COMISIÓN DE CIENCIA, INNOVACIÓN Y TECNOLOGÍA

PERÍODO ANUAL DE SESIONES 2024 - 2025

ACTA

DÉCIMA SÉPTIMA SESIÓN ORDINARIA

SEMIPRESENCIAL

Lima, 05 de mayo de 2025

Aprobación de Acta	***1.*** **El presidente** sometió a votación la aprobación del Acta de la Décima Sexta Sesión Ordinaria de la Comisión de Ciencia, Innovación y Tecnología, celebrado el lunes 05 de mayo 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 9:12 horas del lunes 05 de mayo de 2025, se reunieron, bajo la presidencia del congresista Alfredo Pariona Sinche, contando con la presencia de los congresistas: Carlos Javier Zeballos Madariaga, George Edward Málaga Trillo, Carlos Enrique Alva Rojas, Ernesto Bustamante Donayre, Miguel Ángel Ciccia 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 séptima sesión ordinaria de la Comisión de Ciencia, Innovación y Tecnología, para el periodo de sesiones 2024 - 2025, semipresencial. **Ausentes con licencias de los congresistas:** Karol Ivett Paredes Fonseca, Segundo Héctor Acuña Peralta, Waldemar José Cerrón Rojas y Abel Augusto Reyes Cam. Por otro lado, el presidente manifiesta que antes de pasar al primer punto de la agenda, lamenta los hechos de criminalidad suscitados en la provincia de Pataz, región La Libertad. En ese sentido, la Comisión de Ciencia, Innovación y Tecnología expresa su más profunda solidaridad y condolencias con las familias de las 13 personas cobardemente secuestradas y asesinadas en la provincia de Pataz, región La Libertad.

	Este hecho atroz enluta no solamente al norte del país sino al Perú entero y, además, eleva las voces de todos los peruanos que exigen acciones firmes y resultados reales frente a la lucha contra el crimen organizado para que estas muertes no pasen a formar parte de las estadísticas, sino alcancen una verdadera justicia para consuelo de las familias. Condenamos enérgicamente los actos de violencia y criminalidad que hoy afectan gravemente no solo a la población de Pataz sino a todos los peruanos y exigimos enérgicamente al Gobierno Central replantear de manera inmediata y efectiva sus estrategias para enfrentar la criminalidad organizada y capturar a los responsables de este terrible crimen. Como muestra de respeto y en memoria de las víctimas, **solicito guardar un minuto de silencio**. 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 25 al 30 de abril de 2025. Se pasa a la estación de informes.
Informes	No hubo informes de los señores congresistas
Pedidos	**El presidente** manifiesta que el 25 de marzo del presente año, desde su despacho presentó el proyecto de Ley N° 10615/2024-CR, que propone la "Ley que declara de interés nacional y necesidad pública la integración de contenidos vinculados a la inteligencia artificial en el Currículo Nacional de la Educación Básica". Al respecto, dicho proyecto fue derivado a la Comisión de Educación, como única Comisión dictaminadora. En ese sentido, solicita a la presidencia del Congreso de la República que este proyecto de ley sea derivado también a la comisión en calidad de segunda comisión dictaminadora. Asimismo, señala que resulta fundamental que la Comisión de Ciencia, Innovación y Tecnología participe en el análisis de esta iniciativa legislativa, a fin de garantizar una evaluación integral y

	especializada del proyecto, considerando que la incorporación de contenidos vinculados a la inteligencia artificial involucra no solo aspectos pedagógicos, sino también científicos y tecnológicos, que competen directamente al ámbito de esta Comisión. El presidente *puso a votación para que el* Proyecto de Ley N° 10615/2024-CR, que propone la "Ley que declara de interés nacional y necesidad pública la integración de contenidos vinculados a la inteligencia artificial en el Currículo Nacional de la Educación Básica sea derivado a la Comisión de Ciencia, Innovación y Tecnología nuestra Comisión en calidad de segunda comisión dictaminadora, *siendo* ***APROBADO POR UNANIMIDAD****, con los votos* de los congresistas presentes: *Pariona Sinche Alfredo*(a favor), Carlos Javier Zeballos Madariaga (a favor), George Edward Málaga Trillo (a favor), Carlos Enrique Alva Rojas (a favor), Ernesto Bustamante Donayre (a favor), Víctor Seferino Flores Ruíz (a favor), David Julio Jiménez Heredia (a favor), Silvia María Monteza Facho *(a favor)* y Magally Santisteban Suclupe (a favor*)*; en calidad de miembros titulares. **El presidente** comunica que **FUE APROBADO POR UNANIMIDAD** para que el Proyecto de Ley N° 10615/2024-CR, que propone la "Ley que declara de interés nacional y necesidad pública la integración de contenidos vinculados a la inteligencia artificial en el Currículo Nacional de la Educación Básica sea derivado a la Comisión de Ciencia, Innovación y Tecnología nuestra Comisión en calidad de segunda comisión dictaminadora.
Orden del Día	1. **Como primer punto de orden del día** se tiene la participación de los representantes del Organismo Supervisor de la Inversión en Energía y Minería (OSINERGMIN), Registro Nacional de Identificación y Estado Civil (RENIEC), Superintendencia Nacional de Administración Tributaria (SUNAT) y el Ministerio del Interior (MININTER), quienes informarán a la comisión sobre los recientes casos de extorsión que vienen afectando a trabajadores de OSINERGMIN, así como la presunta filtración de datos personales, habiendo sido facilitados mediante el acceso indebido a información contenida en bases de datos de entidades públicas. • En primer lugar, interviene el señor **MIGUEL ÁNGEL GOETENDIA ALARCÓN**, Gerente de Administración y Finanzas del

