PERÚ | Ministerio de Justicia y Derechos Humanos

Siempre con el pueblo

BICENTENARIO DEL PERÚ 2021 - 2024

CIBERDELINCUENCIA

REPORTE DE INFORMACIÓN ESTADÍSTICA Y RECOMENDACIONES PARA LA PREVENCIÓN

PERÚ | Ministerio del Interior

Poder Judicial del Perú

Ministerio Público Fiscalía de la Nación

INEI Instituto Nacional de Estadística e Informática

Defensoría del Pueblo

ANGR Asamblea Nacional de Gobiernos Regionales

CONASEC Consejo Nacional de Seguridad Ciudadana

INPE

CIBERDELINCUENCIA

REPORTE DE INFORMACIÓN ESTADÍSTICA Y RECOMENDACIONES PARA LA PREVENCIÓN

FÉLIX INOCENTE CHERO MEDINA
Ministro de Justicia y Derechos Humanos

JIMMY MARCOS QUISPE DE LOS SANTOS
Viceministro de Justicia

BEYKER CHAMORRO LÓPEZ
Director General de Asuntos Criminológicos

ARTURO HUAYTALLA QUISPE
Coordinador del Observatorio Nacional de Política Criminal – INDAGA

Responsables del documento:
Christian Flores Calderón
Tadeo Rodríguez Vargas
Julissa Urbizagastegui Manrique
Luis Guerra Pallqui
Lucero Retuerto Blas

Diagramación:
Michael Bances Sandoval

Observatorio Nacional de Política Criminal
Calle Scipión Llona 350, Miraflores
https://indagaweb.minjus.gob.pe

Agosto de 2022

MESA CONSULTIVA PARA LA ELABORACIÓN DE LA ESTRATEGIA NACIONAL CONTRA LOS CIBERDELITOS

FISCALÍA DE LA NACIÓN

Aurora Remedios Fátima Castillo Fuerman

Rocío Gala Gálvez

MINISTERIO DEL INTERIOR

Juan Antonio Pozo Castillo

POLICÍA NACIONAL DEL PERÚ

John Rigner Meléndez Meléndez

PODER JUDICIAL

Yetzabe Villanueva Cárdenas

INSTITUTO NACIONAL PENITENCIARIO

Diego Alarcón Donayre

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA

Eduardo Corilla Baquerizo

Lourdes Condori Huahuachampi

Edgar Huamán Vera

DEFENSORÍA DEL PUEBLO

Carlos Fernández Millán

CONSEJO NACIONAL DE SEGURIDAD CIUDADANA

Freddy Isaac de la Cruz Baquerizo

DIRECCIÓN GENERAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Oliver Ricardo Quispe Rojas

PRESENTACIÓN

Conforme avanzamos hacia la superación de la pandemia, aumentan las expectativas por reencontrarnos con las condiciones de vida en las que estábamos antes de los contagios y del aislamiento social. Sin embargo, a pesar de la mejora en las cifras fatales, así como del paulatino retorno al uso de los espacios públicos, hemos experimentado un avance de múltiples formas delictivas, las que a su vez han encontrado en el clima de virtualidad impulsado por la pandemia, un contexto de oportunidad para ampliar su alcance y perfeccionar sus prácticas criminales, afectando a la integridad y la seguridad de miles de ciudadanos y ciudadanas que emplean las nuevas tecnologías con fines educativos, laborales, comerciales o de entretenimiento.

Por esta razón, desde las instituciones encargadas de las políticas públicas destinadas a la lucha contra la criminalidad, realizamos importantes acciones por contribuir con la adecuada implementación de medidas que consigan resultados en el campo de la prevención, investigación, persecución y castigo del ciberdelito (para los fines de este documento, reemplaza la denominación normativa de "delitos informáticos"). En ese sentido, este documento es una pieza de información adicional que responde a la preocupación por el avance de los ciberdelitos que han ocurrido desde que inició la pandemia; y, se construye a partir de los registros de denuncias que reciben tanto las dependencias policiales como las fiscalías en todo el Perú.

Convencidos de que la lucha contra los fenómenos criminales se robustece cuando se ve apoyada por la evidencia medible, trasladamos este documento que posee datos concisos sobre el estado de los ciberdelitos, especialmente de aquellos ocurridos entre los años 2020 y 2021. De igual forma, complementamos los alcances de información con un grupo importante de recomendaciones para evitar y/o reducir las posibilidades de ser víctimas de ciberdelitos, teniendo en cuenta la diversidad de usuarios y formas de consumo de las tecnologías de la virtualidad.

Esperamos que este trabajo consolide la generación de conocimiento en las instituciones del Estado frente a los ciberdelitos, hoy tan necesaria ante el contexto pandémico.

