Área de Transcripciones

CONGRESO DE LA REPÚBLICA

SEGUNDA LEGISLATURA ORDINARIA DE 2024

COMISIÓN DE CIENCIA, INNOVACIÓN Y TECNOLOGÍA

15.ª SESIÓN ORDINARIA

(Matinal)

LUNES 14 DE ABRIL DE 2025

PRESIDENCIA DEL SEÑOR ALFREDO PARIONA SINCHE

—A las 09:04 h, se inicia la sesión.

El señor PRESIDENTE.— Muy buenos días, colegas congresistas.

Hoy, 14 de abril del año 2025, para igualmente desde la Comisión desearle a los familiares del escritor Mario Vargas Llosa, las condolencias inmensas por esta irreparable pérdida.

Bien, señor secretario técnico, constatar la asistencia de los señores congresistas, por favor.

El SECRETARIO TÉCNICO pasa lista:

Muy buenos días, señor presidente, muy buenos días, señores congresistas.

Se va a pasar asistencia.

Congresista Pariona Sinche.

El señor PARIONA SINCHE (BS).— Presente.

El SECRETARIO TÉCNICO.— Congresista Pariona Sinche, presente.

Congresista Zeballos Madariaga (); congresista Málaga Trillo.

El SECRETARIO TÉCNICO.— Congresista Zeballos Madariaga, presente.

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

El señor BUSTAMANTE DONAYRE (FP).— Presente.

El SECRETARIO TÉCNICO.— Congresista Bustamante Donayre, presente.

Congresista Alva Rojas, presente.

Congresista Jiménez Heredia, presente.

Congresista Cerrón Rojas.

El señor CERRÓN ROJAS (PL).— Cerrón Rojas, presente.

El SECRETARIO TÉCNICO.— Congresista Cerrón Rojas, presente.

Congresista Ciccia Vásquez.

Congresista Ciccia Vásquez, presente.

Congresista Flores Ruíz.

Congresista Flores Ruíz, presente.

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

Señor presidente, han respondido a la asistencia ocho señores congresistas.

Hay el cuórum respectivo para la presente sesión.

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

En consecuencia, colegas siendo 9 de la mañana con 8 minutos damos inicio a la Décima Quinta Sesión Ordinaria de la Comisión de Ciencia, Innovación y Tecnología.

Haciendo constancia también que el colega Abel Augusto Reyes Cam se encuentra con licencia.

Bien, empezamos por la primera parte para poner a disposición la aprobación del Acta.

Colegas congresistas, se pone a consideración de los miembros de la comisión el Acta de la Décima Cuarta Sesión Ordinaria, cuyos acuerdos fueron dispensados de aprobación siendo remitidos con la agenda documentada.

Los colegas que tuvieran alguna observación pueden indicarlo.

Si no hay observaciones se dará por aprobada.

Ha sido aprobada.

Pasamos a la estación de Despacho.

DESPACHO

El señor PRESIDENTE.— Documentos recibidos y enviados.

Colegas congresistas, se ha remitido con la agenda documentada la relación de los documentos enviados y documentos recibidos entre el 4 y el 11 de abril del presente año.

Pasamos a la estación de informes.

Informes

El señor PRESIDENTE.— Colegas congresistas, hacemos de conocimiento para que cada uno de ustedes puedan formular sus informes, con lo cual le concedemos la palabra.

¿Algún colega ha realizado su informe respectivo?

Bien, si no hubiera, desde la presidencia vamos a hacer el Informe siguiente.

El pasado 11 de abril se realizó el Foro Panel "LATAM-GPT: Primer Modelo de Lenguaje de Inteligencia Artificial Latinoamericana", con los destacados ponentes como el doctor Román Ulises Flores y el doctor José Luis Segovia.

En este evento se abordó el estado actual de la Inteligencia Artificial en la región Latinoamericana, su rol en los diversos actores de la sociedad actual y su capacidad para difundir y generar información relevante.

Asimismo, se contó con la participación de representantes de sectores como el CONCYTEC, Educación, Cultura, Comercio Exterior y Turismo, entre otros, así como de representantes de organizaciones del sector privado y la ciudad civil.

De la comisión agradecemos también la presencia y participación activa de los colegas congresistas Ernesto Bustamante y el colega Carlos Zeballos.

Entonces, de esta manera hemos desarrollado esta actividad tan importante.

Bien pasamos a la siguiente estación.

Pedidos

El señor PRESIDENTE.— Estación de pedidos.

Igualmente invitamos a los colegas congresistas, a fin de formular los Pedidos que es conveniente.

¿Algún colega?

Bien. Entonces, pasemos a la siguiente estación.

ORDEN DEL DÍA

El señor PRESIDENTE.— Estación quinta, Orden del Día.

Colegas congresistas, como primer punto del Orden del Día, tenemos la participación de tres sectores gubernamentales invitados para abordar los avances y desafíos en materia de Ciberseguridad, Ciberdefensa y Ciberdelincuencia.

En ese sentido, damos o en todo caso, consultamos al equipo técnico si están nuestros invitados por favor.

Entonces, toca hacer una breve suspensión para recibir a nuestros invitados, colegas congresista de la comisión.

El señor CICCIA VÁSQUEZ (RP).— Señor secretario, señor presidente, buenos días. Miguel Ciccia, para confirmar mi asistencia en la sesión.

Gracias.

El señor PRESIDENTE.— Conforme, colega.

Bien, colegas continuamos con esta sesión.

Ya tenemos con nosotros a nuestros invitados. Por un lado, tenemos al ingeniero Orlando Vásquez Rubio, secretario de Tecnologías y Seguridad Digital de la Secretaría de Gobierno y Transformación Digital.

Tenemos, igualmente al General de Brigada Ejército Peruano, John Rivera Machuca de Ministerio de Defensa, y al Mayor Policía Nacional, Pierre Ruíz Contreras, jefe de la División de Investigación de Alta Tecnología de la Dirección de Investigación Criminal de la Policía Nacional del Perú.

Colegas congresistas, a efectos de una mejor forma llevar la intervención fluida de nuestros invitados y la participación activa de los miembros de la comisión, se otorgará la palabra de forma seguida a los funcionarios señalados, luego lo cual se abrirá una ronda de oradores para las respectivas preguntas y comentarios.

En ese sentido, dándoles la cordial bienvenida a todos los invitados.

Vamos a empezar a invitar al ingeniero Orlando Vázquez para que pueda hacer su intervención hasta por 10 minutos.

Ingeniero, tenga usted la palabra.

El SUBSECRETARIO (e) DE LA SUBSECRETARÍA DE TECNOLOGÍAS Y SEGURIDAD DIGITAL, señor Orlando Vásquez Rubio.— Sí, preparé una presentación.

Sí, presidente, por intermedio traigo el saludo del nuestro señor Premier y también del secretario César Vílchez, quien ha tenido un inconveniente por el cual no está presente.

Avancemos, por favor.

La Secretaría de Gobierno y Transformación Digital, ente rector del Sistema Nacional de Transformación, define muchos temas de coordinación a nivel de proyectos, servicios, Cooperación Técnica Internacional y también un tema de gobernanza digital, que es un tema de regulación. En el cual se manejan entes o normas que definen todo el accionar del Sistema Nacional de Transmisión Digital.

Tenemos un nivel base a nivel normativo, que es el tema de la política del Estado 35 de Acuerdo Nacional, donde se define el

tema del Sistema Nacional de Información que es muy importante para el desarrollo de cualquier país que quiere ingresar al OCDE.

Tenemos a nivel estratégico la política nacional de transformación digital, en los cuales se define que debemos mejorar el tema de habilidades digitales para el 2030 de nuestros ciudadanos. Queremos llegar a ocho habilidades, tal como se manejan muchos países de avanzada.

Nuestro decreto de urgencia que son muy importantes, un decreto de urgencia, creo que importante para esta sesión, es que ya tenemos un reglamento el cual se ha pedido las mejoras y comentarios por parte de la sociedad civil.

Esto ha sido publicado hace una semana y lo que se quiere es mejorar el ámbito del tema gubernamental y también del tema privado. En la mayor parte de países importantes en Asia y en Estados Unidos se manejan muchos temas de coordinación, tanto de la parte privada como del estado. Y tenemos un tema, creo que es de real importancia, que es el tema de innovación tecnológica. Sobre todo, el tema de Seguridad Digital está muy ligado ahorita para el tema de Inteligencia Artificial.

Existen agentes de seguridad digital que van a permitir que debemos tener más cuidado en el tema de regulación y en el tema de infraestructura que vamos a comprar.

La política maneja seis objetivos importantes. El acceso inclusivo, la seguridad digital, la economía sostenible a través de la economía digital y el comercio electrónico, servicios públicos digitales, por lo cual se denomina que esta política nacional de transformación digital va evocada hacia el ciudadano. El fin de los trámites y servicios es el ciudadano y cómo de alguna manera desde la secretaría se impulsan políticas para mejorar la digitalización y la mejora de esta calidad de vida que pide el país.

Un tema importante también es el talento digital. El tema de transformación digital es un tema cultural, por los cuales se necesita educar a la ciudadanía en temas de Seguridad Digital. A través del Centro Nacional de Seguridad Digital venimos implementando una serie de webinars, cursos para la ciudadanía en general, para las empresas y también tenemos un curso que se está implementando con el Ministerio de Defensa para el tema de ciberseguridad, el cual se divide a través de dos módulos. El primer módulo es el tema de fundamento de ciberseguridad, y el segundo para que pueda ser un analista en el tema de Seguridad Digital.

Como ustedes pueden ver, lo que queremos es duplicar el ejercicio de la ciudadanía digital al 2030, ¿no?

¿Podemos avanzar?

Pero ¿cómo podemos mejorar todo el tema de fortalecer el tema de Seguridad Digital? Primero es obtener o comprar o adquirir una infraestructura de ciberseguridad. Después también tenemos el tema de regulación digital, que es de gobernanza. Necesitamos mejorar el tema de políticas de ciberdefensa.

Otro tema importante que se ha estado trabajando en la Secretaría y con muchos entes rectores, es el tema de colaboración internacional. Actualmente la Secretaría tiene Memorándum de Entendimiento con Corea que venimos trabajando desde hace mucho tiempo, y con China.

Estamos trabajando también en Memorándum de Entendimiento con la India y con Israel. Israel, consideramos que es un aliado estratégico debido al alto nivel que maneja este país en tema de tecnología, y también a través de empresas que están dentro del Cuadrante Gartner, como las empresas más especializadas en el tema de Seguridad Digital.

Y, lo más importante, capacitar. Si no capacitamos a nuestro personal, a los ciudadanos, ellos son un vector posible de complicaciones a nivel de seguridad.

A veces, a nivel del Estado, manejamos el sistema de gestión de seguridad de la información, el cual se basa a través del Estándar 27001. Y lo que hemos podido notar dentro del Centro Nacional de Seguridad Digital, que a veces uno puede tener toda la infraestructura adecuada, sin embargo, cuando un servidor no se establece dentro de las reglas debidas es el gran problema o el hueco de seguridad que muchas veces ocasionan problemas informáticos dentro de los entes donde se trabajan. **(2)**

Aparte tenemos los temas de oficiales de seguridad. Si ustedes pueden ver el tema de Seguridad Digital, manejamos varios frentes, ciberdelincuencia, ciberdefensa, ciberinteligencia y a través de la Secretaría manejamos el tema del Comité de Transformación Digital, en el cual es un ente que se trabaja en todo el Estado. Todo ente público tiene que tener un Comité de Gobierno y Transformación Digital, el cual está presidido por el rector o el titular de la entidad o una persona muy allegada a él.