Organismo Supervisor de Energía y Minas (OSINERGMIN), **JOSÉ LUIS LUNA CAMPODÓNICO**, Gerente de Asesoría Jurídica del OSINERGMIN, los representantes del Organismo Supervisor de la Inversión en Energía y Minería – OSINERGMIN, quienes informan a la comisión sobre los recientes casos de extorsión que vienen afectando a trabajadores de OSINERGMIN.

El gerente de Administración y Finanzas del Organismo Supervisor de Energía y Minas (OSINERGMIN), inicia su exposición saludando a los congresistas y funcionarios presentes en la sala de sesiones. Acto seguido, señala que la preocupación de la Comisión de Ciencia, Innovación y Tecnología está referido a los mensajes vía Wassap que recibieron tres funcionarios de OSINERGMIN mensajes que decían que nos vayamos preparando cupos para pagar y de esa manera seguir trabajando, tanto en las sedes del distrito de Miraflores como en Magddalena estos mensajes se hicieron públicos.

Asimismo, indica que estos hechos de inmediato fueron puestos en conocimiento de la fiscalía especializada y a través del procurador público de OSINERGMIN también se ha puesto de conocimiento de la Procuraduría especializada de Delitos Cibernético. Estos hechos ocurrieron el 10 de abril y el 11 y 14 se presentaron las denuncias y a la fecha vienen siendo investigados por la cuarta fiscalía de Lima.

En esa misma línea interviene el señor **JORGE ENRIQUE ABAD JESUS** Oficial de Seguridad y Confianza Digital del Organismo Supervisor de la Inversión en Energía– OSINERGMIN, quien inicia su exposición saludando a los congresistas y funcionarios presentes en la sala de sesiones. Asimismo, señala que se ha tomado las acciones necesarias sobre los mensajes recibidos vía wasap este hecho se ha comunicado también al Centro Nacional de Seguridad Digital para ver si estos números o estos datos personales no fueron producto de una filtración.

Acota que se han realizado algunas coordinaciones a través de la Ciber Patrullaje enviado a OSINERGMIN algunos usuarios y contraseñas estos se han reiniciado algunos han sido falsos positivos se han tomado las medidas necesarias a

	través de la Ciber Seguridad para que no se vean comprometidos los datos de los funcionarios. En ese sentido, señala que se han fortalecido medidas de seguridad internamente como cambio de usuarios y contraseñas que posiblemente hayan sido filtradas a nivel de OSINERGMIN. • **En segundo lugar**, expone el señor **HÉCTOR SARAVIA MARTÍNEZ**, director de Certificación y Servicios Digitales del Registro Nacional de Identificación y Estado Civil (RENIEC), **JAIME HONORES CORONADO**, jefe de la Oficina de Tecnología de la Información de RENIEC, **NANCY VÍLCHEZ LÓPEZ**, Oficial de Seguridad Digital del RENIEC, quienes informan sobre la presunta filtración de datos personales, habiendo sido facilitados mediante el acceso indebido a información contenida en bases de datos de entidades públicas. El señor **HÉCTOR SARAVIA MARTÍNEZ**, director de Certificación y Servicios Digitales del Registro Nacional de Identificación y Estado Civil (RENIEC) inicia su intervención saludando a los congresistas y funcionarios presentes en la sala de sesiones. Asimismo, manifiesta sobre el caso MININTER, donde señala que de acuerdo con la línea de tiempo donde se tuvo un convenio con el MININTER donde el año 2024 se vio el tema de la renovación de convenios que se tenía, debido que el 31 de diciembre este se vencía. En ese sentido, indica que MININTER alcanzó el 12 de diciembre una propuesta lo cual se analizó y se puso algunos controles a los consumos, se vio algunos servicios que no se habían utilizados, los cuales se sacó del convenio, luego se reunieron ambas entidades y se puso topes a los consumos, el MININTER solicitó un millo ochocientos mil para el tema de la línea dedicada mensualmente, sin embargo RENIEC propuso un millón quinientos mil sobre la frecuencia que hacían sus consumos y las estadísticas de los años anteriores, sin embargo, no se tuvo ninguna respuesta desde febrero, pero en marzo el MININTER propone nuevamente treinta millones de consultas mensuales, esto llamó mucho la atención, porque había un uso adecuado, ósea un uso anómalo entre los meses de febrero y marzo, se tomó la decisión de cancelar a todos los usuarios del MININTER, en realidad eran ocho personas, pero el único que estaba

