Área de Transcripciones

CONGRESO DE LA REPÚBLICA

SEGUNDA LEGISLATURA ORDINARIA DE 2024

COMISIÓN DE CIENCIA, INNOVACIÓN Y TECNOLOGÍA

17.ª SESIÓN ORDINARIA

(Matinal)

LUNES 05 DE MAYO DE 2025

PRESIDENCIA DEL SEÑOR ALFREDO PARIONA SINCHE

—A las 09:12 h, se inicia la sesión.

El señor PRESIDENTE.— Muy buenos días a todos los asistentes de este auditorio. Para iniciar la Décimo Séptima Sesión Ordinaria de la Comisión de Ciencia, Innovación y Tecnología, periodo anual de sesiones, 2024-2025.

Para dar inicio invito señor secretario técnico a fin de constatar la asistencia de los señores congresistas.

El SECRETARIO TÉCNICO pasa lista:

Señor presidente, señores congresistas, muy buenos días, se va a pasar asistencia.

Congresista Pariona Sinche

El señor ÁRIONA SINCHE (BS).— Presente.

El SECRETARIO TÉCNICO.— Congresista Pariona Sinche, presente.

Congresista Zeballos Madariaga.

El señor ZEBALLOS MADARIAGA (PP).— Zeballos, presente

El SECRETARIO TÉCNICO.— Congresista Zeballos Madariaga, presente.

Congresista Málaga Trillo.

El señor MÁLAGA TRILLO (NA).— Málaga Trillo, presente.

El SECRETARIO TÉCNICO.— Congresista Málaga Trillo.

Congresista Acuña Peralta (); congresista Alva Rojas (); congresista Bustamante Donayre (); congresista Cerrón Rojas (); congresista Ciccia Vásquez

El señor CICCIA VÁSQUEZ (RP).— Miguel Ciccia, presente señor secretario.

El SECRETARIO TÉCNICO.— Congresista Ciccia Vásquez, presente.

El SECRETARIO TÉCNICO.— Congresista Flores Ruiz.

El señor FLORES RUIZ (FP).— Flores Ruiz, presente, buenos días.

El SECRETARIO TÉCNICO.— Congresista Flores Ruiz, presente.

Congresista Jiménez Heredia.

Señor presidente, el congresista Jiménez Heredia, expresa su asistencia a través del chat de la plataforma.

Congresista Jiménez Heredia, presente.

Congresista Monteza Facho (); congresista Paredes Fonseca (); congresista Santisteban Suclupe ().

Señor presidente, se va a llamar la asistencia por segunda vez a los congresistas que no han respondido la asistencia.

Congresista Acuña Peralta (); congresista Alva Rojas (); congresista Bustamante Donayre (); congresista Monteza Facho.

La señora MONTEZA FACHO (AP).— Monteza, presente.

El SECRETARIO TÉCNICO.— Congresista Monteza Facho, presente.

Congresista Paredes Fonseca (); congresista Santisteban Suclupe ().

Señor presidente, hay el cuórum respectivo para la presente sesión.

El señor PRESIDENTE.— Muchas gracias, señor secretario técnico.

Bien, siendo las nueve de la mañana con doce minutos, damos inicio a la sesión de la Comisión de Ciencia, Innovación y Tecnología, y contando con el cuórum reglamentario a esta sesión semipresencial de la comisión.

Para ello, estimados colegas congresistas antes de comenzar la agenda y frente a los lamentables hechos de criminalidades suscitadas en la provincia de Pataz, La Libertad, desde la Presidencia de la Comisión de Ciencia, Innovación y Tecnología expresamos nuestra más profunda solidaridad y condolencias a las familias de las 13 personas secuestradas y asesinadas en la provincia de Pataz, región de la Libertad. El hecho enluta no solamente al norte del país, sino al Perú entero y además eleva las voces de todos los peruanos que exigen acciones y resultados contra este mal que se está organizando dentro del país.

Por ello, solicito a los integrantes de la comisión y a los asistentes brindarle y guardar un minuto de silencio.

—A pedido del presidente de la comisión se hace un minuto de silencio por los lamentables hechos criminales suscitados en la provincia de Pataz, La Libertad.

El señor PRESIDENTE.— Gracias, colegas. Gracias, asistentes.

El señor BUSTAMANTE DONAYRE (FP).— Presidente, por favor, quisiera marcar mi asistencia, Bustamante.

El señor PRESIDENTE.— Bien, iniciamos entonces con esta actividad, estimados colegas.

El SECRETARIO TÉCNICO.— Presidente, antes de empezar la sesión, para informarle de la asistencia del congresista Bustamante Donayre y de la congresista Magally Santisteban.

El señor PRESIDENTE.— Conforme.

Se va a poner a consideración de los miembros de la comisión el acta de la décima sexta sesión ordinaria, cuyos acuerdos fueron dispensados.

Los congresistas que tuvieran alguna observación al acta pueden indicarlo.

Si no hay observaciones se dará por aprobada.

Ha sido aprobada.

Colegas, continuando, pasamos a la estación Despachos.

DESPACHO

El señor PRESIDENTE.— Se han remitido a todos los miembros de la comisión la agenda documentada, una relación conteniendo la sumilla de los documentos enviados y recibidos del 25 de abril al 30 de abril del año 2025.

Pasamos a la estación de Informes.

Informes

El señor PRESIDENTE.— Se les ofrece el uso de la palabra a los señores congresistas que desean realizar algún informe.

Tienen la palabra colegas congresistas.

De no haber informes pasamos a la siguiente sesión, estación de Pedidos.

Pedidos

El señor PRESIDENTE.— Se les ofrece el uso de la palabra a los señores colegas congresistas que desean realizar algún pedido.

Bien, colegas, de no haber pedidos de los colegas la presidencia hará el siguiente pedido.

Colegas congresistas, el 25 de marzo del presente año desde mi despacho presenté el Proyecto Ley N°10615/2024, 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 de la Comisión de Educación como única comisión dictaminadora.

En ese sentido, solicito que como Comisión de Ciencia acordemos solicitar a la Presidencia del Congreso que este proyecto de ley sea también derivado a nuestra comisión en calidad de segunda comisión dictaminadora.

Al respecto, resulta fundamental que la Comisión de Ciencia participe en el análisis de esta iniciativa legislativa a fin de garantizar una evaluación integral 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.

Señor secretario, invoco a que pueda recoger los votos de los colegas congresistas referentes a este petitorio.

El SECRETARIO TÉCNICO pasa lista para la votación nominal:

Correcto, señor presidente.

Congresista Pariona Sinche.

El señor PARIONA SINCHE (BS).— A favor.

El SECRETARIO TÉCNICO.— Congresista Pariona Sinche, a favor.

Congresista Zeballos Madariaga.

El señor ZEBALLOS MADARIAGA (PP).— Zeballos, a favor.

El SECRETARIO TÉCNICO.— Congresista Zeballos Madariaga, a favor.

Congresista Málaga Trillo.

El señor MÁLAGA TRILLO (NA).— Málaga Trillo, a favor.

El SECRETARIO TÉCNICO.— Congresista Málaga Trillo, a favor.

Congresista Acuña Peralta (); congresista Alva Rojas, congresista Alva Rojas (); congresista Bustamante Donayre.

El señor BUSTAMANTE DONAYRE (FP).— Bustamante, a favor.

El SECRETARIO TÉCNICO.— Congresista Bustamante Donayre, a favor.

Congresista Cerrón Rojas (); congresista Ciccia Vásquez.

El señor CICCIA VÁSQUEZ (RP).— Miguel Ciccia, a favor, señor secretario.

El SECRETARIO TÉCNICO.— Congresista Ciccia Vásquez, a favor.

Congresista Flores Ruiz.

Congresista Flores Ruiz, a favor.

Congresista Jiménez Heredia (); congresista Monteza Facho.

La señora MONTEZA FACHO (AP).— A favor.

El SECRETARIO TÉCNICO.— Congresista Jiménez Heredia, a favor.

Congresista Monteza Facho, a favor.

Congresista Santisteban Suclupe.

Congresista Santisteban Suclupe, a favor.

Señor presidente, el pedido ha sido aprobado por unanimidad.

El señor PRESIDENTE.— Muchas gracias, señor secretario Técnico.

Bien, colegas congresistas, luego pasaremos a la Orden del Día.

ORDEN DEL DÍA

El señor PRESIDENTE.— Primer punto del Orden del Día.

Colegas congresistas, como primer punto del orden del Día tenemos la participación de representantes de Osinergmin, Reniec, Sunat y Ministerio del Interior, quienes informarán a la Comisión sobre los recientes casos de extorsión que vienen afectando a trabajadores de Osinergmin, así como la presunta filtración de los datos personales habiendo sido facilitados mediante el acceso individual a información contenida en bases de datos de entidades públicas. En ese sentido, vamos a invitar, por favor, a nuestros visitantes.

Por un lado, por Osinergmin, al señor Miguel Goetendia, Gerente de Administración y Financias. Igualmente, al señor José Luis Luna Campodónico, Gerente de Asesoría Jurídica y la señora Amparo Acevedo Flores, Gerente de Sistema y Tecnología de la Información.

También damos la bienvenida a los representantes del Registro Nacional de Identificación y Estado Civil, Reniec, señor Héctor Saravia Martínez, Director de Certificación de Servicios Digitales, el señor Jaime Honores Coronado, Jefe de la Oficina de Tecnología de la Información y la señora Nancy Vilchez López, Oficial de Seguridad Digital.

Igualmente vamos a saludar a presencia de los representantes del Ministerio de Interior, señor Luis Bruno Chávez Retamoso, director general de la Oficina General de Tecnologías de la Información y Comunicación, señor Josué Cruz Ugarte, oficial de seguridad y señor César Vivanco Ibáñez, director de la Oficina de Gestión y Gobierno Digital.

Asimismo, damos la bienvenida a los representantes de la Supervisión Nacional de Aduanas y de Administración Tributaria

Sunat, señor Francisco Esparza Chao, intendente Nacional de Sistemas de Información, señor Omar González Elías, gerente de Seguridad Informática, señor Johnny Valdez Arévalo, gerente de Arquitectura.

Colegas, congresistas, a efectos de facilitar la intervención fluida de nuestros invitados y la participación de los miembros de la comisión, se otorgará la palabra de forma seguida a los funcionarios señalados, luego del cual se abrirá una ronda de oradores para las respectivas preguntas y comentarios. En ese contexto, reiterando la bienvenida a cada visitante de las instituciones mencionadas, vamos a invitar a los señores representantes, en este caso, de Osinergmin, quién empezará con su participación, es decir el doctor José Luis Luna Campodónico.