También ahí está adicionalmente la gente de presupuesto, la gente personal, el jefe de Sistemas. Un actor importante es el Oficial de Seguridad de la Información, quien de alguna manera es o hace de nuestros soldados en cada entidad para salvaguardar el tema de la seguridad de la información, y también esto ¿qué hace el comité?, implementa el Sistema de Gestión de Seguridad de la Información.

Avancemos por favor.

A nivel de indicadores internacionales, el Perú está en la Capa 3 de Sudamérica a través de la A y TU 2024. Y estamos en la

posición 9 con respecto a la Capa 3, pero en Sudamérica estamos en la posición 7.

Entonces, ¿cómo estamos pensando mejorar este tema? Estamos trabajando mucho en el tema de identidad digital. Y la identidad digital tiene que ver con la implementación de validaciones seguras a través de…

El señor BUSTAMANTE DONAYRE (FP).— Presidente, disculpe una interrupción pequeña. Quisiera saber ¿cuál es la fuente de esto?, ¿cómo es que se elabora este indicador?, ¿quién es el que dice que estamos en ese puesto?

Gracias.

El SUBSECRETARIO (e) DE LA SUBSECRETARÍA DE TECNOLOGÍAS Y SEGURIDAD DIGITAL, señor Orlando Vásquez Rubio.— Sí, le voy hacer llegar en forma escrita. Ahorita lo voy a corroborar, por favor.

Sí, como le digo, no es una buena posición, o sea, estamos en una posición no muy buena, porque estamos 7 en Sudamérica.

Entonces, lo que se quiere es, ¿cómo podemos mejorar? El Centro Nacional de Seguridad Digital, a través de un Proyecto BIT, está utilizando recursos para implementar una mejor infraestructura. Necesitamos mejorar la infraestructura, necesitamos tener también equipos idóneos, Licencias SAS, que son Servicios de Software que puedan mejorar la calidad de servicios que brindamos actualmente en el centro nacional.

¿Cuál es el desafío digital que tenemos? Hay un 40% de aumento de delitos entre los años 2023 y 2024, hay 1685 alertas emitidas, en los cuales la subsecretaría trabaja con boletines interdiarios para que las entidades públicas y el público en general sepan los peligros que están ocurriendo en el día a día de estos trabajos.

Entonces, de alguna manera alertamos a todas las entidades públicas cuando hay un problema de un fallo de seguridad o una nueva alerta.

Dentro de la subsecretaría hemos capacitado a más de 4000 personas en temas de formación de Seguridad Digital.

Tenemos una estrecha coordinación con los entes militares, con la Marina, con la Policía, con la DINI, y también con el tema de protección de datos.

Avancemos, por favor.

Trabajamos en diferentes frentes como la Fuerza Aérea y el tema de vigilancia de la estación aéreo digital. La PCM es la entidad que coordina todo el tema de articulación a niveles de políticas nacionales.

Avancemos, por favor.

Y, eso se ve reflejado en las diferentes reuniones que hemos tenido con los diferentes entes armados en el Perú, con el Comando Conjunto, con el Ejército y con la Marina de Guerra del Perú.

También tenemos una coordinación con el Mininter, a través de dos comisiones. Una comisión para la estandarización de cámaras de videovigilancia. Lo que se quiere es tener un sistema estandarizado por los cuales podamos tener una mayor seguridad a nivel de seguridad ciudadana.

Lo que se quiere es tener todo un trabajo integrado con el Mininter y a través del Mininter con la Policía para tener cámaras digitales que nos puedan servir para el tema de seguimiento del tema de delincuencia. Eso está en pleno trabajo y se espera concluir este año los diferentes términos de este proyecto.

Un tema en conjunto que indica el tema de coordinación que tiene la Secretaría, es el Plan de Seguridad Digital que se trabajó en el APEC, en el cual se trabajó una estrategia de cómo evitar algún tipo de problemas o delitos informáticos dentro de esta cumbre.

Se congregaron a más de 400 especialistas en el tema de Seguridad Digital y Ciberdefensa, y los resultados han sido exitosos, porque no hemos tenido algún problema público y tampoco hemos tenido algún problema dentro de esta cumbre, lo cual nos indica que la colaboración dentro del Estado es muy importante para poder obtener resultados exitosos.

Dentro del Centro Nacional de Seguridad Digital, se manejan muchos servicios, se asesora a las entidades cuando tienen un problema informático a través de la implementación del SGSI.

También el Estado maneja los equipos de respuesta inmediata llamados CSIRT, igual que los comités dentro de cada entidad.

Manejamos también análisis de vulnerabilidades, apoyamos en temas de *ethical hacking*, manejamos un monitoreo de un NOC y el SOC para saber en qué momento hay problemas dentro de las entidades y se le brinda todo el asesoramiento adecuado.

Este Centro Nacional de Seguridad maneja temas de gestión, articulación, supervisión y tenemos un punto en contacto para que podamos mejorar las condiciones informáticas dentro de las entidades del Estado.

¿Puedo continuar?

No, no, sino que pensaba que no podía ver.

Congresistas, y por nuestro intermedio presidente, la fuente es la UIT, es una encuesta a nivel mundial el tema de Seguridad Digital, lo que me está preguntando el congresista Ernesto Bustamante Donayre.

Entonces, dentro de nuestra red que tenemos, tenemos 800 oficiales de Seguridad Digital.

El año 2023 se ha ampliado y mejorado el perfil de estos oficiales de seguridad dentro del Estado. Se está pidiendo gente con certificaciones 27001, a fin de que ellos puedan servir de apoyo al trabajo del Centro Nacional de Seguridad Digital.

El Centro Nacional de Seguridad Digital no puede trabajar solo, por eso amplía toda esta red de oficiales de seguridad, a fin de poder tener noticias concretas o eventos donde haya problemas del corte informático.

El monitoreo que hace nuestra red es todo el día. Trabajamos en una articulación estratégica con la Policía Nacional, con el sector Defensa y entidades de protección digital, como es el tema de la regulación de datos personales.

Y también estamos dentro de la Red de Cooperación Internacional a través del CSIRT América.

¿Qué logros hemos tenido en el 2024? Hemos asistido técnicamente a más de 1500 entidades. Hemos capacitado a más de 4000 funcionarios.

Con respecto al tema de Seguridad digital y SGSI. Hemos trabajado conjuntamente con entes rectores con respecto a la protección de la APEC, y tenemos una frecuencia de un simulacro internacional en los cuales verificamos el tema de vulnerabilidades en los diferentes sistemas que hay en las entidades del Estado.

¿Qué avance tenemos en el 2025? Tenemos incidentes atendidos, 164; situaciones críticas resueltas, nuestras alertas emitidas son 223. Las alertas emitidas son boletines de lo que se encuentra como lo último de vulnerabilidades de los sistemas informáticos para advertir a los oficiales de seguridad que puedan implementar las medidas necesarias, a fin de no llevar algún tipo de problemas dentro de las entidades.

Tenemos un tema de implementación de herramientas. 20 entidades han sido apoyadas y se han implementado soluciones de seguridad con la vía de actualización.

Y, hemos emitido 36 informes de vulnerabilidades digitales a las diferentes entidades que nos han solicitado.

Avancemos, por favor.

¿Y cuáles son los resultados del CNSD? Tenemos más de 800 incidentes gestionados, 1180 alertas emitidas y 90 casos hemos derivado hacia la PNP, a la DIVINDAT, y 60 a la protección de datos.

Avancemos.

El resultado de todo este trabajo es que tenemos 185 equipos conformados para el tema de incidentes o de CSIRT. Manejamos un tema de trabajo conjunto con Cooperación Internacional acerca del tema de CSIRT en los países miembros de la OEA, con los cuales tenemos un benchmarking con respecto a la situación que está sucediendo en cada país.

Y también trabajamos para el tema de protección de datos a través de la eliminación de 60 publicaciones con respecto a los foros de hacking, es decir, el equipo del Centro Nacional de Seguridad Digital está validando o verificando, monitoreando las publicaciones que hay en los foros de hacking, a fin de eliminar estas publicaciones y que puedan servir de vulnerabilidades para los ciudadanos.

En el tema de capacitación, estamos capacitando a más de 6000 ciudadanos en temas de Ciberseguridad. Tenemos una alerta nacional, en la cual tenemos 11 sesiones con respecto a la protección de datos.

Más de 1400 ciudadanos han sido sensibilizados en el tema de archivos digitales y también tenemos un programa con respecto a una iniciativa de la OEA para la participación femenina en Ciberseguridad.

También hemos tenido un evento en los cuales hemos verificado con respecto al personal femenino, no hay muchas expertas dentro del Perú con respecto a la Seguridad Digital.

Avancemos.

También hacemos simulacro internacional de ataques informáticos, a fin de poder mejorar el tema de vulnerabilidades dentro de los diferentes sistemas que administramos.

Y, este es el programa de Ciberseguridad y Ciberdefensa que hemos establecido con el Ministerio de Defensa, a fin de poder mejorar la calidad no solamente de los funcionarios, sino también de los ciudadanos. Entendemos que, si un ciudadano no es educado en temas digitales, hay una gran posibilidad de que sea un problema dentro de su vida familiar, como lo hemos verificado a través de las estadísticas.

Pero, ¿qué hacemos con respecto a todo este tema? Nosotros estamos aprobando un Decreto de Urgencia 007, que es el tema de confianza digital. Estamos validando y recibiendo los comentarios de la sociedad civil, a fin de fortalecer este reglamento.

¿Avanza, por favor?

¿Pero qué necesitamos para realizarlo? Necesitamos fortalecer la seguridad, promover la participación y una articulación. Necesitamos también que tanto el Estado como los entes privados

cumplan los estándares internacionales con respecto a Seguridad Digital.

¿Cómo estamos estructurando este reglamento? Primero, la Secretaría que es el ente rector del marco de confianza digital, en el cual se articulan las políticas y se supervisa la implementación.

El centro nacional, el cual gestiona los incidentes, monitorea los riesgos y promueve una cultura de Seguridad Digital. Y también el tema de protección de datos personales y defensa del derecho del consumidor digital, que se hace a través de *COPI.

¿Cuáles son las medidas que nos emite este documento, este reglamento o este decreto de urgencia? En el sector público, identificación de actividades críticas, gestión de riesgo anual y lo importante que es el oficial de seguridad tenga mayor peso y reforzamiento en sus habilidades digitales.

Con respecto al sector privado, se está pidiendo la implementación de Estándares ISO y NIS, un nivel de confianza, Nivel 3, a fin de que se vulneren los servicios digitales del sector privado, y también que sean notificados los incidentes **(3)** hacia el Centro Nacional de Seguridad para poder tener un apoyo y una coordinación más importante. Sí, a nivel de este reglamento, tenemos la gestión de incidentes y fortalecimiento. Queremos trabajar en el tema de detección, notificación, fortalecimiento y respuesta con respecto a los diferentes incidentes que hay en el Perú.

¿Cuáles son las próximas acciones dentro del paquete de mejoras o cómo mejoramos? Primero tenemos que fortalecer el CNSD, en lo cual se van a invertir 50 millones para poder tener un SOC a nivel de todos los países de avanzada en Sudamérica. Estamos en proceso de la aprobación de la Estrategia Nacional de Ciberseguridad, la cual tiene que estar alineada a la Política Nacional al 2030. Y también tenemos que hacer un trabajo conjunto con respecto a la protección electoral y la votación digital.

¿Cuáles serían las próximas acciones? Necesitamos coordinar con el tema del sector financiero, el cual ha sido vulnerado el anterior año, para poder trabajar en forma colaborativa y conjunta con respecto a estos tipos de riesgos, ya que son las entidades que tienen más ataques en el Perú. También hay un tema de inclusión de género, queremos a través del proyecto de transformación digital con equidad, mejorar este cuadro dentro de las áreas de tecnología.