FÉLIX INOCENTE CHERO MEDINA
Ministro de Justicia y Derechos Humanos

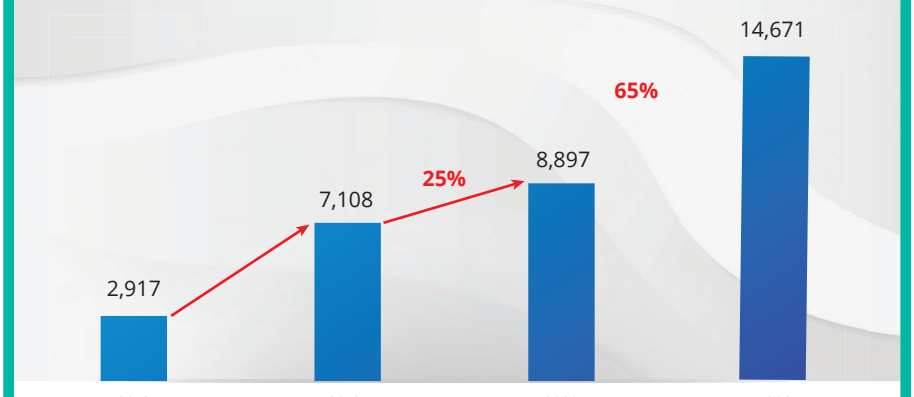
ÍNDICE


RESUMEN EJECUTIVO
14,671 denuncias por delitos informáticos (PNP) en el año 2021, lo que significa 65% más que el año anterior (8 897 denuncias en 2020).
5% más de denuncias (PNP) por delitos informáticos durante el primer semestre del año 2021, respecto de la segunda mitad del mismo año
437 denuncias (MPFN) por delitos contra datos y sistemas informáticos en el año 2020, mientras que en el año 2021 se registraron 581 por el mismo tipo de delitos (33% más).
92.9% de denuncias adicionales (MPFN) en torno a delitos informáticos, entre los años 2020 y 2021 (de 9 642 pasamos a 18 596)
59.2% más de denuncias (MPFN) por delitos informáticos contra la indemnidad y libertad sexual, entre los años 2020 y 2021 (de 76 a 121 denuncias sentadas).
38.8% más de denuncias (MPFN) por delitos informáticos contra la intimidad y el secreto de las comunicaciones, solo entre el 2020 y 2021 (345 casos a 479 casos).
356.9% denuncias (MPFN) aumentaron entre los años 2020 y 2021, en torno a delitos informáticos contra la fe pública (751 a 3 431 casos)
11,768 denuncias (MPFN) por delitos informáticos contra el patrimonio en el 2021 (117.1% más que en el 2020 (5 420).

CIBERDELITOS EN EL PERÚ

Con base en información estadística oficial proporcionada por las fuentes de registros de la Policía Nacional del Perú, así como del Ministerio Público - Fiscalía de la Nación, encontramos un conjunto de indicadores que nos permiten aproximarnos hacia la comprensión de los ciberdelitos durante los últimos años.

GRÁFICO 01 » Variación porcentual de denuncias por delitos informáticos registrados en la PNP, 2018-2021



Tal como podemos observar (ver gráfico 1), en los últimos cuatro años hemos pasado de acumular 2 mil 917 denuncias en el año 2018, hasta llegar a 14 mil 671 denuncias en el año 2021, es decir, la cifra del último año es cinco veces mayor que la registrada al inicio del periodo. Así es posible distinguir que se ha producido un incremento sostenido de las denuncias entre los años 2018 al 2021. Comparando los valores registrados año a año, en el gráfico se visualiza un incremento del 144% en el año 2019, en comparación con el año 2018; en el 2020 el incremento corresponde al 25%, en comparación con el año 2019; y, en el año 2021, el aumento es del 65% en comparación con el 2020.

Ampliando la mirada hacia el año 2021, y buscando ahondar en la incidencia de los ciberdelitos de acuerdo al territorio (ver cuadro 1), encontramos que Lima encabeza la lista de los departamentos que registran la mayor cantidad de denuncias por ciberdelitos (delitos informáticos) durante los años 2019,

2020 y 2021. Llama especialmente la atención este crecimiento sostenido de las denuncias por ciberdelitos durante los tres años en mención, y de forma especial, el crecimiento experimentado hacia el último año (2021), en el que aumentaron las denuncias en todos los territorios, pero especialmente en el departamento de Lima con un total de 7 mil 324 casos señalados ante las autoridades policiales. Así también, es importante volver a destacar el crecimiento de las denuncias a nivel nacional desde el 2020 hacia el 2021, en el que pasamos de 25% a 65% más denuncias por este tipo de ilícitos.

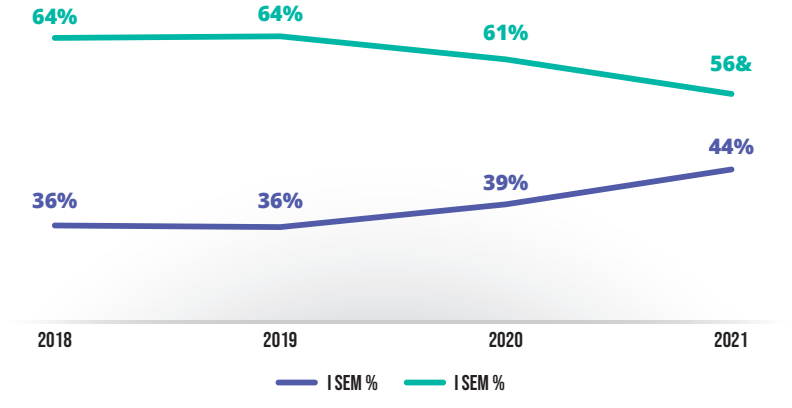
CUADRO 01 » Número de denuncias por delitos informáticos registrados en la PNP según departamento, 2019-2021

Lima	4,139	4,527	7,324
Arequipa	496	645	877
La Libertad	483	602	835
Callao	341	510	774
Lambayeque	306	466	719
Piura	223	325	576
Tacna	83	126	426
Ancash	193	285	405
Huánuco	80	232	358
Junín	58	162	338
Cusco	178	225	308
Ica	115	142	236
San Martín	31	73	189
Ucayali	47	85	187
Moquegua	56	83	184
Loreto	78	92	167
Puno	19	49	163
Ayacucho	36	42	142
Cajamarca	26	57	120
Amazonas	45	49	101
Apurímac	21	46	66
Pasco	9	34	62
Huancavelica	20	15	51
Tumbes	16	18	34
Madre de Dios	9	7	29
Total	7,108	8,897	14,671
Variación porcentual		25%	65%

Fuente: PNP, SIDPOL, información preliminar
Elaboración: Observatorio Nacional de Política Criminal INDAGA

De forma complementaria, respecto de las variaciones en las denuncias desde una mirada semestral, encontramos que, durante la segunda mitad de cada año, entre el 2018 y el 2021, se registra una mayor cantidad de denuncias por delitos informáticos. A pesar del descenso que se manifiesta desde el año 2020, se observa que la variación se eleva durante la primera mitad del año, reduciéndose la distancia entre ambos semestres, tal como se puede apreciar (ver gráfico 2).

