

ANÁLISIS DEL CIBERDELITO EN CENTROAMÉRICA Y REPÚBLICA DOMINICANA



infoSEGURA

Programa de las Naciones Unidas para el Desarrollo

El PNUD se asocia con personas de todos los niveles de la sociedad para ayudar a construir naciones que puedan resistir las crisis e impulsar y mantener el tipo de crecimiento que mejora la calidad de vida de todos. En el terreno, en más de 170 países y territorios, ofrecemos una perspectiva global y conocimiento local para ayudar a empoderar vidas y construir naciones resilientes.

Pueden obtener más información en www.undp.org o seguirnos en @PNUD

© 2022 PNUD y USAID. Todos los derechos reservados.

Programa de las Naciones Unidas para el Desarrollo

Centro Regional del PNUD en América Latina, Edificio 220, Ciudad del Saber.

Ciudad de Panamá, Panamá.

Cita recomendada: PNUD. (2022). Análisis del ciberdelito en Centroamérica y República Dominicana

Centro Regional del RBLAC/PNUD en Panamá

José Cruz-Osorio

Gerente del Centro Regional del PNUD para América Latina y el Caribe

Jairo Acuña-Alfaro

Líder de Equipo de Gobernabilidad y Paz del PNUD en América Latina y el Caribe

Proyecto Regional PNUD-Infosegura

Marcela Smutt

Coordinadora regional del proyecto PNUD Infosegura

Juan Pablo Gordillo

Coordinador adjunto del proyecto PNUD Infosegura

Elvia Tapia-Santamaría

Especialista en gestión del conocimiento e investigaciones PNUD Infosegura

Coordinación del estudio

Marcela Smutt

Juan Pablo Gordillo

Investigación

Manuel Sánchez Masferrer

Revisión editorial

Tania Góchez

Diseño y diagramación

Betzy Flores

Oficinas del PNUD

El documento fue posible gracias al trabajo y revisión de los equipos de nuestras oficinas del PNUD en los países en los que opera el Proyecto Regional Infosegura, y agradecemos a Laura Rivera y Daniel Carsana en El Salvador; Claudia Saravia, Eduardo Díaz y Silvia Mendoza en Guatemala; Tania Martínez y Carmela Lanza en Honduras; Randall Brenes, Gerald Mora y Karol Sánchez en Costa Rica; Marilyn Lee en Belice; y Pura Hernández y María del Mar Pérez en República Dominicana.



La elaboración de este documento ha sido posible gracias al apoyo brindado por el Gobierno de los Estados Unidos por medio de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID, por sus siglas en inglés) y a la asistencia técnica del Programa de las Naciones Unidas para el Desarrollo para América Latina y el Caribe (PNUD).

Las opiniones y los puntos de vista que se presentan en este documento son exclusiva responsabilidad de sus autores y no reflejan necesariamente las opiniones ni los puntos de vista de las agencias y los organismos que apoyaron la realización de esta publicación, ni tampoco aquellos de los países miembros de las Naciones Unidas.

© 2022 PNUD y USAID. Todos los derechos reservados.

Pandemia y ciberdelito

- El auge del trabajo remoto ha aumentado la vulnerabilidad al crimen informático.
- Cada vez más dispositivos están conectados a Internet, lo que crea nuevas vulnerabilidades.
- La pandemia aceleró las tendencias al teletrabajo y a realizar cada vez más actividades de manera virtual.
- El resultado es un aumento de amenazas conocidas y el surgimiento de otras nuevas.
- La región suma el reto de poner al día sus capacidades para enfrentar el ciberdelito, es decir, hacer frente a estas nuevas amenazas.
- El reto es cerrar las brechas de conocimientos sobre seguridad y de institucionalidad, para prevenir, detectar, bloquear y perseguir los ciberataques.

Cada año, la incidencia de los delitos informáticos aumenta. Sin embargo, 2020 marcó un punto de quiebre en la tendencia histórica. Las restricciones a la movilidad asociadas a la pandemia de COVID-19 volcaron a las personas al teletrabajo y a las actividades a través de Internet, y junto con la ubicuidad de los dispositivos conectados, constituyeron un botín irresistible para atacantes y delincuentes informáticos.

Aunque no es posible obtener cifras exactas de los ataques y delitos cometidos, debido a que gran parte de ellos no se reporta, se puede obtener una idea de su tendencia e importancia mediante la combinación de datos de diferentes fuentes y la proyección de tendencias, de acuerdo con las características y condiciones de cada país de la región de Centroamérica y República Dominicana.