En cooperación internacional creo que es un punto muy importante, se está trabajando muchos temas con la gente de Corea, con China, con la India, con Estados Unidos y con Israel. Creo que es muy importante aprovechar las experiencias de estos países a fin de poder implementar un marco digital más seguro. Y tenemos que reescribir también el tema de los protocolos de respuesta.

Creo que eso es todo, pero creo que lo más importante es que estamos trabajando con el tema de identidad digital. Estamos haciéndolo a través de la Secretaría y lo que se quiere es que cada servicio sea validado por el ciudadano. ¿A través de qué?, a través de mecanismos biométricos. para evitar los grandes problemas que tenemos con respecto a las contraseñas y las claves usuarios dentro del Estado. Creemos firmemente en que este mecanismo de implementación biométrica va a mejorar, y estamos también verificando un tema de avanzada como es la implementación de un *blockchain* tal como lo tiene China, Corea y muchos países de avanzada.

Muchas gracias.

El señor PRESIDENTE.— Agradecemos al ingeniero Orlando Vásquez Rubio, subsecretario de tecnologías y seguridad digital de la Secretaría de Gobierno y Transformación Digital. Muchas gracias.

Vamos a invitar al general de brigada E.P. John Rivera Machuca, igualmente para abordar en esta sesión hasta por 10 minutos.

Estimado general, tiene la palabra.

El COMANDANTE DEL COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS, general de brigada E.P. John Rivera Machuca.— Muy buenos días, señor presidente. Expreso el saludo del señor Walter Astudillo, ministro de Defensa, para dar inicio a la presentación.

El tema que nos ha convocado es exponer los avances y desafíos en materia de ciberdefensa en el Estado peruano. Quiero iniciar esta presentación con una reflexión que hizo hace una década John Chambers, ex CEO de Cisco, en la cual quiere expresar que el mundo actual está viviendo una lucha constante, donde las grandes organizaciones públicas o privadas tratan de mantener asegurados sus redes, sus sistemas, pero por otro lado hay grupos individuales, colectivos, organizaciones estatales que tratan de irrumpir y alterar o apoderarse de esas redes y sistemas. En suma, es una lucha permanente por proteger nuestras redes y sistemas.

El marco legal que tenemos en cuestión de ciberdefensa, consideramos tres puntos muy importantes. El primero es nuestra Constitución Política, que en su artículo 44 establece que uno de los deberes primordiales del Estado es asegurar, proteger a la población contra las amenazas a su seguridad, entendiéndose como una de estas amenazas a la seguridad, cualquier tipo de afectación a la seguridad digital.

El segundo marco importante para la ciberdefensa está constituido por el Decreto Legislativo 1412, mediante el cual se aprueba La ley de Gobierno Digital, en ella se establece que el marco de seguridad digital se compone de 4 ámbitos, uno de ellos el ámbito de la ciberdefensa. En este caso, se establece que el

Ministerio de Defensa es la entidad que dirige, supervisa y evalúa todas las normas en materia de ciberdefensa en el Estado peruano.

El otro aspecto importante dentro del marco legal de la ciberdefensa es la Ley número 30999, Ley de ciberdefensa, que tiene la singularidad de establecer la regulación de la ciberdefensa en el Perú, y además porque se define de manera específica que la ciberdefensa es una capacidad militar, es una atribución exclusiva de las organizaciones militares en el Perú.

Esto, por supuesto, también enmarca que estas operaciones militares de ciberdefensa están a cargo del Comando Conjunto de las Fuerzas Armadas y que en el principio de legalidad también deben estar sujetas al artículo 51 de la Carta de Naciones Unidas que expresa que todo Estado tiene el derecho a la legítima defensa cuando son atacados por otros países.

Asimismo, se establece que la finalidad de la ciberdefensa es, entre otras, la protección de los activos críticos nacionales y los recursos clave.

Quiero mencionar, en una breve línea de tiempo, todas las acciones que se han estado llevando a cabo en el aspecto de ciberdefensa desde el año 2018, cuando el Comando Conjunto emite su Doctrina de Operaciones de Ciberfensa. Hay que recordar que en el mundo la Organización del Tratado del Atlántico Norte ya en el 2016 establece que el ciberespacio es el quinto dominio de la guerra. Hasta ese entonces solamente se había considerado tierra, aire, mar y espacio para el control y dominio de las operaciones militares por supuesto.

Sin embargo, a partir del año 2016 ya se considera el ciberespacio como aquel ámbito en el cual se pueden desarrollar operaciones militares, tanto para la defensa como para la explotación y la respuesta. En ese sentido, reitero, en el 2018, el Comando Conjunto emite su Doctrina de Operaciones de Ciberdefensa, en el 2018 también se crean de manera experimental las primeras unidades de ciberdefensa por parte del Ejército y la Marina; y al año siguiente, en 2019, el Comando Conjunto también activa un Comando Operacional de Ciberdefensa, entendiéndose que es el Comando Conjunto quien es el que conduce y desarrolla operaciones militares.

A lo largo de los años 2019 y 2020 se ha participado de manera recurrente en algunas actividades, por ejemplo, en el 2019 la operación de ciberdefensa en apoyo a los Juegos Panamericanos, que consistió básicamente en monitorear cualquier evento o incidente digital que tenga intenciones de afectar a los sistemas que estaban ejecutándose en ese momento. Otro hito que tenemos acá, como ya les había comentado, el 9 de agosto se promulga la Ley de Ciberdefensa, que marca el inicio del reconocimiento de la capacidad del Estado para actuar en materia de ciberdefensa.

En el año 2024 se aprueba el reglamento de esta Ley de Ciberdefensa y ese mismo año también se han ejecutado operaciones de apoyo a la realización de la APEC en nuestro país. En abril del 2024 también se solicita al Congreso facultades legislativas para modificar los decretos legislativos del Comando Conjunto, del Ejército y de la Marina con la finalidad de incorporar en estos decretos legislativos las competencias en temas de ciberdefensa, las funciones que atañen a las entidades; y, asimismo, las funciones que le corresponde al comandante general de cada institución.

Actualmente ya estamos finalizando, luego que se han aprobado los decretos legislativos correspondientes, estamos en la adecuación de los reglamentos de estos decretos legislativos.

¿Cuáles son los avances en las Fuerzas Armadas a la fecha? De manera resumida les podemos decir, en primer lugar, se crearon las unidades de ciberdefensa, luego ha habido todo un proceso que se sigue llevando hasta ahora en la formación, capacitación y entrenamiento en operaciones de ciberdefensa en todas las instituciones, y a la implementación de software para el desarrollo y la capacitación de nuestro personal.

Respecto a la creación de unidades de ciberdefensa, ya con la expedición de los decretos legislativos se formalizan las entidades de ciberdefensa en nuestras instituciones, el Comando Conjunto tiene un Comando Operacional de Ciberdefensa que se encarga de planificar, organizar, conducir las operaciones militares de ciberdefensa y tiene tres organizaciones bajo su mando; el componente de ciberdefensa de Marina, materializado por la Comandancia de Ciberdefensa; el componente de ciberdefensa del Ejército, materializado por un centro de operaciones cibernéticas; y el componente de ciberdefensa de la fuerza aérea materializado por un centro de operaciones ciberespaciales de la Fuerza Aérea materializado por un centro de operaciones ciberespaciales de la Fuerza Aérea.

Su organización es como la que estamos viendo en estos momentos, el Comando Conjunto en el encargado de la planificación y ejecución de las operaciones en el ciberespacio, tiene a su órgano que es el Comando Operacional de Ciberdefensa, y este a su vez a los tres componentes de ciberdefensa de las instituciones.

Como veremos en estas diapositivas, desde el año 2015 en las instituciones se viene formando nuestro personal en operaciones cibernéticas, contándose a la fecha con 138 oficiales capacitados en estos cursos. Asimismo, la Escuela Superior Conjunta de las Fuerzas Armadas ya viene desarrollando un programa de fundamentos básicos del ciberespacio, dirigido al personal de oficiales del grado de capitán, tenientes y también a la plana de suboficiales.

Por su lado, el Centro de Altos Estudios Nacionales brinda la maestría en ciberseguridad y ciberdefensa, dirigido a oficiales de seguridad de información, consultores de seguridad y profesionales que tienen relación con el ámbito de la ciberdefensa y ciberseguridad.

En cuanto a la capacitación, se ha estado participando en el ejercicio internacional de defensa cibernética, por ejemplo, en Brasil en el año 2021 y 2025; y acá quisiera hacer mención, por ejemplo, en el 2021 un oficial de nuestro de nuestras Fuerzas Armadas logró ocupar el primer puesto en esta pasantía lo cual de alguna manera evidencia que tenemos personal capacitado, que tenemos personal con las habilidades para seguir mejorando en el tema de la ciberdefensa.

También estamos participando en los simulacros organizados por la Secretaría de Gobierno de Transformación Digital, como el Primer simulacro de ataques cibernéticos realizado el 2022; y el último en el 2024 en el Primer simulacro internacional de ataques cibernéticos.

Participación en los foros iberoamericanos de ciberdefensa, participación en los ejercicios de guardián cibernético organizado por el Ejército de Brasil. Esto tiene una importancia especial porque se trata de la protección de los activos críticos nacionales de un Estado.

Participación en el ejercicio multinacional Resolute Sentinel del año pasado, realizado en nuestro país.

La protección durante los Juegos Panamericanos, como les había mencionado anteriormente.

Durante el 2020, la protección al grupo de trabajo Te Cuido Perú, mediante vigilancia de los activos digitales del Ministerio de Salud. **(4)**

Monitorea de los activos digitales del Ministerio de Salud.

Tenemos una activa cooperación internacional y esto se materializa mediante reuniones bilaterales de intercambio.

Reunión entre representantes del Comando Operacional de Ciberdefensa del Comando Sur de los Estados Unidos.

Algunos desafíos de ciberdefensa están fundamentados básicamente con el desarrollo de las tecnologías emergentes, que cada vez impulsan que los ciberatacantes tengan muchas más herramientas como para poder irrumpir en nuestras redes y sistemas, en todo orden, tanto en las entidades públicas como en las entidades privadas.

Ante esto, lo que siempre pensamos que es necesario es mejorar nuestra colaboración público-privada, invertir en el talento local, no solamente de las Fuerzas Armadas sino también de los universitarios. Sabemos que hay algunas universidades que están

ya con carreras de ingeniería de ciberseguridad. Eso es muy bueno, necesitamos alentar que nuestros jóvenes talentos se dediquen mucho más a la ingeniería de datos, a la ingeniería de ciberseguridad.

Proveer las regulaciones dinámicas y eso ya fundamentalmente mediante la Ley de Ciberdefensa y su reglamento se ha conseguido.

Y, finalmente, desarrollar alianzas estratégicas, básicamente pensamos que el Ministerio de Defensa debería mejorar este tipo de alianzas, sobre todo con la academia, con la universidad, para promover la tecnología.

Conclusiones:

La Ley de Ciberdefensa y su reglamento marcan el paso inicial para el inicio del desarrollo de la ciberdefensa en el Estado peruano, sin embargo, consideramos que es necesario mantener un equilibrio entre el constante avance tecnológico que se desarrolla de manera exponencial con la inversión en los recursos humanos que tenemos, no solamente a nivel de Fuerzas Armadas sino a nivel de la sociedad, y esto sumado a la cooperación estratégica en todos los niveles.

Y, finalmente, que la tecnología siempre va a ser masificada, presenta retos, pero también presenta oportunidades que son las que debemos aprovechar.