GRÁFICO 02 » Denuncias por delitos informáticos según semestre registradas en la PNP, 2018-2021



Fuente: PNP, SIDPOL, información preliminar
Elaboración: Observatorio Nacional de Política Criminal INDAGA

Respecto de las modalidades de ciberdelitos más recurrentes durante el periodo 2019-2021, de acuerdo con los registros de denuncias de la Policía Nacional, encontramos que los delitos en torno a la comisión de fraude informático son los que más afectan a los ciudadanos y ciudadanas, los que han reunido un total de 6 mil 946 denuncias en el año 2020, llegando hasta 10 mil 924 para el siguiente año. En un segundo lugar, con un crecimiento que no pasa desapercibido, la modalidad de suplantación de identidad pasó de 935 denuncias en el 2020, hasta un total de 2 mil 666 denuncias para el 2021 (ver cuadro 2).

CUADRO 02 » Número de denuncias según Ley de delitos informáticos, modificada por Ley 30171, por modalidad 2019, 2020 y 2021

Modalidad	2019	2020	2021
Fraude informático *	5,878	6,946	10,924
Suplantación de identidad *	462	935	2,666
Abuso de mecanismos y dispositivos informáticos	258	572	538
Atentado a la integridad de datos informáticos *	255	164	226
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos *	72	82	98
Atentado a la integridad de sistemas informáticos *	65	72	86
Interceptación de datos informáticos *	83	75	69
Acceso ilícito *	35	51	64
Total	**7,108**	**8,897**	**14,671**

Nota técnica: *….

Fuente: SIDPOL, información preliminar
Elaboración: Observatorio Nacional de Política Criminal INDAGA

De modo más acotado al año 2021, y en una lógica de caracterizar los ciberdelitos durante el último año, podríamos decir que 3 de cada 4 ciberdelitos en el Perú están relacionados a la comisión de fraudes informáticos (ver cuadro 3).

CUADRO 03 » Denuncias según Ley de delitos informáticos, modificada por Ley 30171, por modalidad 2021

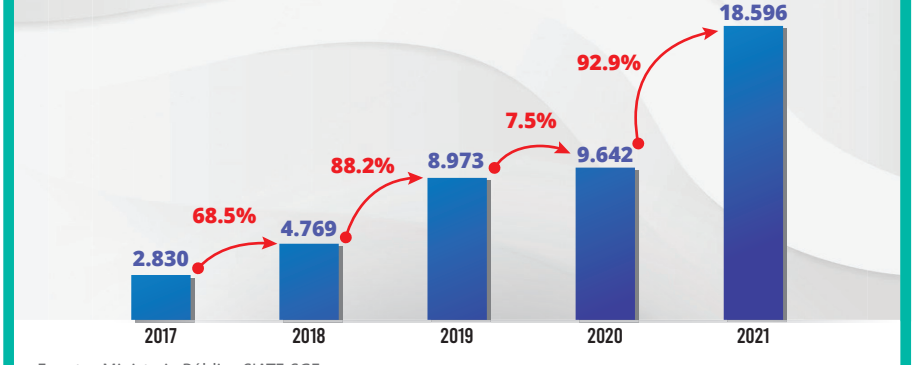
Modalidad	2021	%
Fraude informático *	10,924	74.5%
Suplantación de identidad *	2,666	18.2%
Abuso de mecanismos y dispositivos informáticos	538	3.7%
Atentado a la integridad de datos informáticos *	226	1.5%
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos *	98	0.7%
Atentado a la integridad de sistemas informáticos *	86	0.6%
Interceptación de datos informáticos *	69	0.5%
Acceso ilícito *	64	0.4%
Total	**14,671**	**100%**

Nota técnica: *….

Fuente: SIDPOL, información preliminar
Elaboración: Observatorio Nacional de Política Criminal INDAGA

Complementando la información, desde la perspectiva de las denuncias registradas en el Ministerio Público (ver gráfico 3), encontramos que, durante los últimos cinco años, entre el 2017 y 2021, se observa que se pasó de 2 mil 830 denuncias en el inicio de período a 18 mil 596, al término del mismo. Estos delitos se sextuplicaron en el Ministerio Público. Es importante precisar que en el período 2020-2021, se registró una variación porcentual del 92%. En este incremento confluyen diferentes factores, dentro de los que resaltaría la implementación de la unidad especializa en ciberdelincuencia en este organismo autónomo.

GRÁFICO 03 » Delitos informáticos denunciados en el Ministerio Público a nivel nacional, 2017-2021



Fuente: Ministerio Público SIATF-SGF
Elaboración: Observatorio Nacional de Política Criminal INDAGA

Desde una mirada por tipo de delitos, vemos que para el año 2021 (ver cuadro 4) los delitos informáticos de acceso ilícito concentran gran parte de estos (386 de un total de 581). Seguidamente, están los atentados contra la integridad de datos informáticos (82) y finalmente los ataques a la integridad de sistemas informáticos (20).

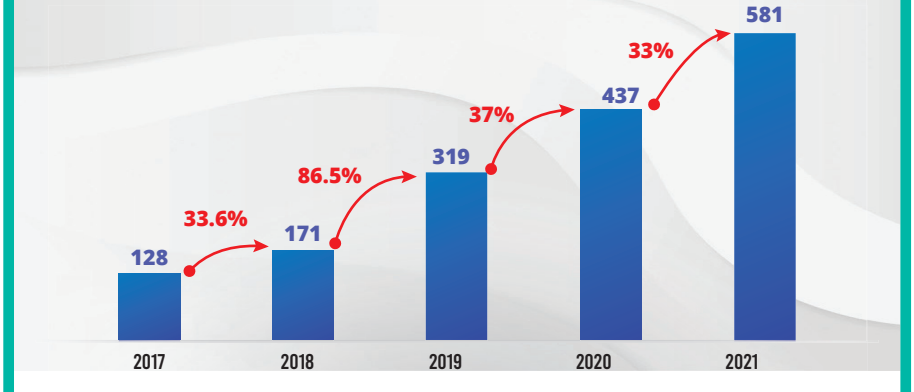
CUADRO 04 » Delitos contra datos y sistemas informáticos denunciados en el Ministerio Público a nivel nacional según tipo de delito, 2017-2021

Delito / Artículo	2017	2018	2019	2020	2021
Art.2: Acceso ilícito	53	70	139	209	386
Art.3: Atentado contra la integridad de datos informáticos	25	28	56	121	82
Art.4: Atentado contra la integridad de sistemas informáticos	2	11	11	11	20
S/A: Sin especificar	48	62	113	96	93
Total	**128**	**171**	**319**	**437**	**581**

Fuente: Ministerio Público SIATF-SGF
Elaboración: Observatorio Nacional de Política Criminal INDAGA

Adicionalmente, sobre los casos de delitos cometidos contra los datos y sistemas informáticos, encontramos que estos también muestran un importante crecimiento, entre el 2019 y el 2020, presentando un aumento de hasta en 37%; mientras que del 2020 al 2021, incrementaron en 33%. Por tanto, podríamos inferir que existe una tendencia creciente que podría mantenerse para los próximos años.

