

COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL

ACTA DE LA SESIÓN No. 021-2019-2021

Lugar:	D.M. Quito
Fecha:	Miércoles, 02 de octubre de 2019.
Hora de inicio:	10h16
Hora de finalización:	13h39

a) Inicio de la Sesión.-

En la ciudad de Quito, Distrito Metropolitano, a los dos días del mes de octubre del año dos mil diecinueve, siendo las 10h18, se instala en sesión la Comisión Especializada Permanente de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral de la Asamblea Nacional, de conformidad con las normas previstas en la Ley Orgánica de la Función Legislativa y el Reglamento de las Comisiones Permanentes y Ocasionales, en la sala de sesiones de la Comisión, ubicada en el séptimo piso del Palacio Legislativo.

El Asambleísta René Yandún, Vicepresidente de la Comisión Especializada Permanente de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral de la Asamblea Nacional, dirige la sesión No. 021-2019-2021 como Presidente de esta Comisión, y actúa como Secretaria Relatora, la Abogada Denise Zurita Chávez.

Por disposición del Presidente encargado de la Comisión, la Secretaria Relatora, abogada Denise Zurita Chávez, constata el quórum reglamentario.

No.	ASAMBLEÍSTA	PRESENTE	AUSENTE
1	Cecilia Salas (Alternata)	X	-
2	René Yandún	X	-
3	Oswaldo Coronel (Alternata)	X	-
4	Carlos Sucushagñay (Alternata)	-	X
5	Augusto Espinosa	X	-
6	Fafo Gaviláñez	X	-
7	Yofre Poma	X	-
8	Fabrizio Villamar	-	X
9	Pedro Curichumbi	X	-
10	Esther Cuesta	X	-
11	Lexi Loor	-	X
12	Dennis Marín	X	-



**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

La Secretaria Relatora certifica la presencia de nueve (9) Asambleístas de los doce (12) miembros que conforman la Comisión, e informa que el señor Asambleísta Fernando Flores, con oficio No. 619-2019-FFV-AN de 01 de octubre de 2019, se excusa de no asistir a la sesión y principaliza a su Asambleísta Alterna, Cecilia Salas; de igual manera informa, que la Asambleísta María Encarnación Duchi, con oficio No. ED-146-2019 de 24 de septiembre de 2019 (Tr. 380514), mediante el cual principaliza a su Asambleísta alterno, Carlos Sucushagñay, y el Asambleísta César Carrión, con oficio No. 157-CC-AN-2019 de 16 de septiembre de 2019 (Tr. 379245), mediante el cual principaliza a su Asambleísta alterno, Oswaldo Coronel; es así que existiendo el quórum se puede dar inicio a la sesión No. 021-2019-2021.

Una vez constatado el quórum reglamentario, el Asambleísta René Yandún, Presidente encargado de la Comisión, manifiesta que de conformidad con lo establecido en el artículo 27 de la Ley Orgánica de la Función Legislativa, da inicio a la sesión No. 021-2019-2021 y por disposición del Presidente encargado de la Comisión, la Secretaria Relatora procede a dar lectura de la convocatoria y el Orden del Día en los siguientes términos:

b) Lectura de la Convocatoria y del Orden del Día.-

Por disposición del Asambleísta Fernando Flores Vásquez, Presidente de la Comisión Especializada Permanente de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral, y de conformidad con lo establecido en el artículo 27, numeral 1 y en el artículo 28, numeral 3 de la Ley Orgánica de la Función Legislativa, en concordancia con el artículo 8, numeral 2 y artículo 10, numeral 4 del Reglamento de las Comisiones Especializadas Permanentes y Ocasionales, se convoca a ustedes a la sesión No. 021-2019-2021, a realizarse el día miércoles 2 de octubre de 2019, a las 10H00, en la sala de sesiones de la Comisión, 7mo. piso, ala oriental, de la sede de la Asamblea Nacional, ubicada en la calle Piedrahita y avenida Gran Colombia, con el objeto de tratar el siguiente Orden del Día:

1.- Dar cumplimiento a la "Resolución que dispone a la Comisión Especializada Permanente de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral de la Asamblea Nacional, inicie una investigación a fin de determinar responsabilidades frente al caso de la posible filtración de datos de ciudadanos ecuatorianos", aprobada por el Pleno de la Asamblea Nacional el 17 de septiembre de 2019, remitida a la Comisión, por el doctor John De Mora Moncayo, Prosecretario General Temporal, con el memorando No. SAN-2019-1380 de 20 de septiembre de 2019 (Tr. 379724), para lo cual se recibirán las siguientes comparecencias:

1.1.- Doctora María Paula Romo, Ministra de Gobierno.

1.2.- Licenciado Andrés Michelena, Ministro de Telecomunicaciones y de la Sociedad de la Información.



COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL

1.3.- Abogada Lorena Naranjo Godoy, Directora Nacional de Registro de Datos Públicos. **1.4.-** Licenciada Martha Moncayo Guerrero, MBA., Gerente General de la Corporación Nacional de Telecomunicaciones.

c) Aprobación y tratamiento del Orden del Día.-

La Secretaria Relatora informa que no han ingresado solicitudes de cambio de Orden del Día.

El Vicepresidente en ejercicio de la Presidencia de la Comisión pone a consideración de los demás Asambleístas el Orden del Día, aprobándose de manera unánime, por lo que solicita a la Secretaria Relatora dar lectura al primer punto del Orden del Día, dándose lectura al mismo a continuación:

1.- Dar cumplimiento a la "Resolución que dispone a la Comisión Especializada Permanente de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral de la Asamblea Nacional, inicie una investigación a fin de determinar responsabilidades frente al caso de la posible filtración de datos de ciudadanos ecuatorianos", aprobada por el Pleno de la Asamblea Nacional el 17 de septiembre de 2019, remitida a la Comisión, por el doctor John De Mora Moncayo, Prosecretario General Temporal, con el memorando No. SAN-2019-1380 de 20 de septiembre de 2019 (Tr. 379724), para lo cual se recibirán las siguientes comparecencias:

1.1.- Doctora María Paula Romo, Ministra de Gobierno.

El Presidente encargado de la Comisión pone a consideración de los señores Asambleístas, que las autoridades intervengan por un lapso de quince minutos, para luego abrir el debate, consideración que se aprueba de manera unánime, por lo que dispone a la Secretaria Relatora que se reciba a la doctora María Paula Romo, Ministra de Gobierno como primera autoridad, y le concede la palabra.

Doctora María Paula Romo, Ministra de Gobierno: Inicia citando el marco legal de la materia a tratar y considerando que esto es necesario para lograr el objetivo encomendado por el Pleno de la Asamblea Nacional; prosigue refiriéndose al Art. 140 de la Ley Orgánica de Telecomunicaciones, el cual le otorga la competencia y rectoría en materia de seguridad de la información, tecnología e informática al Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL), dándole la facultad de establecer políticas, directrices y planes aplicables en estas áreas, más no al Ministerio de Gobierno que regula la seguridad ciudadana y pública, al igual que lo establecido en el artículo 141 del mismo cuerpo legal que regula el uso de las tecnologías y el uso de la información dentro de los órganos de la administración pública. Indica las disposiciones del Código Orgánico Integral Penal en los artículos 178 y 229, que penaliza el uso y divulgación de datos personales obtenidos sin autorización o a través de bases de datos, permitiendo al Estado proceder contra las personas cuando determine quién

**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

divulgó o manipuló las bases de datos. Además, se refiere a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), y el Centro de Respuestas a Incidentes Informáticos del Ecuador (ECUCERT), como instituciones adscritas al MINTEL que cumplen funciones específicas en estas áreas.