Este reporte sondea las tendencias y los datos disponibles de fuentes oficiales, como los reportes de incidencia de delitos informáticos en Costa Rica y El Salvador, y también utiliza información de la encuesta conducida en cinco países de la región a través del empleo del cuestionario del módulo estandarizado de ciberdelincuencia de la Iniciativa para la encuesta de victimización delictiva en Latinoamérica y el Caribe 2020, e información disponible de tendencias globales y latinoamericanas.

El panorama que se presentó para 2021 combina la creciente incidencia del ciberdelito con marcos legales e institucionales que deben superar retos importantes para hacer frente a la amenaza que representa esta actividad criminal.

Índice

Introducción 1

1. Tendencias globales..... 2

2. Tipos de ciberdelitos..... 3

 2.1 Delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas y datos informáticos..... 3

 2.2 Delitos relacionados con las tecnologías informáticas 4

 2.3 Delitos relacionados con contenidos informáticos..... 4

3. Pandemia y ciberdelito 7

 3.1 Tendencias del ciberdelito en la pandemia a nivel global 7

4. Ciberdelito en Centroamérica y República Dominicana..... 8

 4.1 El Salvador: se duplican los hurtos y estafas informáticas 8

 4.2 Costa Rica: crecen estafas y suplantación de identidad 11

5. La cifra oculta del ciberdelito 14

 5.1 Contexto: conectividad en Centroamérica y República Dominicana..... 15

 5.2 Principales resultados de la “Encuesta sobre ciberdelito en Centroamérica y República Dominicana” 17

 5.3 Resultados regionales 18

 5.4 Todas las personas son víctimas del ciberdelito 19

 5.5 Ciberacoso..... 22

 5.6 Hackeo de cuentas de redes sociales 23

 5.7 Robo de información de tarjeta de crédito 24

 5.8 Denuncias por ciberdelito 25

 5.9 Tasa de reporte para diferentes tipos de ciberdelito 26

 5.10 Denuncias de ciberdelito ante las autoridades oficiales 27

 5.11 Denuncias de ciberdelito ante las autoridades de justicia 28

 5.12 Denuncia y cifra oculta para el ciberdelito 29

 5.13 Razones para no denunciar..... 31

6. Monitoreo de redes sociales 32

7. Hacer frente al ciberdelito..... 33

8. Educación, prevención y protección 34

9. Plataformas y mecanismos de atención y ayuda 35

10. Investigación del ciberdelito y atención a víctimas..... 36

11. Enfrentar el ciberdelito desde lo público y a través de la colaboración internacional.. 37

Reflexión final 38

Referencias 40

Anexo: Marcos legales para el combate contra el ciberdelito en la región de Centroamérica y República Dominicana 41

Cuadros

Cuadro 1 Diez estadísticas globales de ciberdelito 6

Cuadro 2 Número de delitos denunciados ante la Fiscalía General de la República bajo la Ley Especial contra Delitos Informáticos y Conexos en El Salvador (2019-2020)..... 9

Cuadro 3 Distribución porcentual del total de delitos denunciados bajo la LDI en El Salvador (2019-2020) 11

Cuadro 4 Número de delitos informáticos denunciados al Organismo de Investigación Judicial (2019-2021)..... 12

Cuadro 5 Distribución porcentual de los delitos informáticos denunciados en Costa Rica 2019-2021..... 14

Cuadro 6 Prevalencia del ciberdelito en los últimos 12 meses, en porcentajes y por grupo de población (2021)..... 20

Cuadro 7 Prevalencia del ciberacoso en los últimos 12 meses, en porcentaje y por grupo de población (2021)..... 22

Cuadro 8 Prevalencia del hackeo de redes sociales en los últimos 12 meses, en porcentajes y por grupo de población (2021) 23

Cuadro 9 Prevalencia del robo de información de tarjeta de crédito o débito en los últimos 12 meses, en porcentajes y por grupo de población (2021)..... 25

Cuadro 10 Porcentaje de víctimas que reporta de manera formal el ciberdelito, incluidas autoridades de justicia y empresas privadas (2021) 26

Cuadro 11 Porcentaje de víctimas que denuncia de manera formal el ciberdelito ante las autoridades de justicia (2021) 28

Cuadro 12 Porcentaje de víctimas que denuncia de manera formal el ciberdelito ante las autoridades de justicia 29

Gráficos

Gráfico 1 Distribución porcentual de usuarios de Internet en Centroamérica y República Dominicana (2020) 15