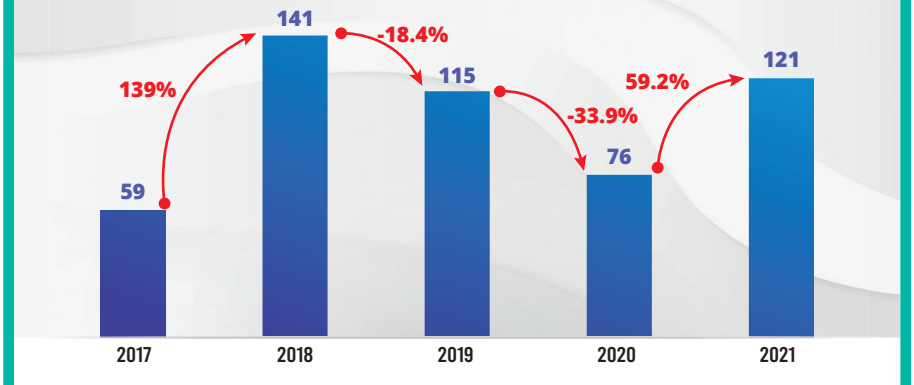
GRÁFICO 04 » Variación porcentual de delitos contra datos y sistemas informáticos denunciados en el Ministerio Público a nivel nacional, 2017-2021



Fuente: Ministerio Público SIATF-SGF
Elaboración: Observatorio Nacional de Política Criminal INDAGA

Por otro lado, en cuanto a los ciberdelitos contra la indemnidad y libertad sexuales a través de medios virtuales recurrentes, encontramos que hay una variación un tanto inestable, con aumentos y descensos claramente diferenciados. De este modo, vemos que entre los años 2020 y 2021 se produce un aumento de hasta en 59.2% de casos, luego de que entre el 2019 y 2020 se notó un descenso de hasta 33.9% (ver gráfico 5).

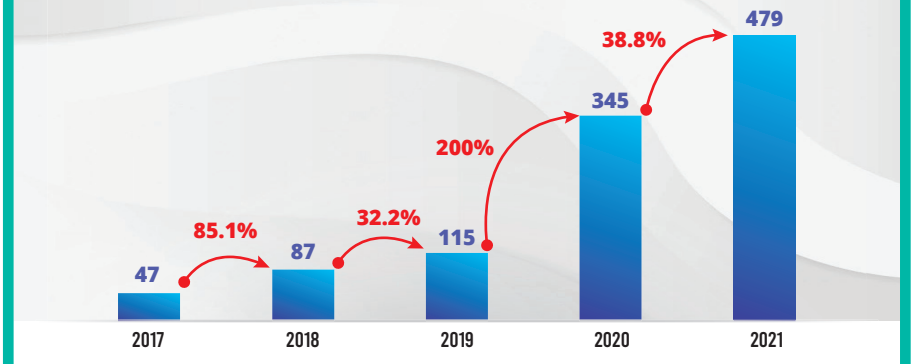
GRÁFICO 05 Variación porcentual de delitos informáticos contra la indemnidad y libertad sexuales denunciados en el Ministerio Público a nivel nacional, 2017-2021



Fuente: Ministerio Público SIATF-SGF
Elaboración: Observatorio Nacional de Política Criminal INDAGA

En cuanto a los delitos cometidos mediante el uso de estas tecnologías y/o espacios virtuales, afectando la intimidad y el secreto de las comunicaciones, encontramos que sí existe un notable y sostenido aumento, pasando de 47 delitos en el año 2017 hasta 479 en el año 2021; siendo que entre el 2020 y el 2021, el aumento fue de hasta un 38.8%; aspecto que llama especialmente la atención, teniendo en cuenta que en el año 2020 se registró un aumento del 200% de los casos en comparación con el año 2019 (ver gráfico 6).

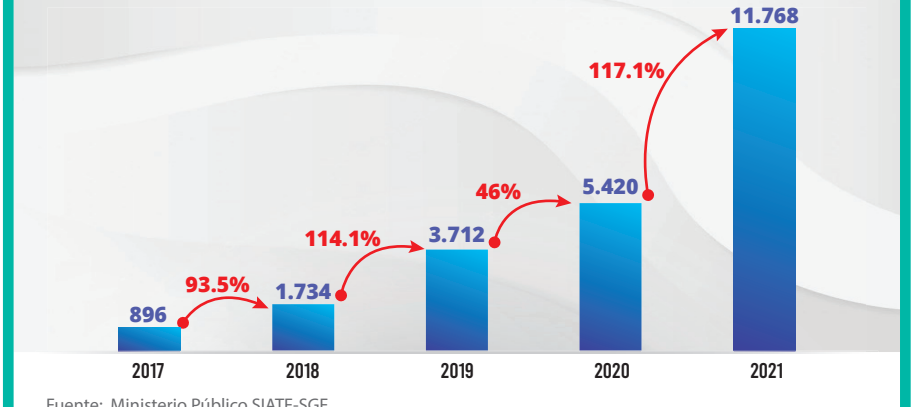
GRÁFICO 06 Variación porcentual de delitos informáticos contra la intimidad y el secreto de las comunicaciones denunciados en el Ministerio Público a nivel nacional, 2017-2021



Fuente: Ministerio Público SIATF-SGF
Elaboración: Observatorio Nacional de Política Criminal INDAGA

Respecto de los delitos contra el patrimonio realizados con el uso de las TIC y/o medios virtuales, también notamos un aumento importante, pasando de 896 delitos en el 2017 hasta 11 mil 768, en el 2021. Solo en el último año, se presentó una variación del 117.1% respecto del año anterior, a pesar de que se notaba un importante crecimiento sostenido en el tiempo, tomando en cuenta el contexto pandémico desde el año 2019 este dato trastoca lo esperado (ver gráfico 7).