Señala que en la discusión del tema en el Pleno de la Asamblea Nacional hubo confusión en los términos seguridad de la información y seguridad ciudadana, el procedimiento a seguir y en donde entra el Ministerio de Gobierno a ejercer sus competencias, recalando que la seguridad cibernética forma parte de los nuevos retos que el Estado debe asumir porque existe una serie de delitos que se pueden cometer a través de la tecnología de la información por lo cual muestra los datos de los mismos, refiriéndose a los casos de amenazas *phising*, robo de identidad entre otros y finaliza señalando el término *dark web*, sitio donde se perpetraron los delitos más graves, como drogas, pornografía, armas y espionaje; aclarando que aunque es de conocimiento de la Policía Nacional la existencia de estos delitos, se requiere entrenamiento y herramientas idóneas para combatirlos porque éstos se dan en un espacio que no está bajo el control de la Policía Nacional.

Menciona que la digitalización de la sociedad y el manejo de recursos en el ciberespacio hacen más susceptibles a la población a este tipo de delitos, y hace referencia que a pesar de que la legislación penal contiene disposiciones al respecto debe ser adecuada con el fin de poder combatirlos eficazmente.

Muestra cifras de denuncias por delitos relacionados con el internet de los años 2018 y 2019, donde se observa mayormente la estafa a través de medios informáticos, y hace consideraciones a este tipo de delitos que son a distancia, es decir, pueden ser cometidos fuera de territorio ecuatoriano de forma masiva y que pueden tener o no víctimas, como es el caso de *phising*, donde se envían correos de manera masiva esperando ver quienes caen en la estafa para el robo de datos o identidad sumado el hecho de que en muchos casos estas víctimas son anónimas, por cuanto no se registran o no son denunciados, en la investigación de estos delitos puede encontrar a una persona culpable fuera del Ecuador.

Afirma que es importante que esta Comisión indique al Pleno de la Asamblea Nacional la necesidad de la aprobación de la Ley de Seguridad Digital que se encuentra ingresada en esta Asamblea porque tipifica los delitos cibernéticos, lo que permite establecer los tipos penales y la ampliación de las herramientas para proceder en presencia de los delitos informáticos, afirmando que existe un proyecto conjunto con la Organización de Estados Americanos (OEA), para capacitar a los órganos de seguridad en esta materia de ciberdelitos y ciberseguridad.

Indica que la Asamblea Nacional debe ratificar la adhesión del Ecuador al Convenio de Budapest, entendiendo que éste es una herramienta que permite investigar, tipificar y perseguir ciber delitos, facilitando el desarrollo en este tipo de defensa por el carácter extraterritorial que esos delitos pueden poseer considerando que el Ecuador ya lo suscribió pero que aún no lo ratifica, recalca la necesidad de hacerlo para mejorar la defensa y seguridad en este espacio, finaliza preguntando al Presidente encargado ¿Cuál será la mecánica para absolver las preguntas planteadas por los señores Asambleístas?



COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL

El Vicepresidente en ejercicio de la Presidencia de la Comisión indica que serán absueltas las preguntas que ya han sido formuladas por escrito para luego abrir el debate, y concede la palabra al Asambleísta Dennis Marín.

Asambleísta Dennis Marín: Aclara que trajo sus propias preguntas y desea realizarlas una vez que se agoten las preguntas realizadas previamente por escrito.

El Presidente encargado de la Comisión señala que efectivamente se dará contestación a las preguntas realizadas previamente para abrir el debate, y concede la palabra a la Ministra de Gobierno, doctora María Paula Romo.

Ministra de Gobierno, Doctora María Paula Romo: Responde la primera pregunta referida al conocimiento del evento de filtración de datos, señalando que se enteró del mismo el día 16 de septiembre del presente año a través de los medios CNN y BBC; al conocer de las mismas contactó al Ministerio de Telecomunicaciones, quien le manifestó que ya conocían de dicho evento y que se había bloqueado el acceso a esa base de datos, iniciando investigaciones al respecto, por lo que sugirió que se compartiera la información pública con la finalidad de que la Fiscalía pudiese iniciar las investigaciones por tratarse de un presunto tipo penal que debía hacerse un parte policial, que en efecto generó dos allanamientos donde se detuvo a dos personas que rindieron declaraciones ante las autoridades acotando en ese punto la actuación del Ministerio de Gobierno, afirmando que no es la Policía Nacional quien debe continuar con esta investigación.

En cuanto a la segunda pregunta referida a quién o a nombre de quién se presentó la denuncia, informa que no se colocó denuncia alguna, sino que se elaboró un parte policial por esto la Fiscalía de oficio iniciará la investigación correspondiente asegurando que las siguientes autoridades comparecientes en esta sesión indicarán qué acciones tomaron al respecto, pero que al Ministerio de Gobierno no le correspondía hacer ninguna denuncia afirmando que conoce que ECUCERT presentó en fecha 24 de septiembre una denuncia, pero le corresponde al representante de esta entidad hacer la respectiva aclaratoria.

Respondiendo a la tercera pregunta sobre qué ha hecho la Policía Nacional; reitera que se levantó el debido parte policial y se colaboró con la Fiscalía en el ámbito de sus competencias.

En relación a la pregunta de qué ha hecho el Ministerio de Gobierno en esos años sobre el delito de comercialización de datos, señala que la comercialización o cesión de datos no se encuentran tipificados en el Código Orgánico Integral Penal, por lo que mal sería hablar de ellos como delitos y no se puede accionar frente a ellos, pero indica que se trasladó a la Cancillería la necesidad de adherirse al Convenio de Budapest, conociendo cuáles son los requisitos para adherirse al mismo, que son: legislación que penalice los ciberdelitos, legislación procesal que permita a los cuerpos de seguridad y funcionarios judiciales, los mecanismos para obtener evidencias electrónicas, y seguir el procedimiento para la adhesión al mencionado convenio.

**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

Acerca de las preguntas de cuáles han sido las investigaciones y sanciones a las personas involucradas, así como las indemnizaciones a los ciudadanos afectados, indica que este caso se encuentra actualmente en fase de investigación por parte de la Fiscalía General del Estado por tanto está bajo reserva judicial por lo que no cuenta con la información para responder estas preguntas, afirmando que con esto absuelve todas las interrogantes que fueran enviadas previamente por escrito.

El Presidente encargado de la Comisión concede la palabra al Asambleísta Dennis Marín, para que realice las preguntas a la Ministra de Gobierno, doctora María Paula Romo.

Asambleísta Dennis Marín: Considera interesante el análisis del ámbito jurídico que establece las competencias en materia de ciberseguridad, sin embargo, indica que el Art. 1 del Acuerdo de la Secretaría de la Administración Pública N° 166, dispone a todas las entidades adscritas al Ejecutivo, la obligatoriedad de uso de normas técnicas ecuatorianas (NTE) ISO/IEC 27000 para la Gestión de Seguridad de la Información en las entidades gubernamentales, y señala que el Acuerdo está vigente, por lo que pregunta ¿Qué ha hecho el Gobierno actual para el cumplimiento específico de estas normas técnicas de seguridad en cada una de las instituciones del Estado? Reflexiona que si las mismas acogen estas normas, se hubiese podido evitar esta fuga masiva de información, por lo que al parecer cada entidad sigue llevando sus propias políticas sin tomar en consideración estas medidas manteniendo así los problemas de seguridad de la información.

Manifiesta estar de acuerdo con la señora Ministra de Gobierno en que Ecuador se debe adherir al Convenio de Budapest y señala que personalmente está impulsando que desde la Asamblea Nacional se inste al Presidente de la República para que ratifique este instrumento porque es necesario contar con las herramientas para este tipo de delitos, en virtud de que mucho de estos delitos se cometen fuera de las fronteras del Ecuador.

Pregunta a la señora Ministra de Gobierno ¿La Cartera de Estado cumple con las normas técnicas del aludido acuerdo N° 166? ¿Se ha creado el Comité Técnico de Seguridad dispuesto en el mismo? y ¿El personal de la misma está capacitado para enfrentar estos riesgos de ciberseguridad en el país?