Entonces, cada sector, por favor, **(2)** tendrá que mantener el tiempo respectivo de diez minutos, si son dos o tres para poder fraccionarse cada uno, rogamos esa comprensión para dar la agilidad respectiva a la presente sesión.

Entonces, sin más palabras, invitamos al doctor José Luis Luna Campodónico.

Tiene la palabra.

El GERENTE DE ASESORÍA JURÍDICA DEL ORGANISMO SUPERVISOR DE LA INVERSIÓN EN ENERGÍA Y MINERÍA (OSINERGMIN), señor José Luis Luna Campodónico.— Buenos días, señor presidente, congresistas, buenos días a todos.

En efecto, entendemos que la preocupación manifestada por la comisión está referida a unos mensajes que se han hecho públicos en los cuales, vía WhatsApp, tres de nuestros funcionarios recibieron unas comunicaciones, repito por WhatsApp, en las que decían que prácticamente vayan preparando sus cupos que van a tener que pagar para poder trabajar, tanto en la sede que tenemos en Miraflores como en la sede principal que mantenemos en Magdalena.

Estos hechos fueron inmediatamente puestos en conocimiento de la Fiscalía Especializada, y a través de nuestro procurador público también se ha puesto en conocimiento de la Procuraduría Especializada en Delitos Cibernéticos.

Entendemos que a la fecha, estos hechos ocurrieron el día 10 de abril, el 11 y 14 presentamos las denuncias y a la fecha estas denuncias vienen siendo debidamente investigadas por la Fiscalía, por la Cuarta Fiscalía de Lima.

Esa es la información que nosotros podríamos brindar hasta el momento, no tenemos mayor dato que brindarles, sino que simplemente estas comunicaciones por WhatsApp que, como repito, han sido recibidas por tres de nuestros funcionarios, han sido debidamente puestos en conocimiento de las instancias

especializadas para que hagan las investigaciones correspondientes.

El señor PRESIDENTE.— Muchas gracias, doctor Luna.

¿Algún otro integrante de su representada?

El GERENTE DE ASESORÍA JURÍDICA DEL ORGANISMO SUPERVISOR DE LA INVERSIÓN EN ENERGÍA Y MINERÍA (OSINERGMIN), señor José Luis Luna Campodónico.— Sí, de repente, aquí el señor Abad, que es nuestro oficial de seguridad y confianza digital, va a poder hacer algún complemento desde el punto de vista técnico de lo que ha ocurrido con la base de datos y nuestros sistemas informáticos.

El señor PRESIDENTE.— Adelante, por favor.

El OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL DEL ORGANISMO SUPERVISOR DE LA INVERSIÓN EN ENERGÍA Y MINERÍA (OSINERGMIN), señor Jorge Abad Jesús.— ¿Qué tal?, buenos días con todos, señor presidente, congresistas, buenos días con todos.

Efectivamente, respecto a los mensajes que se ha recibido vía WhatsApp, se han tomado las acciones necesarias, también se ha comunicado al Centro Nacional de Seguridad Digital para ver si estos números o estos datos personales no hayan sido producto de una filtración.

Se ha hecho la coordinación, nos han mandado una serie de... a través de un ciber-patrullaje que ellos hacen nos han mandado algunos usuarios y contraseñas, ¿no?, estas han sido debidamente reseteadas, algunos han sido unos falsos positivos, se han tomado las medidas necesarias a nivel de ciber-seguridad o datos personales para que no se vean comprometidos nuestros datos de nuestros funcionarios.

Se han fortalecido medidas de seguridad al interno, como el cambio de contraseñas, reseteos de las contraseñas que, posiblemente, hayan sido filtradas.

En ese sentido, digamos, la parte informática que nosotros manejamos están debidamente aseguradas con las medidas que nosotros tenemos a nivel de Osinergmin.

Eso sería por mi parte.

El señor PRESIDENTE.— Muchas gracias.

Enseguida vamos a invitar al señor Héctor Saravia Martínez, director de Certificación y Servicios Digitales, Registro Nacional de Identificación y Estado Civil (Reniec), quien [?] sobre los protocolos y mecanismos de seguridad actualmente vigentes para el acceso y tratamiento de la información personal.

Entonces, invitamos al señor Héctor Saravia Martínez.

Tiene la palabra.

El DIRECTOR DE CERTIFICACIÓN Y SERVICIOS DIGITALES DEL REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL (RENIEC), señor Héctor Saravia Martínez.— Buenos días, señor.

Tengo una presentación, no sé si la pueden... sí, esa es.

Bien, buenos días.

Me toca hablarles por parte de Reniec, todo lo relacionado con el caso Mininter, que nosotros lo hemos denominado así, un tema de uso inadecuado de información.

La siguiente, por favor.

En esta lámina les estoy mostrando la línea de tiempo en lo que hemos tenido nosotros con el Mininter. El año pasado habíamos comenzado ya a ver el tema de la renovación del convenio que teníamos, ya que en el 31 de diciembre este se vencía.

El Mininter nos alcanzó una propuesta el 12 de diciembre, el cual nosotros lo analizamos y al analizarlo, porque ya en esta administración nosotros estamos colocando una serie de controles a los consumos, vimos que había algunos servicios que en realidad no se habían utilizado y, por lo tanto, nosotros los sacábamos del convenio.

Luego nos reunimos, pusimos topes a los consumos, y el Mininter nos solicitó un millón ochocientos mil para el tema de línea dedicada mensuales, y nosotros le propusimos un millón quinientos mil por, digamos, la frecuencia que hacían sus consumos y las estadísticas de los años anteriores.

Sin embargo, no tuvimos respuesta desde febrero, y en marzo ya nos proponen que sean treinta millones de consultas mensuales, lo cual nos llamó la atención. Justo en esos días estábamos revisando los consumos mensualmente y nos dimos cuenta de que había un uso inadecuado, un consumo anómalo, entre los meses de febrero-marzo, cancelamos todos los usuarios, en realidad eran muchos, pero el único que estaba siendo accedido era de una persona, Blanca Saavedra, fue inactivado; luego nos pidieron activar a otra persona más, a Eduardo Cabrejos, se volvió a repetir el hecho de consumo inadecuado, y desde esa fecha nosotros le cortamos el servicio de línea dedicada porque ya era imposible saber si es que, digamos, arreglaban sus problemas de seguridad en el Mininter.

El 31 de marzo, nosotros le hemos remitido una adenda la cual hasta ahorita no la hemos podido suscribir con topes y condiciones para los nuevos servicios.

El 1 de abril, todos conocimos la publicación de Bridge Fórum en el cual manifestaban, mostraban toda la información que habían emitido.

Aquí ustedes pueden ver el correo con el cual nos piden que la consulta de línea (ininteligible) a 30 millones mensuales, sin tener ninguna, digamos, un sustento de acuerdo a los consumos anteriores, y ahí pueden ver ustedes lo que consumieron en enero y en febrero.

Nosotros, en realidad, dada la situación de inseguridad que se veía, no podíamos nosotros cortarle simplemente la línea, sin embargo, luego al repetirse el hecho ya no pudimos hacer más temas.

En la siguiente ya pueden ver ustedes el resumen de todo lo que les he comentado.

La siguiente lámina, por favor.

Aquí lo que nosotros hemos hecho, pues, a través de esos oficios que ven, dirigidos a nuestro oficial de seguridad y, perdón, de datos personales y a la Procuraduría han actuado para hacer las denuncias pertinentes y le hemos pedido al Mininter que nos informe de todas las acciones realizadas, además de los reportes de inseguridad.

Lo que sí nosotros queremos precisar es que estas incidencias nunca se han referido a una vulneración de nuestros sistemas informáticos, sino es un incidente de un uso indebido por parte de un usuario del Mininter.

En la siguiente, estas son las disposiciones de las que hablaba, nuestro oficial de protección de datos personales comunicó a la autoridad de datos personales del Ministerio de Justicia y Derechos Humanos, informando sobre esta situación el 6 de marzo, ya unos días después, nada más, igual nuestra Procuraduría el 7 de marzo denunció ante la Fiscalía Corporativa Especializada en estos temas contra Blanca Norma Saavedra Lozada, Gamberti Eduardo Cabrejos, y los que resulten, pues, responsables de este abuso en el uso inadecuado de la información.

En la siguiente quisiera mostrar las disposiciones que ha tomado Reniec o que viene tomando ya Reniec.

Como ustedes saben, Reniec, a través de convenios, suministra información de consulta de los ciudadanos. Lo hacemos a múltiples empresas, entre privadas y públicas, las del sector financiero, al sector de telecomunicaciones, a las entidades públicas, y muchas de las entidades públicas lo hacemos porque en realidad hay normas que nos obligan a dar esa información y, sobre todo, sin costo alguno, lo cual en realidad ha representado un problema.

Nosotros, de seis mil convenios que heredamos en esta administración, hemos comenzado a hacer unas depuraciones y hasta el mes pasado teníamos tres mil ochocientos.

En la siguiente podrán ver ustedes la cantidad de usuarios también que hemos dado de baja, los hemos depurado en el 2023, casi trescientos mil usuarios que no hacían uso de información, esto debido a que hemos actualizado la directiva de seguridad de información y aquellos usuarios que no hagan uso por más de 30 días, simplemente los estamos depurando, inactivando.

En la siguiente ustedes pueden ver otra de las acciones que ya lo ha publicitado Reniec, que es que en tanto la Ley de Gobierno Digital y su reglamento nos pide a Reniec que hagamos una plataforma de autenticación, esta ha sido construida, se llama el ID-Perú, a través del ID-Perú simplemente las personas con su DNI electrónico o su rostro, si no lo tuvieran, pueden autenticarse para cualquier tipo de transacción no presencial.

Esto de aquí lo hemos hecho para evitar que las entidades estén, tanto públicas como privadas, estén haciendo uso de las consultas al Reniec para validar si la persona es o no la que quiere entrar a alguna transacción.

Ya hemos tenido más de cuatro millones de personas que se autentican solamente con el rostro y otros tantos con el DNI electrónico, lo hemos colocado, incluso, para nuestras consultas en línea, los señores usuarios que quieren entrar a consultar esta información tienen que autenticarse, a través de esta herramienta, lo que nos ha permitido bajar la cantidad de transacciones que antes se hacían.

