

COMISIÓN DE CIENCIA, INNOVACIÓN Y TECNOLOGÍA

PERÍODO ANUAL DE SESIONES 2024 - 2025

ACTA

DÉCIMA QUINTA SESIÓN ORDINARIA

SEMIPRESENCIAL

Lima, 14 de abril de 2025

Aprobación de Acta	1. El presidente sometió a votación la aprobación del Acta de la Décima Cuarta Sesión Ordinaria de la Comisión de Ciencia, Innovación y Tecnología, celebrado el lunes 07 de marzo de 2025, siendo aprobado por UNANIMIDAD.
Introducción	En Lima, en la Sala de Sesiones N° 1 (Carlos Torres y Torres Lara) del Edificio Víctor Raúl Haya de la Torre del Congreso de la República y a través de la Plataforma Microsoft TEAMS, siendo las 9:08 horas del lunes 14 de abril de 2025, se reunieron, bajo la presidencia del congresista Alfredo Pariona Sinche, contando con la presencia de los congresistas: Carlos Javier Zeballos Madariaga, Carlos Enrique Alva Rojas, Segundo Héctor Acuña Peralta, Ernesto Bustamante Donayre, Waldemar José Cerrón Rojas, Miguel Ángel Ciccía Vásquez, Víctor Seferino Flores Ruíz, David Julio Jiménez Heredia, Silvia María Monteza Facho y Magally Santisteban Suclupe; en calidad de miembros titulares. Con el quórum reglamentario se inició la décima quinta sesión ordinaria de la Comisión de Ciencia, Innovación y Tecnología, para el periodo de sesiones 2024 - 2025, semipresencial. <i>Ausentes con licencias de los congresistas:</i> George Edward Málaga Trillo, Abel Augusto Reyes Cam y Karol Ivett Paredes Fonseca Se pasa a la estación de despacho.
Despacho	El presidente dio cuenta que se ha enviado a los correos institucionales de los congresistas miembros de la comisión, los documentos enviados y recibidos desde el 04 al 11 de abril de 2025. Se pasa a la estación de informes.

Informes	El presidente informa que el 15 de abril se llevó a cabo el evento Foro Panel denominado: "LATAM-GPT: Primer modelo IA del lenguaje (LLM) Latinoamericano", realizado el viernes 11 de abril del presente año, en el horario de las 10:00 hrs. en el Sala Héroes de la Democracia del Congreso de la República. Se pasa a la estación de pedidos.
Pedidos	No hubo pedidos de los señores congresistas Se pasa a la estación de la Orden del Día.
Orden del Día	1. Como primer punto de orden del día, el presidente da la bienvenida al señor ORLANDO VÁSQUEZ RUBIO, Secretaría de Gobierno y Transformación Digital (PCM), quien informa sobre los avances y desafíos en materia de Ciberseguridad, Ciberdefensa y Ciberdelincuencia. El secretario de Gobierno y Transformación Digital (PCM), inicia su exposición saludando a los congresistas y funcionarios presentes en la sala de sesiones. Asimismo, manifiesta que existe un problema de infraestructura. "Actualmente tenemos un proyecto con el Banco Interamericano de Desarrollo para potenciar las herramientas que en su mayoría son caras", aseveró el funcionario. Asimismo, informó que viene trabajando en identidad digital que tiene que ver con la implementación de validaciones seguras a través del RENIEC. También, dijo se trabaja en computación cuántica, a través de un grupo de expertos, ya que va a afectar la seguridad digital "Venimos trabajando en nuestro reglamento 007 a fin de poder trabajar con entes privados siguiendo la recomendación de los expertos coreanos", refirió el funcionario. Dentro de los indicadores internacionales: • Nivel 3 Perú en "Estableciendo la ciberseguridad" según ITU 2024 • Nivel 7 Entre 35 países del continente: Brasil lidera en Latinoamérica (capa 1), seguido por Ecuador, México y Uruguay (capa 2). Perú integra la capa 3 junto con Chile, Colombia y otros países en desarrollo de capacidades. • Nivel 9 Posición Mundial: Entre los 49 países de la capa 3

Con relación a la coordinación y articulación, esta colección corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, en el marco del Centro Nacional de Seguridad Digital (CNSD).