El Presidente encargado de la Comisión concede la palabra a la Ministra de Gobierno, doctora María Paula Romo.

Ministra de Gobierno, Doctora María Paula Romo: Menciona que respecto a la adhesión al Convenio de Budapest no hace falta tal exhorto, por cuanto ya la decisión del Ejecutivo está tomada y sólo resta adecuar el marco legal a los requisitos exigidos por el Consejo Europeo, porque el Estado ecuatoriano tiene la intención de adherirse, reiterando la responsabilidad de la Asamblea Nacional de legislar los tipos penales necesarios y las normas procesales de obtención de pruebas en este campo para poder continuar con el trámite de ratificación a



**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

través de la Cancillería, reiterando la comunicación del Estado ecuatoriano al Consejo Europeo en abril de 2019.

Al referirse al Acuerdo N° 166, informa que también se está trabajando en el Plan Nacional del Ecuador Electrónico del año 2018 y se están adelantando gestiones al respecto para que el Gobierno pueda cumplir con lo dispuesto en este plan antes del año 2021, señalando que consta la implementación de un esquema gubernamental de seguridad de la información y manifiesta que responderá por escrito el nivel de cumplimiento de las normas técnicas de este plan, por cuanto no dispone de la cifra en ese momento.

El Presidente encargado de la Comisión concede la palabra al Asambleísta Augusto Espinosa.

Asambleísta Augusto Espinosa: Señala que tiene preguntas puntuales referidas al hecho de que la señora Ministra de Gobierno tenía conocimiento sobre la filtración de datos y la posterior notificación al señor Ministro de Telecomunicaciones: ¿Se presentó denuncia antes del 24 de septiembre? ¿Existe algún protocolo que se activó con este evento? también pregunta, ya entendiendo que la rectoría en esta materia la posee el Ministerio de Telecomunicaciones y Sociedad de la Información, ¿Estos delitos pueden ser detectados en flagrancia? ¿Hay en Ecuador algún precedente al respecto y que sucedió en este caso?

El Presidente encargado de la Comisión concede la palabra a la Ministra de Gobierno, doctora María Paula Romo.

Ministra de Gobierno, Doctora María Paula Romo: Recalca en primer lugar que desconoce los procedimientos internos de ECUCERT, la ARCOTEL o MINTEL, reiterando que sólo habló con el señor Ministro y se limitó a pedir la información para el parte policial, no obstante indica que a su entender, el Ministro Andrés Michelena estará presente posteriormente en la sesión y podrá resolver estas inquietudes. Referente a la segunda pregunta de la detención en flagrancia, señala que eso significaba tener policías vigilando constantemente el ciberespacio y no se tiene una unidad especializada para ello; lo que existen son denuncias de personas que han sido víctimas de delitos a través de medios electrónicos, en cuyos casos se activan los protocolos normales de la Policía Nacional.

Agrega que en otros países existen la vigilancia de *Deep web* y *Dark web* para detectar pornografía, y Ecuador ha avanzado en este tema a través de un convenio con los Estados Unidos de Norteamérica para que se alerte sobre pornografía infantil, para que al ser detectado un usuario o dirección IP dentro del territorio ecuatoriano se nos alerte inmediatamente con el fin de activar los protocolos respectivos y poder dar con los responsables, por esto se compromete a enviar la información sobre un procedimiento de pornografía infantil que fue detectado gracias a este convenio donde la Policía actuó y los responsables fueron detenidos.

COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL

El Presidente encargado de la Comisión concede la palabra al Asambleísta invitado, Homero Castanier.

Asambleísta invitado, Homero Castanier: Destaca que su propuesta ante el Pleno de la Asamblea Nacional hace quince días obedeció a la preocupación por un tema delicado para la seguridad y tranquilidad de todos los ecuatorianos que tenía que ser investigado; prosigue refiriéndose a la Ley de Protección de Datos Personales presentada a la Asamblea Nacional por el Gobierno Nacional, donde se debería incluir los datos biométricos y el aprovechamiento de la tecnología, para tener una base de datos de huellas digitales y rostros, incluso como apoyo al combate contra la delincuencia y la inseguridad, si es competencia del Ministerio de Gobierno; manifiesta tener preguntas puntuales: ¿Conoce si actualmente en el Gobierno y en las instituciones del Estado que manejan información privilegiada, tienen custodios o responsables de esta información? De los 18 Gigabytes de información de aproximadamente veinte millones de ecuatorianos, ¿Qué fue lo que se filtró? ¿Sabe qué tipo de información, de qué entidades, cuáles fueron los datos que se filtraron, datos de cuentas, claves, para conocer a qué se atienden los ecuatorianos?

El Presidente encargado de la Comisión, concede la palabra a la Ministra de Gobierno, doctora María Paula Romo.

Ministra de Gobierno, Doctora María Paula Romo: Aclara que en efecto hubo una reacción de la Asamblea Nacional ante el peligro en la seguridad y privacidad de los datos, porque es una preocupación general; referente al almacenamiento de datos biométricos de la población por parte del Estado, es un tema que se debate a nivel mundial y existen personas que se oponen rotundamente a que los Estados almacene esa información por lo que considera que en la Asamblea Nacional del Ecuador, sea donde se discuta esta posibilidad, afirmando que es preocupante la desinformación existente sobre quiénes son responsables en estos casos y qué se puede hacer; destaca que el Ministro de Defensa Nacional es quien preside el Gabinete de Seguridad Estratégica y podrá en consecuencia dar mayores detalles sobre la conformación de un Comité de ciberseguridad en donde se encuentran: Cancillería, Ministerio de Telecomunicaciones y Sociedad de la Información, Ministerio de Defensa Nacional, entre otros por la dimensión que la ciberseguridad puede abarcar.

Respecto a la primera interrogante indica que desconoce si existen custodios de la información, pero a su criterio el inconveniente se presenta en los casos en los que la información no depende de un único funcionario, ejemplificando con el tema de migración de ecuatorianos en el exterior señalando que esta es una información que está al alcance de cualquier funcionario de migración que se encuentre en un punto migratorio del territorio ecuatoriano, y el único mecanismo que se posee para controlar esto es identificar al funcionario que accedió al sistema para usar esos datos o entró a buscar los mismos de la base disponible; respecto a la segunda pregunta sobre la información filtrada, reitera que se



**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

desconoce y que se debe esperar a que avance la investigación de la Fiscalía General del Estado para poder contar con esos datos.

El Presidente encargado de la Comisión concede la palabra al Asambleísta Oswaldo Coronel.

Asambleísta Oswaldo Coronel: Reiteró que es preocupante que la ciudadanía ecuatoriana se enteró de estos hechos por la prensa internacional cuando se trata de información de ciudadanos ecuatorianos; se desea saber si se han realizado ejercicios prácticos para evitar que este tipo de actos se presenten en organismos públicos, con información más delicada y sensible o hasta secreta que pueda poner en riesgo la seguridad de toda la nación y ¿Cuáles son las garantías de que el Gobierno y la ciudadanía puedan estar tranquilos de que esto no haya sucedido?


El Presidente encargado de la Comisión concede la palabra a la Ministra de Gobierno, doctora María Paula Romo.

Ministra de Gobierno, Doctora María Paula Romo: Insiste que la rectoría en seguridad de la información corresponde al Ministerio de Telecomunicaciones y Sociedad de la Información quien es el organismo que debe absolver esa duda.

El Presidente encargado de la Comisión concede la palabra al Asambleísta Dennis Marín.