En la siguiente lámina pueden ver parte de las medidas que nosotros hemos tomado, lo que ya les decía yo, la eliminación de usuarios y la cancelación de convenios que incumplen con la directiva de seguridad de información.

Hemos implementado y ya tenemos más de una veintena de entidades que usan el ID-Perú en sus transacciones; estamos actualizando nuestra directiva para, digamos, que esté acorde con la reglamentación que ha salido, a partir del 30 de abril, de la Ley de Protección de Datos Personales.

No está allí, pero, digamos, aparte de hacer un mayor seguimiento y monitoreo de las consultas que nos está llevando a inactivar a una serie de empresas y usuarios, también Reniec y ustedes han leído ya el sábado, ha emitido una resolución jefatural en la cual se disminuyen la cantidad de datos que se proporcionan a través de las consultas en línea.

Esta es la Resolución 82/2025 y se va a implementar, gradualmente, en los servicios de manera tal de que se desincentive el tema de estar buscando información en las consultas en las cuales nosotros nos vemos obligados a dar por norma y no sea, pues, un tema atractivo para que las personas estén exponiendo este tipo de información.

Eso es todo en el tiempo que puedo darle y dispuesto a cualquier pregunta que nos tengan a bien formular.

Muchas gracias, señor.

El señor PRESIDENTE.— Las gracias al señor Héctor Saravia Martínez.

Si tuviera algún otro integrante que agregar sobre el tema, puede hacerlo.

El señor .— Sí, buenos días, presidente, señores congresistas, señores presentes todos.

Solamente para precisar y reafirmar que la base de datos de Reniec no ha sido en ningún momento vulnerada, nosotros, como decía Héctor, por norma estamos obligados a dar información a otras entidades públicas.

Lo que hemos detectado y acá esto no va dirigido a ninguna persona o funcionario en particular, sino que esto es algo que viene de tiempo.

Por lo tanto, yo creo que deberíamos trabajar ya una política de Estado porque las aplicaciones que se han desarrollado en el sector público en su momento, de repente, una década atrás, hemos tenido o se ha tenido como prioridad siempre la funcionalidad, pero este escenario, este contexto ha cambiado. Hoy día la industria que más lucro tiene es, justamente, estas empresas de ciber-delincuencia.

Por lo tanto, esa visión que se tenía de las aplicaciones tiene que cambiar rotundamente. Nosotros tenemos toda una plataforma de seguridad **(3)** que impide que nuestra data sea vulnerada. Sin embargo, a la hora que compartimos la información, que normativamente nos obligan a hacerlo, no encontramos que todas las entidades tienen el presupuesto y las capacidades, y a veces la diligencia para hacer lo mismo. Ante eso, bueno, ya Héctor ha podido explicar y detallar la medida que hemos tomado.

Es todo, gracias.

El señor PRESIDENTE.— Muchas gracias a los integrantes del Reniec.

Bien, vamos a pasar, esta vez invitando al señor Luis Bruno Chávez Retamozo, director general de la Oficina General de Tecnologías de la Información y Comunicación del Ministerio del Interior, quien informará sobre los protocolos y mecanismos de seguridad actualmente vigentes para el acceso y tratamiento de información personal, la conexión existente entre Mininter y el Reniec, y otras entidades respecto a la protección de datos personales, así como las medidas implementadas para prevenir futuras vulneraciones.

Entonces, invitamos al señor Luis Bruno Chávez Retamoso a fin de hacer el uso de la palabra.

El DIRECTOR DE LA OFICINA DE GESTIÓN DE GOBIERNO DIGITAL DE LA OFICINA GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, señor César Martín Vivanco Ibáñez.— Buenos días, señor presidente. Buenos días, señores congresistas presentes, funcionarios de las entidades de Osinerming y Reniec. Les habla el ingeniero César Martín Vivanco Ibáñez. Voy a pronunciarme en reemplazo del ingeniero Retamozo.

Mi cargo en el Ministerio del Interior es el de oficial de Gobierno Digital.

Quisiera, si pudieran, por favor, colocar la lámina del Mininter.

Bien, mientras ubican la PPT, podría ir adelantando para no hacer inútil el tiempo que transcurre.

Bueno, coincido en algunas con respecto a la línea de tiempo que ha manifestado mi colega, el ingeniero Héctor Saravia de Reniec, con la línea de tiempo, pero siendo también... resaltando, como también lo hemos escuchado, manifiestan que un empleado del Mininter haya cometido quizás un delito de robo de datos.

Por las comunicaciones que hemos nosotros, todos nosotros, leído —comunicados de Reniec — indican que se le sindica a la funcionaria Blanca Saavedra como la responsable de la filtración de datos.

Pero quiero resaltar lo siguiente: como parte del protocolo del convenio, Reniec suele solicitar a las entidades un representante administrativo que representa a la entidad, y en el caso del Ministerio del Interior, justamente, es la servidora Blanca Saavedra. Quiere decir que, en lugar de registrar en las consultas al usuario que las realiza, en todas las consultas va a estar registrado en el sistema de Reniec a la funcionaria que es la representante administrativa, y a ella se le sindica como la que ha filtrado la información.

Entonces, ahí hay una contradicción, porque por lógica del mismo procedimiento de Reniec, ellos saben que no es la funcionaria Blanca Saavedra, sino que podría ser otra persona. Esta funcionaria ha sido muy afectada justamente en su protección de datos; se le ha sindicado en todos los medios de comunicación —prensa, televisión, radios— como la responsable.

Mi persona y todo el personal de Administración Interior respalda a esta servidora, porque no es dable que se le haya tildado a sabiendas de que ella es la representante administrativa del Ministerio, y eso es un procedimiento de Reniec. Reniec también sabe que hay una investigación en curso que, a través de nuestro órgano de control interno, ya ha

llegado a Fiscalía y también está en investigación de la Divindat para esclarecer.

Asimismo, nosotros teníamos, como ustedes ven en la línea de tiempo, al 7 de marzo ya una buena relación con Reniec. Nos habían habilitado el restablecimiento del servicio. Sin embargo, el día 8 de marzo, un funcionario del Ministerio del Interior que hace las veces de operador de infraestructura, de nombre Marco Cumbicos, sin autorización alguna, levanta el sistema RUEBAR, que tenía esta problemática.

El sistema Ruebar es un sistema que desarrolló el Ministerio del Interior para la Policía Nacional, y con una resolución ministerial también se le dio la administración plena de dicho sistema. Es decir, ellos tenían que darle la seguridad, la administración, y son los únicos que hacen la consulta a ese sistema.

Como la Policía... Bueno, aquí estamos todos en confianza, señor presidente, la Policía Nacional carece de infraestructura tecnológica; por lo tanto, el Ministerio del Interior le cedió la infraestructura, es decir, el hardware necesario, las comunicaciones necesarias, para que corra ese sistema del Ruebar.

Sin embargo, este funcionario, que en su descargo manifiesta que levantó ese sistema para investigarlo, no cursó ninguna llamada telefónica, no emitió ningún correo electrónico, acudió a su servicio el día sábado 8 de marzo y, por cuenta propia, levantó ese sistema. Y, cuando terminó su facción, se retiró a su domicilio y no dio cuenta de nada.

El día lunes, el personal del Ministerio de OGTIC se dio cuenta de que estaba ese sistema nuevamente levantado, y obviamente lo cortó. Pero, para entonces, el día 9 de marzo en la madrugada, que cayó domingo, ese sistema RUEBAR empezó a hacer transacciones, alrededor de unas... no recuerdo muy bien el número, pero en un número abundante por minuto.

Entonces, voy a hacer una acotación allí. Si bien es cierto, a inicios del mes de marzo, el Reniec nos envió una comunicación de que estábamos haciendo un uso masivo de consulta de datos. Conversamos acá con el oficial de seguridad del Ministerio del Interior, el ingeniero José Cruz, y empezamos a revisar todos los sistemas, porque, como bien sabemos, hay un posible uso de... [..?] que es una metodología que hacen los criminales de la ciberdelincuencia, haya sido posible que hayan infiltrado ese sistema. Entonces, lo aislamos. Ese sistema fue dado de baja de producción y estaba en un ambiente cerrado, seguro, justamente en investigación.

Sin embargo, como vuelvo a repetir, el día 9 de marzo ese sistema se habilitó y sin autorización de ningún director del

Ministerio del Interior. Entonces, esa persona está actualmente en investigación.

Pero lo que quiero también atraer a la colección es lo siguiente: si entre los primeros días de marzo el Reniec detectó el consumo masivo de datos, ¿qué pasó el día 9 de marzo en la madrugada? Nuevamente se hizo el consumo de este sistema y volvió a ser consulta masiva. Lo que destaco ahí es que no hubo ninguna acción que corrija en RENIEC ese consumo masivo.

Sin embargo, quisiera leer lo que acaba de preguntar nuestro señor presidente de Comisión: ¿Qué acciones ha tomado el Ministerio del Interior con respecto a todos los sistemas que hacen consumo de los servicios de Reniec?

Se procedió a implementar la autenticación mediante tokens en todas las aplicaciones que consumen los servicios de Reniec. Se dispuso la implementación del mecanismo de Captcha a todas las aplicaciones para mitigar solicitudes automatizadas, como este caso, asegurando que solo usuarios humanos puedan interactuar con el servicio.

Tabla de auditorías por usuario de aplicación. Se implementó el mecanismo que permite auditar peticiones de usuario por aplicación. La implementación de un MOOC con datos simulados para los ambientes de desarrollo y calidad. También implementamos una microplataforma de interoperabilidad, una mini PIDE, para integrar los servicios de la PIDE de RENIEC y PNP, para que sean consumidos desde distintos aplicativos de Mininter. Esto lo hicimos con el fin de ya no consumir más datos por línea dedicada de Reniec.

También se inició el cambio de consultas de línea dedicada a esta microplataforma para las aplicaciones cuya naturaleza no es COR, es decir, que no son vitales para la seguridad pública.

Se creó una alerta vía correo electrónico para los casos de consumo sospechosos y anómalos, lo que significa que, al haber un consumo masivo, automáticamente le llegaba un correo electrónico y un mensaje de texto al administrador de red para que tomara acción.

Se procedió a implementar en la base de datos un [… ?] que ejecuta un […?] en periodos de tiempo administrables para evitar la cantidad de peticiones a Reniec.

Se procedió a solicitar formalmente una evaluación del comportamiento laboral del personal con acceso a activos críticos. Bueno, en este momento a todo el personal le estamos pasando polígrafo.