accedido era de la señora Blanca Saavedra la cual fue inactivado, luego solicitaron que se active el usuario del señor Eduardo Cabrejos pero se volvió a repetir el consumo inadecuado, por tanto, desde esa fecha se cortó el servicio de línea dedicada, debido que era imposible saber la fecha de arreglo del problema de seguridad en el MININTER. Asimismo, el 31 de marzo se envío una adenda la cual hasta el momento no se ha podido suscribir con topes y condiciones para los nuevos servicios.

En ese sentido, de acuerdo con la línea de tiempo se muestra las fechas del incidente en el servicio de consultas en línea vía línea dedicada del caso MININTER:

- **USO INDEBIDO** el 06 de marzo, RENIEC informa al MININTER sobre posible uso indebido del servicio de consultas en línea y desactiva todos los usuarios registrados del MININTER.

- **ACCIÓN INMEDIATA** el 07 de marzo MININTER identifica y neutraliza la aplicación comprometida "RUEBAR" y, se realizan coordinaciones con el RENIEC para reestablecer el servicio.

- **CORTE DEFINITIVO** el 10 de marzo MININTER detecta la reactivación no autorizada del RUEBAR y fue nuevamente neutralizada. RENIEC corta de manera definitiva el servicio en cuestión.

- **ACUERDOS** el 11 de marzo RENIEC y MININTER acuerdan que este último remita un informe de las acciones tomadas garantizando que el incidente no se repita, a fin de evaluar la reactivación del servicio.

- **ACCIONES ADOPTADAS** el 13 y 17 de marzo MININTER remite a RENIEC un informe de las medidas implementadas y otro informe ampliatorio según lo solicitado por RENIEC.

16 días después:

- **DECLARACIÓN** 22 y 23 de abril La segunda fiscalía especializada en ciberdelincuencia solicita a los

funcionarios del RENIEC y MININTER brindar declaración policial de los hechos.

- **REUNIÓN DE ALTO NIVEL** el 7 de abril los funcionarios del RENIEC y MININTER sostienen reunión presencial para discutir la renovación de la quinta adenda y la publicación de fotografías.

- **INICIO DE DENUNCIA** el 5 de abril La ssecretaría General del MININTER solicita a la Procuraduría Pública del Sector Interior iniciar la denuncia sobre el presunto delito informático contra los que resulten responsables.

- **RESPUIESTA DEL MININTER** el 4 de abril En respuesta, MININTER reitera su preocupación a RENIEC y solicita una investigación conjunta. Así como una reunión para garantizar la protección de los datos.

- **COMUNICIÓN DE LA RENIEC** el 2 de abril RENIEC informa al MININTER que ya no mantendrá un convenio con el servicio de línea dedicada. Asimismo, pone de conocimiento de la publicación de fotografías de ciudadanos en foros de la *dark web*.

El usuario de la DIRPOCOM registra en el RUEBAR las cuentas de usuario para los clubes deportivos.

Con relación a los lineamientos de la RENIEC proporciona una línea de comunicación exclusiva con el Ministerio del Interior, asegurando que las consultas se realicen de forma controlada, bajo parámetros técnicos acordados.
Diversos sistemas institucionales hacen uso de este servicio para verificar la identidad de ciudadanos como parte de sus procesos.

Una línea dedicada es un contrato de servicios contraído entre un proveedor y un cliente, por lo que el proveedor se compromete a entregar una línea de telecomunicaciones simétrica que conecta dos o más lugares a cambio de una renta mensual (de ahí el arrendamiento a largo plazo). A veces se conoce como un "circuito privado" o "línea de datos".

Aplicaciones que usaban servicio de consulta en línea RENIEC:

- RUEBAR (registro de barristas)
- Mesa de Partes Digital – MININTER
- Mesa de Partes Digital – PNP
- Sistema de Trámite Documentario (SGD)
- SIPCOP Municipal
- Sistema de Convocatorias (SISCONVIR)
- Intranet del MININTER, entre otros.

Asimismo, interviene el señor **JAIME HONORES CORONADO**, jefe de la Oficina de Tecnología de la Información de RENIEC quien precisa y reafirma que la base de datos del Registro Nacional de Identificación y Estado Civil (RENIEC) no ha sido vulnerado, por tanto, señala que por norma están obligados a brindar información a otras entidades públicas y lo que se ha detectado no va dirigido a ninguna persona o funcionario en particular, sino es algo que viene de tiempo, por tanto, manifiesta que se debería de trabajar una política de estado, debido que las aplicaciones que se han desarrollado en el sector público en su momento, ósea hacía una década atrás se tuvo como una funcionalidad, pero actualmente este escenario o contexto ha cambiado, porque hoy en día la industria que más lucro tiene es justamente las empresas de ciberdelincuencia, por tanto, esa misión que se tenía con las aplicaciones deben ser cambiados rotundamente.