Asambleísta Dennis Marín: Recuerda a la señora Ministra de Gobierno la necesidad de que la Comisión conozca el cumplimiento del esquema de seguridad gubernamental que tiene esa cartera de Estado, así como la fiscalización de cada una de las instituciones que deben cumplir con esta norma, señalando que es importante validar ¿Qué normas de seguridad aplicadas en el Ministerio de Gobierno se apegan al esquema de seguridad gubernamental informática?, ¿Qué seguimiento se hace a ese cumplimiento?, así como ¿Quién es la persona encargada del mismo?, para poder verificar el efectivo cumplimiento, y si ¿Los equipos informáticos de las instituciones del Estado permiten hacer algún tipo de auditoría?, para afianzar la seguridad digital dentro del Estado.

El Presidente encargado de la Comisión concede la palabra a la Ministra de Gobierno, doctora María Paula Romo.

Ministra de Gobierno, Doctora María Paula Romo: Afirma que hará llegar la información sobre el esquema de seguridad gubernamental informático en lo que corresponde al Ministerio de Gobierno, sin embargo recalca que MINTEL y ARCOTEL pueden ofrecer mejores datos respecto a todo el panorama nacional, y señala que la seguridad en materia digital del Estado es muy grande por lo que considera que el trabajo debe ser articulado, ratificando el compromiso de remitir a la Comisión la información sobre la cartera de Estado que dirige. 

**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

Asambleísta Dennis Marín: Aclara que la responsabilidad de cumplimiento de estas normas de seguridad la tienen exclusivamente aquellas adscritas a la función Ejecutiva conforme a lo dispuesto en el Acuerdo N° 166 y por ello es necesario conocer el seguimiento que hacen las instituciones adscritas al Ejecutivo, más allá de la responsabilidad del resto de instituciones del Estado.

El Presidente encargado de la Comisión concede la palabra al Asambleísta Fafo Gavilánez.

Asambleísta Fafo Gavilánez: Manifiesta que el trabajo de protección y ciberseguridad es un trabajo que debe realizarse en equipo, y señala que la Ministra de Gobierno debe entregar la hoja de ruta o el cronograma del Comité de Ciberseguridad así como la Asamblea Nacional debe ejecutar el proyecto de ley del Asambleísta Juan Carlos Yar sobre seguridad digital, sin embargo la conmoción que generó en la población la filtración de datos es razón suficiente para estudiar esta hoja de ruta y trabajar en conjunto en el mismo propósito y fortalecer desde esta Comisión la propuesta de seguridad digital como un tema de Estado, y no descarta invitar a otros países que ya cuentan con este tipo de legislación para orientar el camino que se debe seguir en este tema, por lo que pregunta sobre el Comité de Seguridad Digital ¿Cuándo y cómo se reúnen? ¿Cuál es la ruta? ¿Pueden ser convocados a esta Comisión?

El Presidente encargado de la Comisión, concede la palabra a la Ministra de Gobierno, doctora María Paula Romo.

Ministra de Gobierno, Doctora María Paula Romo: Se compromete a trasladar esa inquietud a quien dirige el Gabinete de Seguridad Estratégica, el señor Ministro de Defensa Nacional, General Oswaldo Jarrín, para que él pueda hacer llegar a la Comisión los avances de ese Gabinete y recalca la importancia de tener claras las competencias y responsabilidades de cada cartera de Estado para que el aporte en este tema por parte de la Comisión sea el más óptimo, por cuanto uno de los inconvenientes presentados cuando este tema salió a la luz era el desconocimiento de los responsables y los órganos competentes en cada materia.

El Presidente Encargado de la Comisión agradece la participación de la señora Ministra de Gobierno, doctora María Paula Romo, y recuerda los compromisos adquiridos durante su intervención, e indica que la siguiente autoridad a recibir, es el señor Ministro de Telecomunicaciones y Sociedad de la Información, pero debido a que se encuentra atrasado para asistir a la Comisión, pone en consideración de los miembros de la Comisión que se reciba entretanto a la abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos (DINARDAP).

Asambleísta Dennis Marín: Recalca que la convocatoria se hizo con la debida anticipación y que la sesión obedece a una delegación realizada por el Pleno de la Asamblea Nacional a la



**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

Comisión para tratar este tema tan delicado con datos públicos, por lo que considera importante dejar sentado que no se encuentra presente la persona que es la cabeza de la cartera de Estado y que por ley es responsable de estos temas; solicita avanzar con la siguiente exposición y actuar con mayor firmeza ante este tipo de actitudes, porque a su criterio es una falta de respeto con los Asambleístas de la Comisión no estar presente conforme fue convocado, lo que denota irresponsabilidad de parte de los funcionarios.

El Presidente Encargado de la Comisión concuerda con el Asambleísta Dennis Marín y recalca que las cuatro autoridades convocadas confirmaron la participación, por lo que solicita a la Secretaria Relatora informe si existe alguna excusa posterior del señor Ministro de Telecomunicaciones y de la Sociedad de la Información, a lo que la Secretaria Relatora informa que en efecto le fue entregado un documento de excusa hace un momento.

El Presidente Encargado de la Comisión dispone a la Secretaria Relatora, dar lectura al oficio N° MINTEL-MINTEL-2019-004-0 del 02 de octubre de 2019 entregado vía correo electrónico, mediante el cual el señor Ministro de Telecomunicaciones y de la Sociedad de la Información, licenciado Andrés Michelena, se excusa de asistir a la sesión y nombra un delegado para asistir a la misma.

El Presidente Encargado de la Comisión manifiesta lamentar la respuesta tardía para la excusa, sin embargo pone en consideración de los miembros de la Comisión aceptar la comparecencia del delegado propuesto por el señor Ministro de Telecomunicaciones y de la Sociedad de la Información, quedando sentado que la Comisión manifiesta su rechazo a lo sucedido con esta autoridad, por cuanto fue convocada con la debida antelación y la comparecencia fue debidamente confirmada, lo que representa una falta de respeto a la Comisión y a la Asamblea Nacional.

Posteriormente solicita se reciba a la abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos (DINARDAP) para continuar con el desarrollo del tema y le concede la palabra, indicando que posee quince minutos para su exposición.

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Inicia indicando que la Dirección del Registro Nacional de Datos Públicos posee atribuciones complejas en virtud de que lleva a su cargo el sistema de gestión registral que comprende la coordinación, regulación, administración y organización de los registros mercantiles y de los registros de la propiedad en concurrencia con los Municipios. La DINARDAP se encarga de velar por la adecuada implementación de los procesos registrales así como la organización, vigilancia y la recepción de quejas, los libros, que ya no son solamente físicos, sino también digitales; otra función de la DINARDAP es presidir el Sistema Nacional de Registros Públicos, donde se regula, administra y supervisa aquellas instituciones que conforme al Art. 13 de la Ley Nacional de Registros Públicos conforman este sistema donde cada entidad del Estado



**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

tiene sus propias bases de datos y en ese orden de ideas, la DINARDAP posee un alcance limitado a cada columna en la base, porque sería de alto costo al igual que humana y técnicamente imposible mantener un servidor capaz de almacenar toda la información de todas la entidades.

Aclara que no todas las bases de datos forman parte de este sistema nacional de registros públicos porque en éste sólo se encuentran aquellas bases de datos que tienen esta categoría, y el funcionario sólo tiene acceso necesario para autorizar el ingreso a la base y en los datos en los que requiera tener acceso, señalando que es así como funciona el Sistema Nacional de Registro Nacional de Datos Públicos (SINARDAP) con una estructura que ayuda a satisfacer a las entidades fuentes y a las entidades consumidoras.

Manifiesta que existen 37 instituciones que son fuentes y 425 que son consumidoras, diferenciándose las mismas básicamente por el nivel de seguridad; respecto a la infraestructura indica que es la Corporación Nacional de Telecomunicaciones (CNT) la institución que se encarga de las conexiones llamadas contacto virtual-data-center que significan la existencia de servicios web que a través de configuraciones de enlace de datos logra que la institución que recibe y la que envía se puedan conectar eficientemente, pero todo esto tiene costos económicos, de recursos humanos y de conocimientos técnicos.

