



LEY QUE DECLARA DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA CREACIÓN DEL COMITÉ DE ALTO NIVEL DE CIBERSEGURIDAD DEL ESTADO PERUANO

El congresista que suscribe, **RAÚL HUAMÁN CORONADO**, integrante del Grupo Parlamentario **FUERZA POPULAR**, en el ejercicio, del derecho de iniciativa legislativa que les confiere el artículo 107° de la Constitución Política del Perú y conforme lo establecen los artículos 22° inciso c), 67°, 75° y numeral 2 del artículo 76° del Reglamento del Congreso de la República, presenta el siguiente proyecto de ley:

FÓRMULA LEGAL

PROYECTO DE LEY

EL CONGRESO DE LA REPÚBLICA

Ha dado la siguiente ley:

LEY QUE DECLARA DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA CREACIÓN DEL COMITÉ DE ALTO NIVEL DE CIBERSEGURIDAD DEL ESTADO PERUANO



Firmado digitalmente por:
JIMENEZ HEREDIA David
Julio FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 08/09/2024 17:34:46-0500



Firmado digitalmente por:
SANTISTEBAN SUCLUPE
Magally FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 08/09/2024 17:08:01-0500

Artículo único. Declaratoria de interés nacional y necesidad pública la Ley que Declara de Interés Nacional y Necesidad Pública la Creación del Comité de Alto Nivel de Ciberseguridad del Estado peruano.

Declárese de interés nacional y necesidad pública la creación del **COMITÉ DE ALTO NIVEL DE CIBERSEGURIDAD DEL ESTADO PERUANO**, a fin de implementar herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los datos activos de una organización y de los usuarios de un ciberentorno.

Dese cuenta



Firmado digitalmente por:
RAÚL REZ GARCIA Mery
Estefany FAU 20161749126 hard
Motivo: Soy el autor del documento
Fecha: 08/09/2024 14:51:14-0500



Firmado digitalmente por:
HUAMÁN CORONADO Raul FAU
20161749126 soft
Motivo: Soy el autor del documento
Fecha: 05/08/2024 11:32:18-0500



Firmado digitalmente por:
INFANTES CASTAÑEDA Mery
Eliana FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 08/09/2024 18:31:25-0500

RAÚL HUAMÁN CORONADO
Congresista de la República
Documento firmado digitalmente



Firmado digitalmente por:
VENTURA ANGEL Hector Jose
FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 08/09/2024 17:25:37-0500



Firmado digitalmente por:
LOPEZ MORALES Jeny Luz
FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 08/09/2024 15:52:13-0500



Firmado digitalmente por:
CHACON TRUJILLO Nilza
Mery FAU 20161749126 soft Plaza Bo
Motivo: Soy el autor del documento
Fecha: 08/09/2024 18:13:48-0500



Firmado digitalmente por:
ALEGRIA GARCIA Luis
FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 05/09/2024 17:58:32-0500

EXPOSICIÓN DE MOTIVOS

A fin de exponer la necesidad de declarar de interés nacional y necesidad pública la Creación del **COMITÉ DE ALTO NIVEL DE CIBERSEGURIDAD DEL ESTADO PERUANO**, a fin de implementar herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los datos activos de una organización y de los usuarios de un ciberentorno, resulta importante exponer la realidad de la seguridad en el ciberespacio, el cual afecta a la sociedad peruana.

I. PROBLEMÁTICA

Los avances tecnológicos han facilitado las acciones de las personas en los ámbitos laborales, sociales, comerciales y de entretenimiento. Cada año, la humanidad observa cómo los medios tecnológicos avanzan tan rápidamente que muchas personas no pueden comprender estos avances. En la actualidad, las herramientas tecnológicas se están volviendo cada vez más importantes en nuestras vidas, lo que significa que no podemos realizar nuestras actividades sin ellas.

Debido a que los medios tecnológicos son una necesidad y una realidad en el progreso de la vida de los peruanos, es nuestra responsabilidad mantenernos informados. Lamentablemente, la criminalidad evoluciona junto con la tecnología. De esta manera, se concluye que los delincuentes se han adaptado a estos nuevos tipos de delitos, lo que da lugar a lo que se conoce como cibercriminalidad, que se define como el fenómeno delictivo que emplea herramientas tecnológicas.

