							
		Tener a cargo el trámite documentario de la Oficina de Telecomunicaciones (IT)							
		Apoyar en el control de los pagos de telefonía móvil y fija (IT)							
		Realizar seguimiento y monitoreo de los requerimientos que se reciben a través de la Mesa de Ayuda.							
		Servicio de mantenimiento correctivo a los equipos de radioenlace del Ministerio de Defensa(Casa Odría y comando conjunto)		36,000.00		36,000.00		36,000.00	108,000.00
		Servicio de Mantenimiento preventivo y correctivo del sistema de video vigilancia CCTV (Centro de Datos Principal y alternativo) vence abril 2025		15,000.00		15,000.00		15,000.00	45,000.00
		Servicio de Mantenimiento de la Central Telefónica del MINDEF	15,000.00						15,000.00
		Servicio de implementación del Plan de Transición al Protocolo IPV6	18,000.00						18,000.00
		IOARR Adquisición de Antenas de Amplificación de señal celular INDOR para el Ministerio de Defensa-POR 5 AÑOS	635,000.00	23,800.00	23,800.00	23,800.00	23,800.00	23,800.00	754,000.00
		IOARR Reposición de Central telefónica del Ministerio de Defensa			200,000.00				200,000.00
IOARR Reposición de Core de datos de comunicaciones del Ministerio de Defensa			2,000,000.00				2,000,000.00		
TOTALES			764,000.00	170,800.00	2,319,800.00	170,800.00	119,800.00	170,800.00	3,716,000.00

PROYECTOS Y ACTIVIDADES DEL PORTAFOLIO DEL PLAN DE GOBIERNO DIGITAL 2025-2030

NRO.	PROYECTO	ACTIVIDADES DE LOS PROYECTOS	2025	2026	2027	2028	2029	2030	TOTAL
9	IMPLEMENTACION DE PROYECTOS RELACIONADOS A LA ADMINISTRACION DE BASE DE DATOS	Servicio de soporte y mantenimiento de productos Oracle o equivalente para PCA. Vence julio 2025	340,233.00						340,233.00
		Servicio de Soporte y Mantenimiento de Motor de Base de Datos del MINDEF	90,000.00	90,000.00	90,000.00	90,000.00	90,000.00	90,000.00	540,000.00
		IOARR Renovación del soporte y mantenimiento de productos Oracle o equivalente para PCA por 3 AÑOS		340,233.00	340,233.00				680,466.00
TOTALES			430,233.00	430,233.00	430,233.00	90,000.00	90,000.00	90,000.00	1,560,699.00

PROYECTOS Y ACTIVIDADES DEL PORTAFOLIO DEL PLAN DE GOBIERNO DIGITAL 2025-2030

NRO.	PROYECTO	ACTIVIDADES DE LOS PROYECTOS	2025	2026	2027	2028	2029	2030	TOTAL
10	IMPLEMENTACION DE PROYECTOS DE SOPORTE TÉCNICO ESPECIALIZADO Y ATENCION A LOS USUARIOS	Atención a los ticket de mesa de ayuda del MINDEF	48,000.00	48,000.00	48,000.00	48,000.00	48,000.00	48,000.00	288,000.00
		Elaboración de documentos para la continuidad de servicios de impresión y equipos informáticos del MINDEF							
		Elaboración de conformidades de servicios							
		Elaboración de Especificaciones técnicas							
		Servicio para renovación de licencias de videoconferencias y reuniones para el MINDEF ZOOM vence nov 2025	29,000.00	29,000.00	29,000.00	29,000.00	29,000.00	29,000.00	174,000.00
		Adquisición de Certificado digital de Reniec (Licencia para 800 usuarios)	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	36,000.00
		Adquisición de 100 Tarjetas y/o Tokens Criptográficos tipo USB	9,000.00	9,000.00	9,000.00	9,000.00			36,000.00
		Adquisición de suministros de impresión	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	180,000.00
		Servicio de soporte informático a usuarios del MINDEF-SERVICIO DE SOPORTE INFORMATICO	60,000.00	60,000.00	60,000.00	60,000.00	60,000.00	60,000.00	360,000.00
		Servicio de soporte informático a usuarios del MINDEF-SERVICIO DE SOPORTE INFORMATICO	60,000.00	60,000.00	60,000.00	60,000.00	60,000.00	60,000.00	360,000.00
		Servicio de soporte informático a usuarios del MINDEF-SOPORTE TECNICO EN REDES	42,000.00	42,000.00	42,000.00	42,000.00	42,000.00	42,000.00	252,000.00
		Servicio de soporte informático a usuarios del MINDEF-ADMINISTRACION DE REDES	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	432,000.00
		Servicio de soporte informático a usuarios del MINDEF-SOPORTE TECNICO DE SERVIDORES	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	432,000.00
		Servicio Especializado para el Soporte y Mantenimiento de todas las Base de Datos del MINDEF	90,000.00	90,000.00	90,000.00	90,000.00	90,000.00	90,000.00	540,000.00
Servicio Especializado para la administración de la red informática del MINDEF	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	72,000.00	432,000.00		
TOTALES			590,000.00	590,000.00	590,000.00	590,000.00	581,000.00	581,000.00	3,522,000.00