También indica que la RENIEC tiene una plataforma de seguridad que impide que su data sea vulnerada, sin embargo, cuando comparten informaciones que normativa se les obliga hacerlo, pero lamentablemente no todas las instituciones cuentan con el presupuesto y las capacidades o las diligencias para hacer lo mismo.

- **En tercer lugar**, exponen los señores: Ing° **CÉSAR VIVANCO IBAÑEZ**, director de la Oficina de Gestión y Gobierno Digital del MININTER, **JOSÉ CRUZ UGARTE**, Oficial de Seguridad del MININTER, quienes informan sobre la presunta filtración de datos personales, habiendo sido facilitados mediante el acceso indebido a información contenida en bases de datos de entidades públicas.

	Primeramente, interviene el Ing° **CÉSAR VIVANCO IBAÑEZ**, director de la Oficina de Gestión y Gobierno Digital del MININTER, quien inicia su intervención saludando a los congresistas y funcionarios presentes en la sala de sesiones. Asimismo, indica los comentarios del funcionario de la RENIEC quien de acuerdo con la línea de tiempo sindica que una empleada del MININTER ha cometido un delito de robo de datos esto se ha sabido por los medios de comunicaciones donde se le sindica a la funcionaria BLANCA SAAVEDRA como la responsable de la filtración de datos. En ese sentido, resalta algo importante con relación a la parte del protocolo del convenio, RENIEC suele solicitar a las entidades un representante administrativo, en el caso del ministerio del interior justamente es la servidora Blanca Saavedra, quiere decir que en lugar de registrar al usuario que realiza las consultas, no es así debido que en el sistema de la RENIEC aparece registrada solo los datos de la señora Blanca Saavedra como representante administrativo del MININTER y por este motivo se le sindica como quien ha filtrado la información. Entonces, aquí existe una contradicción que por lógica del mismo procedimiento de la RENIEC saben que no es la persona que ha filtrado la información, sino que podría ser otra persona. Asimismo, señala que la señora Saavedra ha sido muy afectada justamente en su protección de datos, debido que se le ha sindicado en todos los medios de comunicación como televisión, radios como la responsable. En ese sentido, indica que todos los funcionarios del MININTER respalda a esta servidora, porque no es justo que sea tildada como la responsable a sabiendas que ella es la representante administrativamente del MININTER. Además, señala que RENIEC sabe que existe una investigación en curso que se está llevando en la Oficina de Órgano y Control Interno del MININTER el caso del señor Marcos Cumbicos, quien sin autorización alguna levanta el sistema RUEBAN que tenía esta problemática, este sistema desarrolló el MININTER para la Policía Nacional y con una Resolución Ministerial se le dio la administración plena de dicho sistema, es decir que ellos tenían que darle la

	seguridad y la administración a dicho sistema. Por otro lado, indica que la Policía Nacional carece de infraestructura tecnológica, por tanto, el MININTER le sede la infraestructura ósea el Hardware necesario para que corra el sistema del RUEBAN, sin embargo, este funcionario en su descargo manifiesta que levantó el sistema para investigar, pero no cursó ninguna llamada telefónica, no emitió ningún correo electrónico, tras terminar su servicio el 8 de marzo del 2025 por cuenta propia levantó el sistema y luego se retiró a su domicilio. El lunes el personal del MININTER se dio cuenta que el sistema estaba levantado nuevamente, inmediatamente se cortó dicho sistema, pero lamentablemente el 09 de marzo en la madrugada el sistema RUEBAN hizo transacciones por un número abundante por minuto. En ese sentido, acota que si bien es cierto se hizo un uso masivo de consulta de datos donde se revisó todos los sistemas pero debido que existen metodologías que usan los criminales de la ciberdelincuencia se llegó a una conclusión que existe un posible infiltrado, entonces este sistema se dio de baja de producción y se aisló en un ambiente cerrado, seguro y en investigación, sin embargo, el 09 de marzo este sistema fue habilitado por otro personal sin ninguna autorización de algún área del MININTER. Si los primeros días de marzo la RENIEC detectó el consumo masivo de datos, entonces que pasó el 09 de marzo en la madrugada que nuevamente se realizó consultas masivas y lamentablemente la RENIEC nunca los detectó este consumo y tampoco se ha corregido dicha falla. Asimismo, señala algunos temas relevantes sobre los hechos ocurridos: A inicios del mes de marzo de 2025, dentro del control mensual de los consumos, se detectó un consumo anómalo por parte de un usuario perteneciente al Ministerio del Interior (MININTER) en el servicio de "Consultas en Línea vía Línea Dedicada", suministrado por RENIEC. Al identificar esta grave irregularidad, se procedió a suspender el acceso de dicha entidad al servicio y a denunciar los hechos ante las autoridades competentes.