De esta manera, es necesario que las autoridades tomen medidas para proporcionar un tratamiento adecuado y efectivo para prevenir más daño o impunidad en la lucha contra la cibercriminalidad. No obstante, en Perú se registra una alta tasa de delitos cibernéticos, además de la falta de capacidad de las autoridades encargadas de investigar y regular este fenómeno delictivo. Al respecto, a fin de demostrar la necesidad de la implementación de la Creación del Comité de Alto Nivel de Ciberseguridad del Estado peruano resulta necesario exponer la problemática en la seguridad en el ciberespacio. Con la finalidad de demostrar la problemática se tienen documentos e informes de entidades públicas las cuales se exponen a continuación:

1.1. Informe de Análisis N° 04 – Cibercriminalidad en el Perú: Pautas para una Investigación Fiscal Especializada

La siguiente información ha sido recogida por la Oficina de Racionalización y Estadística del Ministerio Público respecto a las denuncias por delitos informáticos (Ley N° 30096), registradas desde el 22 del mes de octubre del año 2013 al 31 del mes de julio del año 2020 en los Sistemas de Gestión Fiscal (SGF) e Integrado de Apoyo al Trabajo Fiscal (SIATF).

De este modo, resulta importante revisar el siguiente cuadro adaptado del reporte de la Oficina de Racionalización y Estadística, remitido a la OFAEC a través de correo electrónico de fecha 18 de agosto de 2020, obtenido del Informe de Análisis N° 04 – Ciberdelincuencia en el Perú: Pautas para una Investigación Fiscal Especializada, elaborado por la Oficina de Análisis Estratégico contra la Criminalidad-OFAEC de la Fiscalía de la Nación, el cual compartimos a continuación.

CUADRO N° 1
Denuncias por delitos informáticos registradas en Fiscalías Penales
Comunes y Fiscalías Mixtas, de octubre 2013 a julio 2020¹

DELITO SUBGENÉRICO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
LIMA	67	325	550	708	1495	2366	3713	1116	10 340	47.68%
LIMA NORTE	3	24	24	99	174	357	717	220	1618	7.46%
AREQUIPA	1	18	47	155	255	291	506	115	1388	6.40%
LIMA ESTE	3	17	26	53	147	251	603	183	1283	5.92%
LA LIBERTAD	3	20	35	36	94	213	487	232	1120	5.16%
LAMBAYEQUE	1	11	31	82	119	182	326	124	876	4.04%
CALLAO	3	15	16	52	57	130	322	101	696	3.21%
LIMA SUR	1	4	9	27	52	120	355	119	687	3.17%
CUSCO	4	33	42	41	79	81	176	81	537	2.48%
ICA		3	10	22	24	91	195	57	402	1.85%
PIURA	3	10	33	15	34	68	134	40	337	1.55%
LORETO	1	7	15	24	48	93	100	32	320	1.48%
MOQUEGUA	1	2	1	5	19	46	141	47	262	1.21%
SANTA		3	3	6	36	20	90	27	185	0.85%
HUANUCO		3	2	3	30	25	61	36	160	0.74%
JUNIN		5	7	5	16	44	52	27	156	0.72%
UCAYALI		4	6	9	18	43	44	15	139	0.64%
SAN MARTIN		3	4	6	32	31	49	13	138	0.64%
AMAZONAS	2	1	2	6	30	18	51	20	130	0.60%
CAJAMARCA	1	3	2	4	5	21	59	31	126	0.58%
AYACUCHO	2	3	2	9	9	24	50	15	114	0.53%
TACNA		6		5	4	20	50	15	100	0.46%
SULLANA		3	12	9	12	15	25	15	91	0.42%
HUAURA		4	6	8	11	20	32	10	91	0.42%
ANCASH		2	4	5	12	20	35	8	86	0.40%
LIMA NOROESTE			2	6	3	15	31	15	72	0.33%
PUNO	1		3	3	12	8	15	6	48	0.22%
APURIMAC		3	1	1	2	18	13	4	42	0.19%
MADRE DE DIOS		2	3		3	1	23		32	0.15%
TUMBES		4	3	2	5	6	8	1	29	0.13%
HUANCABELICA	1	1	2	3		4	17	1	29	0.13%
CAÑETE		1	1	1	1	1	15	3	23	0.11%
SELVA CENTRAL			3		1	1	5	8	18	0.08%
PASCO	1				2	4	4	1	12	0.06%
TOTAL	99	540	907	1410	2841	4648	8504	2738	21 687	100.00%

¹ Ministerio Público – Fiscalía de la Nación. (2021). Informe de Análisis N° 04 – Ciberdelincuencia en el Perú: Pautas para una Investigación Fiscal Especializada.

En atención a la información recogida por el Ministerio Público, se observa que anualmente las denuncias muestran incrementos constantes. Es así que, en el año 2014 se registraron 540 denuncias y en el año 2015 éstas llegaron a 907. En el año 2016 se elevaron a 1 410 y un año después se duplicaron hasta alcanzar las 2 841 denuncias.

Además, en el año 2018, las denuncias continuaron ascendiendo hasta llegar a 4648 y cerrar el año 2019 con 8 504 denuncias, representando este último año el 39% de todas las denuncias que se presentaron, entre los referidos años.