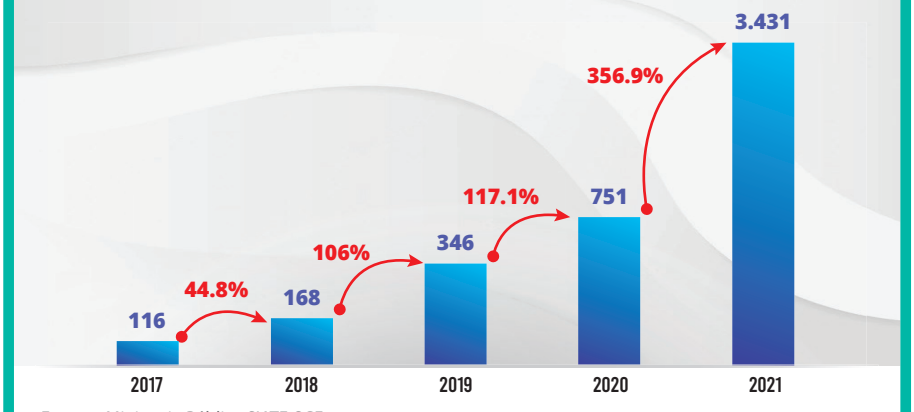
GRÁFICO 07 Variación porcentual de delitos informáticos contra el patrimonio denunciados en el Ministerio Público a nivel nacional, 2017-2021



Fuente: Ministerio Público SIATF-SGF
Elaboración: Observatorio Nacional de Política Criminal INDAGA

Finalmente, sobre los delitos informáticos contra la fe pública vemos que también se pasó de 116 casos en el 2017 hasta 3 mil 431 en el año 2021 (ver gráfico 8).

GRÁFICO 08 » Variación porcentual de delitos informáticos contra la fe pública denunciados en el Ministerio Público a nivel nacional, 2017-2021



Fuente: Ministerio Público SIATF-SGF
Elaboración: Observatorio Nacional de Política Criminal INDAGA

COOPERACIÓN JURÍDICA INTERNACIONAL

La cooperación internacional se encuentra regulada en el Libro VII del Código Procesal Penal, normativa vigente a nivel nacional desde el año 2006, y que a través del artículo 512 del Código Procesal Penal establece que la Autoridad Central recae en la Fiscalía de la Nación.

Mediante la Resolución N°124-2006-MP-FN, del 3 de febrero de 2006, se creó la Oficina de Cooperación Jurídica Internacional y Extradiciones (OCJIE) con el objeto de que esta unidad orgánica se encargue de centralizar la coordinación y ejecución de las acciones reguladas en el Libro Séptimo del Nuevo Código Procesal Penal, funciones que fueron modificadas mediante el Decreto Legislativo 1281, de fecha 29 de diciembre de 2016.

Dentro de las funciones que realiza esta oficina, se encuentran la de gestionar y realizar el seguimiento de las solicitudes de cooperación jurídica internacional, las que son libradas por los jueces y fiscales a nivel nacional. Al respecto, es de precisar que el reconocimiento de las solicitudes de asistencias judiciales internacionales se encuentra vigente en el artículo

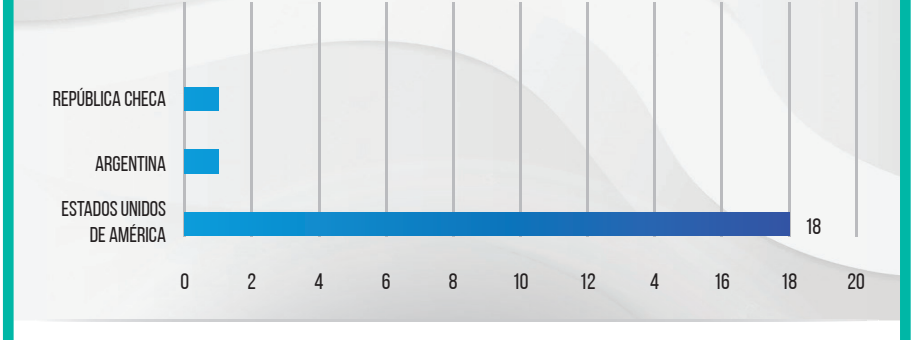
528 al 537 del CPP; entre los cuales se encuentra el facilitar información y elementos de prueba, remisión de documentos e informes, recepción de declaraciones, entre otros.

Es en el marco de la ciberdelincuencia que se hace de conocimiento que desde diciembre del año 2019 entró en vigencia en nuestro país, el Convenio sobre la Ciberdelincuencia (también conocido como Convenio de Budapest), siendo un instrumento jurídico específico en dicha materia, el cual se encuentra suscrito por 66 Estados Parte, y en cuyo capítulo III se encuentra regulada la temática referente a la cooperación internacional, la que comprende a la asistencia mutua, la extradición, la información espontánea y la Red 24/7.

Asistencia judiciales internacionales

Durante el año 2021 se tramitaron 20 solicitudes de asistencia judicial internacional, activos dirigidos a los países de Estados Unidos de América, Argentina y República Checa.

GRÁFICO 09 » Data estadística de pedidos activos de asistencia judicial internacional al amparo del Convenio Budapest 2021



Fuente: Unidad de Cooperación Judicial Internacional y Extradiciones
Elaboración: Ministerio Público – Fiscalía de la Nación

Asimismo, recibieron 02 pedidos pasivos provenientes de República Dominicana.