Las acciones adoptadas fueron comunicadas formalmente mediante los siguientes documentos:

- Oficio N° 000019-2025/DCSD/RENIEC
- Informe N° 000011-2025/DCSD/RENIEC, dirigidos al MININTER, a la Procuraduría Pública y al Oficial de datos Personales del RENIEC.

1. Que el MININTER informe todas las acciones realizadas desde que se puso en conocimiento el consumo anómalo de las consultas realizadas.
2. El reporte y registro del incidente de seguridad ocurrido, en el cumplimiento de la normativa vigente de la Secretaría de Gobierno y Transformación Digital de la PCM.
3. Evidencias de las acciones realizadas para la implementación de los controles de seguridad necesarios para proteger la información de los ciudadanos a los que tuvieron acceso a través del servicio de Consultas en línea vía línea dedicada.

Cabe precisar que estas incidencias no corresponden a una vulneración del sistema informático del RENIEC, sino a un incidente de seguridad relacionado con el uso indebido del servicio de consultas en línea via línea dedicada, operado bajo el convenio del MININTER con el RENIEC, tal como se encuentra documentado en los oficios e informes de respuestas remitidos por el MININTER.

Disposiciones administrativas y/o penales

- ✓ Oficial de Protección de Datos Personales procedió a comunicar a la Autoridad de Datos Personales del Ministerio de Justicia y Derechos Humanos la situación anómala advertida mediante el OFICIO N° 00006-2025/SGEN/PD/RENIEC de fecha **06MAR2025**.

- ✓ La Procuraduría Pública, formuló denuncia penal el **07MAR25** ante la fiscalía provincial Corporativa Especializada en Ciberdelincuencia de Lima, contra Blanca Norma Saavedra Lozada y Gamberti Eduardo Cabrejos León y los que resulten responsables por el presunto delito informático – abuso de mecanismos y dispositivos informáticos en agravio del RENIEC.

Disposiciones de RENIEC

- Reducción de convenios: de 6000 a 3800
- 299,988 usuarios depurados desde el 2023
- 4 millones se autenticaron con rostro a través del ID Perú

medidas que se está tomando y prevé adoptar para prevenir futuras vulneraciones

- Controles de consumos mensuales con frecuencia semanal.
- Reportes de consumos a fin de tenerlos con una frecuencia diaria.
- Eliminación de usuarios y cancelación de convenios que incumplan la Directiva de seguridad de la información.
- Implementación el uso del IDPERU como herramienta de autenticación en los sistemas que hacen uso del servicio de consultas indicado.
- Actualización de la Directiva de convenios de suministro de información, producto de la entrada en vigor del nuevo Reglamento de Protección de Datos Personales.

A modo de acotación interviene el señor **JOSÉ CRUZ UGARTE**, Oficial de Seguridad del MININTER quien saluda a todos los funcionarios de la sala. Asimismo, manifiesta que cuanto tuvieron conocimiento sobre el uso indebido de la filtración de datos personales inmediatamente tomaron acciones y esto fue de acuerdo con dos contextos:

1. El 6 de marzo se tuvo conocimiento a través de un comunicado de la RENIEC, donde dice que hay un posible uso indebido del servicio de consultas en línea dedicada. Inmediatamente el 7 de marzo se tomó acciones donde se erradicó el sistema que estaba comprometido y se implementó 12 inedias adicionales para poder sacar este uso indebido en todos los sistemas que cuenta en el MININTER.

   El 10 de marzo nuevamente se vuelve a cortar el servicio, MININTER trató de negociar con RENIEC con la finalidad se pueda restablecer el servicio con otro usuario, pero

lamentablemente de otra oficina contigua un personal que realiza el monitoreo que hacen los fines de semana restableció este aplicativo que ya estaba aislado, ese mismo día se realizó el corte inmediato y se procedió a solicitar al personal involucrado su descargo administrativo y también se abrió el proceso administrativo correspondiente y actualmente se encuentra contemplado dentro de la denuncia.

2. En el segundo contexto el 2 de abril la RENIEC mediante un oficio comunica a MININTER que existen publicaciones de fotografías en FOROWEK, inmediatamente se muestra la preocupación del MININTER debido que se trata de los datos personales de ciudadanos, se realizó las indagaciones al respecto, pero hasta el momento solo se sabe que se trata de fotografías, no hay informaciones adicionales como temas de firmas ni huellas digitales o de parentescos ni menores de edad.

   El MININTER realizó las denuncias correspondientes a la DIVINDAD de la Policía para determinar cual ha sido el motivo de esta filtración de datos. También se ha recibido la visita de fiscalización de MINJUS de la autoridad nacional de datos personales donde se ha hecho el descargo al respecto.