Respecto al año 2021, se tiene que, según datos del Ministerio Público, se recibieron 18 mil 596 denuncias de casos de cibercrimen, lo que representa un incremento porcentual de 92,9% en comparación con el año 2020².

Conforme a los datos expuestos respecto a las denuncias por delitos informáticos registrados en Fiscalías Penales Comunes y Fiscalías Mixtas, de octubre 2013 a julio 2020 se puede confirmar que los casos van en aumento con el pasar los años, en tal sentido se convierte en una problemática a tender urgente con la finalidad de evitar que estos índices sigan creciendo y se logre proteger a las personas frente a los ciberataques mediante delitos cibernéticos en el ciberespacio.

1.2. Datos del Poder Judicial

En atención a la base de datos del Registro Nacional de Condenas, elaborado por la Sub-Gerencia de Estadística – Gerencia de Planificación del Poder Judicial, podemos conocer la cantidad de personas con sentencia registrada según delitos informáticos y contra el patrimonio relavó al delito informático.

Al respecto, debemos señalar que el Poder Judicial no ha implementado órganos especializados en delitos informáticos o cibercrímenes a diferencia del Ministerio Público o la Policía Nacional del Perú.

Asimismo, el Poder Judicial tampoco ha implementado estrategias o políticas de ciberseguridad a fin de proteger los datos de los usuarios, así como sus sistemas informáticos en el ciberespacio.

En tal sentido compartimos el siguiente cuadro, que hemos adaptado en atención a la información obtenida del Poder Judicial, elaborado por la Sub Gerencia de Estadística – Gerencia de Planificación del Poder Judicial:

² Redacción El Peruano (04 de septiembre de 2022). Denuncias por delitos informáticos se incrementaron en más del 90% en el Perú. Diario El Peruano. Recuperado el 4 de octubre de 2022 de: <https://www.elperuano.pe/noticia/188048-denuncias-por-delitos-informaticos-se-incrementaron-en-mas-del-90-en-el-peru#:~:text=Seg%C3%BAAn%20datos%20del%20Ministerio%20P%C3%BAblico,en%20compa raci%C3%B3n%20con%20el%202020.>

CUADRO N° 2

Personas con sentencia condenatoria registrada según delitos informáticos y contra el patrimonio relativo a delito informático – Periodo 2016 – 2020³.

Delito	Años					Total
	2018	2019	2020	2021	2022 ^o	
Delitos Informáticos (Ley 30096 y 30171)	33	25	142	149	43	392
Acceso Ilícito – Art. 2 – Ley N° 30096		2	1	4		7
Atentado a la Integridad de Datos Informáticos – Art. 3 - Ley N° 30096			4	1	1	6
Atentado a la Integridad de Sistemas Informáticos – Art. 4 - Ley N° 30096		1	1			2
Fraude Informático – Art. 8 - Ley N° 30096	21	9	94	118	30	272
Interceptación de datos informáticos	1	2	2	3	1	9
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos – Art. 5 - Ley N° 30096	8	11	34	23	11	87
Suplantación de Identidad – Art. 9 - Ley N° 30096	3		6			9
Título V Delitos Contra el Patrimonio (Artículo 185 al 208)						
Delitos Informáticos (Artículo 207-A al 207-D)	4	36	3	3	2	48
Alteración, Daño o destrucción de base de datos Art. 207-D				3	2	5
Delito Informático – Art. 207-C Agravantes		1	2			3
Delito Informático Art. 207		34				34
Tráfico ilegal de datos – Art. 207 - Ley N° 30096	1					1
Uso o Ingreso indebido a una base de datos Art. 207-A	3	1	1			5
Total	37	61	145	152	45	440

Al respecto, según la información del Poder Judicial, se tiene que el año 2016 se condenaron a 37 personas, en el año 2017 se condenaron a 61 personas, en el año 2018 se condenaron a 145 personas, en el año 2019 se condenaron a 152 personas y hasta octubre del año 2020 se condenaron a 45 personas. De este modo, desde el año 2016 hasta octubre del año 2020, se registraron un total de 440 sentencias condenatorias.

En atención a lo expuesto, debemos advertir que, a pesar de las miles de denuncias registradas cada año por la Fiscalía, existe una problemática por cuanto solo se han registrado pocas sentencias en el Poder Judicial, de este modo surge la necesidad que el Estado atienda la referida problemática expuesta, a fin de evitar la impunidad en el sistema de justicia, en relación al tratamiento de la cibercriminalidad.

³ Cuadro adaptado de la información brindada de la base de datos del Registro Nacional de Condenas, elaborado por la Sub Gerencia de Estadística – Gerencia de Planificación del Poder Judicial.