El Presidente encargado de la Comisión, da a conocer a los miembros de la Comisión la presencia del Viceministro de Telecomunicaciones y Sociedad de la Información, conforme a la delegación realizada por el señor Ministro, e indica que por una decisión del Pleno de la Comisión fue solicitada la presencia del señor Ministro de Telecomunicaciones y Sociedad de la Información, razón por la que agradeció la presencia del señor Viceministro, indicando que no será recibido en la Comisión en esta ocasión, reiterando la inconformidad del Pleno de la Comisión con la actitud del señor Ministro quien se comprometió a estar presente y no lo ha hecho, situación que se está dejando constar en actas, posteriormente concede de nuevo la palabra la abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos (DINARDAP), para que continúe con su exposición.

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos:
Refiriéndose al SINARDAP y los tres niveles de control de los datos, señalando que la DINARDAP puede saber a través del mismo, qué campos fueron utilizados y por cuál funcionario, más no qué datos fueron utilizados; el segundo nivel, permite que se controle que los campos que usa el funcionario son aquellos para los que está autorizado; y finalmente el nivel jurídico, que a través de resoluciones individuales la DINARDAP determina si se autoriza o no el uso de datos específicos conforme a las competencias que despliega la unidad consumidora de esos datos; de igual forma se refiere a la suscripción de acuerdos de confidencialidad por parte de cada funcionario que tiene acceso a los datos, así como el nombramiento de coordinadores responsables de verificar y reportar anomalías en el servicio o el mal uso de los mismos.



**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**


Alude a la diferencia entre datos públicos y datos personales, así como los distintos marcos jurídicos que los norman ya que los primeros son de acceso libre a toda la población y se encuentran normados claramente en la Ley de Transparencia y Acceso a la Información Pública, mientras que los datos personales no cuentan con un marco jurídico que los desarrolle, lo que complica la labor de la DINARDAP.

En el caso de los libros de registro, existen datos de ambos tipos por lo que unos pueden ser entregados libremente y otros no, lo que hacía que la normativa fuese insuficiente y no determinara cómo actuar en cada caso, por esto desde enero a febrero del año 2018 se emprendió un proceso de diagnóstico y se comparó esta complicación con el resto de instituciones públicas; posteriormente, de marzo a diciembre de 2018 se realizaron sesenta mesas de trabajo con todos los actores involucrados: academia, sector público, sector privado, sector industrial, empresarial, sociedad civil, organismos internacionales e incluso en la Asamblea Nacional, y no sólo en Quito sino en varias provincias del país, destacando que dentro de ese proceso se pudo detectar que había la necesidad de una normativa para todos los que hacen uso de datos, que diga qué se puede y que no, y que se materializó con un anteproyecto ingresado el 19 de enero de este año en un evento realizado en el que se envió oficios a todos los Asambleístas, donde se recibió muchas observaciones, sobre todo de los encargados del plano técnico de seguridad informática, hasta alcanzar la versión final que fue entregada en el Ministerio de Telecomunicaciones y Sociedad de la Información en fecha 04 de mayo de 2019, convirtiéndose así en proyecto de ley el 19 de septiembre del 2019 cuando fue presentado a la Asamblea Nacional en virtud de los hechos de conocimiento público.

Asegura que la importancia del proyecto de Ley Orgánica de Protección de Datos Personales reside en el trabajo de escuchar a las personas y ver sus necesidades; manifiesta que existen derechos digitales que no estaban siendo respetados ni habilitados para su ejercicio y que los mismos exigen entonces que los responsables de su tratamiento, como son todas las personas naturales, jurídicas, públicas o privadas en el ejercicio de sus funciones deben cumplir, lo que se traduce en obligaciones que si no se cumplen, representan infracciones o sanciones por parte de una autoridad de protección de datos.

Prosigue señalando que es triste reconocer que de la región, los únicos tres países que no tenían Ley de Protección de Datos Personales son Venezuela, Ecuador y Bolivia y que los otros países de la región poseen normativas de este tipo desde el año 2002, además de contar con instituciones de autoridad de protección de datos, experiencia y conocimientos; existen asociaciones iberoamericanas de protección de datos personales, hay un reglamento general de protección de datos personales que regula toda esta temática y que es el mayor estándar de protección a nivel mundial y que ya se está pensando en cómo hacer que incluso estas grandes plataformas informáticas existentes en la actualidad se adecúen para proteger los datos de sus ciudadanos, y el Ecuador está recién tratando de entender cómo funciona, por eso la DINARDAP emprendió campañas, entre ellas "Mis datos o yo" que es de empoderamiento de derechos.

Se visitaron escuelas y colegios donde se consultó a los adolescentes si ellos sabían que tienen derechos digitales mostrando los riesgos que puede significar el uso de tecnologías y ciencia,



**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

al reconocer que no existe educación digital y a pesar de no contar con normativa, se hizo una aplicación directa de la Constitución, dictando una guía de protección de datos personales para las entidades del sector público que permite a los ciudadanos ejercer su derecho de acceso, para conocer qué datos tiene cierta institución sobre ellos, señalado que será dejado en copia este documento en la Comisión, añadiendo que se emitió en junio del 2019 y a pesar de que todavía es mejorable, fue con lo que se contó en el momento para tratar de regular al canal de acceso a los sitios web de las instituciones públicas dentro del campo de acción de la DINARDAP, que es la guía de protección de datos personales en la interoperabilidad, afirmando que esto no tiene efectos vinculantes por lo que reitera la necesidad de formalizarse por medio de la ley para que su aplicación pueda ser más efectiva y eficiente.

Explica que la DINARDAP debe resguardar el intercambio de información, por lo que cumple con la seguridad en puntos finales en bases de datos y aplicaciones tecnológicas almacenados desde marzo de este año en las que existen protocolos que permiten tener acceso a saber qué datos tienen de cada uno las organizaciones y cómo los utilizan para fomentar la defensa integral de los derechos, incluso al punto de que el ciudadano decide quién puede tener y manejar sus datos y quién no a través de la expresa habilitación del titular, dando la más amplia seguridad tecnológica, jurídica y organizativa, porque de lo contrario, a su criterio no se puede hablar de manejo de datos personales.

Añade que dentro de la gestión de la información se cubre el derecho que se debe respetar por parte de todos los responsables del tratamiento de la información, cumpliendo sus principios y obligaciones al respecto, pero reiteró que lamentablemente el control es del que elabora y maneja la base; ellos son los responsables de la información o aclaración de cada base respectiva, porque la DINARDAP no podría decirle a otra institución como construir o manejar las bases de datos, limitándose a determinar qué necesidad tiene la otra institución para que su servicio en ventanilla o servicio institucional funcione habilitando el canal controlado, además de lograr efectivamente que haya un sistema de ética que permita el cumplimiento de los tres tipos de control: administrativo organizacional, jurídico y tecnológico, donde se puede reforzar la parte tecnológica pero con el debido apoyo en la parte jurídica.

Así mismo, señala que es necesario conocer cuáles son las fuentes para contar con la información adecuada, y manifiesta que no están presentes los funcionarios de seguridad informática y auditoría para aclarar más a profundidad este punto, pero puntualiza que los datos no son requeridos por la DINARDAP, por cuanto esta entidad sólo es para la administración y no el manejo de las bases, aunado al hecho de que si la base no pertenece al Registro Nacional de Datos Públicos el acceso es aún más limitado y menciona que de las 237 fuentes de las que posee conocimiento, sólo 37 pertenecen a este sistema.

Respecto al seguimiento del cumplimiento de normas de seguridad, indica que se recibe constante monitoreo y evaluaciones periódicas en las que se reciben excelentes calificaciones, mencionando que actualmente se posee el 100% en dichas evaluaciones por lo que asegura que cada día se va avanzando y mejorando en los temas de seguridad.



COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL

Asambleísta Pedro Curichumbi: Agradece la presencia y explicación técnica, pero menciona que no responde el problema central y realiza preguntas puntuales: ¿Cuáles son las bases de datos que fueron sustraídas o robadas? ¿Qué tipo de riesgo corre el país? ¿Las bases de datos que están bajo su control también fueron robadas?

El Vicepresidente en ejercicio de la Presidencia de la Comisión concede la palabra a la abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos (DINARDAP).

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Aclara que en primer lugar que DINARDAP no tiene bajo su control bases de datos y que dicho control es de quien elabora la base y quienes son responsables de la información, pues sólo determinan qué necesita la otra institución, y que de la inquietud de lo que hacen las fuentes es que se ha creado el sistema de protección, además menciona que si se filtraron datos, DINARDAP sólo puede responder por sus competencias y cuenta con un informe técnico que certifica que no han recibido ataques ni *hackeos* a su sistema de intercambio.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, concede la palabra al Asambleísta Augusto Espinosa.

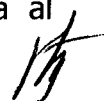
Asambleísta Augusto Espinosa: Resume de lo que ha comentado la abogada Lorena Naranjo y pregunta ¿Bajo ningún concepto ustedes almacenan o tienen una base de algunos de los campos de las bases de datos de las instituciones?

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Indica que sería humanamente imposible y demasiado costoso debido al tamaño, por eso no se almacenan datos ni siquiera como respaldo.

Asambleísta Augusto Espinosa: Pregunta ¿Hay alguna auditoría externa para verificar que no han sido víctimas de *hackeos* o vulneraciones? ¿Con qué regularidad se las hacen?

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Responde que han logrado que exista un sistema de *ethical hacking* que hace monitoreos externos, analizando no solamente si te atacan sino también el grado de vulnerabilidad, lo que constituye otra fuente de revisión de la información para verificar el grado de seguridad de la plataforma y señala que es un sistema implementado desde su gestión dentro de la institución.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, concede la palabra al Asambleísta Augusto Espinosa.



**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

Asambleísta Augusto Espinosa: Pregunta ¿Se ha hecho una auditoría externa de uso de claves?

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Responde que el *ethical hacking* no elabora un informe periódico sino que es un monitoreo, pero es posible levantar un informe si la Comisión así lo requiere.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, concede la palabra al Asambleísta Dennis Marín.

Asambleísta Dennis Marín: Menciona que su explicación fue demasiado amplia, pero desearía que se aclare si esos controles (Administrativo, organizaciones, jurisdiccional, tecnológico) que mencionó anteriormente son parte del cumplimiento del EGSI.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, concede la palabra a la abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos (DINARDAP).

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Responde que en la parte tecnológica sí, en la parte jurídica es en cumplimiento de la Ley del Sistema Nacional de Registros Públicos y en la parte operativa tiene una trama que es del EGSI y una trama institucional que compete a sus obligaciones.

Asambleísta Dennis Marín: Solicita a la Comisión hacer un seguimiento y control del cumplimiento del EGSI en el resto de las instituciones gubernamentales, pues es preocupante que la Ministra de Gobierno no supiera responder sobre la defensa de sus datos y fuentes, y señala que es indispensable porque si ellos reciben datos distorsionados se empañan sus funciones; y por otro lado la no comparecencia del ente rector que debe hacer el trabajo de auditoría a cada una de las instituciones.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, concede la palabra a la abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos (DINARDAP).

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Manifiesta que el EGSI es un esquema gubernamental de seguridad de la información administrado por MINTEL y que la DINARDAP es un cumplidor más, por lo que no se puede exigir el cumplimiento del EGSI de todas las instituciones y sólo puede por las 37 fuentes que son declaradas de servicio público y que constan en el sistema.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, concede la palabra al Asambleísta Dennis Marín.



COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL

Asambleísta Dennis Marín: Pregunta ¿Qué tanto seguimiento tienen al cumplimiento de normas de seguridad informática?

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Responde que están constantemente monitoreando ese cumplimiento con evaluaciones periódicas que son calificadas, y señala que se encuentran en el nivel 2 con un 100% de cumplimiento y cada uno de los niveles evidencian cómo se evoluciona en el tema de seguridad porque no se trata sólo de la parte tecnológica sino de un tema integral.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, concede la palabra al Asambleísta Dennis Marín.

Asambleísta Dennis Marín: Solicita se informe a la Comisión ¿Cuáles son las 37 fuentes? ¿Cuál es el manejo que tienen en la parte de información? y ¿Sobre qué esquemas de seguridad mantienen para administrar la información?

El Vicepresidente en ejercicio de la Presidencia de la Comisión, dispone que se tome nota del pedido que realiza el Asambleísta Dennis Marín y concede la palabra al Asambleísta Juan Lloret.

Asambleísta Juan Lloret: Expresa que lo sucedido respecto a la información es grave, con repercusiones que denotan una fragilidad en el resguardo de la información y considera que el Estado ecuatoriano debió tomar ciertas directrices, porque cabe cuestionar ¿Qué se ha hecho para mejorar la seguridad? y analizar ¿Cuál es el nivel de seguridad que nos ofrecen a los ecuatorianos? Afirma que ninguna de las dos autoridades que asistieron a la sesión responde sobre la fuga de datos, nadie se hace responsable y nadie conoce de lo que ha pasado y señala que existen responsabilidades de carácter político y legal.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, concede la palabra a la abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos (DINARDAP).

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Solicita proyectar nuevamente las diapositivas y afirma que hay temas que ya había mencionado, pero lamentablemente el Asambleísta que pregunta no se encontraba presente, aclara que la normativa a la que se refiere el Asambleísta Juan Lloret representan normativas de refuerzo porque ellos poseen otras resoluciones en las que agregan elementos adicionales de control y la accesibilidad al Registro Nacional de Datos Públicos; reiteró que la seguridad es uno de los ámbitos de la protección por ello la ley que proponen a la Asamblea Nacional es una ley de protección de datos personales, y ratifica que el sistema de protección debe ser integral y la ley que lo rige debe estar asociada desde la persona de ventanilla pidiendo autorización porque se debe cumplir con el ciclo de vida del dato con transparencia pero el tema de cómo

**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

se implementa la seguridad de datos se realiza mediante el ECSI y eso lo hacen todas las instituciones.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, dispone que se tome nota del pedido que realiza el Asambleísta Dennis Marín y concede la palabra al Asambleísta Juan Lloret.

Asambleísta Juan Lloret: Reitera que lo que desea saber es ¿Qué acciones se han tomado conociendo la vulneración de hace un año? porque recién se presenta un proyecto de Ley.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, concede la palabra a la abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos (DINARDAP).

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Explica la línea temporal de la Ley de Protección de datos, alegando que incluso invitaron en diciembre del año pasado a todos los Asambleístas para analizar lo que ahora se está presentando.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, solicita que la información que brinda la Directora del Registro Nacional de Datos Públicos sea entregada por escrito y concede la palabra al Asambleísta Oswaldo Coronel.


Asambleísta Oswaldo Coronel: Solicita que se indique la fecha en la que el proyecto de Ley fue enviado a la Presidencia de la República.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, concede la palabra a la abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos (DINARDAP).

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Señala que dentro del proceso fue el MINTEL el primero en recibirlo para luego enviar al Gabinete Sectorial y luego remitir a la Presidencia, pero manifiesta que no cuenta con las fechas exactas al momento.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, solicita a la Secretaría de la Comisión que dé lectura de las preguntas que han sido entregadas por escrito de algunos Asambleístas miembros de la Comisión para la Abogada Lorena Naranjo.