Acto seguido el presidente da la bienvenida al General de Brigada EP **JHON RIVERA MACHUCA**, Cmdte. Del Comando de Operaciones de CIBERDEFENSA (MINDEF, quien informa sobre los avances y desafíos en materia de Ciberseguridad, Ciberdefensa y Ciberdelincuencia.

El General de Brigada del Comando de Operaciones de CIBERDEFENSA (MINDEF), inicia su exposición saludando a los congresistas y funcionarios presentes en la sala de sesiones. Asimismo, señala que dentro del marco legal de Ciberdefensa consideran 3 puntos importantes:

- **Constitución Política del Perú**, donde en su **artículo 44.-** Deberes del Estado, dice que son deberes primordiales del Estado: defender la soberanía nacional; garantizar la plena vigencia de los derechos humanos; proteger a la población de las amenazas contra su seguridad; y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación.
- **Ley de Gobierno Digital**, en su Decreto Legislativo 1412 (12 Set 18) en su **artículo 30.- LA SEGURIDAD DIGITAL** es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad y los objetivos nacionales en dicho entorno.
- **La Ley N° 30999 ley de CIBERDEFENSA** que tiene la singularidad de establecer el objeto de la regulación de Ciberdefensa en el Perú. Además, porque se define de manera específica como una capacidad militar con atribución exclusiva de las organizaciones militares en el Perú.

La CIBERDEFENSA está a cargo del Comando Conjunto de las Fuerzas Armadas, están sujetas al artículo 51° de la carta de las Naciones Unidas, donde expresa que todos tienen derecho a la legítima defensa cuando sean atacados por otros países.

Asimismo, se establece que la finalidad de la CIBERDEFENSA es entre otros la protección de los activos críticos nacionales y los recursos claves.

Dentro de los avances y desafíos en materia de CIBERDEFENSA:

En abril 2024 el MINDEF solicita facultades legislativas: adecuación Ley 30999.

LEY 30999, LEY DE CIBERDEFENSA SEGUNDA. Modificaciones a normas de las FFAA en materia de ciberdefensa.

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

- Modificar las leyes de las Fuerzas Armadas con el objeto de incorporar la competencia en CIBERDEFENSA, así como precisar la ubicación del órgano de línea en la estructura organizacional de cada una de ellas, teniendo la urgencia por el principio de legalidad.
- Cumplir la misión del COCID, impactando en la protección en el ciberespacio de los acn (56% alta incidencia digital) y RC manteniendo las capacidades nacionales

Dentro de los avances y desafíos en materia de CIBERDEFENSA:

1. El 28 de mayo 2024 el Ministro de Defensa sustenta en el congreso adecuación de las normas de las FFAA a la Ley 30999 (Ley de Ciberdefensa).
2. Aprobado en el Pleno del Congreso el 14 de junio 2024 en 1ra votación, el 01 julio en 2da votación. El 4 de julio se publica en El Peruano (Ley 32089).

3. Decreto Legislativo N° 1639 que modifica el Decreto Legislativo N° 1136 Decreto Legislativo del Comando Conjunto de las Fuerzas Armadas (Competencia y funciones de CIBERDEFENSA).

Funciones del CCFFAA:

- Planificar y ejecutar las operaciones militares de ciberdefensa, en y mediante el ciberespacio, así como el cumplimiento de las responsabilidades asignadas en la normatividad vigente.
- Planificar, coordinar, organizar y conducir operaciones militares de ciberdefensa, en y mediante el ciberespacio, para el control y protección de activos críticos nacionales y recursos claves, de acuerdo con la normatividad vigente.
- Dirigir y centralizar el registro de información sobre ataques informáticos y patrones de amenazas de ciberdefensa de las Fuerzas Armadas, aplicando los mecanismos de información clasificada.