- **En cuarto lugar**, exponen los señores: **FRANCISCO ESPARZA CHAU**, Intendente Nacional del Sistema de Información de la Superintendencia Nacional de Aduanas y de Administración Tributaria - SUNAT, **OMAR GONZÁLES ELÍAS,** Gerente de Seguridad Informática **-** SUNAT, **JOHNNY VALDEZ ARÉVALO,** Gerente de Arquitectura – SUNAT, quienes informan sobre la presunta filtración de datos personales, habiendo sido facilitados mediante el acceso indebido a información contenida en bases de datos de entidades públicas.

  - Primeramente, interviene el señor **FRANCISCO ESPARZA CHAU**, Intendente Nacional del Sistema de Información de la Superintendencia Nacional de Aduanas y de Administración Tributaria - SUNAT, quien inicia su intervención saludando a los congresistas y funcionarios

	presentes en la sala de sesiones. Asimismo, precisa que en la primera exposición corresponde a un pedido de la Comisión de Ciencia, Innovación y Tecnología, para explicar los protocolos y mecanismos de seguridad de información que se han implementado en la SUNAT. En ese sentido, manifiesta que el trabajo de la SUNAT que se ejecutan en un marco legal que rige la seguridad de información del estado peruano. La SUNAT opera bajo el paraguas del marco de confianza digital que fue definido por la Presidencia del Consejo de ministros en el Decreto de Urgencias 007 del 2020. Este marco les proporciona los cimientos que les permite construir la arquitectura de seguridad que tienen en la institución, en ese contexto se ve que la protección de datos está supervisado por el Ministerio de Justicia, mientras otros aspectos de la seguridad digital como CIBERSEGURIDAD, CIBERDELINCUENCIA, CIBERINTELIGENCIA y CIBERDEFENSA están a cargo de otras entidades estatales, entonces ellos como administración tributaria se tienen que alinear todos estos marcos regulatorios en todas sus capas de defensa de su arquitectura, para garantizar su cumplimiento. En ese sentido, adhiere que esto no solo es un ejercicio normativo, sino es sentar las bases para desarrollar las estrategias para poner en cuidado el activo más importante como la información de los contribuyentes y de la información tributaria de los ciudadanos del país. En esa misma línea señala que la SUNAT es consciente de la importancia de preservar 3 pilares fundamentales que es la confidencialidad, integridad y disponibilidad de la información para el cumplimiento de sus funciones y objetivos. Por ello, se compromete a gestionar y mejorar continuamente un Sistema de Gestión de Seguridad de Información que está alineado a una norma internacional que es la ISO 2701 esta norma permite cuidar, identificar los controles internacionales. Asimismo, explica los controles en el acceso a la información administrativamente:

	• Cifrado de extremo a extremo en todas las comunicaciones (TLS 1.2) • Gestión granular de identidades con principio de mínimo privilegio • Zero Trust Architecture para validación continua de cada transacción • Portal seguro dedicado con pistas de auditoria **Clave SOL** ✓ Api de seguridad ✓ Manejo de token ✓ Doble factor ✓ Contraseña de 12 caracteres ✓ Acceso a VPN **SOC** - Defensa perimetral avanzada (NGFW, IPS/IDS, WAF) - Sandbox de seguridad para análisis de amenazas - Protección multicapa con firewalls (FW 1er Nivel, FW ASM, FW 2do Nivel). **Servicios especializados de CIBERSEGURIDAD** • Centro de Operaciones de Seguridad (SOC) • Monitoreo de Dark/Deep Web detección de datos filtrados • Pentesting para escenarios de fuga de datos • Threat Hunting proactivo con inteligencia de amenazas. • Ethical Hacking **Personal de la SUNAT** • Control de acceso basado en roles (RBAC) con segregación estricta de funciones. El personal SOLO accede a información de su competencia (puesto) • Pistas de auditoria en los accesos. • Protección de endpoints con soluciones integradas (Antimalware/DLP/Encriptación de disco) • Conexiones seguras a través de infraestructura MPLS para comunicaciones entre sedes • Servidor centralizado de Active Directory para gestión de identidades y accesos • Monitoreo de actividad inusual en bases de datos • Análisis de tráfico cifrado sin descifrado completo

- Segregación de funciones con workflow de aprobación para acciones críticas.

Conclusiones

La SUNAT implementa mecanismos de protección avanzados:

- La SUNAT cumple con el marco normativo del estado peruano en materia de Seguridad y Confianza Digital.
- La SUNAT cuenta con un Sistema de Gestión de Seguridad de la Información SGSI, alineado a la Norma Técnica Peruana ISO/IEC 27001.
- La arquitectura de seguridad de SUNAT implementa un enfoque de defensa en profundidad con controles técnicos que cubren integralmente los tres pilares fundamentales: los administrados, los colaboradores internos, y la infraestructura tecnológica de la institución.
- La SUNAT gestiona sus activos de información bajo una visión de Zero Trust y Mínimos Privilegios, implementando tecnologías de última generación como firewalls multicapa, sistemas IPS, y DLP con capacidades avanzadas de análisis comportamental.