1.3. Datos de la DIVINDAT - División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú

Conforme a los datos de la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT), quienes están encargados de investigar, denunciar y combatir el crimen organizado transnacional, en el ámbito de delitos que se comentan mediante el uso de la tecnología de información y comunicación, podemos conocer la cantidad de denuncias presentadas respecto a delitos informáticos.

Resulta importante señalar que la información, datos y estadísticas de la DIVINDAT es información relevante al momento de elaborar iniciativas legislativas que contribuyen a la lucha contra la cibercriminalidad por cuanto los efectivos policiales son el órgano de apoyo del Ministerio Público, lo que implica que son los funcionarios más cercanos al tratamiento de este fenómeno criminalidad.

De igual forma, desde su creación la DIVINDAT viene siendo el órgano de apoyo por excelencia en cuanto a investigación de delitos que utilizan la tecnología, por lo que su información resulta relevante. Al respecto la DIVINDAT es un órgano pionero en la investigación del cibercrimen, por cuanto posteriormente el Ministerio Público recién a partir del 2021 implementa su unidad especializada en la investigación de este tipo de delitos.

De este modo, se tiene que la Oficina de Análisis Estratégico contra la Criminalidad-OFAEC de la Fiscalía de la Nación, ha elaborado el documento titulado: Informe de Análisis N° 04 – Ciberdelincuencia en el Perú: Pautas para una Investigación Fiscal Especializada, el cual es importante revisar por cuanto se ha consignado el siguiente cuadro que expone las denuncias de delitos informáticos, el cual compartimos a continuación.

CUADRO N° 3
Denuncias de delitos informáticos investigados por la DIVINDAT. 2013-2020⁴

DELITO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
Abuso de mecanismos y dispositivos informáticos	14	3	6	4	5	1	2	19	54	0.4%
Abuso de mecanismos y dispositivos informáticos	14	3	6	4	5	1	2	19	54	
Suplantación de identidad	10	101	114	134	132	227	247	572	1537	12.6%
Suplantación de identidad	10	101	114	134	132	227	247	568	1533	
Suplantación de identidad virtual								4	4	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	9	9			29	94	49	100	290	2.4%
Contra la indemnidad sexual de menores								2	2	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	9	9			29	94	49	98	288	
Contra datos y sistemas informáticos	38	62	47	47	104	126	159	177	760	6.2%
Acceso ilícito	11	42	1	1	49	84	129	151	468	
Acceso ilícito a una base de datos								2	2	
Atentado a integridad de datos informáticos	21	4	30	22	40	26	5	9	157	
Atentado a la integridad de sistemas informáticos	6	16	16	24	15	9	5	9	100	
Atentado contra la integridad de datos y sistemas informáticos						7	20	6	33	
Contra la intimidad y el secreto de las comunicaciones						3	2	8	13	0.1%
Interceptación de datos								2	2	
Interceptación de datos personales								1	1	
Tráfico ilegal de datos						3	2	5	10	
Fraude informático	298	334	414	610	1219	1928	2097	2615	9515	78.2%
Clonación de tarjeta	83	42	46	44	30	120	25	4	394	4
Compras fraudulentas por internet						287	431	261	979	10
Operaciones y transferencia electrónicas y/o de fondos no autorizados	215	292	368	566	1189	1521	1641	2350	8142	86
TOTAL	369	509	581	795	1489	2379	2556	3491	12169	100.0%

⁴ Ministerio Público – Fiscalía de la Nación. (2021). Informe de Análisis N° 04 – Ciberdelincuencia en el Perú: Pautas para una Investigación Fiscal Especializada. Pg 20. Recuperado el 4 de octubre de 2022 de: <https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%202015%20FEBRERO%202021.pdf>



De lo expuesto en el cuadro anterior, podemos observar que, en el espacio del mes de octubre del año 2013 al mes de diciembre del año 2020, se registraron 12169 delitos vinculados a la Ley 30096 denunciados. Asimismo, se tiene que el delito de fraude informático posee una incidencia 78% (9515 casos) y el delito de suplantación de identidad posee una incidencia de 13% y los delitos contra datos y sistemas informáticos posee una incidencia 6%.

Asimismo, según las denuncias de delitos informáticos investigados por la DIVINDAT de 2013 a 2020, se tiene que en el año 2013 se registraron 369 delitos, en el 2014 se registraron 509 delitos, para el 2015 se registraron 581 delitos, para el 2016 se registraron 795 delitos, para el 2017 se registraron 1 489 delitos, para el 2018 se registraron 2379, para el 2019 se registraron 2 556 delitos y para el 2020 se registraron 3 491 delitos.

1.4. Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú

El Ministerio de Justicia y Derechos Humanos, el 19 de diciembre de 2020 publicó el documento titulado "Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú"⁵, el cual fue elaborado por un grupo de trabajo multisectorial a cargo de la Secretaría Técnica del Consejo Nacional de Política Criminal - CONAPOC.