4. Decreto Legislativo N° 1640 que modifica el Decreto Legislativo N° 1137 Ley del Ejército del Perú (Comando de Operaciones CIBERNÉTICAS).

Artículo 17-A. El Comando de Operaciones Cibernéticas opera, defiende, responde, influye e informa en el dominio del ciberespacio, en el ámbito de su competencia, para proteger y defender la información y las comunicaciones, a través de la capacidad de ciberdefensa, asegurando el comando y control, frente a las amenazas que afecten la seguridad nacional, los intereses nacionales, los activos críticos nacionales (ACN) y recursos claves (RC) para mantener las capacidades nacionales en el área de su responsabilidad. El cargo del comandante General de Operaciones Cibernéticas es ejercido por un Oficial del Grado de General. Su organización interna, conformación y funciones se regulan en el reglamento de la presente norma.

5. Decreto Legislativo N° 1641 que modifica el Decreto Legislativo N° 1138 Ley de la Marina de Guerra del Perú (Comandancia de CIBERDEFENSA).

Artículo 20-A. La Comandancia de Ciberdefensa es un órgano que ejerce el control, la vigilancia y la defensa del entorno digital o ciberespacio, orientado a la defensa y protección de la soberanía, los intereses nacionales, los activos críticos nacionales (ACN) y recursos claves (RC) para mantener las capacidades nacionales en el área de su responsabilidad. El cargo del comandante de Ciberdefensa es ejercido por un Oficial Almirante. Su organización interna, conformación y funciones se regulan en el reglamento de la presente norma."

Los desafíos para la ciberdefensa, en un contexto de intenso desarrollo de las tecnologías disruptivas y emergentes, son variados y complejos:

- Asimetría en capacidades operativas
- Amenazas originadas por tecnologías disruptivas
- Débil nivel de conciencia pública, sobre las amenazas digitales.

Finalmente, las conclusiones que señala son los siguientes:

- La Ley de Ciberdefensa y su Reglamento, representa el paso inicial para el desarrollo de la Ciberdefensa en el Estado peruano.
- El equilibrio entre los avances tecnológicos, el desarrollo de las capacidades humanas, y la cooperación estratégica, será crucial para alcanzar una ciberdefensa robusta.
- La tecnología es cada vez más sofisticada, y con ella se incrementan los retos y las oportunidades para lograr una ciberdefensa capaz de contribuir eficazmente a la Seguridad Digital de nuestro país.

En la misma línea el presidente da la bienvenida al coronel del Ejército Peruano **OCTAVIO MARTÍN FREITAS FARFAN**, jefe de la unidad conjunta de Ciberdefensa del Comando Operacional de Ciberdefensa del Comando Conjunto de las FFAA, quien informa sobre los avances y desafíos en materia de Ciberseguridad, Ciberdefensa y Ciberdelincuencia.

El jefe de la unidad conjunta de Ciberdefensa del Comando Operacional de Ciberdefensa del Comando Conjunto de las FFAA

inicia su exposición saludando a los congresistas y funcionarios presentes en la sala de sesiones. Asimismo, señala que la misión de su institución es prevenir, combatir, investigar y denunciar los delitos informáticos, cometidos a través de la TICs; cometido por delincuentes comunes u organizaciones criminales; asimismo, realizar el análisis informático forense y acciones de geolocalización.

En ese sentido, señala que la manera especial de actuar o trabajar para alcanzar el fin propuesto (MODUS OPERANDI):

- **PHISHING.** - Técnica para lograr obtener información confidencial bancario, laboral, etc.
- **SIM SWAPING.** - Técnica para lograr obtener información confidencial bancario, laboral, etc.

CARDING.- Es cuando el Ciberdelincuente roba información de las tarjetas bancarias para realizar compras en línea de productos y servicios

- **SMISHING.** - Mensajes de texto falso dirigido a los usuarios de telefonía móvil.
- **THIEF TRANSFER.** - Modalidad delictiva que roba información de los equipos móviles sustraídos y/o robados.