Gráfico 2 Suscripciones a telefonía móvil por cada 100 personas en Centroamérica y República Dominicana (2020)..... 17

Gráfico 3 Distribución porcentual según condición de denuncia y cifra oculta del ciberdelito en Centroamérica y República Dominicana 30

Gráfico 4 Distribución porcentual de las razones para no denunciar el último caso de ciberdelito..... 31

Introducción

En la actualidad, las personas viven en un mundo hiperconectado. Las tecnologías de la información y la comunicación (TIC) ofrecen posibilidades poderosas para trabajar, buscar esparcimiento y conectar con otras personas. Lamentablemente, las TIC son también la herramienta por medio de la cual criminales de todas partes del planeta buscan obtener ganancias a partir del robo de información y activos de personas y empresas.

En 2020, la pandemia de COVID-19 aceleró las tendencias del aumento del uso de las TIC. Esto abrió la puerta a más ataques informáticos. Durante ese año, las denuncias por ciberdelitos se incrementaron en 82 % en Estados Unidos (Federal Bureau of Investigation [FBI], 2020). En países como Singapur, el 43 % de todos los casos de delito están vinculados a las actividades informáticas (Cyber Security Agency of Singapore [CSA], 2021). A escala mundial, un dato estimado indica que alrededor de 330 millones de personas se vieron afectadas por el ciberdelito (Help Net Security [HNS], April 14, 2021).

El ciberdelito es ya uno de los principales problemas de seguridad en el mundo y la tendencia apunta a un crecimiento acelerado de este mal. Para 2021, se calcula que el costo del cibercrimen haya llegado a cerca de USD 6 billones, y para 2025, alcanzaría los USD 10.5 billones, es decir, alrededor de la mitad del PIB de Estados Unidos (Morgan, 2020).

Para Centroamérica, las amenazas del ciberdelito se suman a las generadas por la violencia social, las pandillas y el tráfico de drogas (Lucas, 2020), y por otros delitos como la explotación sexual de niños y niñas, la violencia contra las mujeres y niñas, el ciberacoso, la difusión de material xenofóbico, la publicación de noticias falsas y la promoción del terrorismo. En particular, los delitos informáticos en la región se concentran en la vulneración de la información de las personas, en particular la intrusión a sus cuentas de correo y redes sociales, así como el ciberacoso y la introducción de *software* malicioso (Goddard, May 21, 2021).

Combatir el ciberdelito comienza con una cultura de prevención y protección de parte de la ciudadanía y empresas, y requiere también de la disponibilidad de herramientas técnicas para bloquear las amenazas más comunes.

Sin embargo, la sofisticación de los ataques también tiende al alza, por lo que se requiere de estrategias nacionales y globales de prevención y combate del ciberdelito. En este aspecto, la región

de Centroamérica y República Dominicana aún tiene varios retos por delante, vinculados a los marcos legales y a las capacidades institucionales para detectar, investigar y perseguir el cibercrimen.

Con este documento, se busca dar una mirada actualizada a la incidencia y la relevancia del ciberdelito (delitos financieros y robo de identidad) en la región, con el propósito de motivar la discusión sobre el tema y activar agendas de política pública que permitan hacer frente a esta amenaza creciente y dinámica.

El reporte está estructurado en la forma siguiente: en una primera sección, se analizan las tendencias globales; en la segunda, se revisan los datos regionales disponibles, tanto los que son oficiales y provienen de denuncias como aquellos de victimización reportados en encuestas; en la tercera, se proyectan tendencias para los países; y, en la cuarta y última sección, se concluye con algunas reflexiones de política pública.

1. Tendencias globales

No hay una definición universalmente aceptada de qué es el ciberdelito. Sin embargo, en varios conceptos, existen elementos comunes que incluyen: (a) el uso de las TIC, (b) la violación del marco legal y (c) la afectación de los intereses de consumidores y empresas. Asimismo, existen distintas categorías, por ejemplo, cuando: (a) las tecnologías ayudan a la comisión de delitos, (b) las tecnologías permiten la existencia del delito y (c) la perpetración del delito depende de la existencia de las tecnologías.

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, febrero de 2020) define al ciberdelito como un acto que infringe la ley y que se comete con el uso de las TIC para atacar redes, sistemas, datos, sitios web y tecnología, o para facilitar un delito.