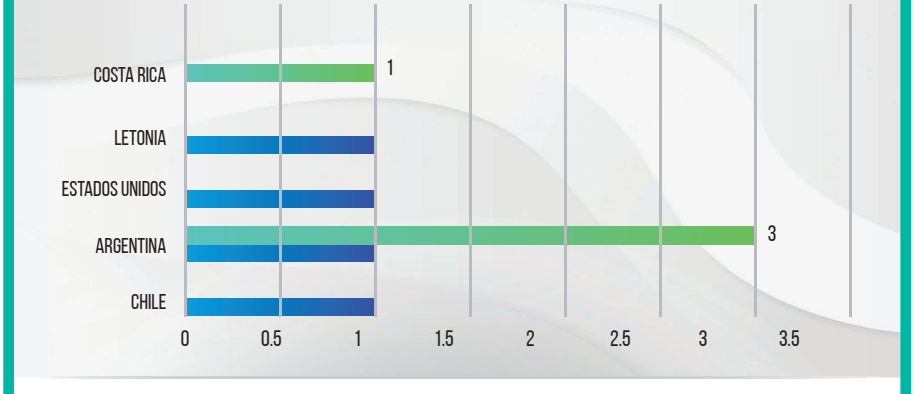
En el transcurso del año 2022 se han librado 48 solicitudes de asistencia judicial internacional activadas dirigidos alos países de Estados Unidos de América, República Francesa, República de Malta, Reino de Marruecos,

República Argentina, Reino de los Países Bajos, Mancomunidad de Australia y República de Polonia.

Transmisiones espontáneas de información

Durante el año 2021 se tramitaron 4 pedidos, derivando información a los países de Chile, Argentina, Estados Unidos de América, Letonia y Costa Rica; con la finalidad de que dicha información contribuya para emprender investigaciones o coadyuvar con las ya existentes en dichos países. Asimismo, se recibieron 3 pedidos de Argentina y 1 de Costa Rica.

GRÁFICO 10



Fuente: Unidad de Cooperación Judicial Internacional y Extradiciones
Elaboración: Ministerio Público – Fiscalía de la Nación

Adicionalmente, durante el año 2022, se vienen tramitando 2 pedidos pasivos provenientes de Argentina.

Red 24/7 del Convenio sobre la Ciberdelincuencia

Los puntos de contacto de la Red 24/7 del Convenio sobre la Ciberdelincuencia recaen en la Oficina de Cooperación Judicial Internacional y Extradiciones, en mérito a lo dispuesto mediante Resolución de Fiscalía de la Nación N°920-2020-MP-FN, de fecha 25 de agosto de 2020.

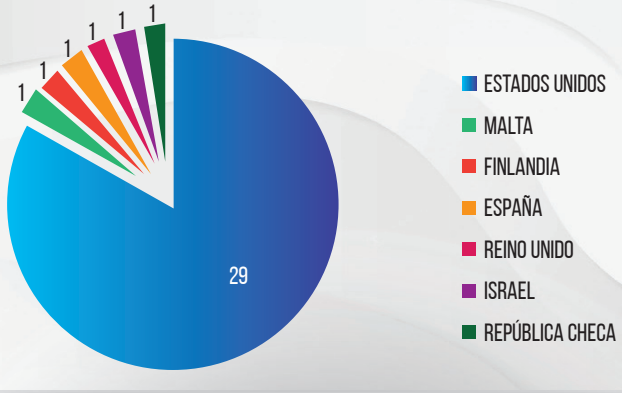
En mérito a las funciones conferidas en virtud del artículo 35 del referido Convenio, los puntos de contacto deben brindar asistencia para facilitar las siguientes medidas:

- Brindar asesoramiento técnico
- Conservación de datos
- Obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos, es en el marco de dichas funciones que se han realizado las siguientes atenciones relativas a las conservaciones de datos:

Pedidos activos

Durante el año 2021 se tramitaron 36 pedidos de conservación activos, los cuales constituyeron requerimientos cursados a los proveedores de servicios como Google, Amazon, Apple, entre otros; para lo cual contó con la cooperación de los países: Estados Unidos, Malta, Singapur, Finlandia, España, Israel, República Checa, entre otros, quienes atendieron con prontitud este tipo de requerimientos.

GRÁFICO 11 » Pedidos de conservación de datos activos de la Red 24/7 del Convenio de Budapest Año 2021



Fuente: Ministerio Público SIATF-SGF
Elaboración: Observatorio Nacional de Política Criminal INDAGA

Pedidos pasivos

Durante el año 2021 se recibieron 02 pedidos pasivos de conservación de datos provenientes de Argentina y de República Checa.

Asimismo, en virtud de lo estipulado en el literal c, numero 1 del citado artículo 35, en los que se establece que la asistencia comprenderá toda acción para la obtención de información, se tramitaron 02 casos de entrega de información

en el que el punto de contacto del Reino de España, brindó de manera célere información sobre compras en Edreams lo que ha contribuido en ambos casos al avance de investigaciones por delito de Fraude informático.

Durante el año 2022, se han tramitado 20 pedidos de conservación de datos dirigidos a los países de la República Francesa, Estados Unidos de América, República de Chipre y la República de Singapur.

Del mismo modo, se tramitaron 02 casos de entrega de información, dichos pedidos fueron remitidos a los puntos de contacto de República Checa y de la República Federal de Alemania, se obtuvo una respuesta positiva en el primer caso, en el cual se obtuvo evidencia electrónica de utilidad para una investigación por los delitos de violación sexual en persona con incapacidad de resistir y violación sexual de menor de edad, delitos en los cuales se hizo uso de una plataforma de videos con contenido pornográfico.

RECOMENDACIONES **PARA PREVENIR LOS CIBERDELITOS**

RECOMENDACIONES PARA PREVENIR LOS CIBERDELITOS

Tomando en cuenta los elementos de información recabados por el Observatorio Nacional de Política Criminal - INDAGA en torno al estado de los ciberdelitos en nuestro país, planteamos un conjunto importante de recomendaciones que puedan resultar de utilidad para prevenir los ciberdelitos y reducir las potenciales víctimas. En ese sentido, alcanzamos varias recomendaciones, distinguiendo las de carácter general, para luego dar paso a las agrupadas por tipo de población vulnerable, en atención a las particularidades de los usuarios y usuarias respecto de las tecnologías de la información y del conocimiento.