PROYECTOS Y ACTIVIDADES DEL PORTAFOLIO DEL PLAN DE GOBIERNO DIGITAL 2025-2030

NRO.	PROYECTO	ACTIVIDADES DE LOS PROYECTOS	2025	2026	2027	2028	2029	2030	TOTAL
11	SISTEMAS BÁSICOS INSTITUCIONALES	Supervisión, control, monitoreo y emisión de los Documentos de Desarrollo Y mantenimiento de Sistemas	78,000.00	78,000.00	78,000.00	78,000.00	78,000.00	78,000.00	468,000.00
		Atención de los requerimientos de Sistemas de información solicitados a OGTIE							
		Seguimiento al cumplimiento de los proyectos informáticos a implementar en el MINDEF							
		Seguimiento a la documentación generada del desarrollo y mantenimiento de Sistemas OGTIE							
		Monitoreo de las actividades del equipo de Innovación tecnológica OGTIE							
		Seguimiento del cumplimiento de la Normatividad Procesos de desarrollo, ISO 27001, ISO 12207							
		Reunión de Trabajo con las direcciones sobre las necesidades de Sistemas informáticos							
		DESARROLLO DEL SISTEMA DE GESTIÓN VEHICULAR – GESTIÓN DE PAPELETAS – GESTIÓN DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO	9,000.00			60,000.00		30,000.00	99,000.00
		SISTEMA DE PARTE DIARIO MILITAR DEL MINDEF	15,000.00						15,000.00
		SISTEMA DE GESTION NORMATIVA DE LA SG – MÓDULO DE USUARIOS / MIGRACIÓN / CONSULTA GENERAL	16,500.00						16,500.00
		SISTEMA DE CONVOCATORIAS DE PERSONAL EN LÍNEA v2.0 DESARROLLO							
		SISTEMA ESTADISTICO – FASE III, INDICADORES Y DASHBOARD PARA SEDE CENTRAL DEL MINDEF-ANALISTA		60,000.00	60,000.00	60,000.00			180,000.00
		ACTUALIZACION SISTEMA DE MANEJO DE EXPEDIENTES JUDICIALES PROCURADURIA	15,000.00						15,000.00
		ACTUALIZACION DEL SISTEMA DE CONTROL DE INGRESOS SEGURIDAD	16,500.00						16,500.00
		SISTEMA DE TESORERÍA SITES V3.0		60,000.00	60,000.00	60,000.00			180,000.00
TOTALES		150,000.00	198,000.00	198,000.00	258,000.00	78,000.00	108,000.00	990,000.00	