RANSOWARE. - Secuestro y robo de datos mediante el cifrado, con fines económicos.

- **VISHING.** - Llamadas telefónicas falsas con el fin de obtener información confidencial, bancario, laboral, etc.
- **THIEF SCAM.** - Modalidad delictiva que el ciberdelincuente utiliza para suplantar la identidad de una víctima desde su cuenta de usuario.

FAKEAPP. - Modalidad delictiva que sustrae la información de un equipo móvil instalado en un falso aplicativo y tomar control de este.

Al respecto, indica que los casos relevantes de ciberdelincuencia fue la venta de información a través del grupo TELEGRAM, así como delitos que van contra la dignidad y libertad sexual.

Dentro de la comparativa normativa:

- **Artículo 2°.- Acceso ilícito**

La pena será no menor de uno ni mayor de cuatro años si:

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado o si accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

- **Artículo 189°.- Robo agravado**

La pena será no menor de doce ni mayor de veinte años si el robo se comete:

9. Sobre equipo terminal móvil, teléfono celular, equipo o aparato de telecomunicaciones, red o sistemas de telecomunicaciones u otro bien de naturaleza similar.

- **Artículo 154°-A.- Tráfico ilegal de datos personales***

La pena será no menor de doce ni mayor de veinte años si el robo se comete:

El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años.

- **Artículo 189°.- Robo agravado**

La pena será no menor de doce ni mayor de veinte años si el robo se comete:

9. Sobre equipo terminal móvil, teléfono celular, equipo o aparato de telecomunicaciones, red o sistemas de telecomunicaciones, red o sistemas de telecomunicaciones u otro bien de naturaleza similar.

Por otro lado, señala sobre las **PROPUESTAS PARA INTEROPERATIVIDAD:**

Creación de una oficina de coordinaciones de conflictos y respuestas operativas en flagrancia.

Fines:

- Operatividad 24/7 incidencias fraudulentas.
- Intercambio de información sobre posibles ataques o vulnerabilidades a clientes con las entidades financieras y empresas prestadoras de servicios de telecomunicaciones.
- Contar con capacitación constante sobre el tratamiento de información.
- Contar con un equipo especial operativo conformado por personal de la DIRCIBERD y agentes de las oficinas de fraudes de las entidades financieras y de telecomunicaciones.

Modificatoria de la Ley de Delitos Informáticos

Objetivo:

- Aumento de la pena efectiva y sus agravantes.
- Análisis de la tipificación del acto ilícito debido al avance de las formas de ciberdelitos.
- Integración o creación de nuevos artículos debido a las nuevas modalidades delictivas y sus medios utilizados.
- Fortalecer la actuación de los efectivos policiales en las investigaciones de los delitos informáticos en el Perú.

En la misma línea intervino el Mayor PNP **PIERRE RUIZ CONTRERAS**, El jefe División de Investigación de Alta Tecnología - Dirección de Investigación Criminal de la Policía Nacional del Perú (DEPIDCATC-DIRCIBERD) – MININTER, quien señala se cuenta con una división especializada dentro de la dirección dónde venimos obteniendo medidas limitativas de derecho que son allanamientos y descerrajes de estas personas que afectan a la juventud, logrando las capturas correspondientes",

El congresista ERNESTO BUSTAMANTE DONAYRE saluda a todos los presentes en la sala de sesiones y a los que se encuentran en forma virtual. Asimismo, realiza las siguientes preguntas al Ing. **ORLANDO VÁSQUEZ RUBIO**, Secretaría de Gobierno y Transformación Digital (PCM), quien mencionó que una de las funciones de la red nacional de seguridad digital, es el monitoreo y habla de la vigilancia permanente del Ciberespacio y, luego indicó sobre los

avances del 2025 menciona que hubo 164 situaciones críticas resueltas.