La elaboración del referido informe contó con la colaboración de instituciones que están relacionadas a la lucha contra la ciberdelincuencia. Este informe incluye desde definiciones operativas y alcances, estadísticas, registros administrativos y documentación relacionado a casos de ciberdelitos, así como conclusiones y recomendaciones en materia de ciberdelitos.

Respecto a las conclusiones del referido informe, en la conclusión número 1 se tiene que se descubren vacíos importantes en relación a la gestión de la información sobre los ciberdelitos, por lo que es más urgente orientar los esfuerzos para hacer que el intercambio de datos sobre la ciberseguridad sea interoperable.

Asimismo, en su recomendación número 6 se recomienda la posibilidad de aprobación de la Ley de Ciberseguridad y la creación de un Comité de Ciberseguridad. Además, en la recomendación número 11 se tiene la de fomentar actitudes de prevención y denuncia ante los ciberdelitos, se pretenden desarrollar acciones de educación en ciberseguridad con un enfoque en los peligros de la ciberdelincuencia.

Conforme a lo expuesto, la implementación de mecanismos de Ciberseguridad resulta idóneo a fin de proteger a las personas en el ciberespacio.

⁵ Ministerio de Justicia y Derechos Humanos. (2020). Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú. Recuperado el 5 de octubre de 2022 de: <https://cdn.www.gob.pe/uploads/document/file/1616607/Diagn%C3%B3stico%20Situacional%20Multisectorial%20sobre%20la%20Ciberdelincuencia%20en%20el%20Per%C3%BA.pdf>

II. MARCO LEGAL

- Constitución Política del Perú
- Convenio Sobre la Ciberdelincuencia de Budapest.
- Ley 30999, Ley de Ciberdefensa.
- Ley N° 27309, Ley que incorpora los Delitos Informáticos al Código Penal
- Ley N° 30096 de Delitos Informáticos
- Ley N° 29733 de Protección de Datos Personales.
- Decreto Supremo 012-2017-DE, Decreto Supremo que aprueba la Política de Seguridad y Defensa Nacional.
- Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo 050-2018-PCM, Decreto Supremo que establece la definición de Seguridad Digital de ámbito nacional.
- Decreto de Urgencia 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Decreto Supremo N° 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N° 006-2020. Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital
- Decreto Supremo N° 029-2021 PCM, que aprueba si Reglamento de la Ley de Gobierno Digital

III. LA SEGURIDAD EN EL CIBERESPACIO

Sobre la definición de seguridad ciudadana, en la Ley N° 27933 – Ley del Sistema Nacional de Seguridad Ciudadana, la cual tiene por objeto proteger el libre ejercicio de los derechos y libertades, garantizar la seguridad, paz, tranquilidad, el cumplimiento y respeto de las garantías individuales y sociales a nivel nacional, que comprende a las personas naturales y jurídicas, sin excepción, en su artículo 2 establece lo siguiente:

Se entiende por Seguridad Ciudadana, para efectos de esta Ley, a la acción integrada que desarrolla el Estado, con la colaboración de la ciudadanía, destinada a asegurar su convivencia pacífica, la erradicación de la violencia y la utilización pacífica, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos. Del mismo modo, contribuir a la prevención de la comisión de delitos y faltas.

En tal sentido, es un hecho que los ataques realizados en el ciberespacio tienen repercusiones en la realidad. Por lo que es una obligación por parte del Estado brindar seguridad a las personas en el ciberespacio.



Por su parte, Silva Reina, la seguridad debe adaptarse a las nuevas tecnologías para que sea dinámica. Si esto es así, se pueden observar respuestas estatales para asegurar la seguridad en el ciberespacio, mediante la protección de la ciberseguridad.⁶

Una de las formas que el Estado pueda garantizar la seguridad ciudadana en el ciberespacio, así como del sistema económico, es por medio de la implementación de mecanismos de ciberseguridad.

IV. CONCEPTO DE CIBERSEGURIDAD

El inicio de la ciberseguridad se remonta al año 1965, cuando el Departamento de Defensa de los Estados Unidos comenzó a salvaguardar sus sistemas de computación. La encriptación de la información ocurrió posteriormente en 1983. Asimismo, se tiene que los primeros virus informáticos aparecieron en el año 1985.

Posteriormente, en el año 1990, con el propósito de protegerse contra los ciberataques, se empleaba el término "seguridad en sistemas operativos y redes". En el año 2000, también se empleaba el término "Seguridad Informática General". Finalmente, recién en el año 2009 se empezó a discutir con relación al concepto y definición de "Ciberseguridad"⁷.