PROYECTOS Y ACTIVIDADES DEL PORTAFOLIO DEL PLAN DE GOBIERNO DIGITAL 2025-2030

NRO.	PROYECTO	ACTIVIDADES DE LOS PROYECTOS	2025	2026	2027	2028	2029	2030	TOTAL
12	SISTEMAS PARA LA PRESTACIÓN DE SERVICIOS	SISTEMA DE CONVOCATORIAS DE PERSONAL EN LÍNEA v2.0 AN ALISTA	18,000.00	21,000.00	21,000.00				60,000.00
		SISTEMA CENTRALIZADO DE REGISTRO MILITAR – INSCRIPCIÓN EN LÍNEA / Vulnerabilidades/ Integración	15,000.00				18,000.00		33,000.00
TOTALES			33,000.00	21,000.00	21,000.00		18,000.00		93,000.00

PROYECTOS Y ACTIVIDADES DEL PORTAFOLIO DEL PLAN DE GOBIERNO DIGITAL 2025-2030

NRO.	PROYECTO	ACTIVIDADES DE LOS PROYECTOS	2025	2026	2027	2028	2029	2030	TOTAL
13	SISTEMAS PARA LA PARTICIPACIÓN DIGITAL DEL SECTOR	SISTEMA ESTADISTICO FASE II – MODULO TELEMATICA DEL SECTOR DEFENSA	12,000.00						12,000.00
		SISTEMAS DE BENEFICIOS DE PERSONAL TROPA DEL SECTOR DEFENSA	60,000.00			60,000.00			120,000.00
		SISTEMAS PARA EL CONTROL DE PERSONAL CON DISCAPACIDAD DEL SECTOR DEFENSA	30,000.00						30,000.00
		SISTEMA CENTRALIZADO DE LEGAJOS DEL SECTOR – DATOS DE PROYECTOS DE INVESTIGACIÓN		60,000.00					60,000.00
		SISTEMA CENTRALIZADO DE REGISTRO MILITAR – MÓDULO DE RECLUTAMIENTO DEL SECTOR DEFENSA		60,000.00					60,000.00
		SISTEMA DE PARTE DIARIO DEL SECTOR DEFENSA RRHH DESARROLLO	78,000.00	60,000.00					138,000.00
		SISTEMA DE PLANIFICACIÓN, REGISTRO Y SEGUIMIENTO DE ACCIONES CÍVICAS DEL SECTOR DEFENSA		60,000.00					60,000.00
		SISTEMA DE PLANEAMIENTO DEL SECTOR DEFENSA V 2.0			60,000.00	60,000.00	60,000.00		180,000.00
		SISTEMA PARA EL REGISTRO DE CONTROL DE PANDEMIAS DEL SECTOR DEFENSA	30,000.00						30,000.00
TOTALES			210,000.00	240,000.00	60,000.00	120,000.00	60,000.00		690,000.00