¿Puede dar algunos ejemplos de estas situaciones críticas resueltas? para tener una idea si se trata de cosas sencillas o un abanico de ellas

Por otro lado, realiza otra pregunta al General de Brigada EP **JHON RIVERA MACHUCA**, Cmdte. Del Comando de Operaciones de CIBERDEFENSA (MINDEF), quien mencionó sobre el quinto dominio de guerra en el Ciberespacio.

El personal que está asignado a esta división, quienes rotan después de dos o tres años, lo mismo pasa en CONIDA. También existe otro grupo de personal civil que está adscrito y contratados por un sistema de locación, no tienen estabilidad y existe mucha fuga de talentos.

¿Como está organizado el personal a nivel de Ciberdefensa?

También hace otra pregunta al Mayor PNP **PIERRE RUIZ CONTRERAS**, El jefe División de Investigación de Alta Tecnología - Dirección de Investigación Criminal de la Policía Nacional del Perú (DEPIDCATC-DIRCIBERD) – MININTER, quien mencionó el MODOS OPERANDI, como es: PHISHING, SIM SWAPING, SMISHING, THIEF TRANSFER, VISHING y THIEF SCAM.

Porque muchos de ellos son llamadas extorsivas, pero también tratan de llegar a la intimididad personal.

¿Que se está haciendo con relación a las llamadas SPAM?

El presidente formula algunas interrogantes sobre la inseguridad en el país, donde se ha escuchado diversos plataformas y mecanismos para enfrentar, sin embargo, algunos opinan que en la actualidad la delincuencia y otros males como la corrupción que se ha institucionalizado en casi todas las entidades.

Por otro lado, señala un débil sistema judicial, la pobreza y la desigualdad que se ha incrementado. Asimismo, sucede con el crecimiento del crimen organizado donde existe falta de inversión para la prevención.

¿Qué acciones viene impulsando la secretaria, para garantizar que las entidades públicas cuenten con un protocolo unificado de respuesta ante el ciber ataque, considerando el incremento de incidencias en los últimos años?

¿Existe la voluntad política y el presupuesto necesario para avanzar hacia una arquitectura de Ciberdefensa nacional?

Por otro lado, realiza algunas preguntas al Ministerio de Defensa

El Comando conjunto de Ciberdefensa frente a la Ciber amenazas provenientes de actores estatales y extranjeros, considerando el actual contexto geopolítico de recientes reportes de amenazas híbridas en América Latina.

¿Cuál es el papel que se está cumpliendo frente a estas amenazas?

¿Cuáles son los principales cuellos de botella que se está enfrentando para consolidar una capacidad operativa y sostenida en Ciberdefensa, especialmente en términos de recurso humanos especializados en tecnología?

Por otro lado, realiza algunas preguntas a la Policía Nacional del Perú

¿Qué tan efectiva ha sido la colaboración entre la división de investigación de delitos de alta tecnología y el ministerio público para judicializar casos complejos de Ciber delitos y que reformas normativas se necesita para agilizar estos procesos?

Estamos en la era de la digitalización y la tecnología, sin embargo, las denuncias en línea no se pueden realizar debido que se encuentra en mantenimiento.

Concluida la exposición del jefe de la unidad conjunta de Ciberdefensa del Comando Operacional de Ciberdefensa del Comando Conjunto de las FFAA., los congresistas formularon intervenciones y preguntas, las mismas que fueron absueltas por el invitado en el desarrollo de la sesión.

El presidente, agradece la presencia del coronel del Ejército Peruano **OCTAVIO MARTÍN FREITAS FARFAN**, jefe de la unidad

conjunta de Ciberdefensa del Comando Operacional de Ciberdefensa del Comando Conjunto de las FFAA. Asimismo, comunica que puede abandonar la sala virtual cuando lo estime conveniente.