Finalmente, quiero presentarles una reflexión de John Chambers que decía que lo que va a diferenciar a los ganadores de los perdedores no será quién tenga más tecnología o quién tiene más capital financiero sino las organizaciones o los estados que tengan más liderazgo y la voluntad de aprender.

Muchas gracias, con esto concluyo la participación.

Muchas gracias al general de brigada ejército peruano John Rivera Machuca por abordar o hacer de conocimiento referente a los avances y desafíos en materia de ciberseguridad, ciberdefensa y ciberdelincuencia.

En la misma medida vamos a continuar esta vez presentando también al coronel ejército peruano del Comando de Fuerzas Armadas Octavio Martín Freitas Farfán; y también tenemos al mayor de Policía Nacional Pierre Ruiz Contreras, quienes podrían compartir los minutos para poder abordar todo caso.

Invitamos a ambos destacados invitados, adelante, tienen la palabra.

El JEFE DE LA DIVISIÓN DE INVESTIGACIÓN DE DELITOS DE ALTA TECNOLOGÍA DE LA DIRECCIÓN DE INVESTIGACIÓN CRIMINAL DE LA POLICÍA NACIONAL DEL PERÚ, mayor PNP Pierre Ruiz Contreras.— Señor Congresista, muy buenos días; señor congresista Bustamante, buenos días, reciban el saludo de nuestro general José Zavala Chumbiauca, director de ciberdelincuencia.

Decirles que tiene una problemática muy concisa esto del delito de ciberdelincuencia y por la experiencia que tengo en el tema me ha nombrado con la finalidad de poder llegar y tocar unos temas puntuales.

Primero que nada, la Dirección de Ciberdelincuencia ha sido creada como una dirección que se basa dentro de la estructura de la Divindat, que es la División de Investigación de Delitos de Alta Tecnología. Hemos subido de nivel, hemos cambiado de división ahora a dirección, debido a las nuevas vulnerabilidades que se vienen dando o desarrollando día a día, dentro de las cuales está como idea principal, como objetivo, prevenir, combatir e investigar cualquier tipo de denuncias que se produzcan a través de las TIC, que son las Tecnologías de Información y Comunicación, a todos los datos de sistemas informáticos a nivel nacional.

Tiene como principal herramienta recibir las denuncias, investigarlas y, a la vez, tomar acciones en el tema de geolocalización, que es muy importante no solamente para los delitos tecnológicos o ciberdelincuencia, sino para todos los delitos en general.

Tenemos un grupo de denuncias que se han venido recibiendo de acuerdo a las diversas modalidades delictivas en marco a la Ley de Delito Informático, dentro de las cuales las estadísticas abordan que nuestro pico más alto fue en el año 2022, que llegamos a 4326 denuncias cometidas en su mayoría a través de fraude informático en sus diversas modalidades que voy a detallar más adelante.

Dentro de las principales modalidades delictivas enmarcadas en los delitos informáticos, venimos recibiendo denuncias de fraudes en la modalidad de *phishing, smishing, vishing, sync swapping, thief transfer, carding, ransomware* y el *Fake App*, cuya principal modalidad es el phishing, en la cual estos ciberdelincuentes o ciberataques que se vienen realizando a personas naturales y jurídicas se basa en poder obtener datos sensibles de ellos, como son cuentas bancarias, *password*, contraseñas, con la finalidad de poder despojar de su patrimonio a cada uno de las personas, en los cuales se utilizan unas páginas suplantadas o clonadas, en este caso de entidades bancarias, como se ve en el ejemplo, con la finalidad de poder inducir el error y poder esas personas digitar esas claves confidenciales con la finalidad de poder despojarlas su patrimonio.

Hemos tenido en estas modalidades la mayor tasa de denuncias en la Diver Cyber, y también en lo que es la modalidad del *Fake App* o falso aplicativo, en la cual estas personas inducen a los ciudadanos que puedan descargar un malware y apoderarse de datos con la finalidad de despojarlos de su patrimonio.

Dentro de las denuncias recibidas con las diversas modalidades, tenemos una alza o un índice alto en los que son la modalidad del *phishing* y el *vishing*, que es la modalidad que más se abunda en la actualidad donde utilizan estos delincuentes la ingeniería social con la finalidad de perfilar a sus víctimas y lograr un envío masivo de correos o mensajes de texto para que estas personas piensen que están hablando con entidades bancarias o entidades financieras con la finalidad de poder ingresar a esos enlaces que llevan a un malware, poder descargarlos y estas personas puedan de esa manera cometer el delito informático y poder sustraerles de sus aplicativos bancarios que se encuentran ahora en la actualidad en los diversos equipos o terminales móviles y puedan despojarlos de su patrimonio a través de cuentas receptoras y puedan así beneficiarse de ellos.

También un punto general que se debe tocar y tomar en cuenta y también sensibilizar es el tema de las Sim Card que son activadas a nombre de terceras personas y que en la actualidad hemos tenido sendos operativos y recuperar 17 069 Sim Card que han sido activados a nombre de terceras personas, que como uno sabe los ciberdelincuentes buscan la clandestinidad a través de estos Sim Card que han sido activados de manera ilegal para poder cometer o entablar la conversación con los agraviados o las víctimas, y puedan inducirlas al error, con la finalidad de poder despojarlas de su patrimonio.

Pero acá hay una peculiaridad, que el delito de los Sim Card activadas está dentro de marco legal, dentro de los delitos en el Código Penal en artículo 222 B, y no dentro de la Ley de Delitos Informáticos, que es delito en por el cual esta dirección combate la delincuencia. Cuando hemos tomado a cargo debido a que sea un delito enmarcado dentro de la legislación peruana como un Código Penal, en el Código Penal como delito de propiedad intelectual, debería este articulado en lo principal ser extraído —una sugerencia, señores congresistas— de esa configuración legal y pasarlo a la Ley de Delitos Informáticos, porque es un delito en el cual, no solamente lleva a poder lograr el desprendimiento patrimonial de las personas víctimas de delitos, sino extorsiones, sicariato y las demás modalidades delictivas en las cuales nosotros, la Dirección de Ciberdelincuencia, tiene el personal capacitado para poder irrumpir en este tipo de actividad ilícita y alcanzar los logros que venimos a exponer el día de hoy, obteniendo 83 personas, donde también una sugerencia, señores congresistas, la pena no nos permite lograr una medida coercitiva o una medida limitativa de libertad, ya que está por debajo de la prognosis de los cinco años.

Es de uno a tres años a aquella persona que pueda activar una Sim Card a nombre de terceras personas para acometer los diversos ilícitos que he detallado, sin embargo, la pena no nos permite

a nosotros como el ente encargado de poder pedir una medida limitativa, restrictiva, ni tampoco el Ministerio Público.

Haciendo una medida comparativa normativa, debido también a la noticia actual en la cual se ha filtrado información de muchos ciudadanos a través de una filtración de los datos sensibles de Reniec, en lo cual quiero sensibilizar también al auditorio, una pena de un robo agravado de un teléfono celular o un terminal puede tener una pena de 12 hasta 20 años, pero si a una persona le sustraen más de 29 millones de datos del sistema de Reniec se estaría investigando un acceso ilícito en la cual la pena sería no mayor de cuatro años y no menor de un año, en lo cual quiero sensibilizar y poder sugerir que se pueda a través de una fórmula legal o un espíritu de la norma poder cambiar estas modificatorias que nos permitan a nosotros tal vez lograr las medidas restrictivas y limitativas de derecho para aquellas personas que cometen este tipo de hechos penales y nos puedan tener más armas para la finalidad de poder llevar a cabo diversos operativos.

Igual sensibilizar al auditorio sobre el tráfico ilegal de datos, que es la comercialización de información no pública, lo cual también está enmarcado dentro del Código Penal y no en la Ley Especial de Datos Informáticos, en la cual si vemos la prognosis de pena es no menor de dos ni mayor a cinco años, en los cuales también los que comercializan a través de los diversos grupos Telegram o grupos WhatsApp, de información sensible de diversas personas: árbol genealógico, datos biométricos, fotos, Reniec, antecedentes, sistemas en los cuales este comercio tiene en la actualidad dentro de la legislación peruana una pena mínima, en la cual no podemos llegar a una medida limitativa ni restrictiva de derechos de estas personas.

Los casos relevantes que hemos tenido en la Dirección de Ciberdelincuencia, ya que venimos hablando del tema de la filtración de datos, fueron a personas que hemos logrado detener en la comercialización de estas informaciones a través de grupos Telegram, que es una página Zorrito Rumrum, que fue muy conocida hace años, en los cual se logró desarticular esta banda que era conformada por personas mexicanas y peruanas, y All cool all catcher que tenía todo el dinero acumulado, en los cuales hemos logrado, accediendo a información lícita dentro de un proceso legal, una pena efectiva a estas personas, pero vinculándolos no simplemente al tema informático, sino al agravante de ser una banda criminal estructurada en el tiempo, como el concurso de dos o más personas que se reparten roles y tienen una estructura criminal definida para comercializar estos datos, en los cuales, luego de acopiar los elementos de convicción, poder presentar el caso a un juez especializado y lograr unas medida limitativa de derechos a aquellas personas que vendían información confidencial de diversas personas que en la actualidad se han visto vilmente vulneradas. Otro de los casos mediáticos que

investigamos dentro de agresiones de la ciberdelincuencia son aquellos delitos que van contra la indemnidad y libertad sexual, el *grooming,* que van a aquellas personas que reclutan o tratan de interactuar con personas menores de edad, menores de 14 años, con la finalidad de poder obtener material pornográfico, de tener un encuentro sexual con ellas, donde tenemos una división especializada de ciberprotección infantil dentro de la Dirección de Ciberdelincuencia, donde venimos obteniendo medidas limitativas de derecho, que son allanamientos y descerrajes de estas personas que dañan a la juventud peruana, las cuales tratan de obtener filmaciones de menores de edad y encuentros sexuales con la finalidad de saciar sus apetitos sexuales o ese fetiche que tienen.

Dentro de lo cual esta Dirección de Ciberdelincuencia ha logrado también sendas, capturas, en los cuales están todas esas estadísticas. Y en estas particularidades sí la prognósis de pena en ese punto nos permite lograr unas medidas limitativas de derecho, ya que la pena menor es de seis y la mayor es de nueve años, lo cuales también lo vinculamos con un tema de trata de personas. **(5)**

Dentro de las propuestas que queremos plantearles dentro de la Dirección de Ciberdelincuencia tenemos un marco de denuncias en el cual si bien es cierto denuncian a través del Ministerio Público a través de denuncias directas a la Dirección de Ciberdelincuencia tenemos un porcentaje de denuncias en las cuales las personas civiles no comunican la noticia criminal, vale decir, son víctimas de un fraude y solamente llaman al banco, bloquean las cuentas, pero esas entidades bancarias al tener conocimiento de la noticia criminal no lo comunican a la unidad especializada, ni mucho menos cuando son víctimas de temas cibernéticos a través de las terminales de comunicación, reportan hacia Osiptel y también esa empresa no comunica a la Dirección de Ciberdelincuencia, por lo cual, se propone la creación de una Oficina de Coordinación de Conflictos, a través de 24/7 para poder trabajar denuncias de flagrancia en este tipo.

Y también la modificatoria de la Ley de Delitos Informáticos, en la actualidad la que tenemos nosotros, como bien lo he sustentado de manera muy rápida, a veces las penas no son muy permitidas y los verbos rectores han cambiado en la actualidad de acuerdo a la tecnología, en los cuales ahora tenemos delitos generados por Inteligencia Artificial, donde una fotografía pueden ponerle voces, hacerle movimientos e incitarlos a diversos tipos de temas que dañan la moral y la imagen de las personas, en los cuales debe haber una pequeña modificatoria en los agravantes, en la prognosis de pena y en poner nuevos verbos rectores a los nuevos delitos que tenemos en la actualidad.