Al respecto, la Unión Internacional de Telecomunicaciones en su Resolución 181, Recomendación UIT - TX.12 del 05 de noviembre de 2010, sobre el concepto de ciberseguridad estableció lo siguiente:

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciber entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciber entorno. Las propiedades de seguridad incluyen una o más de las

⁶ Silva Reina, A. (2021). Política Pública de Seguridad Ciudadana con Enfoque de Derechos Humanos – Hacia un Modelo de Seguridad Democrática. Fundación Friedrich Ebert. Pg. 8. Recuperado el 26 de octubre de 2022 de:

⁷ Trama, G. y Vergara, E. (2017). Operaciones Militares Cibernéticas: Planteamiento y ejecución en el nivel operacional. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Pp. 66-67. Recuperado el 26 de octubre de 2010 de: https://esgcfcaa.edu.ar/pdf/ESGCFCAA-2016_pdf-49.pdf

siguientes: 1) disponibilidad; 2) integridad, que puede incluir la autenticidad y el no repudio; y 3) confidencialidad⁸.

En atención a la definición expuesta, podemos entender que la ciberseguridad resulta una necesidad a fin de garantizar la seguridad, no solo de las personas en el ciberespacio, sino, también a sistemas informáticos a fin de mitigar cualquier tipo de ciberataques.

V. CIBERSEGURIDAD EN LA ORGANIZACIÓN DE ESTADOS AMERICANOS - OEA

La Organización de los Estados Americanos – OEA, creada en el año 1948 con la misión de lograr en sus Estados Miembros, como lo establece el Artículo 1 de la Carta de la OEA, "un orden de paz y de justicia, fomentar su solidaridad, robustecer su colaboración y defender su soberanía, su integridad territorial y su independencia".

Al respecto, desde hace más de una década la OEA viene expresando su compromiso en la lucha contra los ciberataques y el resguardo de la seguridad cibernética, realizando aportes importantes a fin de defender la seguridad de los Estados Miembros en el ciberespacio.

Desde su fundación hasta el año 2000, la OEA reconoció que el concepto de seguridad no puede entenderse como un concepto estático, ya que se basaba en un concepto tradicional de seguridad. No obstante, se consideró que el concepto de seguridad debía ser actualizado después de la Guerra Fría. La Declaración sobre Seguridad de las Américas del año 2003 establece la necesidad de actualizar el concepto de seguridad nacional para reconocer problemas multifacéticos, como el terrorismo, el crimen organizado, la degradación del medio ambiente, la pobreza, la migración, los ciberataques y otros.⁹

Se tiene que en el año 2004 los Estados Miembros de la OEA aprobaron la Resolución AG/RES. 2004 (XXXIV-O/04) mediante la cual se presenta la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética. En la referida estrategia se adopta el concepto de seguridad multidimensional, mencionado en el párrafo anterior, abordándose como nuevas amenazas "ataques a la seguridad cibernética".

⁸ Unión Internacional de Telecomunicaciones (UIT), Ciberseguridad. RESOLUCIÓN 181 (GUADALAJARA, 2010). Recuperado el 26 de octubre de 2022 de: <https://www.itu.int/en/council/Documents/basic-texts/RES-181-S.pdf>

⁹ Sequera, M., Ucciferri, L y Toledo. (2018). Derechos Humanos y Seguridad Digital: Una Pareja Perfecta - El Rol de organizaciones multilaterales en la agenda latinoamericana de seguridad digital: El caso de la OEA. N° 2. Análisis de políticas sobre ciberseguridad y derechos humanos en Latinoamérica. Pg. 5. Recuperado el 02 de noviembre de 2022 de: <https://adc.org.ar/wp-content/uploads/2019/06/040-derechos-humanos-y-seguridad-digital-una-pareja-perfecta-2-05-2018.pdf>

5.1. Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética

En la cuarta sesión plenaria, celebrada el 8 de junio de 2004, los Estados Miembros aprobaron la Resolución AG/RES. 2004 (XXXIV-O/04) la cual contiene la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética. Asimismo, en el referido punto 1, se menciona sobre la adopción de la Estrategia Interamericana Integral de Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética.

La mencionada estrategia recoge lo establecido sobre el tema de la seguridad cibernética en la Conferencia Especial sobre Seguridad (ciudad de México, México, del 28 al 20 de octubre de 2003) los Estados Miembros, acordando lo siguiente:

"Desarrollaremos una cultura de seguridad cibernética en las Américas adoptando medidas de prevención eficaces para prever, tratar y responder a los ataques cibernéticos, cualquiera sea su origen, luchando contra las amenazas cibernéticas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas. Reafirmamos nuestro compromiso de desarrollar e implementar una estrategia integral de la OEA sobre seguridad cibernética, utilizando las contribuciones y recomendaciones elaboradas conjuntamente por los expertos de los Estados Miembros y por el Grupo de Expertos Gubernamentales de la REMJA en Materia de Delito Cibernético, el CICTE, la Comisión Interamericana de Telecomunicaciones (CITEL) y otros órganos apropiados, teniendo en cuenta el trabajo que desarrollan los Estados Miembros coordinado con la Comisión de Seguridad Hemisférica".