En adición a ello, el personal que se encuentra relacionado con la administración de los activos involucrados en el incidente ha firmado declaraciones juradas actualizadas de acceso

privilegiado. Es decir, que al incumplir cualquiera de estas normativas es procesado inmediatamente.

Bueno, eso es lo que quisiera acotar con respecto a esa línea de tiempo y con las medidas de seguridad que hemos establecido, señor presidente.

El señor PRESIDENTE.— Muchas gracias, señor César Vivanco.

De repente, algo que complementar al que le acompaña a su institución, por favor.

El OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL DEL MINISTERIO DEL INTERIOR, señor José Cruz Ugarte.— Buenos días, presidente de la comisión, estimados funcionarios y ciudadanos que nos ven a través de las redes sociales. Soy el ingeniero José Cruz Ugarte, el oficial de Seguridad y Confianza Digital del Ministerio del Interior.

Como lo mencionaba el director de la Oficina de Gestión del Gobierno Digital, nosotros tomamos conocimientos —hay que ponerlo en contexto a todos los ciudadanos y a los que estamos acá presentes— dos contextos.

El primer contexto: el momento en que nosotros tomamos conocimiento del uso indebido, digamos, de la filtración de datos personales. Nosotros tomamos conocimiento el 6 de marzo a través de un comunicado oficio de el Reniec, donde nos dice un posible uso indebido del servicio de consultas en línea dedicada.

Nosotros, inmediatamente, tomamos acción el día 7 de marzo. Tomamos acciones —lo explicó acá el director—, 12 medidas, principalmente 12 medidas. Una de ellas es erradicar el sistema que estaba comprometido; lo erradicamos totalmente e implementamos 12 medidas adicionales para poder erradicar este uso indebido en todos los sistemas, no solamente el comprometido, sino todos los sistemas que cuenta el Ministerio del Interior.

Luego, posteriormente, el 10 de marzo se vuelve a cortar el servicio. Nosotros tratamos de negociar con Reniec a fin de que nos vuelvan a restablecer el servicio con otro usuario. Sin embargo, como lo comentó un personal de nuestra oficina, en el monitoreo continuo que hace en los fines de semana, restableció este aplicativo que ya estaba aislado.

Nosotros, el lunes a las 8 de la mañana, el 10 de marzo, lo erradicamos nuevamente al detectar este evento y procedimos a solicitarle al personal su descargo administrativo correspondiente. Y luego, esto ha pasado por un proceso administrativo también en ese lugar del Ministerio del Interior y también está dentro de la denuncia contemplado esto.

Por favor, ¿puede regresar a la línea de tiempo? Gracias. **(4)**

Entonces, ese es el primer contexto, digamos, de lo sucedido. Hasta ahí no sabíamos nada de las publicaciones de fotografías. Luego, el 2 de abril, mediante oficio, la reunión nos comunica, nos comunica, nos hace poner de conocimiento que hay publicaciones de fotografías en foros *web*, como lo indica en su oficio.

Inmediatamente nosotros también notamos la preocupación del Ministerio del Interior. Obviamente, son datos personales de ciudadanos. Hicimos la indagación correspondiente y, hasta el momento, se sabe solamente que son fotografías, solamente fotografías, no información adicional como datos de nombres, etcétera. Y, además, podemos afirmar que no hay, digamos, uso de firma, porque este aplicativo no usaba tampoco temas de firma. No se contaba con temas de firma, huellas digitales, o de parentescos o de menores de edad.

Hasta el momento sabemos eso. Hemos hecho también este denunciado también a la Divindat, a la Policía, este evento, por la misma preocupación que tenemos, para poder determinar cuál ha sido el alcance de esta filtración de datos. También hemos recibido la fiscalización del Minjus, de la Autoridad Nacional de Datos Personales. Hemos hecho nuestro descargo, hemos manifestado nuestra preocupación y tenemos todo el apoyo, digamos, conjunto con la Policía Nacional del Perú.

Voy a darle el paso a mi director.

Muchas gracias.

El DIRECTOR DE LA OFICINA DE GESTIÓN DE GOBIERNO DIGITAL DE LA OFICINA GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL MINISTERIO DEL INTERIOR, señor César Martín Vivanco Ibáñez.— Señor presidente, con respecto a la información que nos ha advertido también Reniec hace unos minutos, que se le ha solicitado a el Reniec un volumen de treinta millones de consultas mensuales. Acabo de conversar con la Dirtic de la Policía Nacional y ellos enviaron un correo electrónico, como se ha mostrado, pero ellos indican que esos treinta millones son anuales, no mensuales.

Revisando la necesidad, porque también es una necesidad de Reniec poder soportar toda esa infraestructura para poder permitir e interpelar su información con todas las entidades públicas, es que también requiere que se les habilite el mecanismo TUPA para que también las entidades públicas paguen una cantidad de cuotas que los ayuden a solventar esa necesidad.

Bueno, actualmente ellos también tienen convenios con entidades privadas como son la sociedad o la asociación de bancos, AFP, etcétera, mineras, y ellos tienen el control de ese tráfico de información. Bueno, por conocimiento general, sabemos que las entidades privadas solicitan todos los datos de los peruanos, ¿no?, como son fotografías, hasta firmas. ¿Por qué? Porque, por

ejemplo, cuando nosotros o todos los profesionales pasamos por una entrevista en una entidad privada y ellos nos filtran todo, entonces necesitan esa información.

Pero, volviendo al punto de las transacciones o de la consulta que necesita el sector, es decir, el Ministerio y la Policía Nacional, se necesitarían mensualmente —hablando ya de números— un millón cuatrocientos dieciséis mil setecientos soles mensuales para solventar las consultas que requieren tanto el Ministerio del Interior como la Policía Nacional.

Esto anualmente refleja diecisiete millones de soles. Este presupuesto es inexistente en el Ministerio del Interior. Por lo tanto, no tendríamos, salvo que se habilite un presupuesto adicional, para ayudar a la necesidad que tiene el Reniec. Eso es lo que quería contar.

Gracias.

El señor PRESIDENTE.— Muchas gracias al señor Cesar Vivanco Ibáñez, integrantes del Ministerio del Interior.

Bien, vamos a luego invitar a los representantes de la Sunat, comenzando con el señor Francisco Esparza Chao, Intendente Nacional de Sistemas de Información de la Sunat, quien informaba sobre los protocolos y mecanismos de seguridad implementados en su institución para resguardar la información personal que administra, en particular aquella vinculada a trabajadores del sector público, las políticas de control de acceso de dichas bases de datos y las acciones que se vienen desarrollando para fortalecer la protección de datos en conexión con otras entidades del Estado.

Entonces, igualmente tiene la palabra hasta por diez minutos.

El INTENDENTE NACIONAL DE SISTEMAS DE INFORMACIÓN DE LA SUNAT señor Francisco Javier Esparza Chau.— Buenos días, señor presidente Alfredo Pariona. Buenos días a los miembros de la Comisión de Ciencia, Innovación y Tecnología. Buenos días a todos.

Quiero precisar que la siguiente exposición refiere a un pedido de la Comisión de Ciencia, Innovación y Tecnología para explicar los protocolos y mecanismos de seguridad de la información que se han implementado en la Sunat.

Siguiente lámina, por favor.

El trabajo de la Sunat se ejecuta en un marco legal que rige la seguridad, en este caso, de la información del Estado peruano.

En la lámina que se presenta se puede observar el ecosistema de la seguridad digital del Estado peruano. La Sunat, en este caso, opera bajo el paraguas del marco de confianza digital, marco que fue definido por la Presidencia del Consejo de Ministros, en el Decreto de Urgencia 007, desde el 2020.

Este marco nos proporciona los cimientos que nos permite construir la arquitectura de seguridad que tenemos en la institución. En ese contexto, vemos que la protección de datos está supervisada por el Ministerio de Justicia, mientras otros aspectos de la seguridad digital, como la ciberseguridad, ciberdelincuencia, ciberinteligencia y ciberdefensa, están a cargo de otras entidades estatales.

Nosotros, como Administración Tributaria, tenemos que alinear todos esos marcos regulatorios en todas nuestras capas de defensa de nuestra arquitectura para garantizar justamente su cumplimiento. Esto no solamente es un ejercicio normativo, sino que sienta las bases para desarrollar las estrategias para poner en cuidado el activo más importante, que es la información de los contribuyentes y la información tributaria de los ciudadanos del país.

Siguiente lámina, por favor.

Dicho esto, la Sunat es consciente, es consciente de que tiene que preservar y cuidar, en este caso, tres pilares importantes, que corresponden a la confidencialidad, la integridad y la disponibilidad de la información de la administración tributaria.

Para eso, la Sunat, en este caso, ha implementado un sistema de gestión de seguridad de la información que está alineado a una norma internacional, que es la ISO 27001. Esta norma da marcos conocidos internacionales que permiten cuidar e identificar, mitigar los riesgos de información. Y también nos dan los controles con estándares internacionales para ello.

Y es importante este sistema de gestión de seguridad porque nos permite profundizar en la defensa que vamos a enseñar a continuación.

Siguiente lámina, por favor.

Ahora, ¿toda esta política cómo se concretiza dentro de los sistemas? Entonces, nosotros tenemos una arquitectura de defensa y seguridad de información con varias capas.

Entonces, lo que vamos a hacer: en esta lámina, en el lado izquierdo, ustedes lo que van a ver es el viaje que tiene el contribuyente. Los contribuyentes o los administrados que utilizan los servicios digitales de la institución lo hacen a través de un portal, un portal seguro, un portal en el cual, cuando registran sus solicitudes, estas viajan a través, primero, de internet, a través de proveedores de internet.

Tenemos tres proveedores de internet, en el caso de que tengamos algún problema con estos proveedores, se mantiene el servicio con los otros dos. Y también, a través de estos proveedores, tenemos una primera capa de defensa. Se identifica si las

transacciones son de ataque masivo, que se les conoce como denegación de servicios, y luego de eso pasamos a la siguiente.

Les pediría, por favor, que vayamos dando clic. Un siguiente, por favor. Uno más. De acuerdo. Vamos dando los clics hasta… para que vayamos entendiendo la presentación.

Entonces, hay una primera capa que es a través del viaje de estas solicitudes. Todas las solicitudes de los contribuyentes vienen cifradas a través de un protocolo seguro extremo a extremo, TLS 1.2. Luego que pase la revisión de los proveedores de internet la transacción pasa a un segundo nivel.