La Secretaria de la Comisión procede a dar lectura de las preguntas realizadas por el Asambleísta René Yandún y Fabricio Villamar como se indica a continuación



COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL

¿Cuáles han sido las medidas de seguridad adoptadas en los sistemas informáticos para evitar la fuga de datos de los ciudadanos ecuatorianos?

¿La DINARDAP concentra la información de bases en un servidor físico bajo la responsabilidad de su dirección?

¿Qué tipo de protocolos técnicos y otros aplica para la protección física y digital de su acceso?

El Vicepresidente en ejercicio de la Presidencia de la Comisión, concede la palabra a la abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos (DINARDAP).

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Afirma que la DINARDAP no almacena información porque sólo son un bus de interoperabilidad e intercambio de información y sus protocolos son técnicos, organizativos y jurídicos que se reflejan en el tratamiento que dan a su trabajo, que es exclusivamente el intercambio de información que se hace en la plataforma y en la atención de las distintas instituciones con sus respectivos coordinadores institucionales, únicos autorizados para acceder a la información de la plataforma, así como los supervisores y visualizadores que son quienes tienen clave de acceso sólo para los elementos para los cuales han sido previamente calificados su acceso; prosigue indicando que poseen las reclusiones para quienes deseen acceder a la información, puedan hacerlo desde su competencia y menciona que se enviará a la Comisión la Resolución N° 7 que determina las formas de acceso y cómo se tratan los pedidos de interoperabilidad. Respecto a la tecnología señala que poseen protecciones periféricas acordes al cumplimiento del EGSI, protección con *ethical hacking* y protocolos organizativos y físicos que requiere el sistema para que la plataforma de interoperabilidad funcione.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, Asambleísta René Yandún, encarga temporalmente la presidencia al Asambleísta Fafo Gavilánez para intervenir y éste le concede la palabra inmediatamente.

Asambleísta René Yandún: Menciona que existe la tarea del Poder Legislativo para buscar un responsable respecto a la filtración de datos, por lo que solicita a la Secretaria Relatora que se dé lectura al Art. 26 de la Ley del Sistema Nacional del Registro de Datos Públicos y al Art. 13 de su Reglamento a la Ley del Sistema Nacional de Registros Públicos. Una vez leídos menciona que la ley es clara en establecer responsabilidades, razón por la cual para poder cumplir con el deber y hacer el respectivo informe, la ley dice que la responsabilidad recae en el reglamento que se encuentra bajo su dirección, por lo que pregunta ¿Qué se ha hecho para evitar toda esta trama? ¿Si se ha cumplido con el mandato de la ley y del reglamento?

El Presidente encargado Asambleísta Fafo Gavilánez concede la palabra a la abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos (DINARDAP).



**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Aclara que las normas citadas hacen referencia a la seguridad y al responsable de la misma que es la fuente quien responde por la base de datos, mencionando que los artículos leídos son exclusivamente a temas de interoperabilidad e insiste que la DINARDAP no tiene competencias sobre bases de datos que maneja cada institución y por esto cuestionan qué requiere el Ecuador en seguridad de datos y desde que asumió esa dirección ha venido trabajando para construir la propuesta de seguridad de datos que han presentado.

Asambleísta René Yandún: Replica aludiendo que con la explicación dada se afirma que el control está descentralizado, entonces formula los siguientes cuestionamientos: ¿A quién damos la responsabilidad, a cada una de las instituciones? ¿Esto llegó a conocimiento de la Contraloría General del Estado, tuvo alguna auditoría? Y


El presidente encargado concede la palabra a la abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos (DINARDAP).

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos: Explica con un ejemplo de cómo se ejecuta en Colombia el uso de bases de datos y lo adelantados que están, indicando que cada una de las instituciones públicas o privadas son responsables de la implementación de esa seguridad y de los criterios a aplicar al respecto existiendo una sanción ante el incumplimiento, entonces considera que si es cada uno quien debe hacer un manejo adecuado de sus datos pues lógicamente es cada institución la que tiene que implementar mecanismos y análisis de riesgo para saber si los datos tratados son sensibles para establecer estándares adicionales.

El Asambleísta Gavilánez devuelve la Presidencia de la Comisión al Asambleísta René Yandún, y éste concede la palabra al Asambleísta Dennis Marín.

Asambleísta Dennis Marín: Menciona que le preocupa que se niegue por parte de las autoridades pertinentes que ha existido *hackeo* o filtración por lo que presume que hubo un robo de información por parte de algún funcionario y manifiesta que hay que investigar lo que pasó, con sus responsables y ver qué instituciones se encuentran implicadas en este hecho.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, menciona que como Comisión, se debe realizar un informe y establecer responsabilidades; que de acuerdo a la Ley la responsabilidad recae sobre la institución que está compareciendo, pero que tiene que recabar información relevante que determine de mejor manera a los responsables y concede la palabra a la abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos (DINARDAP).



**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

Abogada Lorena Naranjo, Directora del Registro Nacional de Datos Públicos:

Menciona que respecto al ámbito de competencia de la DINARDAP, reitera que sólo hacen interoperabilidad y no manejo de la fuente de la información porque la ley sólo habilita para la interoperabilidad y en el Art. 31 que se menciona por parte del Asambleísta René Yandún, recalca que ellos como institución no pueden solicitar información a las fuentes puesto que la norma como está diseñada sólo permite el intercambio y cómo administra su base de datos alguna institución es autónomo y la DINARDAP no puede intervenir; sobre el tema de la Contraloría General del Estado, manifiesta que no posee conocimiento alguno de que ellos hayan tenido intervención en alguna institución en el tema de seguridad y lo que se ha logrado es enviar a la Contraloría toda la información que no estaba en CNT y velaron para que ese intercambio cumpla con todos los temas de seguridad.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, solicita a la Secretaria Relatora que tome nota para que se pida el informe enviado por la DINARDAP a la Contraloría General del Estado.

Asambleísta Dennis Marín: Aclara que el único pedido que realiza a la abogada Lorena Naranjo, Directora de la DINARDAP, es que se diga cuáles son esas 37 instituciones fuentes mediante un oficio y que la Comisión pueda solicitar se explique sus respectivos procedimientos para el control de la seguridad de la información.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, continuando con el orden del día invita a que comparezca a la sesión a la Licenciada Marta Moncayo, Gerente General de la Corporación Nacional de Telecomunicaciones (CNT) y le concede la palabra.

Licenciada Marta Moncayo Herrero, Gerente General de CNT: Inicia destacando que como institución, a CNT le corresponde explicar las capacidades y la potencia que tiene como entidad que presta el servicio, y también los límites como empresa pública. Describe que CNT posee 2 *data center*, uno en Quito y otro en Guayaquil y también señala que tienen una alta disponibilidad del 99.99% es decir, que jamás ha dejado de trabajar y la información ha estado protegida; en seguridad física en el *data center* existen 7 niveles de seguridad física, explicando cada paso para el ingreso y señalando que adicionalmente, existe vigilancia 24/7 y circuito cerrado de seguridad.

En cuanto a la seguridad lógica, explica que son todas las otras herramientas que son de los clientes, que son usadas para proteger a los datos de posibles ataques o los datos de cada cliente, e indica que dentro de los servicios nunca tienen acceso a los datos para que el cliente tenga procesos más confiables en todo el sistema, señalando que CNT tiene la capacidad de almacenar virtualmente la información sin importar la condición que tengan los equipos de los clientes y a través de *partners* se brinda el Canal Seguro, un sistema que reacciona ante cualquier intento de vulneración.



**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

Posteriormente expone las características de los *data center* señalando que hay dos tipos de opciones para los clientes; los que quieren administración de la información con asesores y protocolos sin ser responsables sobre la información, o la de quienes sólo necesitan que la información llegue como se envía sin ninguna modificación.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, solicita a la Secretaria Relatora se haga lectura de las preguntas que se han formulado por escrito para la Licenciada Marta Moncayo, Gerente General de CNT.