La mencionada estrategia resulta un hito importante por cuanto expone la necesidad de desarrollar la cultura de seguridad cibernética, a fin de resguardar la seguridad de las personas en el ciberespacio.

5.2. Observatorio de Ciberseguridad en América Latina y el Caribe

Mediante el Observatorio de la Ciberseguridad en América Latina y el Caribe, el cual cuenta en su información institucional apoyo del Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA), en la Agenda de Seguridad Cibernética.

Al respecto, se han emitido dos informes importantes los cuales exponen el estado de la ciberseguridad en los Estados Miembros, así como muestran directrices a fin de mejorar las capacidades naciones en ciberseguridad.

Los referidos informes son Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? – Informe Ciberseguridad 2016 y Ciberseguridad Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe – Reporte Ciberseguridad 2020, los cuales resultan importante su revisión.

a) Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? – Informe Ciberseguridad 2016

Se tiene que el Informe 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe, gestionado por el BID y la OEA, a fin de mostrar el estado de la seguridad cibernética en los Estados Miembros. Se tiene que este informe se compone en dos secciones principales, la primera sección, consiste en las "contribuciones de expertos", mediante ensayos sobre la seguridad cibernética, la segunda "Reporte de países" presenta una visión general del estado de la seguridad cibernética, en el 2016, en los países de la región del Caribe y América Latina respecto a los datos obtenidos mediante un mecanismo en línea creado con la cooperación del Global Cyber Security Capacity Centre (GCSCC), de conversaciones con funcionarios de los Estados Miembros y la investigación documental¹⁰.

Este informe fue útil por cuanto ayuda a los gobiernos de los Estados Miembros de la OEA conocer el estado de la ciberseguridad en comparación a otros países de la región.

Respecto al caso peruano, en el informe en mención se indica que la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú (PNP), indica que entre los constantes desafíos que se enfrentan, cabe citar su limitada capacidad técnica para el manejo de evidencia electrónica en los tribunales y la falta de una política de divulgación para el sector privado¹¹.

Asimismo, también se indica que el Equipo de Respuesta a Incidentes de Seguridad Informática del Perú, PeCERT, trabaja óptimamente en atención a los ciberataques. Además, también menciona que, en el Perú, cuenta con la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), a fin de trabajar con la OEA para desarrollar un marco de seguridad cibernética.

b) Ciberseguridad Riesgos, Avances y el Camino a seguir en América Latina y el Caribe – Reporte Ciberseguridad 2020

Respecto al informe Ciberseguridad Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe – Reporte Ciberseguridad 2020, este

¹⁰ Observatorio de la Ciberseguridad. (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? – Informe Ciberseguridad 2016. OAS y BID. Pg. 13. Recuperado el 07 de noviembre de 2022 de: <https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf>

¹¹ Observatorio de la Ciberseguridad. Op. Cit. Pg. 108.

también fue gestionado por el BID y la OEA. Al igual que el informe del 2016, este también muestra una sección de contribuciones de expertos, así como una sección de reporte de países sobre el estado de su seguridad cibernética de los países de la región del Caribe y América Latina.

En atención al reporte del caso peruano, en el referido informe se indica que el Perú no cuenta con una estrategia nacional en cibernética, pero que ha iniciado una Política Nacional en Ciberseguridad. Debemos mencionar que en la actualidad el Perú no tiene una estrategia nacional o una ley de ciberseguridad implementada.

Además, se hace mención del Decreto Supremo N° 106-2017-PCM el cual aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales.

Aunado a ello, se hace mención de la Ley del Gobierno Digital, al igual de la Ley N° 30096 – Ley de Delitos Informáticos y la Ley N° 29733 – Protección de Datos Personales. En atención a lo expuesto, el Estado peruano tuvo avances en la lucha contra los ciberataques respecto a lo reportado en el 2016.

VI. SOBRE LA NECESIDAD DE LA CREACIÓN DEL COMITÉ DE ALTO NIVEL DE CIBERSEGURIDAD DEL ESTADO PERUANO

Conforme a lo expuesto, es evidente la necesidad de implementar estrategias, acciones, actividades e iniciativas para el desarrollo de la ciberseguridad en el Perú, por lo que resulta necesario la creación del Comité de Alto Nivel de Ciberseguridad del Estado Peruano, órgano de carácter estratégico dependiente de la Presidencia del Consejo de Ministros, que tiene por objeto la coordinación multisectorial, articulación y promoción de las acciones relacionadas al desarrollo y consolidación de las estrategias, acciones, actividades e iniciativas para el desarrollo de la ciberseguridad en el Perú, a fin de implementar el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los datos de los usuarios, así como los activos de una organización de un ciberentorno.