La congresista MAGALLY SANTISTEBAN SUCLUPE, saluda a todos los invitados presentes en la sala. Asimismo, señala que la digitalización de los servicios públicos requiere un enfoque transversal y estratégico, especialmente a amenazas que sientes cuando los ataques tienen infraestructuras críticas, instituciones como el Poder Judicial, la SUNAT y el MINSA han sido víctimas de estos ataques, así como de filtraciones de datos sensibles que expone la información de millones de peruanos, sin embargo, señala que es fundamental enfocar esfuerzos en la prevención del Ciberdelito que afectan directamente a los ciudadanos como la suplantación de identidad, el fraude y la extorsión y esto no siempre se recibe una reacción inmediata de parte de las autoridades.

En ese contexto realiza las siguientes preguntas:

- ¿Si todos los sectores avanzan al mismo nivel de coordinación?*
- ¿Si cuentan con las capacidades técnicas necesarias?*
- ¿Si la inversión en protección digital es realmente suficiente?*

En el marco de los esfuerzos por fortalecer la Ciberseguridad y avanzar en la transformación digital realizar las siguientes preguntas a la secretaría de la PCM.

¿Qué acciones concretas de articulación intergubernamental, se vienen implementando a nivel de los gobiernos regionales y locales?

¿Cómo se está garantizando que estas circunstancias cuenten con las capacidades técnicas y los recursos necesarios para sumarse de manera efectiva a ese proceso?

Resulta clave promover la información de talento digital, mediante becas, convenios y alianzas internacionales a nivel nacional. La Ciberseguridad debe abordarse con un enfoque preventivo y colaborativo, no se puede esperar a que se comprometa información crítica para reaccionar.

El congresista ERNESTO BUSTAMANTE DONAYRE, con relación a las llamadas SPAM que están legítimamente motivadas comercialmente, por ejemplo "Quiero que te pases de Movistar a Entel" o "Que me compres una póliza de seguros o que te cambies de banco", sin embargo, existen otras llamadas de las plataformas de Call Center donde mimetizan llamadas de tipo delincuenciales de operadores de teléfonos.

Asimismo, existen muchas llamadas del extranjero, por ejemplo, del país de Colombia, en ese sentido realiza la siguiente pregunta:

¿Que se está haciendo al respecto o cómo se puede evitar estas llamadas?

2. Como segundo punto de orden del día el debate y aprobación del predictamen recaído en el Proyecto de Ley 9558/2024-CR que, con texto sustitutorio propone la Ley que declara de interés nacional la creación, construcción e implementación del centro de innovación agropecuaria y tecnológica local de Chivay en el departamento de Arequipa.

El Proyecto de Ley 9558/2024-CR, presentado a iniciativa del congresista Esdras Ricardo Medina Minaya, fue decretado a la Comisión de Ciencia el 24 de noviembre de 2024 como única comisión dictaminadora.

La fórmula legal del presente Predictamen tiene un artículo único, por el cual se propone mejorar la productividad y la competitividad empresarial mediante la transferencia de tecnología y el aprovechamiento de tecnologías emergentes. Se busca, además, aumentar el valor agregado de los recursos naturales y productos regionales del distrito de Chivay. Este esfuerzo será fundamental para el desarrollo sostenible de la región y el bienestar de su comunidad.

El distrito de Chivay es uno de los veinte distritos que conforman la provincia de Caylloma en el departamento de Arequipa y en su caracterización económica productiva destacan actividades económicas como: La Ganadería (alpacas, llamas, vicuñas, vacunos, ovinos), la minería, el comercio y la actividad turística. Por las condiciones climáticas y 7 geográficas más del 90% de los productores se dedican a su crianza, comercializando la carne y fibra de alpaca.

La ubicación geográfica del distrito de Chivay, lo convierte en un lugar estratégico para el desarrollo de tecnologías adecuadas y la mejora de la infraestructura. Esta situación permitirá potenciar tanto la producción ganadera como la agrícola, lo que, a su vez, elevará la calidad de vida de la comunidad y contribuirá al desarrollo económico de la región.

La Ley del SINACTI define a los Parques científicostecnológicos (PCT) como "espacios geográficos especiales con vínculos formales con una o más universidades, además de otras instituciones, públicas y privadas, que buscan promover la innovación basándose en el conocimiento científico y tecnológico en aras de contribuir a la mejora de la productividad y competitividad empresarial.