La Secretaria de la Comisión procede a dar lectura de las preguntas realizadas por los Asambleístas miembros de la Comisión, como se indica a continuación

¿Cuál es el argumento técnico para tener concentrado en un solo *data center*?, ¿Es más seguro que información descentralizada?

Licenciada Marta Moncayo Herrero, Gerente General de CNT: Señala que la información no está en un *data center* sino detrás de la seguridad georeferenciada, porque existen 4 lugares en donde se respalde la información y no se dañe, para cuidar la información, para combatir desastres físicos, y si por ejemplo la información se daña en Quito, se levanta en Guayaquil.

¿Cuáles son los protocolos técnicos y análogos que se implementan para que personal con acceso a las bases concentradas en el data center no puedan ser filtradas?

Licenciada Marta Moncayo Herrero, Gerente General de CNT: Asegura que CNT jamás ha sido filtrado, porque siempre van a existir canales seguros, y en caso de que se intente una vulneración el sistema resguarda la información de manera inmediata y automática.

La capacidad de tecnología con la que cuenta CNT ¿Garantiza la protección de los datos personales de los ciudadanos ecuatorianos?

Licenciada Marta Moncayo Herrero, Gerente General de CNT: Señala que CNT no es responsable del contenido de los datos sino que todo lo que se envíe no sea alterado y se mantenga resguardado, afirmando que cuentan con el aval del ISO 7000-1.

¿Existe coordinación entre CNT y las demás entidades del Estado que cuentan con unidades especializadas de seguridad?

Licenciada Marta Moncayo Herrero, Gerente General de CNT: Indica que CNT es proveedor, por lo que si se contrata un asesoramiento se dará a un asesor que acompañe al cliente indicando los procesos correctos a seguir y que siempre el dato le pertenece a la



**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

empresa o institución que genera o tiene el dato, y CNT se limita a generar los niveles de seguridad. Asegura que CNT coopera en la política de protección de datos y ciberseguridad dirigida por el Gobierno Central porque el *data center* de CNT es de nivel internacional.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, concede la palabra al Asambleísta Pedro Curichumbi.

Asambleísta Pedro Curichumbi: Felicita a la Gerente de CNT porque menciona que es la única que ha brindado seguridad respecto a la protección de sus datos y asegura que no ha sufrido filtraciones, aun así cuestiona que si se han realizado auditorías externas ¿Quiénes reciben los resultados de las auditorías? y pregunta si podría enviar esa información a la Comisión para elaborar el informe; además pregunta si ¿existe alguna infraestructura adicional en el país aparte de los dos *data center* que resguarde la información que poseen?.

Licenciada Marta Moncayo Herrero, Gerente General de CNT: Primero expone que las ISOS son auditorías internacionales y se puede verificar los certificados que posee CNT entre otras cosas porque la Contraloría General del Estado verifica las contrataciones y procesos administrativos. Sobre la segunda pregunta señala que desconoce si existe esa infraestructura.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, concede la palabra al Asambleísta Dennis Marín.

Asambleísta Dennis Marín: Interroga ¿Quién evalúa la seguridad de CNT y quién lo certificó? ¿El personal está calificado para atender a los clientes e instituciones públicas? ¿Cuál es la experiencia de CNT, su historial y cuáles son las 37 instituciones y qué tipo de servicios tienen contratados?

Licenciada Marta Moncayo Herrero, Gerente General de CNT: Aclara que no se puede relacionar las 4 líneas de negocio con la línea de negocio corporativo de CNT, pues son completamente aparte; señala que tiene avales internacionales del más alto nivel y no solamente es por la seguridad sino por el personal capacitado para responder a las situaciones, porque se debe demostrar que se tiene lo que cada una de las certificaciones avalan para seguir garantizando seguridad y en cuanto al personal, afirma que no solamente posee contratos de confidencialidad sino que el personal no puede llegar a la información, no tienen acceso; señala que con gusto entregará los nombres de las instituciones pero siempre y cuando se mantenga la confidencialidad, y respecto al historial señala que cuentan con 53 entidades públicas y 17 privadas.

Asambleísta Dennis Marín: Menciona que el resto de servicios si están en mejora ¿Cómo el *data center* va a funcionar óptimamente si el servicio no es óptimo? También habla del



**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

acuerdo 166 donde no han direccionado al resto de instituciones para resguardar los datos a través de CNT.

Licenciada Marta Moncayo Herrero, Gerente General de CNT: Recalca que el servicio corporativo no tiene fallas, y si los servicios a usuarios no es óptimo responde a varios factores que ya mencionó en su intervención, y que el funcionamiento del *data center* es diferente.

Asambleísta Dennis Marín: Solicita que se aclare sobre el nivel de servicio corporativo con los *partners* y los proveedores que tienen convenio con CNT.

Licenciada Marta Moncayo Herrero, Gerente General de CNT: Menciona que sobre quienes representan a las empresas internacionales aquí en el Ecuador ellos tiene contratos de confidencialidad con CNT y también con sus propios representantes siendo contactos de soporte. Pide que si necesitan nombres de intermediarios e información se haga por escrito.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, expresa que no se hablado de todos los peligros cibernéticos que se dan a nivel mundial, y existiendo tantas empresas extranjeras ¿No cree que con la tecnología que existe a nivel mundial, puedan hacer un *hacking*? ¿Cree que la tecnología que usted tiene es infalible para ser *hackeada*? y ¿Estos dos *data centers* son suficientes para cubrir la demanda?

Licenciada Marta Moncayo Herrero, Gerente General de CNT: Aclara que si bien los *data center* de CNT no fueron *hackeados* no significa que no hayan sufrido atentados, pero existe un sistema de seguridad muy grande que brinda alertas por medio de varias herramientas y si llegaran a ingresar, el sistema se apaga, se bloquea y no se puede penetrar, es un sistema que cumple con los estándares internacionales.

El Vicepresidente en ejercicio de la Presidencia de la Comisión, solicita que se haga llegar a la Comisión la certificación de que no han sido *hackeados* los Data Center de CNT y hace la aclaración sobre el tiempo límite para entregar este informe que era el 05 de octubre del 2019, y el Asambleísta Fernando Flores solicitó la prórroga al Presidente de la Asamblea Nacional por 15 días más, por lo que se espera la comparecencia de más autoridades en la Comisión para poder entregar el informe debidamente sustentado.

d) Clausura de la sesión.-

Siendo las 13h39, el señor Vicepresidente en ejercicio de la Presidencia de la Comisión, agradece la comparecencia de las y los Asambleístas y procede a clausurar la sesión. Sin perjuicio del contenido del presente documento, se estará a lo previsto en el Art. 141 de la

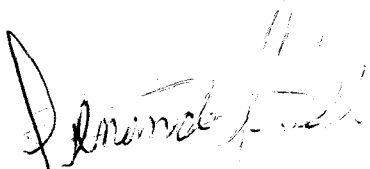


**COMISIÓN ESPECIALIZADA PERMANENTE DE SOBERANÍA, INTEGRACIÓN, RELACIONES
INTERNACIONALES Y SEGURIDAD INTEGRAL**

Ley Orgánica de la Función Legislativa y en el Art. 33 del Reglamento de las Comisiones Especializadas Permanentes y Ocasionales.

Forma parte de la presente acta, el disco con el audio completo de la sesión.

Firman para constancia el señor El Vicepresidente en ejercicio de la Presidencia de la Comisión y la señorita Secretaria Relatora.


Asambleísta René Yandún Pozo
Vicepresidente en ejercicio
de la Presidencia de la Comisión




Abg. Denise Zurita Chávez
Secretaria Relatora



Acción	Nombre	Cargo
Elaborado por:	Abg. Miguel Torres	Prosecretario
Revisado por:	Abg. Denise Zurita	Secretaria