Protección de datos personales

Para que no se comprometa tu privacidad ni utilice información sobre ella en tu contra, generándote problemas o conflictos de diversa índole, es importante poder tener en cuenta lo siguiente:

1. Actualizar regularmente el sistema operativo y el software instalado de todos los dispositivos que empleas regularmente para conectarte a internet.

2. Instalar un antivirus y actualizarlo con frecuencia. Analizar con el antivirus todos los archivos nuevos, especialmente aquellos que se descargan de internet.

3. Instalar un firewall con el fin de restringir accesos no autorizados de internet.

4. Prestar atención a la política de servicios y de privacidad de las aplicaciones más sensibles que suelan utilizar en internet, con el objetivo de resguardar información personal.

5. Desactivar la geolocalización cuando no la uses.

6. Utilizar contraseñas seguras, que estén compuestas por ocho caracteres como mínimo, que puedan combinar distintos tipos de letras, entre mayúsculas y minúsculas, además de números y símbolos. No es recomendable emplear la misma contraseña para todos los aplicativos.

7. Navegar por páginas web seguras y de confianza, especialmente si se realizan compras online o se facilita información confidencial. Para identificarlas, debes observar que cumplan con dos requisitos:

- La URL debe comenzar con https:// en lugar de http.
- En la barra del navegador debe aparecer un ícono de un candado cerrado. Esto es una señal de que se trata de un sitio web seguro.

8. No abrir mensajes de correo de remitentes desconocidos o señalados por el correo como "sospechoso".

9. No confiar en correos electrónicos en los que las entidades bancarias o sitios de venta solicitan las contraseñas.

10. No reenviar mensajes de correo con contenidos dudosos y/o de aquellos que solicitan ser reenviados a sus contactos (cadenas). Este tipo de mensajes son creados con el objetivo de captar direcciones de correo de usuarios a los que posteriormente se les remiten mensajes con virus o spam.

11. Evitar compartir información personal y/o familiar a desconocidos a través de internet.

12. Procurar no dar información de terceros sin su consentimiento.

13. Confirmar la identidad de quienes te envían alguna solicitud de amistad a través de las redes sociales.

1 Seguridad de niños y niñas

14. Tratar de estar al tanto o informarse –a través de medios serios y confiables– sobre las principales aplicaciones o sitios web favoritos de los niños y niñas de tu hogar, con el objetivo de conocer sobre los contenidos que ofrecen.

15. Encontrar la manera de establecer un lazo de confianza que te permita saber sobre aquellas personas con las que alguna vez pudieron iniciar una conversación en internet.

16. Establecer prohibiciones sobre el uso de dispositivos con acceso a internet puede ser contraproducente y afectar la confianza generada con los niños y niñas en el hogar. En lugar de ello, buscar alternativas de acompañamiento durante la navegación o el uso de estos dispositivos, y así informar más sobre los contenidos digitales que consumen.

17. Resulta fundamental generar buenos hábitos de consumo de dispositivos con acceso a internet, estableciendo reglas y horarios que deben de cumplirse como parte del entretenimiento que es indispensable al interior de casa.

18. Promover el acceso a plataformas de videos y juegos en línea, en espacios comunes de la casa, evitando que esta actividad se traslade a lugares que dificulten la supervisión, haciéndolos más vulnerables.

19. Consultar al proveedor de internet o a la asistencia al cliente, sobre la activación de las herramientas de control parental que ayuden a filtrar los contenidos digitales inapropiados para niños y niñas.

20. Buscar recursos didácticos y sencillos que faciliten la explicación sobre los riesgos que un niño o una niña puede tener cuando accede sin precauciones al internet, brindando especial énfasis a determinadas herramientas tales como las cámaras web o los teléfonos celulares.

21. Cuando se produzcan las primeras experiencias de acercamiento de los niños hacia las redes sociales, tomar medidas sobre las configuraciones de privacidad de las cuentas, evitando informar más de lo necesario hacia el exterior.

22. Apoyar a los niños y niñas a que extiendan lazos sanos de comunicación cuando usen redes sociales, identificando a sus familiares y amigos de confianza, con la finalidad de identificar con quiénes se comunican cuando notan riesgos o amenazas en la web.

23. Prestar mucha atención hacia los cambios repentinos en el ánimo y los estados de conducta de los niños y niñas, e identificar su relación con las horas de acceso a internet.

2 Bienestar de adolescentes y jóvenes

24. Al igual que con los niños, es vital mantener adecuadas relaciones de confianza que permitan informarse sobre las principales aplicaciones o plataformas de información y de entretenimiento que frecuentan cuando se vinculan a dispositivos con acceso a internet.

25. Buscar recursos amigables que faciliten la sensibilización sobre los riesgos que corren al compartir o intercambiar elementos con contenido explícito (sobre sexo y violencia, principalmente) a través de las redes sociales.

26. Monitorear la actividad en redes sociales y sobre las personas que interactúan con ellos o ellas, tratando de identificar perfiles falsos o identidades sospechosas, sin que ello afecte su privacidad.

27. Buscar momentos propicios para conversar sobre las últimas incidencias en las redes sociales, permitiendo que ellos o ellas se manifiesten sobre aquellos aspectos que les llaman la atención o que les preocupan, con el objetivo de brindar la debida orientación de seguridad.

28. Promover las prácticas empáticas de uso e interacción en las redes sociales, tratando de incentivar la solidaridad y la comunicación emocional ante casos de acoso cibernético o de ciberbullying.