Con relación a la validación internacional

- La SUNAT ha superado exitosamente las auditorías realizadas por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), en el marco del Foro Global sobre Transparencia e Intercambio de Información con Fines Fiscales. Dichas auditorías evalúan específicamente los mecanismos de protección de información confidencial, seguridad de datos y capacidades técnicas para el intercambio seguro de información tributaria entre 168 países.
- Este nivel de certificación sólo lo obtienen las administraciones tributarias que cumplen con los más exigentes estándares internacionales de seguridad, tales como Alemania, Francia, Reino Unido, Canadá y Japón, países que son reconocidos por sus avanzados

sistemas tributarios y que han pasado por este mismo proceso.

El presidente abrió una ronda de intervenciones de los congresistas.

El congresista Alfredo Pariona Sinche manifiesta que actualmente todos estamos en la era de la digitalización, la informática y la inteligencia artificial, pero lamentablemente a pesar de contar con estos adelantos digitales es paradójico que estas herramientas sean utilizadas por la delincuencia y la extorsión porque estamos siendo afectados por estos males que se ve a diario en la ciudad.

¿Es posible que se haga frente a esta ola de criminalidad entre otros que estamos viviendo en el país?

Preguntas al Organismo Supervisor de la Inversión en Energía y Minería (OSINERGMIN):

¿Qué medidas está tomando OSINERGMIN para garantizar la integridad de sus plataformas digitales?

¿Qué protocolos de atención se exigen para acceder a los sistemas internos y plataformas digitales del organismo?

¿Si OSINERGMIN realiza auditorias o pruebas de penetración de sus sistemas informáticos y con qué frecuencia se realiza esto?

Preguntas al Registro Nacional de Identificación y Estado Civil (RENIEC):

¿Qué tipo de cifrado protege los datos biométricos, como huellas, firmas y rostro que almacena RENIEC?

¿Si RENIEC cumple con los estándares internacionales?

¿RENIEC ha sido objeto de auditorias del sistema de Ciberseguridad en los últimos 5 años, si es así como fueron corregidos?

¿Existe alguna clara cementación entre los entornos de salud, prueba, producción de los sistemas de gestión de la información del personal?

Preguntas a la Superintendencia Nacional de Administración Tributaria (SUNAT):

	¿Qué protocolos siguen los funcionarios de la SUNAT para acceder a los datos de los contribuyentes y como se auditan estos accesos? ¿Qué mecanismos emplea la SUNAT para evitar las filtraciones de información a los procesos de fiscalización electrónica y cruzada de datos? ¿Qué controles existe para asegurar que terceros contratistas o proveedores tecnológicos de la SUNAT no tengan acceso indebido a la información tributaria? **Preguntas al Ministerio del Interior (MININTER):** ¿Qué medidas concretas ha implementado el ministerio del interior para garantizar la protección de los datos personales que se encuentra en el poder de la Policía Nacional y otras dependencias bajo su dirección? ¿El Ministerio del interior cuenta con protocolos de Ciberseguridad y auditoria regular para tener accesos no autorizados, filtraciones o usos indebidos de la información de los ciudadanos almacenados en el sistema del ministerio? Concluida las exposiciones del gerente de Administración y Finanzas del Organismo Supervisor de Energía y Minas (OSINERGMIN), el gerente de Asesoría Jurídica del OSINERGMIN, el director de Certificación y Servicios Digitales del Registro Nacional de Identificación y Estado Civil (RENIEC), el jefe de la Oficina de Tecnología de la Información de RENIEC, el Oficial de Seguridad Digital del RENIEC, el director de la Oficina de Gestión y Gobierno Digital del MININTER, el Oficial de Seguridad del MININTER, el Intendente Nacional del Sistema de Información de la Superintendencia Nacional de Aduanas y de Administración Tributaria - SUNAT, el Gerente de Seguridad Informática **–** SUNAT y el Gerente de Arquitectura – SUNAT. 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 de los señores: **MIGUEL ÁNGEL GOETENDIA ALARCÓN**, Gerente de Administración y Finanzas del Organismo Supervisor de Energía y Minas