Ese segundo nivel es un *firewall*, que debería decirse que es como una muralla, un anillo, es un primer anillo de seguridad, donde se revisa la autenticación, la autenticidad de dónde proviene esa transacción o esa solicitud de los administrados.

Luego de eso, pasa un balanceador que es un GTM, un *Global Transport Manager*, que lo que hace es como un director general de tránsito. Él define a qué centro de cómputo va a enviar esa solicitud.

Una vez que define a qué centro de cómputo va a ir esa solicitud, pasa a un segundo nivel nuestras transacciones y solicitudes, ya a través de un *firewall* de ASM, *Application Security Manager*. O sea, se revisa la trama a nivel de HTTP, HTTPS, y se ve, en este caso, que no tenga ninguna táctica o una estrategia usada por los hackers para justamente apropiarse ilícitamente de la información.

Una vez que se revisan todos estos controles, pasa a un segundo nivel, que es el balanceador local. Ya en el centro de cómputo, este balanceador decide a qué servidor se va a ir esta transacción. Obviamente, lo que busca es ver que estén disponibles esos servicios para poder dar el pase.

Y hay un tercer nivel, y ese tercer nivel es el IPS, que es un sistema de instrucción, que lo que está mirando es el comportamiento, si hay un patrón anómalo, inusual, de esa transacción, para bloquearla y no darle pase.

Si pasa ese nivel de seguridad, recién se entrega la información al servidor de aplicaciones. Y este servidor de aplicaciones también cuenta, en este caso, con software que permite, como *antimalware*, ver que no tengamos riesgos de información.

Una vez que está ya en el servidor de aplicación, hace la gestión, va a la base de datos, donde están los datos, y también hay ahí un proceso de autenticación. Y de ahí se devuelve la información.

Ese es el viaje que tiene el contribuyente: un viaje seguro, un viaje con varias capas que controlan la información de la administración tributaria.

Ahora, el viaje del personal de la Sunat también tiene un cuidado similar e incluso más estricto. Importante indicar que todas las sedes de la institución de la Sunat están con redes. No se conectan con los centros de Internet, sino se conectan a través de redes privadas que se llaman las redes MPLS.

Entonces, esa es una garantía, con redes redundantes incluso, para garantizar la atención y el tratamiento a los ciudadanos. Todos los equipos, en este caso, personal de Sunat, tienen dispositivos que cuidan justamente que la información esté en buen recaudo. Entonces, los discos de las laptops están encriptados, los USB están encriptados, es decir, si quieren copiar información y sacarla por los USB, el USB viaja de manera encriptada. Es decir, si el USB lo quieres poner en otro lado, solamente podrás hacerlo dentro de un equipo de la institución.

También contamos con mecanismos de DLP, que son *Data Loss Prevention*, que lo que están midiendo es que esa información no fuge.

Vamos, por favor, al siguiente.

Y contamos con un SOC, que es un Centro de Operaciones de Seguridad, que está analizando constantemente los comportamientos en las redes y los comportamientos, en este caso, de vulnerabilidad en cualquiera de las aplicaciones.

Vamos a la siguiente lámina, por favor, de los controles de acceso a la información.

Hablaba del viaje de los administrados. Los administrados cuentan con la clave SOL. Es una clave construida con un API segura, con autenticación de tokens.

En este caso, todo el cifrado de la comunicación de los contribuyentes y los administrados es segura, con protocolos TLS 1.2.

También tenemos **(5)** la arquitectura Zero Trust, es decir todas las transacciones que entran a la institución son validadas, todas. Y en este caso un portal seguro que tienen las pistas de autoridad de todo lo que hacen los contribuyentes.

En el caso del personal Sunat, todo, comentar, que los accesos están basados en segregación estricta de funciones. ¿Qué quiere decir?

Que el personal, solamente tiene acceso a lo que le compete a su función, al puesto. No puede ver otro tipo de información.

Asimismo, contamos con productos de antimalware, DLP, encriptación en todos los dispositivos, que justamente permiten dar todas las seguridades que corresponden.

Siguiente lámina, por favor.

Como conclusiones, tenemos implementados 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 que es el SGSI, alineado a la norma técnica peruana ISO 27001 y la arquitectura de la seguridad de la SUNAT implementa un enfoque de defensa en capas y en profundidad, con controles técnicos que cubren integralmente tres pilares, los administrados, en este caso los colaboradores, el personal de la SUNAT y toda la infraestructura tecnológica y gestionamos todos los activos de información bajo una visión cero tras cero confianza y mínimos privilegios implementando tecnologías de última generación como *Firewalls*, Multicapa, sistemas IPS y *Data Loss Provention*.

Asimismo, contamos con validación internacional. Hemos superado exitosamente auditorías realizadas por el Organismo para la Cooperación y Desarrollo Económico, el OCDE, que justamente en el marco del Foro Global de Transparencia, Intercambio e Información para Fines Fiscales, evalúa, y qué evalúa, señor presidente, el OCDE, los mecanismos de protección de información confidencial, uno, la seguridad de datos y las capacidades técnicas para intercambio.

Gracias a esas auditorías, el Perú es aspirante miembro y a través de ese logro del país es que tenemos acceso financiero a más de 168 países del mundo. Y quiero resaltar también, que el nivel de certificación que han obtenido estas auditorías también las obtienen administradores tributarios que cumplen con los más exigentes estándares internacionales de seguridad como son Alemania, Francia, Reino Unido, Canadá y Japón.

Eso es, señor presidente. Con eso concluyo mi presentación y quedamos atentos a cualquier pregunta que pueda tener usted y la comisión.

Gracias.

El señor PRESIDENTE.– Muchas gracias, a nuestros invitados por haber expresado referente a la agenda, tanto representantes de el Reniec, del Ministerio del Interior, de Osinergmin, como también de la Sunat.

Enseguida, vamos a invitar a los colegas congresistas, a fin de generar las preguntas, los comentarios, para luego también tener las respuestas de nuestros invitados.

Colegas congresistas, se apertura la participación para cada uno de ustedes. Colegas congresistas, ¿alguna participación?

Bien, estimados invitados, desde la presidencia vamos a generar algunas preguntas, empezando con algunos comentarios. Si bien es cierto estamos en la era de la digitalización, de la informática, de la inteligencia artificial y tantos otros

adelantos, pero es algo paradójico que, a pesar de contar con estas herramientas últimas, hoy estamos siendo afectados fuertemente por los males que se están presentando en la sociedad. En este caso, las extorsiones, empleando, precisamente, algunos aparatos tecnológicos, algunas herramientas digitales, entre otras.

Entonces, si quisiéramos retroceder 10 años atrás, no había nada de esto, y también la sociedad estaba un poco más tranquila.

Claro, se veían algunos otros males, pero eran de menores proporciones. Hoy, ¿cuál es la explicación? ¿Qué cosa podemos nosotros interpretar y cómo podemos solucionar? ¿Es posible que podamos enfrentar esta ola criminal entre otros dentro del país que estamos viviendo? Una pregunta general.

Igualmente, general para Osinergmin, ¿qué medidas Osinergmin toma para garantizar la integridad y disponibilidad de sus plataformas digitales? ¿Qué protocolos de atención se exigen para acceder a los sistemas internos y plataformas digitales del organismo? Igualmente, Osinergmin realiza auditorías o pruebas de penetración en sus sistemas informáticos. ¿Con qué frecuencia.

Para el Reniec, ¿qué tipo de cifrado protege los datos biométricos, huellas, rostros, firmas que almacena Reniec? ¿Cumple con estándares internacionales? Igualmente, ¿ha sido objeto de auditorías externas el Reniec de ciberseguridad en los últimos cinco años? Si es así, ¿qué hallados críticos se detectaron y cómo fueron corregidos? Por otro lado, ¿existe alguna segmentación clara entre los entornos de desarrollo, prueba, producción de los sistemas que gestionan la información personal?

Para la Sunat, ¿qué protocolos siguen los funcionarios de la Sunat para acceder a los datos de los contribuyentes y cómo se auditan estos accesos? ¿Qué mecanismos emplea en la Sunat para evitar filtraciones de información a los procesos de fiscalización electrónica o cruzada de datos? ¿Qué controles existen para asegurar que terceros contratistas o proveedores tecnológicos de la Sunat no tengan acceso indebido a información tributaria?

Y también para el Ministerio de Interior, ¿qué medidas concretas ha implementado el ministerio, para garantizar la protección de los datos personales en poder de la policía nacional y otras dependencias bajo su jurisdicción? ¿Cuenta el Ministerio del Interior con protocolos de ciberseguridad y auditoría regular para permitir accesos no autorizados, filtraciones o usos indebidos de la información ciudadana almacenada en sus sistemas?

Son algunas que podemos formular. Colegas, congresistas, si de repente tienen participación, por favor, pueden hacerlo en estos instantes.

Entonces, a nuestros invitados, igualmente a cada uno vamos a acceder hasta por 5 minutos para poder responder o de repente generar otra información, no proporcionada que complemente a la exposición.

Entonces, vamos a empezar invitándole a nuestro visitante, en este caso de la Osinergmin, por favor, pueden hacer…

El GERENTE DE ADMINISTRACIÓN Y FINANZAS DEL ORGANISMO SUPERIOR DE ENERGÍA Y MINAS (Osinergmin), señor Miguel Ángel Goetendía Alarcón.– Gracias, presidente.

Solamente mencionar que en el caso que nos competa a nosotros está relacionado con unas comunicaciones recibidas por 3 funcionarios vía WhatsApp. A la fecha, nosotros no tenemos evidencia alguna de que haya existido alguna filtración de datos de nuestra base. Sin perjuicio a ello, quisiera cederle la palabra, por favor, al señor Abad, quien va poder ampliar la respuesta en el sentido de cómo nos protegemos nosotros y nuestra base de datos, cómo están protegidas.

Gracias.

El señor PRESIDENTE.– Adelante, por favor.

El OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL DEL ORGANISMO SUPERVISOR DE LA INVERSIÓN EN ENERGÍA Y MINAS, señor Jorge Enrique Abad Jesús.– Que tal, presidente. Congresistas y público en general.

En Osinergmin, nosotros contamos con un Sistema de Gestión de Seguridad de la información sobre los procesos core.

Estos procesos están certificados e implementados bajo la norma ISO 27001. Aún sumado a ello, tenemos controles de ciberseguridad, de seguridad de la información fuertes. Tenemos un cyberSOC también que está 24 a 7. Y lo que nosotros debemos destacar es que nuestros sistemas de información no han sido vulnerados.