Eso es todo por la parte de la Dirección de Ciberdelincuencia de la Policía Nacional de Perú, gracias.

Muchas gracias.

El señor PRESIDENTE.— Coronel, ¿algún dato más, por favor?

El JEFE DE ESTADO MAYOR DEL COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUEZAS ARMADAS, coronel E.P. Octavio Martín Freitas Farfán.—Buenos días, señores congresistas, traigo el saludo de parte del señor general de ejército, David Guillermo Ojeda Parra, jefe del Comando Conjunto de la Fuerza Armada, así como del mayor general Roberto Aranda del Castillo, comandante general del Comando Operacional de Ciberdefensa.

Estamos atentos a cualquier pregunta, yo vengo con el señor general Rivera por parte del Ministerio de Defensa, como su órgano ejecutor.

El señor PRESIDENTE.— Muchas gracias, coronel.

Luego de haber escuchado a todos los ponentes, colegas congresistas, referente al avance y desafíos en materia de ciberseguridad, ciberdefensa y ciberdelincuencia que nuestros invitados han podido abordar de manera amplia.

Entonces para continuar esta estación vamos a invitar a cada colega congresista a fin de generar sus preguntas, comentarios o algún otro tipo de información al respecto. Entonces, tienen la palabra, colegas congresistas.

Vamos a comenzar con el colega Bustamante, adelante, colega.

El señor BUSTAMANTE DONAYRE (FP).— Gracias, presidente.

En primer lugar, mi saludo a los distinguidos invitados que aquí nos acompañan para las exposiciones tan interesantes que han hecho sobre el tema de la ciberdefensa y ciberdelincuencia. Yo tengo cuatro preguntas más o menos específicas.

El ingeniero Vázquez, cuando hizo su presentación, mencionó que, por ejemplo, una de las funciones de la Red Nacional de Seguridad Digital es el monitoreo y habla de la vigilancia permanente del ciberespacio sin interrupciones. Y luego, cuando habla de los avances en el año 2025, menciona que hubo 164 situaciones críticas resueltas.

La pregunta es, ¿podría dar usted algunos ejemplos de estas situaciones críticas resueltas como para tener una idea si se trata de cosas muy sencillas o de cosas muy complejas, o quizá un abanico de estas? Esa es una pregunta.

La otra pregunta tiene que ver con la presentación del general Rivera, mencionó que existe, en realidad es muy apropiado, se habla pues con toda claridad del quinto dominio de guerra posible que es el ciberespacio. La pregunta es, ¿el personal que está asignado a esta, no sé si es una división, arma no es todavía en el Perú, pero si fuera arma, mi pregunta no iría, pero como no es arma, entonces lo más probable es que sea personal militar de

diversas armas que circulan por esta división, vamos a decir, y quizá pasan un año, dos años en esa circunstancia y luego rotan.

Por ejemplo, lo mismo ocurre con Conida, donde el personal rota. Y hay también un personal civil que está inscrito y que es más o menos permanente, pero tampoco es tan permanente porque están contratados por el sistema de locación de servicios, no tienen estabilidad, hay mucha fuga de talentos. Y yo me pregunto cómo es que eso está organizado a nivel de ciberdefensa, cosa que me parece muy importante fortalecer. Yo diría que hasta se requeriría tener un arma llamada ciberdefensa, donde haya oficiales que, por supuesto tienen conocimientos generales de otras actividades militares también, pero que deberían especializarse de carrera en esa actividad y ser seleccionados por su talento, por su mérito, en esas áreas específicas. El ser militar no te capacita para tener actividad en ciberdefensa, sino yo creo que es una mezcla de las dos cosas.

Entonces esa es la pregunta para el general Rivera y para el mayor Ruiz Contreras, también muy interesante su presentación sobre ciberdelincuencia, la pregunta tiene que ver con las actividades de *fishing,* de *vishing* y de *texting* con *fishing,* no sé, los acrónimos ahí eran interesantes, algunos nuevos que no conocía. Pero la pregunta es qué se está haciendo al respecto. todos nosotros recibimos llamadas telefónicas, llamadas spam. Entonces uno trata de decir, bueno, es una llamada spam, una llamada spam es de un *call center*. Pobrecita, la gente del *call center* están trabajando, hay que dejarlos trabajar.

Pero muchos delincuentes utilizan las llamadas sorpresa o llamadas de números no conocidos o números a los que no se puede devolver llamadas para hacer llamadas de este tipo. Hoy en día, extorsivas, pero también simplemente tratando de llegar, de tener acceso a la intimidad de la persona, intimidad financiera o intimidad personal con el propósito de cometer un delito.

Entonces la pregunta es ¿qué se está haciendo al respecto? En el Congreso tenemos un proyecto de ley que está medio archivándose, un proyecto de ley que va contra las llamadas spam, pero los principales *lobbies* que se hacen a favor de las llamadas spam, vienen de las compañías de teléfonos. Específicamente. Telefónica, que ahora cambió de dueño Entel, Claro, y hay otra más. Todas las compañías que patrocinan llamadas telefónicas quieren que los *call center* que se dedican supuestamente a insistir en que un cliente se pase de una compañía a la otra, continúen en su actividad.

Eso me parece muy encomiable, pero el problema es que lo hacen de una manera intrusiva, llaman a horas que no corresponde, y sorprenden a la gente, especialmente a gente mayor, que de pronto tiene dificultades para concentrarse, vamos a decirlo así, y caen en ser sorprendidos como que quien llama es un pariente, un nieto o un hijo, un sobrino o alguien no conocido, pero que sin

embargo le dice dos o tres cosas que le suenan familiar a este individuo y de pronto suelta más información, y con eso termina perjudicando la seguridad no solamente de esa persona, sino del entorno familiar de esta persona, muy grave.

Y eso ocurre todo el tiempo, y yo estoy seguro que muchas de estas cosas no se denuncian. Algunas quizás sí. Entonces la pregunta es qué se está haciendo al respecto. ¿Es necesario acabar con las llamadas spam, estas llamadas no deseadas, específicamente provenientes fundamentalmente de compañías de teléfonos, en segundo lugar, de bancos los mismos bancos hacen llamadas a través de *call centers* y las compañías de seguros?

Son las compañías que fundamentalmente usan este sistema intrusivo, pero que también es utilizado por los delincuentes. Los delincuentes que se hacen pasar por bancos, se hacen pasar por compañías de seguros, se hacen pasar por compañías de teléfonos y le sacan información a la gente. Que dónde vive, dónde está tu teléfono, con qué frecuencia, con qué banco, no me pagaste la última cuota. Ese tipo de preguntas o de interjecciones terminan haciendo que la persona pueda divulgar información sensible, que es aprovechada en prejuicio de la sociedad. Entonces la pregunta es esa para el mayor Ruiz Contreras.

Muchas gracias.

El señor PRESIDENTE.— Gracias, colega Bustamante.

¿Algún otro colega?

Bien, vamos a aprovechar también desde la Presidencia para formular algunas interrogantes. Es sabido pues que estamos viviendo una ola de inseguridad en el país. Hemos podido escuchar diversas plataformas, diversos mecanismos que se tiene para poder enfrentar, sin embargo, hoy como que nos está venciendo, nos está ganando la delincuencia y otros males que aquejan a la sociedad.

En ese contexto, ¿qué está ocurriendo?, ¿qué es lo que está pasando? ¿qué nos falta hacer? Algunos opinólogos manifiestan que lastimosamente en el país hay diversos problemas como la corrupción que se ha institucionalizado en todas las entidades, igualmente tenemos un débil sistema judicial, falta de coordinación entre autoridades, la pobreza, la desigualdad que se han incrementado, igualmente el crecimiento del crimen organizado, falta de inversión para la prevención, igualmente desconfianza ciudadana, entre otros, es un caldo de cultivo para estos temas de la inseguridad.

Entonces, teniendo en cuenta todo ello, algunas preguntas de manera general, por favor, para que puedan absolvernos.

¿Qué acciones viene impulsando la secretaría para garantizar que las entidades públicas cuenten con un protocolo unificado de

respuesta ante ciberataques, considerando el incremento de incidentes en los últimos años? Igualmente, para poder manifestar, ¿existe la voluntad política, existe el presupuesto necesario para avanzar hacia una arquitectura de ciberdefensa verdaderamente nacional, o seguimos fragmentados entre sectores que no comparten información?

Por otro lado, también hacer la pregunta para ministro de Defensa, el Comando de Conjunto de Cyberdefensa frente a las ciberamenazas provenientes de actores estatales extranjeros, considerando el actual contexto geopolítico, los recientes reportes de amenazas híbridas en América Latina, ¿cuál es el papel que están cumpliendo?

Igualmente, ¿cuáles son los principales cuellos de botella que enfrentan para consolidar una capacidad operativa sostenida en ciberdefensa, especialmente en términos de recursos humanos especializados en tecnología?

Igualmente, para poder manifestar, en este caso a la Policía Nacional, ¿qué tan efectiva ha sido la colaboración entre la División de Investigación de Delitos de Alta Tecnología y el Ministerio Público para judicializar casos complejos de cíberdelitos y qué reformas normativas se necesitan para agilizar estos procesos?

Y, por último, para la Policía Nacional, si bien es cierto, pues tenemos la era de la digitalización, entre esto la tecnología, sin embargo, parece que la Policía Nacional tiene una plataforma para hacer las denuncias en línea, ¿no? Pero, ¿en estos instantes podemos ingresar a ello? Vamos a encontrar que está en mantenimiento, no funciona. ¿Con qué frecuencia se presentan estos casos de que esté en mantenimiento o con problemas? Y si de repente podemos hacer una muestra en estos instantes si efectivamente funcionara, algunos de ellos entonces que he podido formular.

Entonces, a nuestros invitados igual vamos a darle el espacio de cinco minutos o algo más, lo necesario para poder absolver las interrogantes formuladas.

Empezamos por el ingeniero Orlando Vásquez Rubio, por favor, para que nos pueda absolver estas interrogantes.

El SUBSECRETARIO (E) DE LA SUBSECRETARÍA DE TECNOLOGÍAS Y SEGURIDAD DIGITAL DE LA PRESIDENCIA DEL CONSEJO DE MINISTROS, señor Orlando Vásquez Rubio.— Señor presidente, por su intermedio, quería contestar al congresista Ernesto Bustamante con respecto al tema de las incidencias.

Ese listado es de manejo confidencial, pero igual le voy a poner ejemplos de lo que pasa en este reporte. Hay muchos temas con respecto al robo de identidades tipo *ransomware*, algún tipo de

vulnerabilidades que también tenemos, problemas con spam también dentro de las entidades públicas, y también fugas de información.

Muchas entidades se comunican a través de la secretaría para realizar, por ejemplo, un análisis de vulnerabilidades. **(6)** Ellos manejan sistemas, manejan dominios, por lo cual se necesita escanear el sistema a fin de detectar algún tipo de hueco de seguridad, lo cual el Centro Nacional brinda un reporte técnico para que puedan mejorar con respecto a este aspecto.

Con respecto al tema de *ransomware*, muchas entidades son vulneradas y la información es encriptada. Entonces, se tiene que verificar el tema de la implementación del FGCI, el cual indica que uno tiene que tener los *backup* necesarios a fin de poder ser merced a un secuestro informático. Tanto en las entidades públicas como en las privadas, muchos son atacados por *ransomware*, en los cuales el hacker pide un dinero para que puedan desencriptar esta información. Sin embargo, bajo una implementación correcta de un FGCI, no debería tener mayor importancia. El gran tema es que la implementación del FGCI se necesita potenciar mucho en el Estado.