	(OSINERGMIN), **JOSÉ LUIS LUNA CAMPODÓNICO,** Gerente de Asesoría Jurídica del OSINERGMIN, **HÉCTOR SARAVIA MARTÍNEZ**, director de Certificación y Servicios Digitales del Registro Nacional de Identificación y Estado Civil (RENIEC), **JAIME HONORES CORONADO**, jefe de la Oficina de Tecnología de la Información de RENIEC, **NANCY VÍLCHEZ LÓPEZ**, Oficial de Seguridad Digital del RENIEC, Ingº **CÉSAR VIVANCO IBAÑEZ**, director de la Oficina de Gestión y Gobierno Digital del MININTER, **JOSÉ CRUZ UGARTE**, Oficial de Seguridad del MININTER, **FRANCISCO ESPARZA CHAU**, Intendente Nacional del Sistema de Información de la Superintendencia Nacional de Aduanas y de Administración Tributaria - SUNAT, **OMAR GONZÁLES ELÍAS,** Gerente de Seguridad Informática **-** SUNAT, **JOHNNY VALDEZ ARÉVALO,** Gerente de Arquitectura – SUNAT. Asimismo, comunica que pueden abandonar la sala virtual cuando lo estimen conveniente. **2. Como segundo punto de Orden del Día se tiene el debate y aprobación del predictamen recaído en el proyecto de Ley** 9356/2024-CR que, con texto sustitutorio propone la ley que modifica la Ley 30220, Ley universitaria y la Ley 31250, Ley del sistema nacional de ciencia, tecnología e innovación, a fin de fortalecer la investigación científica en la educación superior universitaria. Se recuerda que el predictamen fue sustentado y debatido en la décima sexta sesión ordinaria de fecha 28 de abril de 2025; posteriormente se recibieron las intervenciones de los congresistas participantes. En el desarrollo del debate, diversos congresistas manifestaron su apoyo a la iniciativa; sin embargo, cuestionaron la modificación del literal 13.4 del artículo 13 de la Ley Universitaria, que restablece el licenciamiento temporal de las universidades. En ese sentido, se planteó una cuestión previa para que el dictamen retorne a Comisión para un mejor análisis, el mismo que fue aprobado por mayoría de los miembros titulares. Por las consideraciones expuestas hoy presentamos el nuevo texto sustitutorio que la comisión recomienda la aprobación y recoge los aportes de los señores congresistas del Proyecto de Ley 9356/2024-CR que, con texto sustitutorio, propone la Ley

	que modifica la Ley 30220, Ley Universitaria, y la Ley 31250, Ley del Sistema Nacional de Ciencia, Tecnología e Innovación, a fin de fortalecer la investigación científica en la educación superior universitaria. **El señor presidente** abrió una ronda de intervenciones de los señores congresistas. Luego del debate y no habiendo más intervenciones se puso a votación el **predictamen recaído en el proyecto de Ley** 9356/2024-CR que, con texto sustitutorio propone la ley que modifica la Ley 30220, Ley universitaria y la Ley 31250, Ley del sistema nacional de ciencia, tecnología e innovación, a fin de fortalecer la investigación científica en la educación superior universitaria, siendo aprobado **POR UNANIMIDAD** con los votos de los congresistas presentes: *Pariona Sinche Alfredo*(a favor), Carlos Javier Zeballos Madariaga (a favor), George Edward Málaga Trillo (a favor), Carlos Enrique Alva Rojas (a favor), Ernesto Bustamante Donayre (a favor), Víctor Seferino Flores Ruíz (a favor), David Julio Jiménez Heredia (a favor) y Magally Santisteban Suclupe (a favor*)*; en calidad de miembros titulares. ***El presidente*** *comunica que* **FUE APROBADA POR UNANIMIDAD** *el* **predictamen recaído en el proyecto de Ley 9356/2024-CR** que, con texto sustitutorio propone la ley que modifica la Ley 30220, Ley universitaria y la Ley 31250, Ley del sistema nacional de ciencia, tecnología e innovación, a fin de fortalecer la investigación científica en la educación superior universitaria. **3. Como tercer punto del orden del día**, se tenía la sustentación del proyecto de Ley 10626/2024-CR, que propone la "Ley que declara de interés nacional la creación, construcción e implementación del Parque Científico Tecnológico de Ucayali" a cargo de la congresista **FRANCIS PAREDES CASTRO**. Al respecto, informa que de acuerdo con el Oficio N° 640-2024-2025/FJPC/CR de fecha 05 de mayo del presente año, la congresista Francis Paredes Castro, solicita la reprogramación de su sustentación por atender temas personales programados con anterioridad.
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 10:58 am., diez con cincuenta y ochos minutos de la mañana, se levantó la sesión.
Firmas	FIRMA DIGITAL Firmado digitalmente por: PARIONA SINCHE Alfredo FAU 20161749126 soft Motivo: Soy el autor del documento Fecha: 14/05/2025 10:43:53-0500 ..... ***ALFREDO PARIONA SINCHE*** *Presidente* FIRMA DIGITAL Firmado digitalmente por: MALAGA TRILLO George Edward FAU 20161749126 soft Motivo: Soy el autor del documento Fecha: 14/05/2025 11:48:07-0500 ..... **GEORGE EDWARD MÁLAGA TRILLO** *secretario*