De manera regular, hacemos pruebas de validaciones o de vulnerabilidades para ver que nuestra infraestructura tecnológica esté al día y no presente ninguna falla. En relación a ello, nosotros manejamos controles fuertes, como el MFA, el Múltiple Factor de Autenticación, para todas nuestras transacciones que nosotros realizamos a través de la autenticación y autorización de usuarios.

En ese sentido, tenemos controles implementados en relación a nuestras políticas específicas de seguridad de la información que es implementados y que todos los funcionarios venimos cumpliendo al interno de Osinergmin.

Eso sería.

El señor PRESIDENTE.– Muchas gracias.

El GERENTE DE ADMINISTRACIÓN Y FINANZAS DEL ORGANISMO SUPERIOR DE ENERGÍA Y MINAS (Osinergmin), señor Miguel Ángel Goetendía Alarcón.– Si me permite, señor presidente…

El señor PRESIDENTE.– Continúe, por favor.

El GERENTE DE ADMINISTRACIÓN Y FINANZAS DEL ORGANISMO SUPERIOR DE ENERGÍA Y MINAS (Osinergmin), señor Miguel Ángel Goetendía Alarcón.– Un comentario, adicional. Nosotros consideramos que es de suma relevancia esta sesión y por eso quizás nos permitimos hacer una sugerencia, un poco en la línea de lo que comentaba el representante Reniec hace unos momentos, todas las instituciones públicas estamos obligados a entregar información que establece la norma, establece la ley.

Y sin ir más lejos, todos nuestros teléfonos y nuestros puntos de contacto están publicados. Y no solamente por cumplimiento de la normativa que emite el Ministerio de Justicia, sino inclusive nuestras declaraciones juradas son de público conocimiento con los datos. Estamos hablando no solamente de DNI, domicilios, estamos hablando de teléfonos, correos electrónicos, ingresos. Es sumamente importante que quizá usted, señor presidente de esta comisión, pueda hacer alguna gestión para modificar esta normativa que cada vez a los funcionarios públicos nos expone más, este tipo de ataques.

Gracias.

El señor PRESIDENTE.– Muchísimas gracias, lo tendremos en cuenta. Igualmente, para dar paso a los representantes del Reniec.

Por favor, adelante.

EL DIRECTOR DE CERTIFICACIÓN Y SERVICIOS DIGITALES, señor Héctor Eduardo Saravia Martínez.– Sí, gracias, señor presidente.

Mire, nosotros en Reniec estamos muy comprometidos en revertir todos estos temas. En verdad, consideramos que ya en la actualidad, como usted mismo lo manifestó con tanta tecnología, se tienen que cambiar todos estos mecanismos que vienen por diseños desde hace mucho tiempo.

En realidad, nosotros entendemos que para atender a cualquier persona, uno va con su DNI. Y si va con su DNI, en verdad, no entendemos la necesidad de ir a Reniec para validar los datos que están en un DNI. O sea, eso en realidad tiene que cambiar esa mecánica. Ese es uno.

Dos, en el DNI debe haber información que en verdad no exponga a la persona. Hemos visto con buenos ojos que aquí en el Congreso tienen un, entiendo que ya está por aprobarse en el Pleno, en

la cual reduce la cantidad de datos que tiene el documento de identidad. O sea, un documento de identidad no tiene por qué estar con la dirección y una serie de campos, porque imagínense si a una dama le roban la cartera, pues, que seguro tiene la llave, tiene la dirección incluso para ir a cometer algún acto delictivo, la persona que lo robó.

Esas son cosas en las que nosotros estamos abocados, en ir reduciendo la cantidad de datos que se necesitan para hacer transacciones. Ahora bien, les indiqué que ya salió una resolución jefatural nuestra en la cual disminuye la cantidad de datos que vamos a otorgar a través de los suministros de información. Pero aun así, nosotros también queremos que se revise bien la regulación en la cual nos obligan a dar información a las entidades públicas por una u otra razón.

También nosotros dentro de las medidas es que estamos trasladando los suministros de información que se da por línea dedicada, es decir, de punto a punto una conexión a través de los servicios web. Ustedes han visto en la presentación que nos hizo el colega de la Sunat, en la cual hay una serie de mecanismos a través del internet en los cuales se pueden evitar muchas de estas cosas con toda la tecnología que hay.

Ahora bien, además de eso, nosotros también pensamos y estamos haciendo ya toda la masificación del DNI electrónico con este DNI 3.0, que tiene muchas más medidas de protección y vamos a colocar a disposición de las entidades públicas como privadas servicios disponibles para que puedan realmente validar la información que tiene un DNI, sin tener que ir a Reniec para estar consultando esa información, en realidad no tiene ningún sentido.

Lo otro es que todos los servicios que da Reniec son solamente para actividades core de las empresas y las entidades, no pueden estar usándose, digamos estas consultas para temas administrativos, para contratar personas, etcétera. Para eso tienen que cambiar sus mecanismos.

Ahora, como finalmente ya para darle el paso a Jaime, que puede indicar todos los temas tecnológicos y a la ingeniera Nancy para ver todas las certificaciones de seguridad, nosotros tenemos en nuestro *roadmap* ir llevando la seguridad de la identificación a temas mayores. Y esto es en cuanto a la seguridad digital y estamos seguro que con la implementación del ID Perú vamos a lograr una mayor protección y una seguridad de las personas que están entrando.

Sin embargo, como ya lo han manifestado las otras entidades, el tema presupuestal es importante. O sea, **(6)** tenemos que darle mucha importancia y los recursos necesarios para que estas medidas tecnológicas que estamos nosotros colocando tengan el

sustento y la viabilidad para que sean utilizados de manera masiva.

Eso es todo lo que le puedo decir, señor presidente.

Le doy el pase a Nancy.

El señor PRESIDENTE.— Conforme.

Adelante, estimada Nancy.

La OFICIAL DE SEGURIDAD DIGITAL DEL REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL (RENIEC), señora Nancy Haydee Vílchez López.— Buenos días, señor presidente; buenos días con todos, señores congresistas que están en la aula virtual; buen día con todos.

Un poco comentando el tema que Héctor ha precedido. Recuerden que el Reniec está obligado a dar información justamente para poder identificar a los peruanos a través de convenios de suministro de información, por decreto ley o por la plataforma de interoperabilidad.

¿Qué es lo que está pasando? Cuando hablamos nosotros de seguridad de la información, tenemos que hablar de tecnología, sí, tenemos que hablar de personas y tenemos que hablar de procesos. La tecnología ha evolucionado, hay muchos mecanismos de seguridad y los compañeros han podido demostrar en la lámina que tecnológicamente se cuenta con las herramientas y Reniec también está en esa misma línea.

Sin embargo, el tema de procesos, las instituciones no están cambiando sus procesos al paso que cambia la tecnología y tenemos que, por ejemplo, cuando una persona va al lugar, tiene que dejar el DNI y muchas veces hasta fotografían los señores vigilantes el DNI. ¿Quién controla, por ejemplo, ese proceso? Y ya guardando la información y esa información también es expuesta.

Héctor decía: "no debemos, cuando alguien va a identificarse, no tiene que venir a preguntar a Reniec, tenemos que encontrar otros mecanismos". Los procesos misionales, el proceso de suministro de información es para el proceso misional de la institución. Pero encontramos instituciones que hasta para el control de asistencia consultan al sistema de información de la base de datos del Reniec.

Entonces, las personas, el mayor problema y la cadena, el eslabón más débil de toda la cadena son las personas. No son conscientes de la importancia en tanto del uso del dato como de la protección y ese es un grave problema, porque, por ejemplo, en este caso específico también del Mininter, ¿cómo se da esta exposición de información? Por un aplicativo, que estaba publicado y que no tenía ningún control de seguridad. El

ciberdelincuente encontró esa brecha de seguridad y extrajo la información.

¿Por qué desarrollamos aplicaciones y no las controlamos? Porque si yo desarrollo una aplicación y ya no la voy a utilizar, la tengo que dar de baja. No puedo dejar aplicaciones publicadas, sabiendo que hay un mundo ciberdelincuencial que va a buscar cualquier brecha de seguridad para poder extraer la información.

Entonces, ese es el gran problema que nosotros tenemos. ¿Tenemos que dar información? Sí. Pero la pregunta es: ¿las instituciones están siendo lo suficientemente conscientes para proteger esa información? La respuesta es no, porque después de lo que pasó en el Mininter, nosotros hemos cortado el servicio, si bien es cierto, al Mininter, pero lo dejamos abierto para la Policía Nacional. Y esto sin ánimos de golpear, ni inculparnos, pero es la realidad.

¿Qué pasó la siguiente semana? Como estamos en un estado de emergencia, no le podíamos cortar el servicio a la policía porque tenía que hacer sus investigaciones. Pero casi en forma diaria identificábamos que con un usuario de la policía estaban exponiendo información en Telegram.

Nosotros contamos con un servicio de SOC 24 horas, en el cual monitorean las redes sociales y la web para ver dónde están exponiendo información de los ciudadanos y tenemos que estar nosotros, ser los policías y decir: "tú expones, te corta". Al día siguiente, horas más, horas menos, otro usuario y estamos cortando y eso es insostenible, no podemos estar así.

Entonces, si ya teníamos ese problema, que se había expuesto esa información, ¿qué cosa se está haciendo para evitar que eso no vuelva a pasar? El mismo problema tenemos también con otras instituciones. Por eso es que tenemos alrededor de 50 denuncias realizadas a la Autoridad Nacional de Protección de Datos, donde nosotros, como Reniec, identificamos esa exposición de datos.

Nos hemos sentado con la Secretaría de Gobierno y Transformación Digital, con la autoridad, manifestándole la preocupación y justamente ellos nos dicen: "lo que pasa es que encontramos que, por ejemplo, una municipalidad que está en un lugar alejado hace demasiadas consultas y no tiene ningún control, y ellos los están sancionando. Entonces, la pregunta es: ¿es la responsabilidad del Reniec ser el policía de cada una de estas instituciones y estar mirando qué haces con la información?

Nosotros no tenemos forma de saber cuántos ciudadanos atiende, por ejemplo, una municipalidad, una institución, cuántas aplicaciones tiene, cuántos usuarios tiene. Y nuestros convenios lo dicen bien claro, que la responsabilidad del control de los usuarios, el uso y las aplicaciones es de la propia institución y no se está realizando.