No sé si eso contesta a la pregunta o desea algún tipo de detalle.

Como le digo, con respecto al Centro Nacional de Seguridad Digital, también hay muchos ciudadanos que nos piden por acceso a la información, sin embargo, como son temas de activos digitales, no estamos permitidos a entregar la información.

Pero esa es la mayor parte de información que nos brindan las entidades, y nosotros, como el Centro Nacional de Seguridad Digital emitimos muchas cartas y oficios para indicar, si algunas entidades han sido vulneradas, cuál es la problemática que ha sucedido. ¿Para qué?, para que podamos tener este *lock* o esta auditoría y poder indicar a las demás entidades la problemática que han sufrido a fin de que no vuelva a suceder.

Y con respecto a lo que me indicaba, señor presidente, sí tenemos un gran problema de infraestructura. Tenemos actualmente un proyecto, este año se está trabajando con la gente del BID y lo que se quiere es potenciar.

Como ustedes saben, las herramientas informáticas, sobre todo el tema de ciberseguridad son herramientas costosas. Sin embargo, nosotros como ente rector vemos que es un tema muy crítico manejar un tema de gobierno digital, y el gobierno digital significa a veces digitalizar, pero cuando digitalizas ya no tienes que cuidar a través de personal de seguridad, sino que tienes que comprar temas de seguridad perimetral, acceso a la información.

También hay herramientas que pueden navegar sobre la red oscura, la *deep web*, para brindar información, porque también el equipo del Centro Nacional de Seguridad Digital lo hace con herramientas

Open source. Lo que estamos viendo por conveniente es repotenciar con equipos de mayor calidad.

Como ustedes saben, Inteligente Artificial ha implementado todo el tema de herramientas tecnológicas en los diferentes campos, como el tema de seguridad. Actualmente, también estamos trabajando el tema de computación cuántica a través de una reunión de un grupo de expertos, porque la computación cuántica va a afectar mucho el tema de seguridad digital. O sea, lo que ahorita mantenemos como seguro, en un tiempo vamos a tener que implementar herramientas de ese corte a fin de evitar esa problemática. Pero estamos trabajando también en nuestro decreto, nuestro reglamento de la 007, a fin de que podamos trabajar también con los entes privados.

Eso es lo que nos falta y hemos visto a través de los expertos coreanos que tenemos que en Corea hay una colaboración estrecha, tanto de la parte estatal como de la parte privada, y lo que hace es fortalecer ese tipo de ganancia de educación que tenemos con los problemas diversos que hay en el tema privado, a veces es por un tema de dinero, pero de alguna manera favorece ese tipo de circunstancias al tema de las actividades estatales.

El señor PRESIDENTE.— Muchas gracias al ingeniero Orlando Vázquez Rubio.

Antes de darle la palabra al general, damos la bienvenida al colega Esdras Medina, quien se encuentra ya aquí en la sala de sesiones.

El señor MEDINA MINAYA (RP).— Muchas gracias, señor presidente, muy buenos días; y también saludar a mi colega congresista presente, el congresista Bustamante, y también a todos los presentes, a los generales, al coronel, a los representantes de diferentes instituciones.

Muy amable, gracias.

El señor PRESIDENTE.— Gracias, colega.

Entonces, igualmente, para que pueda absolver las interrogantes, invitamos al general de brigada John Rivera Machuca.

El COMANDANTE DEL COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS, general de brigada E.P. John Rivera Machuca.— Gracias, señor presidente.

Respondiendo a la pregunta del señor congresista Bustamante, es cierto, es sabido por todos que, en el Ejército, o en las Fuerzas Armadas en general, la rotación es parte de los procedimientos de los recursos humanos; y hasta que apareciera la especialidad de ciberdefensa, esto era normal, porque un oficial de artillería que trabaja en Lima puede trasladarse a otra unidad de artillería en otro lugar del país y no tienen ningún problema. Sin embargo, ahora se está presentando esta problemática, en el sentido que

las instituciones están capacitando a su personal, pero por las normas legales actuales relacionadas a las leyes de ascenso, al cabo de 2 o 3 años estos oficiales tienen que ir a otras dependencias, con lo cual se pierde el *expertise*, se pierde la experiencia que han acumulado a lo largo de dos o tres años.

Pero aparte hay otra problemática, porque hay empresas que están viendo el talento humano y los están incentivando a abandonar, en el caso de oficiales asimilados, a abandonar ya el término de su contrato y pasarse al ámbito privado, ofreciéndoles por supuesto mayores incentivos económicos.

Al respecto, antes del fin de mes ya debe estar creándose la Unidad Funcional de Ciberespacio en el Ministerio de Defensa, esta unidad funcional tiene el rango de una dirección dentro de la Dirección General de Política Estratégica, con la finalidad de establecer lineamientos y normas en materia de ciberdefensa en los órganos ejecutores del ministerio.

Y una de las líneas de acción por la que vamos a tomar parte es justamente en ver cómo a través de la modificación de los anexos 3, 4 y 5 de las leyes de ascenso de las instituciones armadas podemos establecer mecanismos para que el recurso humano que ya había sido capacitado y que cuente con la experiencia permanezca por más tiempo en su especialidad de ciberdefensa. Al respecto, por ejemplo, la Marina ya ha tomado una decisión al respecto, está manteniendo una permanencia de ocho años como mínimo en la especialidad de ciberdefensa.

Con respecto a la pregunta del congresista Pariona, es cierto, tenemos muchas preocupaciones sobre los riesgos, tanto de actores estatales como de actores no estatales que constantemente están tratando de hacer daño a nuestra infraestructura, sobre todo a los activos críticos nacionales. Al respecto, se está invirtiendo mucho en la capacitación del personal, como habrán visto ustedes en mi presentación, se promueve la participación tanto en ciber ejercicios nacionales como internacionales y se promueve también que los mejores cuadros realicen cursos especializados en el extranjero.

Uno de los mayores obstáculos, es lo que acabo de referirme a la rotación del personal, esperamos podamos modificar esto para mejorar el tema de la permanencia de nuestro personal en esta especialidad tan importante de la ciberdefensa.

No sé si el coronel puede tener alguna participación.

El señor PRESIDENTE.— Adelante, coronel.

El JEFE DE ESTADO MAYOR DEL COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUEZAS ARMADAS, coronel EP Octavio Martín Freitas Farfán.— Muchas gracias, señor presidente; señor congresista Bustamante, para complementar lo que acaba de referir nuestro general Rivera, debemos tener en cuenta que el

Comando Conjunto tiene como misión principal la de planear, conducir y ejecutar las operaciones militares en y mediante el ciberespacio, se llama ciberdefensa.

Y los institutos armados tienen la finalidad de preparar a la fuerza. Entonces, en este contexto de qué personal trabaja en este ámbito, en este nuevo dominio, tenemos que dar cuenta de qué personal trabaja en ese ámbito, en este nuevo dominio, tenemos que dar cuenta que el Comando Conjunto se nutre de los institutos armados para hacer las operaciones militares. Y las instituciones armadas tienen que preparar a la fuerza, preparar capacidades, preparar al personal, no solamente para proteger su propio entorno virtual, sino también para que cuando hay una situación de crisis o el país lo requiera, sea parte de la participación de esta ejecución de las operaciones militares.

Entonces, es así como nuestra norma nos indica cómo estamos organizados para hacer frente a estas situaciones de crisis.

Respondiendo a la pregunta del señor presidente Alfredo Pariona, señor presidente, tenemos que darnos cuenta que el Perú está conectado a la internet hay que establecer el límite fronterizo de la internet y hay que protegerlo. Y este límite empieza con las tres conexiones que tiene el Perú a internet. Una en Máncora, una en Lurín, una en Ilo, y una muy probable que está creciendo y podrá entrar por la amazonia.

Entonces, ese es nuestro límite que hay que proteger, proteger una infraestructura de comunicación. Pero para proteger una infraestructura de comunicación, se tiene que tener una infraestructura de seguridad. Ya el señor Orlando Vásquez, mi señor general lo ha indicado, el señor **[…]** lo ha indicado, tenemos que implementar, desarrollar y mantener una infraestructura de seguridad digital mediante proyectos de inversión viables, cualquier sea el modo.

Porque todo esto que estamos hablando acá, solamente se va a proteger con una infraestructura sólida, con recursos, con personal necesario y con políticas que permitan colaborar en todo momento con cualquier operador que esté en riesgo su entorno digital. Y si hay alguna inestabilidad o hay alguna situación de crisis, poder ser la parte que neutralice esa amenaza de manera directa.

Eso es todo, muchas gracias.

El señor PRESIDENTE.— Gracias, estimado coronel.

Entonces, pasamos al mayor PNP Pierre Ruiz Contreras.

El JEFE DE LA DIVISIÓN DE INVESTIGACIÓN DE DELITOS DE ALTA TECNOLOGÍA DE LA DIRECCIÓN DE INVESTIGACIÓN CRIMINAL DE LA POLICÍA NACIONAL DEL PERÚ, mayor PNP Pierre Ruiz Contreras.— Claro que sí, señor presidente, para absolver las preguntas de

su persona y del congresista Bustamante, muy interesantes las preguntas.

Relacionado a las llamadas telefónicas que recibimos en spam los organismos encargados del Estado son Indecopi y Osiptel, nosotros la policía vemos el tema de investigación.

Pero para que más o menos los señores congresistas sepan cómo venimos llevando el tema de investigación en la policía, y lo presenté en una diapositiva, venimos interviniendo los locales donde venden este tipo de Sim Card activados a nombre de terceras personas, donde nuestros números, lo he podido exponer, y hemos tenido diversas cantidades de personas detenidas por esa esa conducta delictiva.

El tema es que esos *call center* cuando utilizan las llamadas de números fijos o llamadas de números híbridos que pueden conseguirlos a través del internet, ahí tenemos un problema para poder investigarlos. Pero cuando estas personas utilizan dentro de los *call center* números telefónicos celulares, que creo que a muchos de nosotros nos llaman mañana, tarde y noche, como dice el congresista Bustamante, esos Sim Card que utilizan estos *call center,* son Sim Card que están activados a nombre de terceras personas, que estas personas no saben de la existencia de esas líneas telefónicas.

Vale decir, son personas que pertenecen por temas de investigación, podemos sacarles la titularidad a esas personas que son personas que están en el anexo 5, de Pueblo 5, del Caserío, un ejemplo, de Cerro de Pasco, que no tienen ni siquiera luz ni agua, sin embargo, pueden adquirir o pueden haberles sacado diversas cantidades de líneas telefónicas a diversas personas. Es ahí donde nosotros ingresamos con la tipicidad jurídica para poder intervenir en estos *call center* por la posesión ilegal de los Sim Card.

Por eso la sugerencia dentro de la normatividad era que el artículo 222-B que, del Código Penal, pase a la normatividad de la legislación especializada en informática, que es la 30096, y poner una prognosis de pena con la finalidad de que nos puedan llevar, muy al margen de llegar al tema de flagrancia delictiva, poder tener medidas coercitivas o pedir unas medidas limitativas de derecho que nos puedan entregar.

Con el tema de las denuncias en línea, que nos presentó el doctor congresista Pariona, el tema de las denuncias en línea no lo manejamos tampoco en la Dirección de Ciberdelincuencia, lo maneja la Dirtic, que es la Dirección de Tecnología de la Información de la Policía, donde ellos suben el programa y suben el tema para poder denunciar a las diversas personas utilizando las tecnologías de información y comunicación.

Sé que está en mantenimiento, pero los mayores detalles señor congresista, eso lo tendría que ver la unidad especializada.