Existen diferentes situaciones consideradas como ciberdelito, incluidos los ataques contra la privacidad y la confidencialidad de la información, y la disponibilidad y la integridad de servicios, sistemas y datos informáticos, así como crímenes tradicionales cometidos con apoyos informáticos, como el acoso, la extorsión o el chantaje. La definición del diccionario Oxford recoge que ciberdelito es un “delito cometido mediante el uso de métodos informáticos o a través de Internet o las redes virtuales”.

Sea cual sea la manera como se clasifique, el ciberdelito constituye una realidad en franco aumento. Las cifras y proyecciones globales muestran esta tendencia que representa un reto enorme para la

integridad de la gente usuaria (puede llegar a tener un impacto psicológico y emocional), para las compañías dedicadas a la seguridad informática y, sobre todo, para las autoridades y los cuerpos de seguridad de cada país, pues deben hacer frente a un entorno de cambios rápidos que, además, contiene amenazas muy importantes para la actividad económica, la seguridad de los recursos y la información de personas y empresas.

2. Tipos de ciberdelitos

2.1 Delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas y datos informáticos

Hackeo: es el acceso no autorizado a sistemas, redes y datos informáticos. Esto puede ser con el objeto de romper la confidencialidad de la información, realizar chantajes o extorsiones a personas y empresas, así como alterar registros financieros y transferir dinero o propiedad de recursos.

Intercepción de información transmitida en la red.

Ataques de negación de servicio (DDoS): se dan cuando múltiples computadoras lanzan un ataque destinado a saturar servidores y prevenir el funcionamiento y el acceso normal a un sistema o servicio.

Malware o software malicioso: busca obtener acceso o interferir con los recursos de la víctima. Existen múltiples tipos de *malware*, entre los cuales están:

- Los **gusanos informáticos (worms)**, que se reproducen sin necesidad de involucrar al usuario.
- Los **virus**, que requieren que el usuario realice una actividad (como abrir un correo electrónico) para reproducirse.
- Los **troyanos**, que simulan ser *software* legítimo para infectar el sistema del usuario.
- El **software espía (spyware)**, que envía al atacante información de la víctima obtenida del sistema infectado.
- El **ransomware o software de rescate**, que obtiene el control del sistema de la víctima hasta que se paga un rescate.

- El **cryptoransomware** o **software de rescate**, que usa encriptación, es decir, encripta la información en el sistema de la víctima y amenaza con borrarla a menos que se pague un rescate.
- El **doxware**, que amenaza con publicar datos privados de la víctima si no se paga un rescate.

2.2 Delitos relacionados con las tecnologías informáticas

Incluyen aquellos donde es inherente el uso de los sistemas informáticos.

Fraude o falsificación: es un tipo muy común de delito informático que implica la falsificación de la identidad de un sistema o servicio legítimo para obtener información sensible de la víctima. Algunos tipos son:

- El **phishing**, en el que la víctima recibe un vínculo fraudulento que la conduce a un sitio web falsificado donde ingresa sus credenciales, las que luego son robadas. Los mensajes de *phishing* suelen involucrar afirmaciones de urgencia o necesidad.
- El *phishing* dirigido a un usuario específico se conoce como **spearphishing**, y busca que una víctima particular revele información o envíe dinero.
- El **whaling** consiste en hacerse pasar por un ejecutivo de una empresa para hacer que la víctima (un empleado) envíe fondos.

Venta de información de usuarios: credenciales, números de tarjeta de crédito e información bancaria para fines fraudulentos, incluida la suplantación de identidad.

Violación a los derechos de autor y marcas registradas: a través de la Internet, es común la copia no autorizada de obras musicales, libros, películas y *software*, así como la revelación de secretos comerciales y patentes.

Ataques personales: incluye situaciones como el ciberacoso.

Grooming: es la selección y manipulación de víctimas a través de internet, especialmente niñas y niños, por parte de depredadores sexuales.

2.3 Delitos relacionados con contenidos informáticos

Incluye:

- Delitos donde existe contenido informático ilegal.
- Material relacionado con el abuso sexual infantil.

- Explotación sexual de niñas y niños, incluida la transmisión en vivo de actos de abuso en niñas o niños, así como el tráfico de personas con fines de abuso sexual.
- Material xenofóbico o racista que puede ser ilegal en algunos países.
- Publicación de información falsa o difamatoria.
- Promoción del terrorismo

La dimensión y alcance de los delitos por internet nos permite conocer el impacto económico que tienen estas actividades a nivel mundial (ver cuadro 1).