Entonces estamos nosotros, nos hemos visto forzados, porque la base de datos del Reniec no ha sido vulnerada. Esta información no ha salido, porque si no ingresaran a nuestros sistemas, a nuestra base de datos. Nosotros guardamos la trazabilidad de cada consulta, de cada peruano que se realiza. ¿Qué quiere decir? Sabemos qué institución, sabemos qué usuario de la institución, hora, fecha, minuto y segundo que se hizo la consulta y a través de qué servicio. Tenemos esa trazabilidad.

Entonces, cuando identificamos, empezamos a bloquear y a suspender incluso convenios. Héctor hablaba de 6 mil convenios que heredó esta gestión, estamos en 3 mil 800. Entonces, nos hemos visto obligados a poner controles que deberían poner las instituciones. Uno de ellos es, cuando un usuario deja de laborar, las instituciones no les dan de baja. Yo no puedo saber si, por ejemplo, los caballeros de Osinergmin hoy día es su último día de trabajo o trabajan hasta fin de mes. Y dice la responsabilidad: "tú, institución, tienes que dar de baja a tu usuario", no lo hace.

Entonces, ¿qué hemos hecho? Que cuando un usuario en 30 días no hace ninguna consulta, asumimos que ya no está, y eso nos ha permitido depurar la base de datos en 300 mil. O sea, eso era responsabilidad de las instituciones.

Entonces, un poco para ir cerrando la idea y la preocupación del Reniec, Reniec está muy comprometido y está trabajando y a veces por hacer nuestro trabajo, también nos golpean, porque sale en las redes sociales diciéndole al ciudadano: "no te puedo atender porque Reniec me bajó el servicio, porque Reniec no funciona, porque los servidores del Reniec se cayeron". No, señores, no se les da servicio porque probablemente se haya identificado que ese usuario ya estaba siendo mal usado y por eso nos hemos tenido que ver con la obligación de cortar ese servicio, a fin de evitar que se exponga la información de los ciudadanos.

Entonces esta tarea, señores, es responsabilidad de todos y creemos que tenemos que empezar a formar la consciencia desde nuestros hijos, desde los colegios, de la importancia de la protección de los datos personales, del buen uso que debemos hacer en ellos.

Muchas gracias, señor congresista.

El señor PRESIDENTE.— Muy amable.

Bien. Vamos a…

¿Sí?

Adelante, por favor.

La señora Nancy Haydee Vílchez López.— Bueno, sí, en el caso del Reniec, para complementar lo que han dicho Héctor y Nancy,

también tenemos la debida protección en las aplicaciones, en la infraestructura, algo similar también a lo que ha expuesto Sunat. Sin embargo, considero que es necesario indicar que el pensamiento que muchas veces tenemos nosotros es que ponemos tecnología, se habla de inteligencia artificial, se habla de robótica y muchas cosas más, y pensamos que la tecnología es la varita mágica que va a transformar todo, que va a cambiar todo. Compramos tecnología y por arte de mágica se van a resolver los problemas que las entidades sufren, y no es así. O sea, hoy día se habla mucho de transformación digital, que estamos en el camino a la transformación digital, pero realmente la transformación digital no es comprar tecnología, no es implementar software, ni servidores, sino va por un tema de personas, de procesos, como lo decía Nancy, y en eso estamos bastante descuidados como Estado.

O sea, compramos tecnología pero con el mismo proceso, compramos tecnología sin capacitar al personal y encontramos mucha resistencia al cambio también del personal. Personal que está acostumbrado a un trabajo manual, a un formato en papel, a firmas manuscritas, a que la gente venga y haga cola, ese escenario, señores, tiene que cambiar. La tecnología es la herramienta, pero no lo va a lograr solo, o sea, no es un disruptor, no es un agente que cambia la tecnología por sí solo, yo enchufo el equipo y se resuelve el problema.

Yo mañana le pongo el equipo más rápido y mejor configurado a todas las personas que trabajan en atención al ciudadano, mesa de partes, y eso no asegura que el proceso sea más rápido, más ágil, con más empatía y mayor educación. No. Lo que estamos viendo acá, lo que decimos nosotros es la famosa capa 8 ¿no? Tenemos el modelo, ese que tiene 7 capas y en esas 7 capas tenemos la tecnología ya definida e implementada. Pero si el personal no está comprometido, capacitado, sensibilizado, de nada va a servir.

Entidades que cuando venimos a una visita nos quitan el DNI. ¿Qué hacen con ese DNI durante ese tiempo? Nosotros hemos encontrado con extranjeros que cuando van a una entidad nos cuentan eso. ¿Cómo es posible que en tu país, cuando tú entres, te quiten el documento de identidad? ¿Qué pueden hacer durante ese momento, durante todo ese tiempo con tu documento de identidad?

Y eso es algo que está muy familiar en muchas entidades públicas, incluido el Congreso. Nosotros hemos entrado hoy día y nos han quitado el DNI y durante ese tiempo qué puede pasar con ese DNI. Y así muchas entidades más. Entonces, esas prácticas son comunes, pero están nuestros datos, ahí está nuestra dirección, nuestra huella, nuestra foto. Y como dicen, muchas entidades se han acostumbrado para sus tareas domésticas, administrativas, para encuestas, para exámenes, usar el servicio del Reniec, cuando se han hecho esos servicios para

procesos misionales, para que tú tengas un proceso de tu misión y lo puedas hacer de una manera más rápida, pero no para cosas realmente que son triviales.

Entonces, yo creo que más que abocarnos hoy día en pensar en seguir comprando tecnología, hay que ver qué tenemos que cambiar en la mentalidad, en el paradigma de las personas. O sea, no se está haciendo más, y es un trabajo no solamente del área de Recursos Humanos, sino que tienen que también las autoridades tomar conciencia de eso.

Nosotros en el Reniec tenemos nuestra alta dirección que apoya mucho todos estos temas. Pero encontramos que en otras entidades de repente esto no es una prioridad, no está de repente incluso en su presupuesto. ¿Cuánto de presupuesto se asigna a la seguridad de la información en cada entidad pública? ¿Cuánto de presupuesto da el Estado? ¿Cuánto se preocupa el Estado por eso? ¿Cuánto de presupuesto le da a la Reniec, que es el ente rector en seguridad de la información? ¿Cuánto se le da a la DINI?, ¿Cuánto se le da al Ministerio de Defensa, al Ministerio del Interior?

Si no tenemos eso, lastimosamente no vamos a poder avanzar en estos temas que hoy día están reportando y que realmente todos pensamos que se arreglan con más equipos o con más tecnología.

Gracias.

El señor PRESIDENTE.— Muchas gracias.

Bien. Entonces pasando esta vez a la Superintendencia Nacional, igualmente para que puedan absolver la interrogante o información complementaria que podría proporcionar.

Adelante, por favor.

El señor Francisco Javier Esparza Chau .— Muchas gracias, señor presidente.

Sobre los protocolos para el personal, el personal de la Sunat que accede a información de la Administración Tributaria pasa por pruebas de integridad, que son evaluaciones para ver la probidad del personal realizadas por Recursos Humanos. Se cuenta con dos capacitaciones de seguridad de información obligatorias al año. El acceso es por segregación de funciones, es decir, son accesos con autorizaciones de quienes lideran las áreas de negocio y que solamente se dan al puesto, a la ejecución del puesto.

La autenticación es una autenticación robusta, con doble factor de autenticación. Tenemos trazabilidad de las acciones que realiza el personal. Tenemos servicios o sistemas de data *protection*, que permiten ver cualquier tipo de comportamiento que implique algún riesgo de información. Asimismo, los equipos de todos los colaboradores, como ya había mencionado, sus discos

duros están encriptados en caso de alguna pérdida o robo de estos equipos. Es imposible que la información pueda ser accedida.

También tenemos un control de todos, del monitoreo del personal y de los correos. La defensa de los accesos del personal está monitoreada.

Adicionalmente, respecto a los proveedores, los proveedores no tienen acceso a nuestro sistema, solamente el acceso lo tiene el personal de la Sunat. Y tenemos pruebas de integridad social, cuatro al año, que son técnicas de manipulación y *phishing* para ver y asegurar que el personal de la Sunat esté consciente de la importancia de cuidar la información de la administración tributaria.

Y también tenemos servicios de *hacking* ético, que realizamos cuatro veces al año, donde a través de hackers tratamos de vulnerar las capas de defensa ya comentadas.

Eso es todo.

Muchas gracias.

El señor PRESIDENTE.— Muy amable al señor representante de la Sunat.

Finalmente, a nuestros representantes del Ministerio del Interior.

Tienen la palabra, por favor.

El señor César Martín Vivanco Ibáñez .— Gracias, señor presidente.

Con respecto repito, está en administración plena de la Policía Nacional de Perú, siendo una entidad autónoma. Sin embargo, en las sesiones del Plan de Gobierno y Transformación Digital, en la cual participamos en conjunto, hemos realizado, hemos solicitado, hemos brindado las recomendaciones, y por presupuesto a la fecha no le hemos podido hacer un servicio de *ethical Hacking* interno.

Pero como ya lo ha manifestado mi colega Jaime Honores, a través de la PCM, el ingeniero César Vílchez, preside la Secretaría de Gobierno y Transformación Digital, realiza simulaciones de ataques cibernéticos a todas las entidades del sector, incluyendo al Congreso. **(7)** Lo que solicito es, trabajar en conjunto entre todas las entidades públicas.

Resalto que el Reniec, es el custodio del banco de datos de todos los peruanos.

Y también me permito hacer algunas recomendaciones, señor presidente.

Tengo entendido que la Marina y el Ejército peruano, cuentan con un centro de comando especial para la ciberdefensa, como usted bien debe saber, la ciberdefensa protege al Estado Peruano contra vulneraciones externas, sin embargo, es la Policía Nacional del Perú, la que tiene por misión y funciones estar en guerra 7x24x365.

Asimismo, no existe una ley contra la ciberdelincuencia y/o el cibercrimen.

Resalto esa necesidad, señor presidente, para que, a través de los funcionarios del Ministerio del Interior, podamos colaborar con su presidencia, para emitir una ley de ciberdelincuencia y cibercrimen.

Los actuales funcionarios del Ministerio del Interior, estamos, quizás hemos sido convocados por tener doble especialidad.

En mi caso, soy coronel de la Policía en retiro, pero también soy ingeniero de sistemas e informática, con 30 años de experiencia en el sector privado y público.