Gracias.

El señor PRESIDENTE.— Muchas gracias.

Vamos a invitar a la colega Santisteban, creo que está en línea; luego, al colega Bustamante, por favor.

La señora SANTISTEBAN SUCLUPE (FP).— Buenos días, presidente, colegas congresistas, saludar cordialmente a los invitados y a todos los presentes.

La digitalización de los servicios públicos requiere un enfoque transversal y estratégico, especialmente a amenazas crecientes como los ataques a infraestructuras críticas, instituciones como el Poder Judicial, la Sunat y el Minsa han sido víctimas de estos ataques, así como de filtraciones de datos sensibles que exponen la información de millones de peruanos. **(7)**

Sin embargo, también es fundamental enfocar esfuerzos en la prevención de los ciberdelitos que afectan directamente a los ciudadanos, como la suplantación de identidad, el fraude y la extorsión, frente a los cuales no siempre se observa una reacción inmediata por parte de las autoridades.

En ese contexto, cabe preguntarse si todos los sectores avanzan al mismo nivel de coordinación, si cuentan con las capacidades técnicas necesarias y si la inversión en protección digital es realmente suficiente.

Al respecto, en el marco de los esfuerzos por fortalecer la ciberseguridad y avanzar en la transformación digital del Estado, quisiera consultarle al representante de la Secretaría de Gobierno y Transformación Digital de la PCM qué acciones concretas de articulación intergubernamental se vienen implementando a nivel de los gobiernos regionales y locales.

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

Por otro lado, resulta clave promover la información de talento digital mediante becas, convenios y alianzas internacionales a nivel nacional.

La ciberseguridad debe abordarse con un enfoque preventivo y colaborativo. No podemos esperar a que se comprometa información crítica para recién actuar.

Muchas gracias, presidente.

El señor PRESIDENTE.— Gracias, colega Santisteban.

Colega Bustamante, por favor.

El señor BUSTAMANTE DONAYRE (FP).— Gracias, presidente.

Yo tengo una pregunta breve dirigida al mayor Roy Contreras. Respecto de las llamadas, llamadas spam. Claro, hay las llamadas spam que están legítimamente motivadas comercialmente. Yo quiero que tú te pases de Claro a Movistar o de Movistar a Intel, en fin, o que me compres una póliza de seguros o que te cambies de banco.

También otras llamadas legítimas son: oye, paga tu deuda. También, eso es legítimo.

A lo que me refiero es a aquellas llamadas que utilizan las plataformas de *call center* o que quizá mimetizan las plataformas de *call center* para hacer llamadas ya de tipo delincuencial.

No estoy quitando el aspecto molesto que significa el recibir una llamada de un operador de teléfonos, claro, es molesto, es un tema de Indecopi, yo lo comprendo, pero el que a uno lo llamen con una finalidad extorsiva o una finalidad de obtener información privada de la persona o de la familia o del entorno laboral, eso es delincuencial.

Y para esto, usan los mismos mecanismos tecnológicos que, por ejemplo, los que trabajan en *call center* de manera legítima.

Es decir, hacen simultáneamente llamadas a, por decir, ocho números. El primero que contesta con esa habla. Los otros siete, uno levanta el teléfono y no hay nadie. Y no es que no haya nadie. Simplemente, el robot solo puede hablar con una persona a la vez y toma la primera persona que contesta.

Pero nosotros, al haber contestado, avisaron que existen, entonces van a ser motivo de siguientes llamadas, pero esas llamadas, cuando uno los trata de devolver, el número no existe o no está registrado.

Me sorprendió cuando dijo el mayor Ruiz que esas son llamadas registradas en centros poblados que ni siquiera tienen teléfono o, perdón, electricidad. No conocía ese detalle, pero lo que yo veo es que son números otorgados por las compañías de teléfonos, pero números que no tienen capacidad de recibir llamadas y, por tanto, cuando uno los llama, contesta un robot diciendo "sabe que este número no existe" o "el número no está disponible".

Y viene también el hecho de que muchas de estas llamadas vienen del extranjero. Entonces, al venir del extranjero, mi pregunta también es si es que esto los hace no pasibles de sanción o de persecución, vamos a decir, por parte de la policía o del sistema judicial peruano.

Hay llamadas, muchas de ellas vienen de Colombia y son llamadas que tienen propósito delincuencial y la pregunta es cómo podemos hacer. Todo esto se hace a través del sistema telefónico peruano; inclusive hay algunos mensajes de texto, SMS, que llegan y ofrecen muchas cosas y son evidentemente delincuentes.

Hay gente que cae. Gente que dice: "Te voy a suspender tu cuenta de Netflix porque no he registrado tu pago". Y ponen un enlace. Uno hace clic en el enlace y se acabó. Porque simplemente van a meter un *malware* al teléfono o a la computadora.

Entonces, ¿cómo podemos evitar eso? Si los mensajes de texto vienen a través de un operador telefónico, ¿no es entonces el operador telefónico un facilitador o quizás hasta un cómplice de lo que está ocurriendo?

Eso es lo que quisiera, una reflexión en ese sentido de parte del mayor Roy Contreras, por favor.

Gracias, presidente.

El señor PRESIDENTE.— Gracias, colega Bustamante.

Bien, entonces vamos a darles de dos a tres minutos para que puedan responder realmente algunas preguntas últimamente formuladas o igualmente algún otro punto que agregar y también sus palabras finales a nuestros invitados.

Comenzamos con el ingeniero Orlando VáSquez Rubio. Adelante, ingeniero.

El SUBSECRETARIO (E) DE LA SUBSECRETARÍA DE TECNOLOGÍAS Y SEGURIDAD DIGITAL, señor Orlando Vásquez Rubio.— Sí, con respecto a la consulta, creo que es muy importante indicar que transformación digital es un tema cultural y transformación digital significa un cambio cultural dentro del trabajo.

A veces vemos en entidades que hablan de transformación digital y llaman al encargado de sistemas o al jefe de sistemas e indican que transformen la entidad digitalmente, pero eso no es transformación digital; siendo un tema cultural, es cambiar la percepción de los servicios digitales, evitar el papel.

Y dentro de evitar el papel, nosotros dentro de la secretaría hemos implementado más de 400 entidades a través de la plataforma interoperabilidad, que es la plataforma que colabora con más de 500 entidades a través de los servicios. ¿Y esto qué permite?

Yo soy un convencido de que la transformación digital dentro de las entidades se inicia a través de la gestión documental y en ese avance estamos trabajando con la gente de Corea y este año se está iniciando el desarrollo de un único sistema de trámite documentario para todo el Perú y nosotros queremos llegar hacia los gobiernos locales.

Sabemos que tenemos una problemática de indicadores digitales a nivel de los gobiernos locales, en los cuales hay poco cumplimiento, pero el ente rector no puede hacer todo, y como no puede hacer todo, dentro de cada entidad, por obligación de la ley, tiene un comité de gobierno y transformación digital. Este comité de gobierno y transformación digital genera un plan de gobierno digital. ¿Qué es el plan de gobierno digital? Es una

cartera de proyectos que deberían estar encaminados a digitalizar los servicios.

Y por eso dentro de este comité está la máxima autoridad como presidente del comité, el encargado de contrataciones, el encargado de presupuesto y el encargado de sistemas. Y una persona muy importante, un actor importante, el oficial de seguridad, que tiene que implementar también proyectos de seguridad digital.

Recuerden que el Estado son más de 2500 entidades y en cada entidad debe haber un oficial de seguridad y también el comité de gobierno de transformación digital.

La Secretaría, sin embargo, tenemos un nuevo proyecto trabajando con Elbit; hablamos mucho de temas de seguridad digital y la única forma de asegurar que la persona que está adquiriendo un servicio es a través de la validación con el ente rector, que es Reniec.

Estamos convencidos de que este año tenemos que implementar el tema de la casilla única, en la cual cada ciudadano, a través de su rostro, valide biométricamente el registro de cada servicio.

Dentro de lo que, y ampliando también la consulta es, estamos también trabajando el tema de gestión de talento. Estamos convencidos de que, si las personas no se capacitan, no validan sus conocimientos sobre el tema digital; tenemos muchos problemas.

Y tal como lo decía el congresista Bustamante, a veces llegan por correo electrónico, a veces llegan por teléfonos y a veces la poca capacidad o poca educación con el tema digital hace que se vean comprometidos a veces las cuentas bancarias o hacer caso a veces a ofertas impresionantes, que uno no debería creer, pero eso es parte de la sensibilización.

Desde el centro nacional nosotros tenemos reuniones quincenales con los oficiales de seguridad. También dentro de las entidades tenemos un equipo de respuestas. Este equipo de respuestas se activa cuando hay un problema informático y hace llamado hacia el Centro Nacional para brindar la cooperación adecuada y el adiestramiento adecuado.

Dentro también del Centro Nacional estamos en la campaña de masificar el tema de seguridad digital, no solamente a los servidores, sino también a los ciudadanos. Entendemos que la política nos indica que debemos mejorar al 2030 para ser parte de la OCDE y estamos encaminados a mejorar también las habilidades digitales del ciudadano.

Y como tercer punto, también estamos repotenciando todo el Centro Nacional a través de la compra de equipos y también construir un SOC que esté a la medida de la exigencia que tiene Sudamérica.

Entonces, sí estamos preocupados, pero recuerden que también el tema de transformación digital es un tema colaborativo. Una entidad no lo puede hacer todo.

Por eso justo están las entidades y los comités necesarios para cada actividad.

Gracias.

El señor PRESIDENTE.— Gracias, ingeniero.

Ahora pasamos al general EP Jhon Rivera Machuca. General.

El GENERAL DE BRIGADA EP, general Jhon Rivera Machuca.— No había hecho, no recibí ninguna consulta respecto al punto anterior, pero, sin embargo, me permito agradecer que nos hayan invitado para exponer los avances en materia de ciberdefensa.

Estamos construyendo, estamos en un nivel de maduración que nos va a permitir estar en breve en condiciones de dar una protección eficaz a los activos críticos nacionales cuando sean requeridos.

Gracias.

El señor PRESIDENTE.— Muchas gracias, estimado general.

Ahora pasamos al mayor PNP Pierre Ruiz Contreras, a responder y sus palabras finales.

El JEFE DIVISIÓN DE INVESTIGACIÓN DE ALTA TECNOLOGÍA - DIRECCIÓN DE INVESTIGACIÓN CRIMINAL DE LA POLICÍA NACIONAL DEL PERÚ (DEPIDCATC-DIRCIBERD) – MININTER, mayor PNP Pierre Ruiz Contreras.— Claro que sí, presidente.

¿Cómo están?, congresista Bustamante.

Para resolver la consulta, no es que las llamadas se realicen en lugares donde no hay acceso a luz o internet, sino que los titulares de los sin cara activados son personas que radican y viven ahí.

En el tema, cuando pedimos la titularidad a través de Osiptel, nos indican que son personas que viven en, sacando de Reniec, viven en tales lugares donde es imposible que esa persona haya venido acá a Lima a poder activar diversos números telefónicos de diversas operadoras que hay en el Perú.

Entonces es ahí donde estas personas compran esos *SIM cards* activados y a nombre de terceras personas que viven en lugares remotos con la finalidad de poder cometer ya los fraudes informáticos y estafas en sus diversas modalidades que hemos visto en *phishing, smishing* y ese tipo de actividad delictiva.

Con respecto a la trazabilidad del delito informático, usted lo ha dicho muy bien, señor congresista, pueden estar haciéndose en diversas partes del mundo, porque gracias a la tecnología podemos

llamar aquí a Estados Unidos, Estados Unidos a España, a diversos países, por nombrar algunos países.