PROYECTOS Y ACTIVIDADES DEL PORTAFOLIO DEL PLAN DE GOBIERNO DIGITAL 2025-2030

NRO.	PROYECTO	ACTIVIDADES DE LOS PROYECTOS	2025	2026	2027	2028	2029	2030	TOTAL	
16	PROTECCIÓN DE LA INFORMACIÓN DIGITAL DEL MINDEF	Gestión de la protección de los activos digitales del MINDEF	60,000.00	60,000.00	60,000.00	60,000.00	60,000.00	60,000.00	360,000.00	
		Gestión de los sistemas de seguridad informática para proteger la infraestructura tecnológica del MINDEF.								
		Mantenimiento preventivo para optimizar el rendimiento de los equipos de seguridad informática y realizar correcciones necesarias.								
		Monitoreo y análisis del tráfico de red de forma continua para identificar patrones anómalos, intrusiones o comportamientos sospechosos.								
		Cumplimiento de las directivas, normas y políticas de seguridad establecidas, dentro de las actividades relacionadas con la gestión de los sistemas de seguridad informática.								
		Configuración y actualización de los sistemas de seguridad informática, para mantener su correcta operatividad y/o funcionamiento.								
		Solución de problemas técnicos relacionados con la seguridad informática, con la finalidad de que los servicios de red se mantengan operativos y protegidos ante posibles amenazas.								
		Mantenimiento del Sistema de Seguridad Firewall de Aplicaciones Web - 2022	19,827.80							19,827.80
		Mantenimiento del Sistema de Seguridad Anti-Malware - 2022	21,894.50							21,894.50
		Mantenimiento del Sistema de Seguridad Antidenegador de Servicios - 2022	14,576.00							14,576.00
		Mantenimiento del Sistema de Seguridad Firewall de Base de Datos - 2022	13,889.60							13,889.60
		Mantenimiento del Sistema de Filtrado de Contenido Web - 2022	13,780.90							13,780.90
		Soporte y mantenimiento del Sistema de Seguridad Firewall de capa 3 - 2024	14,160.04	14,160.04	14,160.04					42,480.12
		Mantenimiento del Sistema de Seguridad para Correo Electrónico (Anti-Spam) - 2023	19,780.00	19,780.00						39,560.00
		IOARR Reposición del Sistema de Seguridad Firewall de Aplicaciones Web - 2025	617,500.00							617,500.00
		IOARR Reposición del Sistema de Seguridad Anti-Malware - 2025	760,000.00							760,000.00
		IOARR Reposición del Sistema de Seguridad Antidenegador de Servicios - 2025	570,000.00							570,000.00
		IOARR Reposición del Sistema de Seguridad Firewall de Base de Datos - 2025	760,000.00							760,000.00
		IOARR Reposición del Sistema de Filtrado de Contenido Web - 2025	760,000.00							760,000.00
		Soporte y mantenimiento del Sistema de Seguridad Firewall de Aplicaciones Web - 2025	5,416.67	10,833.33	10,833.33	5,416.67				32,500.00
		Soporte y mantenimiento del Sistema de Seguridad Anti-Malware - 2025	6,666.67	13,333.33	13,333.33	6,666.67				40,000.00
		Soporte y mantenimiento del Sistema de Seguridad Antidenegador de Servicios - 2025	5,000.00	10,000.00	10,000.00	5,000.00				30,000.00
		Soporte y mantenimiento del Sistema de Seguridad Firewall de Base de Datos - 2025	6,666.67	13,333.33	13,333.33	6,666.67				40,000.00
		Soporte y mantenimiento del Sistema de Filtrado de Contenido Web - 2025	6,666.67	13,333.33	13,333.33	6,666.67				40,000.00
		IOARR Adquisición del Sistema de Autenticación de Doble Factor - 2026		570,000.00						570,000.00
		Soporte y mantenimiento del Sistema de Autenticación de Doble Factor - 2026		5,000.00	10,000.00	10,000.00	5,000.00			30,000.00
		IOARR Reposición del Sistema de Seguridad para Correo Electrónico (Anti-Spam) - 2026		570,000.00						570,000.00
		Soporte y mantenimiento del Sistema de Seguridad para Correo Electrónico (Anti-Spam) - 2026			10,000.00	10,000.00	10,000.00			30,000.00
		IOARR Renovación del Sistema de Seguridad para Correo Electrónico (Anti-Spam) - 2029						420,000.00		420,000.00
		Mantenimiento del Sistema de Seguridad para Correo Electrónico (Anti-Spam) - 2029							60,000.00	60,000.00
		IOARR Renovación del Sistema de Seguridad Firewall de capa 3 - 2027			630,000.00					630,000.00
		Mantenimiento del Sistema de Seguridad Firewall de capa 3 - 2027					90,000.00	90,000.00	90,000.00	270,000.00
		IOARR Renovación del Sistema de Seguridad Firewall de Aplicaciones Web - 2028					455,000.00			455,000.00
		IOARR Renovación del Sistema de Seguridad Anti-Malware - 2028					560,000.00			560,000.00
		IOARR Renovación del Sistema de Seguridad Antidenegador de Servicios - 2028					420,000.00			420,000.00
		IOARR Renovación del Sistema de Seguridad Firewall de Base de Datos - 2028					560,000.00			560,000.00
		IOARR Renovación del Sistema de Filtrado de Contenido Web - 2028					560,000.00			560,000.00
		Mantenimiento del Sistema de Seguridad Firewall de Aplicaciones Web - 2028					32,500.00	65,000.00	65,000.00	162,500.00
		Mantenimiento del Sistema de Seguridad Anti-Malware - 2028					40,000.00	80,000.00	80,000.00	200,000.00
		Mantenimiento del Sistema de Seguridad Antidenegador de Servicios - 2028					30,000.00	60,000.00	60,000.00	150,000.00
		Mantenimiento del Sistema de Seguridad Firewall de Base de Datos - 2028					40,000.00	80,000.00	80,000.00	200,000.00
		Mantenimiento del Sistema de Filtrado de Contenido Web - 2028					40,000.00	80,000.00	80,000.00	200,000.00
IOARR Renovación del Sistema de Autenticación de Doble Factor - 2029						420,000.00		420,000.00		
Mantenimiento del Sistema de Autenticación de Doble Factor - 2029						30,000.00	60,000.00	90,000.00		
IOARR Reposición del Sistema de Seguridad Firewall de capa 3 - 2030								855,000.00		
TOTALES			3,675,825.52	1,299,773.36	784,993.36	2,937,916.68	1,400,000.00	1,490,000.00	11,588,508.92	