Me honro en pertenecer al Ministerio del Interior, y tener la Dirección de Transformación Digital, pero solicito que exista un presupuesto para la ciberdefensa, perdón, contra el cibercrimen.

En la *objetin el Inter, el 3 de diciembre, hemos creado el CSIRT, que es un equipo de respuesta ante ataques cibernéticos, pero está conformado por los especialistas, el personal propio que tiene el objetivo.

Es necesario crear dentro del ministerio, crear una división del cibercrimen y ciberseguridad.

Nosotros internamente estamos evacuando ese informe, pero obviamente eso pasará por el Ejecutivo y finalmente por el Congreso.

Espero que cuando llegue a su comisión, tenga bien apoyar a la creación de esta división de cibercrimen y ciberseguridad, que no solamente va a servir para proteger a las entidades del sector Interior, sino también colaborar con todas las entidades, como estamos viendo en el caso de Osinergmin.

Nosotros al interno conociendo a la criminalidad, hemos incluso en varias exposiciones, manifestado lo que ahora está pasando.

En más de una reunión hemos indicado que en cualquier momento los funcionarios de una entidad pública van a ser objeto de reglaje o de solicitud de cupos o de exigencia.

Y esto es ¿por qué? Porque son 33 años que la Policía Nacional viene siendo bombardeada, enajenada, quitada de sus funciones; y, quizás, en un ataque sincronizado, no con balas ni con bombas, sino con acciones que quizás no han tenido a bien ser

analizadas en forma eficiente, y se les ha abandonado, y es hoy cuando está desarmada, desarticulada, y estoy hablando a cómo se encontraba hace exactamente un año.

La policía no ha tenido capacidad de reacción, pero con la dirección del anterior ministro del Interior, ministro Santiváñez, y el actual ministro Julio, estamos trabajando, para justamente darle esa repotenciar a la Policía Nacional.

Estamos trabajando casi al 90% para la Policía Nacional.

El ataque que ha habido hace pocas horas en Pataz. Nuestro director de la base de la Dinoes, ha informado de que ellos han tratado hace exactamente 45 días de intervenir la minería informal de Pataz.

Sin embargo, ellos tuvieron que asistir con unos rayos prácticamente de juguete, que no son hechos para la guerra.

Lo que hemos hecho nosotros, por ejemplo, es informar que ellos requieren ir articulados, aparte de supertrechos militares, con radios de guerra, como son las Harris.

Para los que conocen Pataz, saben que nuestra geografía en el Perú no es una llanura, por lo tanto, las comunicaciones deben ser de esa naturaleza.

Entonces también solicito, señor presidente, de que considere apoyar a la DINOES, bueno ahora se llama *DINOPEC, pero es la DINOES, la Dirección Nacional de Previsiones Especiales, que cuenta, que necesita actualmente hoy contar con Radio Harris, para poder intervenir eficientemente en Pataz.

De hecho, que ahora se están organizando para ir nuevamente, pero no tienen operativamente las radios de comunicación debidas.

Bien, solicito y recalco, al igual que refuerzo la moción de Jaime Honores, en solicitar presupuesto, aun claro, para cibercrimen y ciberseguridad.

Asimismo, respondiendo a su pregunta, el Mininter cuenta actualmente con ISO 27001, estamos a pocas semanas de contar con la versión 2022, contamos con infraestructura de última generación en seguridad perimetral, ojo, conservar transporte, porque lo tenemos tercerizado, y el proveedor cuenta con un *SOC, con el cual nos brinda esta seguridad perimetral que es de primer nivel.

La Policía Nacional de Perú controla los 70 mil usuarios de sistemas de sus 140 mil efectivos. Casi el 50% de la Policía Nacional son usuarios de sistemas de información.

Es un caso aislado lo que ha pasado con este sistema Roebuck, sin embargo, recalco que está en investigación y está en manos ya incluso de la Fiscalía.

Bueno, no es parte de su pregunta, señor presidente, pero también recalco lo siguiente.

La ciudadanía reclama que la Policía Nacional cumple su función, es decir, captura a los delincuentes, llega a la Fiscalía y los libera. Pero me pregunto, y hago la pregunta, yo mismo no voy a responder, la Fiscalía tiene la culpa de esta situación.

La Fiscalía cumple con la legislación vigente, y entiendo que hay legislaciones que son contradictorias.

Por ejemplo, hay una que indica que a los menores de 16 años a 18 que no tienen antecedentes penales, se los tiene que dejar en libertad.

Yo me pregunto, ¿hay algún elemento criminal del hermano país de Venezuela, que lamentablemente están aquí, que tienen antecedentes penales?

Obviamente que no, porque nosotros lo van a tener que dejar libres.

Entonces, si la responsabilidad no es de la policía que cumple su función, la Fiscalía que trata también cumplir con las leyes.

El Poder Judicial solicita en un caso judicial, las pericias correspondientes.

Bueno, este gobierno felizmente está implementando equipos tecnológicos para la lucha contra la criminalidad, pero no está al 100%. No todas las regiones cuentan con equipos de ciber, perdón, de análisis de contra la criminalidad.

Y hablo de pericias básicas, ¿no? Entonces, también es necesario de que converse usted con el Ministerio de Economía, para poderle dotar de estos elementos policiales.

Eso lo quería contribuir con su presidencia, señor presidente.

Gracias.

El señor PRESIDENTE.– Bien.

Muchas gracias, a cada uno de los invitados.

Agradecemos pues, como al señor Miguel Goetendia y a José Luis Luna Campodónico, funcionarios del Organismo Supervisor de Inversión de Energía y Minería, Osinergmin.

Igualmente, a los señores Héctor Saravia Martínez, Jaime Honores Coronado y Nancy Vilchez López, funcionarios de la Registro Nacional de Identificación y Estado Civil, Reniec.

Igualmente, a Josué Cruz Ugarte, César Vivanco Ibáñez, funcionarios del Ministerio del Interior y también, a los señores Francisco Esparza Chau, Omar Gonzales Elías y Johnny Valdez Arévalo, funcionarios de la Superintendencia de Aduanas y Administración Tributaria, Sunat.

Reiteramos los agradecimientos y estaremos atentos para poder canalizar los pedidos, las sugerencias que han formulado cada una de las instancias, para poder contribuir pues a generar las normas que ayuden a controlar los problemas que se presenten en nuestra sociedad.

Reiterando los agradecimientos, invitamos pues a que puedan abandonar a la sala en el momento que estiman por conveniente.

Muchísimas gracias a cada uno de los invitados.

Bien, colegas, brevemente vamos a suspender la sesión para despedir a nuestros invitados.

–Se suspende la sesión.

–Se reanuda la sesión.

El señor PRESIDENTE.– Bien, colegas congresistas, vamos a continuar con la sesión.

Pasaremos al segundo punto de la orden del día.

Colegas congresistas, de conformidad con lo establecido en la orden del día, tenemos el debate y votación del Predictamen recaído en el Proyecto Ley 9356/2024, que, contexto 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.

Se recuerda que el proyecto fue sustentado y debatido en la décima sexta sesión ordinaria de fecha 28 de abril del año 2025.

Posteriormente, se recibieron las intervenciones de los 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. **(8)**

En ese sentido, se planteó una cuestión previa para que el dictamen retorne a la 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.

Colegas, entonces tenemos esta Orden del Día, a fin de que puedan formular alguna intervención al respecto.

Tienen la palabra.

Colegas, no habiendo participación alguna en consecuencia se somete a votación la aprobación del predictamen recaído en el

Proyecto Ley 9356/2024, Congreso de la República, y con texto sustituto, 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.

Señor secretario técnico, proceda a recoger los votos de los señores congresistas.

El SECRETARIO TÉCNICO pasa lista para la votación nominal:

Correcto, señor presidente.

Congresista Pariona Sinche.

El señor PARIONA SINCHE (BS).— A favor.

El SECRETARIO TÉCNICO.— Congresista Pariona Sinche, a favor.

Congresista Zeballos Madariaga (); congresista Málaga Trillo ().

¿Se escucha, disculpen?

Congresista Bustamante Donayre.

Congresista Bustamante Donayre, a favor.

Congresista Málaga Trillo.

El señor MÁLAGA TRILLO (NA).— Málaga Trillo, a favor.

El SECRETARIO TÉCNICO.— Congresista Málaga Trillo, a favor.

Congresista Zeballos Madariaga.

El señor ZEBALLOS MADARIAGA (BDP).— A favor.

El SECRETARIO TÉCNICO.— Congresista Zeballos Madariaga, a favor.

Congresista Alva Rojas.

Congresista Alva Rojas, a favor.

Congresista Ciccia Vásquez (); congresista Flores Ruiz.

Congresista Flores Ruiz, a favor.

Congresista Jiménez Heredia.

Congresista Jiménez Heredia, a favor.

Congresista Monteza Facho (); congresista Santisteban Suclupe.

La señora SANTISTEBAN SUCLUPE (FP).— Santisteban, a favor.

El SECRETARIO TÉCNICO.— Congresista Santisteban Suclupe, a favor.

Señor presidente, el predictamen ha sido aprobado por unanimidad.

El señor PRESIDENTE.— Muchas gracias, señor secretario técnico.

En consecuencia, estimados colegas, el proyecto ha sido aprobado por unanimidad, es decir, el Proyecto de Ley 9558/2024, que con texto sustitutorio propone la ley que modifica la Ley 30220, la 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.

Colegas, congresistas, pasando al tercer punto del Orden del Día, teníamos en esta parte la exposición de la colega Francis Paredes Castro, quien iba a sustentar el Proyecto Ley 10626/2024, Ley que declara interés nacional la creación, construcción e implementación de parque científico, tecnológico de Ucayali. Sin embargo, ha hecho llegar su solicitud, pidiendo, pues, a que se haga la sustentación en una próxima oportunidad.

En consecuencia, colegas congresistas, no habiendo más puntos que tratar en la presente sesión, solicito la dispensa de la aprobación del acta para tramitar los acuerdos adoptados en la presente sesión. Los señores, colegas congresistas, que se opongan a la dispensa solicitada, sírvanse expresarlo. No habiendo ninguna intervención, se da por aprobado.

En consecuencia, colegas congresistas, siendo las diez de la mañana con cincuenta y cinco minutos, se levanta la sesión el día de hoy, 5 de mayo del año 2025.

Muchas gracias.

—A las 10:55 h, se levanta la sesión.