Hemos llevado ya capturas a nivel internacional, donde el último caso que hemos tenido fue que un *call center* estaba en Perú haciendo llamadas de fraudes a ciudadanos de España, donde ellos interactuaban y les lograban despojar de su patrimonio a través de las cuentas receptoras. Estas cuentas receptoras también estaban en España, pero las llamadas telefónicas del *call center* estaban aquí en Perú.

Se hizo un trabajo articulado con Interpol y se logró detener a las personas del *call center* donde hubo acá ciudadanos de otros países que fueron detenidos y también los del *call center* que fueron peruanos.

Tuvimos 22 detenidos en ese operativo con la policía de España, que ellos fueron directamente agraviados y se investigó por los delitos correspondientes aquí en Perú y luego, con un pedido vía la plataforma de cooperatividad internacional, también fueron llevados a rendir cuentas a la ciudad o al país de España.

Lo que se debe entender, señores congresistas, es que en el delito informático podemos ser atacados o víctimas en diversas partes del mundo. Por eso hay la ciberdefensa, ciberinvestigación, hay también ciberresiliencia para ver cómo nos reponemos de esos ataques cuando se den.

Ahora ya no es necesario, como siempre les digo, ir a un banco, como eran años atrás, poner dinamitas, ingresar y poder apropiarse de un patrimonio. Ahora, simplemente con una laptop, una base de datos que se puede comprar a través de la *dark web* y un *bot*, pueden comenzar a sacar dinero a través de los medios. El banco son los medios por los cuales se puede sacar el dinero a través de las cuentas receptoras. Es el medio.

O se puede, no como antes que había ataques a las torres de luz, donde dejaban sin luz a cierta parte de las regiones; ahora simplemente puede haber los ciberataques a los centros hidroeléctricos que son con mantenimientos tecnológicos, donde pueden apagarlos, prenderlos remotamente.

Donde en la actualidad, señor congresista, es muy importante y hay que invertir mucho en lo que es la ciberseguridad, la ciberdefensa, porque podemos ser atacados de diversas partes del mundo y nuestra población requiere leyes fuertes, leyes drásticas, las cuales venimos articulando aquí en diversas entidades del Estado.

Gracias. **(8)**

EL señor PRESIDENTE.— Bien.

Les agradecemos infinitamente la presencia del ingeniero Orlando Vázquez Rubio, subsecretario de Tecnologías y Seguridad Digital de la Secretaría de Gobierno y Transformación Digital.

Igualmente, al general de brigada del ejército peruano Jhon Rivera Machuca, como también al coronel Octavio Martín Freitas Farfán. Asimismo, al mayor del Policía Nacional Pierre Ruiz Contreras, jefe de la División de Investigación de Alta Tecnología de la Dirección de Investigación Criminal de la Policía Nacional del Perú.

Les agradecemos infinito a ustedes y se les invita, pues, a poder abandonar la sala en el momento que sea conveniente.

Muchísimas gracias.

El JEFE DIVISIÓN DE INVESTIGACIÓN DE ALTA TECNOLOGÍA - DIRECCIÓN DE INVESTIGACIÓN CRIMINAL DE LA POLICÍA NACIONAL DEL PERÚ (DEPIDCATC-DIRCIBERD) – MININTER, mayor PNP Pierre Ruiz Contreras.— Muchas gracias.

EL señor PRESIDENTE.— Bien. Colegas, vamos a suspender brevemente la sesión para despedir a nuestros invitados.

Bien. Colegas congresistas, continuamos con la sesión.

Vamos a pasar al segundo punto del orden del día.

Colegas congresistas, de conformidad con lo establecido en el Orden del Día, tenemos el debate y votación del predictamen requerido en el Proyecto de Ley 9558/2024- Congreso de la República, que con texto sustitutorio propone la ley que declara interés nacional la creación, construcción e implementación del centro de innovación agropecuaria y tecnológica local de Chivay en el departamento de Arequipa.

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

La forma legal del presente predictamen tiene un artículo único, por lo cual se propone mejorar la productividad y la competitividad empresarial mediante la transferencia de tecnología y el aprovechamiento de tecnologías emergentes.

Se busca, además, aumentar el valor agregado de los recursos naturales y productos regionales del distrito de Chivay. Este esfuerzo será fundamental para el desarrollo sostenible de la región y el bienestar de su comunidad.

El distrito de Chivay es uno de los 20 distritos que conforman la provincia de Caylloma en la provincia de Arequipa y en su caracterización económica productiva destacan actividades económicas como la ganadería, alpacas, llamas, vicuñas, vacunos, ovinos, la minería, el comercio y la actividad turística.

Por las condiciones climáticas y geográficas, más del 90% de los productores se dedican a la crianza y comercialización de carne y fibra de alpaca. La ubicación geográfica del sitio Chivay lo convierte en un lugar estratégico para el desarrollo de tecnologías adecuadas y la mejora de la infraestructura.

Esta situación permitirá potenciar tanto la producción ganadera como la agrícola, lo que a su vez elevará la calidad de vida de la comunidad y contribuirá al desarrollo económico de la región.

La ley del Sinacti define a los parques científicos tecnológicos como espacios geográficos especiales con vínculos formales con una o más universidades, además de otras instituciones públicas y privadas que buscan promover la innovación basándose en el conocimiento científico y tecnológico en aras de contribuir a la mejora de la productividad y competitividad empresarial.

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

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

En tal sentido, la Comisión de Ciencia, Innovación y Tecnología recomienda su aprobación considerando el marco legal analizado en las opiniones recibidas.

Es pertinente promover la declaración de interés nacional de un centro de innovación agropecuaria y tecnológica local, bajo la administración de la Universidad Nacional San Agustín, fortaleciendo los mecanismos existentes y que promuevan un aumento en las investigaciones de innovación y mejora de las principales actividades tecnológicas del distrito de Chivay.

Bien, colegas, eso es el sustento al dictamen, entonces, invitamos a hacer su participación referente a lo expuesto.

Bien, vamos a conceder justamente al autor del proyecto, el colega Esdras Medina.

Colega Esdras. Adelante.

El señor MEDINA MINAYA (RP).— Muchas gracias, señor presidente de la Comisión de Ciencia, Innovación y Tecnología, congresista Alfredo Pariona Sinche.

Señor presidente, primeramente, quiero agradecer por haber dado la oportunidad de poder dictaminar este proyecto de ley recaído en el Proyecto 9558/202-4CR de mi autoría.

Señor presidente, es necesario manifestar a todos mis colegas congresistas que es necesario que podamos nosotros ayudar a las municipalidades provinciales y sobre todo a provincias que en la realidad necesitan ir mejorando su producción y también comenzar a llegar a tener la tecnología en sus distritos.

Es por eso que yo me permito pedirles a nuestros colegas congresistas que nos apoyen con su voto, ya que de alguna forma estaríamos nosotros ayudando a la implementación científico-tecnológica de un parque en el distrito de Chivay, provincia de Caylloma, donde ya también se ha manifestado la municipalidad provincial, señalando que la propuesta legislativa busca mejorar la productividad y la competitividad empresarial, así como aumentar el valor agregado de los recursos naturales y productos regionales del sector.

Con esta ley vamos a ocasionar que la universidad que está en la región de Arequipa, la Universidad Nacional de San Agustín, pueda acercarse a los productores que necesitan que se les ayude con investigación, con tecnología y que los estudiantes de la Universidad Nacional de San Agustín van a proporcionar progresivamente.

Asimismo, impulsamos a que la Municipalidad Provincial de Caylloma pueda comenzar, a través de esta ley aprobada, a tener un plan de sostenibilidad y que pueda tener objetivos claros y alcances para la articulación en actores del ecosistema de ciencia y tecnología.

Es necesario comenzar a trabajar en conjunto para buscar el desarrollo de nuestros pueblos.

Muchas gracias, señor presidente.

El señor PRESIDENTE.— Gracias, colega Esdras.

Algún colega.

Colega Bustamante, tiene la palabra.

El señor BUSTAMANTE DONAYRE (FP).— Gracias, presidente.

Es una pregunta concreta. He visto en el proyecto, no sé si ya se corrigió, pero hay un informe contrario respecto del gobierno regional de Arequipa.

La pregunta es: ¿Por qué se opone el gobierno de Arequipa a este proyecto? Sí se pudiera, quizá dar lectura a la observación planteada por el gobierno regional de Arequipa.

Gracias.

El señor PRESIDENTE.— El equipo técnico, por favor.

El SECRETARIO TÉCNICO.— En relación a la pregunta del señor congresista Bustamante, es en relación a la ley, congresista. Y hay una ley que crea un parque tecnológico. Es básicamente en ese sentido.

Pero por lo mismo es que se está sugiriendo en este dictamen que sea un centro tecnológico para efecto de que sea sumado al trabajo que viene desarrollando esta ley con los gobiernos locales para efecto de que sea productivo y se dé un mayor impulso a esa ley que ya existe a fin de que pueda recoger y estar.

Ellos ya están presentes en la zona; lo que queremos es darle esa fuerza con esta ley a efecto de poder desarrollar las actividades con mayor fortaleza.

El señor BUSTAMANTE DONAYRE (FP).— Comprendido, gracias.

El señor PRESIDENTE.— Bien.

Entonces, colegas, luego de las intervenciones vamos a invitar al señor secretario técnico a fin de que recoja la votación que corresponda.

El SECRETARIO TÉCNICO pasa lista para la votación nominal:

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 (BDP).— Zeballos, a favor.

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

Congresista Acuña Peralta.

Congresista Acuña Peralta, a favor.

Congresista Alva Rojas.

Congresista Alva Rojas, a favor.

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 (); congresista Flores Ruiz.

Congresista Flores Ruiz, a favor.

Congresista Ciccia Vásquez, a favor.

Congresista Jiménez Heredia.

Congresista Jiménez Heredia, a favor.

Congresista Monteza Facho (); congresista Monteza Facho, su voto.

La señora MONTEZA FACHO (AP).— Monteza, a favor.

El SECRETARIO TÉCNICO.— Congresista Monteza Facho, a favor.

Congresista Santisteban Suclupe.

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

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

Señor presidente, han votado 10 señores congresistas.

El dictamen ha sido aprobado por unanimidad.

El señor CERRÓN ROJAS (PL).— Cerrón Rojas, a favor. Disculpen.

El SECRETARIO TÉCNICO.— Congresista Cerrón Rojas, a favor.

El señor PRESIDENTE.— Gracias, señor secretario técnico.

Colegas congresistas, se ha aprobado por unanimidad el predictamen recaído en el Proyecto de Ley 9558/2024, que con texto sustitutorio propone la ley que declara de interés nacional la creación, construcción e implementación del Centro de Innovación Agropecuaria y Tecnológica local de Chivay en el departamento de Arequipa.

Muchas gracias, colegas congresistas.

Bien. Colegas, pasamos al tercer punto del Orden del Día.

En este estaba considerada la sustentación del Proyecto de Ley 10281/2024 que propone la ley que establece la protección y defensa del consumidor digital a cargo de la colega congresista Acuña Peralta María. Pero, sin embargo, nos ha alcanzado un oficio mencionando, pues, que se posponga esta sustentación.

Entonces, colegas congresistas, terminado la agenda del Orden del Día y no habiendo más puntos que tratar de la presente sesión, solicito la dispensa de la aprobación del acta para tramitar los acuerdos adoptados en la presente sesión.

Los señores congresistas que se oponen a la dispensa solicitada, sírvanse expresarlo.

Si no hay ninguno, se da por aprobada la dispensa.

Siendo 11 de la mañana con tres minutos, se levanta la sesión.

—A las 11:03 h, se levanta la sesión.