PROYECTOS Y ACTIVIDADES DEL PORTAFOLIO DEL PLAN DE GOBIERNO DIGITAL 2025-2030

NRO.	PROYECTO	ACTIVIDADES DE LOS PROYECTOS	2025	2026	2027	2028	2029	2030	TOTAL	
17	DETECCIÓN PROACTIVA DE AMENAZAS CIBERNÉTICAS EN LA INFRAESTRUCTURA DIGITAL DE MINDEF	IOARR Adquisición del Sistema de Gestión de información y eventos de seguridad (SIEM) - 2027			2,850,000.00				2,850,000.00	
		Soporte y mantenimiento del Sistema de Gestión de información y eventos de seguridad (SIEM) - 2027			25,000.00	50,000.00	50,000.00	25,000.00	150,000.00	
		IOARR Renovación del Sistema de Gestión de información y eventos de seguridad (SIEM) - 2030							2,100,000.00	2,100,000.00
		Mantenimiento del Sistema de Gestión de información y eventos de seguridad (SIEM) - 2030							150,000.00	150,000.00
TOTALES					2,875,000.00	50,000.00	50,000.00	2,275,000.00	5,250,000.00	

PROYECTOS Y ACTIVIDADES DEL PORTAFOLIO DEL PLAN DE GOBIERNO DIGITAL 2025-2030

NRO.	PROYECTO	ACTIVIDADES DE LOS PROYECTOS	2025	2026	2027	2028	2029	2030	TOTAL	
18	RESPUESTA RÁPIDA Y COORDINADA ANTE CIBERATAQUES EN EL MINDEF	Gestión de la respuesta ante incidentes de seguridad informática en el MINDEF	108,000.00	108,000.00	108,000.00	108,000.00	108,000.00	108,000.00	648,000.00	
		Desarrollo y gestión de planes de respuesta ante incidentes de seguridad informática.								
		Coordinación con las partes interesadas para la gestión de incidentes.								
		Fortalecimiento de la concientización sobre seguridad informática y respuesta ante incidentes.								
		Implementación, monitoreo y evaluación de la efectividad de las soluciones de seguridad informática implementadas.								
		Fortalecimiento de la infraestructura tecnológica del MINDEF.								
		Respuesta ante incidentes a través de los sistemas de seguridad informática.								
		IOARR Adquisición del Sistema de Seguridad EDR - 2028					475,000.00			475,000.00
		Soporte y mantenimiento del Sistema de Seguridad EDR - 2028 AL 2030					4,166.67	8,333.33	8,333.33	20,833.33
		IOARR Adquisición del Sistema de Seguridad XDR - 2026			760,000.00					760,000.00
		Soporte y mantenimiento del Sistema de Seguridad XDR - 2026 AL 2029			6,666.67	13,333.33	13,333.33	6,666.67		40,000.00
		IOARR Renovación del Sistema de Seguridad XDR - 2029						560,000.00		560,000.00
Mantenimiento del Sistema de Seguridad XDR - 2029 AL 2030						40,000.00	80,000.00	120,000.00		
TOTALES			108,000.00	874,666.67	121,333.33	600,500.00	723,000.00	196,333.33	2,623,833.33	