En ese sentido, hay que considerar que la propuesta plantea de crear un parque científico tecnológico en el distrito de Chivay, provincia de Caylloma, superponiéndose las áreas sobre las que tendría influencia el parque cuya creación se ha declarado de interés en la Ley 31067 y que, además, se encuentra también bajo la administración de la UNSA.

En ese contexto, la iniciativa para la construcción e implementación de un parque científico y tecnológicos en Chivay resulta desproporcionada, ya que las condiciones para la instalación y operación de este tipo infraestructuras son muy limitadas; por lo que, son 8 otros los mecanismos que corresponden desarrollar para propiciar la mejora tecnológica de la zona de interés, como por ejemplo la extensión tecnológica para las actividades agrícolas y ganaderas a las que se dedica la amplia mayoría de productores.

En tal sentido, la comisión de ciencia, innovación y tecnología recomienda su aprobación considerando el marco legal analizado y las opiniones recibidas, es pertinente promover la declaración de interés nacional de un centro de innovación agropecuaria y tecnológica local, que bajo la administración de la Universidad Nacional San Agustín fortalezca los mecanismos ya existentes y promueva un aumento en la investigación, innovación y mejora en las principales actividades económicas del distrito de Chivay.

	El congresista Esdras Medina Minaya (Renovación Popular), autor del proyecto, sostuvo que el Centro de innovación agropecuaria y tecnológica local bajo la administración de la Universidad Nacional San Agustín fortalecerá los mecanismos ya existentes y promoverá un aumento en la investigación, innovación y mejora en las principales actividades económicas del distrito. Luego del debate y no habiendo más intervenciones se puso a votación el predictamen recaído en el Proyecto de Ley 9558/2024-CR que, con texto sustitutorio propone la Ley que declara de interés nacional la creación, construcción e implementación del centro de innovación agropecuaria y tecnológica local de Chivay en el departamento de Arequipa, siendo APROBADO POR UNANIMIDAD, con los votos de los congresistas: Pariona Sinche Alfredo, Zeballos Madariaga Carlos Javier, Acuña Peralta Segundo Héctor, Bustamante Donayre Ernesto, Cerrón Rojas Waldemar, Carlos Enrique Alva Rojas, Ciccía Vásquez Miguel Ángel, Flores Ruiz Víctor Seferino, Jiménez Heredia David Julio y Monteza Facho Silvia María, en calidad de miembros titulares. El presidente comunica que se ha aprobado POR UNANIMIDAD el predictamen recaído en el Proyecto de Ley 9558/2024-CR que, con texto sustitutorio propone la Ley que declara de interés nacional la creación, construcción e implementación del centro de innovación agropecuaria y tecnológica local de Chivay en el departamento de Arequipa. 3. Como tercer punto del orden del día, se tiene la sustentación del proyecto de Ley 10281/2024-CR, que propone la "Ley que establece la protección y defensa del consumidor digital" a cargo de la congresista María Grimaneza Acuña Peralta. Debo informar que llegó a la Comisión, el oficio N.º 1248-2024-2025-MAP/CR de fecha 14 de abril del presente año, donde informa la congresista María Acuña, su postergación a la sustentación del referido proyecto de ley, por motivos de salud. En ese sentido vamos a realizar la reprogramación respectiva.
Dispensa del Acta	El señor presidente sometió a votación nominal sin esperar la aprobación del acta para ejecutar los acuerdos adoptados en la presente sesión, lo que fue aprobado POR UNANIMIDAD.

Cierre de la Sesión	(La transcripción de la grabación magnetofónica de la sesión forma parte de la presente acta). Siendo las 11:03 am., once con tres minutos de la mañana, se levantó la sesión.
Firmas	 ALFREDO PARIONA SINCHE <i>Presidente</i> GEORGE EDWARD MÁLAGA TRILLO <i>Secretario</i>