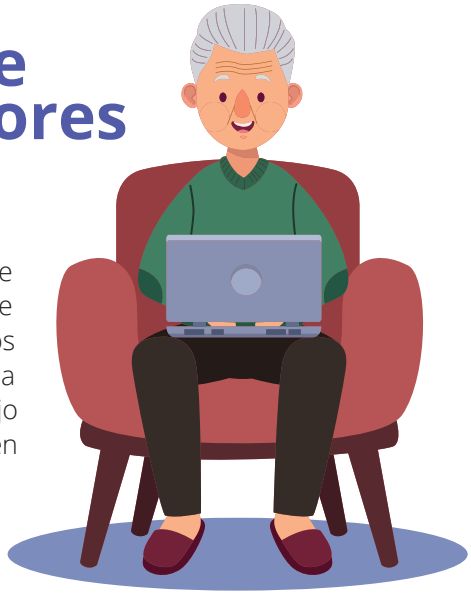
29. Propiciar el diálogo fluido y constante que ayude a detectar cambios en el estado emocional y anímico de los y las adolescentes y jóvenes, observando si tiene conexión con casos de ciberacoso o de ciberbullying.

30. Si comparten computadoras o laptops con información personal (financiera o de trabajo), alertar a los y las adolescentes en casa sobre los peligros de la navegación en la web sin precauciones, realizando hincapié en los enlaces falsos o correos hechizos que podrían generar sustracción de dinero de cuentas bancarias o información laboral.
Ayudar a reconocer contenidos engañosos (enlaces y correos de riesgo) que podrían encontrarse en sitios de descarga de software, páginas de compra de artículos o de servicios de alimentos por internet.

32. Brindar información y consejos sobre cómo evitar problemas y amenazas a la seguridad personal ante casos en los que se comparten accesos a redes de internet inalámbrico (wifi), así como de plataformas de videos y películas en casa.

33. Dialogar y sensibilizar a las y los adolescentes sobre los riesgos de establecer comunicación –a través de redes sociales– con personas o terceros desconocidos, dirigiéndose hacia los temas de acceso a drogas u otros elementos peligrosos (armas, pornografía infantil, principalmente).

3 Resguardo de adultos mayores



34. Por tratarse de personas que temporalmente pudieron haberse distanciado del manejo intuitivo de los dispositivos electrónicos con acceso a internet, es indispensable que el manejo que ellos o ellas puedan realizar en casa, sea asistido y/o acompañado por adultos o jóvenes que cuenten con mayor conocimiento sobre los aspectos de seguridad en internet.

35. Mediante recursos o métodos bastante sencillos, tratar de ayudar a reconocer los distintos tipos de enlaces o correos falsos que pueden afectar a la seguridad de la información en el computador o en el celular.

36. Organizar accesos directos y carpetas que les faciliten el ingreso seguro a las webs y plataformas de comunicación y entretenimiento que suelen usar desde el computador, tablet o celular.

37. Encontrar maneras de familiarizarlos con la reacción a las notificaciones o los avisos emergentes de los antivirus o bloqueadores de contenido malicioso en las páginas web, con el objetivo de que puedan proteger la información alojada en los aparatos digitales que usan regularmente.

38. Practicar con ellos y ellas las diferentes formas que existen para reconocer o confirmar noticias falsas que circulan en internet o a través de redes sociales, con especial énfasis en aquellas que puedan guardar relación con la pandemia y los efectos generados por el coronavirus en nuestro país.

Prestar atención y apoyo cuando requieran acceder a webs o aplicaciones digitales de entrega de medicamentos o comida por delivery, tratando de aproximarlos al manejo seguro de estos instrumentos.

4 Defensa de pequeños emprendimientos

Finalmente, las siguientes indicaciones que pasamos a enumerar, buscan colaborar con los pequeños empresarios en un contexto de apoyo al funcionamiento de sus emprendimientos, teniendo en cuenta el contexto de reactivación económica post pandemia, y que supone volver a poner en marcha determinados servicios y comercios, los que a su vez encontrarán en los dispositivos con acceso a internet, un importante recurso para desarrollarse.

40. Establecer protocolos de protección y responsabilidades sobre el manejo de los datos sensibles que puedan almacenar en las computadoras o laptops de trabajo, con el objetivo de cuidar la información de los y las clientes, de los y las proveedores y del presupuesto.

41. Invertir en software de fábrica es invertir en la seguridad de tu negocio. Evita usar software de origen sospechoso para los equipos electrónicos de tu negocio, y contactar a un proveedor de programas informáticos de confianza.

42. Antes de contratar servicios de mantenimiento o de optimización de las computadoras de tu negocio, evalúa los comentarios y calificaciones que otros clientes pudieron haber realizado en redes sociales sobre ese proveedor.

43. Asegurarse de contar con los sistemas de VPN (Red Privada Virtual) y de antivirus confiable antes de realizar intercambios de información o de efectuar transacciones a través de la banca por internet, o de hacer importaciones desde páginas de ventas virtuales.

44. Generar planes de respaldo periódico de tus datos en discos externos que solo puedan ser manipulados por personas de total confianza en tu negocio, y establece revisiones continuas con el fin de evaluar la forma en la que se organizan los datos indispensables para el funcionamiento del negocio.

45. Distribuir el dinero del negocio en diferentes cuentas bancarias, y evitar así que ante un ataque cibernético se pueda ver afectado todo el presupuesto que sostiene el emprendimiento.

46. Realizar cambios inopinados en las contraseñas de los sistemas de seguridad que almacenan la información más sensible, así como en el acceso a las cuentas desde donde se realizan movimientos o transacciones financieras virtuales.

47. Realizar acciones de sensibilización entre los trabajadores y empleados del negocio sobre el manejo de la información personal de sus clientes, con especial atención al grupo de mujeres, con el objetivo de evitar el ciberacoso.

48. Capacitarse en temas de seguridad virtual durante la actual coyuntura, así como destinar parte de su tiempo para informarse mediante videos y tutoriales gratuitos sobre medidas de protección contra los ciberdelitos.

CIBERDELINCUENCIA

REPORTE DE INFORMACIÓN ESTADÍSTICA Y RECOMENDACIONES PARA LA PREVENCIÓN

PERÚ Ministerio de Justicia y Derechos Humanos

Siempre con el pueblo

BICENTENARIO DEL PERÚ 2021 - 2024