El Estado debe garantizar la paz y el ejercicio de los derechos humanos, de este modo, teniendo que los ataques realizados en el ciberespacio tienen repercusiones en la realidad, es una obligación por parte del Estado brindar seguridad a las personas en el ciberespacio.

La ciberseguridad resulta una necesidad a fin de garantizar la seguridad, no solo de las personas en el ciberespacio, sino, también a sistemas informáticos a fin de mitigar cualquier tipo de ciberataques.

La Organización de los Estados Americanos – OEA, desde hace más de una década la OEA viene expresando su compromiso en la lucha contra



los ciberataques y el resguardo de la seguridad cibernética, realizando aportes importantes a fin de defender la seguridad de los Estados Miembros en el ciberespacio.

Desde hace varios años en muchos países se han implementados políticas o estrategias en ciberseguridad o seguridad en el ciberespacio, sin embargo, en el Perú actualmente no existe una política, Ley o estrategia en temas de ciberseguridad.

Asimismo, conforme al Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú", el cual fue elaborado por un grupo de trabajo multisectorial a cargo de la Secretaría Técnica del Consejo Nacional de Política Criminal – CONAPOC, en su recomendación número 6 se recomienda la posibilidad de aprobación de la Ley de Ciberseguridad y la creación de un Comité de Ciberseguridad. Aunado a ello, en la recomendación número 11 se tiene la de fomentar actitudes de prevención y denuncia ante los ciberdelitos, se pretenden desarrollar acciones de educación en ciberseguridad con un enfoque en los peligros de la ciberdelincuencia.

Conforme a lo expuesto, resulta necesario que el Perú implemente una política o una ley o estrategia relacionada a la Ciberseguridad. De este modo, se presenta una propuesta de estrategia de ciberseguridad, la cual está influenciada en estrategias de otros países que han decidido implementar mecanismos en ciberseguridad desde hace años.

VII. ANTECEDENTES DE LA PROPUESTA LEGISLATIVA

De una revisión general, no se aprecia antecedentes de la presente iniciativa legislativa en el presente periodo.

VIII. EFECTO DE VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

La presente iniciativa legislativa no colisiona ninguna norma vigente al tratarse de una norma declarativa, no contraviene ninguna disposición legal del ordenamiento jurídico peruano y versa exclusivamente sobre la declaración de interés nacional y necesidad pública la Ley que Declara de Interés Nacional y Necesidad Pública la Creación del Comité de Alto Nivel de Ciberseguridad del Estado peruano.

IX. ANÁLISIS COSTO-BENEFICIO

La presente propuesta de Ley propone declarar de Interés Nacional y necesidad pública la Creación del Comité de Alto Nivel de Ciberseguridad del Estado peruano, esta propuesta no implicará asumir costos adicionales.

Asimismo, el beneficio de la presente propuesta es la reforzar la lucha contra la criminalidad en específico lo referente a los delitos informáticos. Esto se



logrará con la declaración de interés nacional y necesidad la Creación del Comité de Alto Nivel de Ciberseguridad del Estado peruano.

X. RELACIÓN CON LAS POLÍTICAS DE ESTADO DEL ACUERDO NACIONAL

El presente proyecto de Ley guarda armonía con el Acuerdo Nacional respecto a los siguientes puntos:

ACUERDO NACIONAL	
I. DEMOCRACIA Y ESTADO DE DERECHO	7. ERRADICACIÓN DE LA VIOLENCIA Y FORTALECIMIENTO DEL CIVISMO Y DE LA SEGURIDAD CIUDADANA
	9. POLÍTICA DE SEGURIDAD NACIONAL
III. COMPETITIVIDAD EN EL PAÍS	20. DESARROLLO DE LA CIENCIA Y LA TECNOLOGÍA

XI. RELACIÓN CON LA AGENDA LEGISLATIVA 2023-2024

Respecto a la Agenda Legislativa para el periodo 2023-2024 aprobada por Resolución Legislativa del Congreso N° 002-2023-2024-CR, publicada el 17 de octubre de 2023 y vigente a la fecha, se cumple con los siguientes temas:

- Tema 18. MEDIDAS EN FAVOR DE LA SEGURIDAD CIUDADANA Y EL CIVISMO
- Tema 29. SOBRE LAS FUERZAS ARMADAS Y LA SEGURIDAD NACIONAL
- Tema 89. SOBRE CIENCIA, INNOVACIÓN Y TECNOLOGÍA