Cuadro 1 Diez estadísticas globales de ciberdelito

1. USD 20 billones fue el costo total del <i>ransomware</i> para las empresas en 2020. El rescate promedio fue de USD 250 000.	6. Una cantidad de 23 000 ataques de denegación de servicio (DDoS) ocurrió cada día durante 2020.
2. El 70 % de todas las violaciones de acceso a la información en 2020 fueron motivadas por ganancia financiera.	7. Un total de 30 000 sitios web fueron hackeados por día en 2020. Los sectores más atacados fueron el financiero, el de la salud, el del gobierno y el del comercio.
3. USD 1,33 billones es el gasto proyectado en seguridad informática por las empresas para 2022.	8. El 70 % de los usuarios utilizó en 2020 la misma contraseña en diferentes sitios web.
4. El 63 % de todas las violaciones de acceso a la información en 2020 fue generado por nombres de usuario y contraseñas filtradas.	9. Siete meses es el tiempo promedio que tardó en 2020 la detección de una vulneración de seguridad en una empresa.
5. Unos 300 000 elementos de <i>software</i> malicioso fueron creados diariamente en 2020.	10. USD 1,5 billones fue la riqueza que pasó a manos de cibercriminales en 2020.

Fuente: Goddard (27 de mayo de 2021)

3. Pandemia y ciberdelito

La pandemia aumentó dramáticamente la dependencia humana de las TIC para el trabajo y el entretenimiento. Las medidas de distanciamiento social y las cuarentenas empujaron a las personas a trabajar de manera remota a través de Internet, así como a comunicarse, comprar y compartir experiencias e información por medio de plataformas digitales, con mayor fuerza y frecuencia que antes.

El ciberdelito no fue ajeno a esta tendencia; así, vinculado a la pandemia, se registró un aumento significativo de la actividad ilegal en dos ejes importantes (Mahadevan, 2020):

- a. Aprovechamiento del temor y de la incertidumbre generados por el COVID-19, a través de información falsa diseminada en redes sociales, intentos de *phishing* en mensajes relacionados con la enfermedad, troyanos embebidos en documentos aparentemente informativos sobre el virus, sitios web maliciosos asociados a la misma temática y venta de medicamentos falsos o no aprobados, entre otros. Como se observa, el Estado también se enfrenta a los peligros de la desinformación y las “noticias falsas” (Programa de las Naciones Unidas para el Desarrollo [PNUD], 2021). En este escenario, Luis Felipe López-Calva, director regional del PNUD para América Latina y el Caribe, establece que la transparencia es un elemento crítico para hacer que la gobernabilidad sea más efectiva. Al hacer que la información esté disponible, crea una base para una mayor rendición de cuentas a la ciudadanía.
- b. Aprovechamiento de las vulnerabilidades generadas por el error humano y la intensificación del teletrabajo y los servicios informáticos. Respecto a este punto, se produjo el hackeo de cuentas individuales y corporativas de servicios de teleconferencia, correo electrónico, financieros, compras en línea, así como el aumento del *phishing* y de intentos de suplantación de identidad.

3.1 Tendencias del ciberdelito en la pandemia a nivel global

- El 85 % de los ataques exitosos fueron engaños a personas.
- La cuota del *phishing* dentro de los ataques exitosos subió del 25 % al 36 % (Verizon, 2021).
- Uso de los mensajes de salud como señuelo y ataques a los sistemas de salud.
- Aumento en los crímenes relacionados con abuso y pornografía infantil (Radoini, 2020).
- Uso de campañas de donación falsas.

- Incremento del *ransowmware* o pago de rescates por devolver el acceso de la información de las víctimas, combinado con la amenaza de publicar o vender los datos de las víctimas si no se realiza el rescate.

Por ejemplo, en el Reino Unido, el ciberdelito se incrementó en 43 % entre mayo de 2019 y mayo de 2020. Los delitos que aumentaron más fueron el hackeo de cuentas personales, en un 77 %; el hackeo de cuentas de redes sociales, en un 54 %; y el fraude al realizar compras en línea, en un 51 % (Buil-Gil et ál., 2021).

4. Ciberdelito en Centroamérica y República Dominicana

En Centroamérica y República Dominicana, al igual que en el resto del mundo, se sufre de un incremento en la cantidad de ataques y delitos informáticos. En el caso de la región los delitos reportados, tanto en cifras oficiales como en las encuestas de opinión, se concentran en la violación a la privacidad de los datos de las personas y en la de los de acceso a los servicios informáticos.

Sin embargo, en línea con lo observado en otras regiones, se detecta una subida en las estafas, así como en el hurto y el robo informáticos, facilitados por el mayor uso de plataformas como la banca y las compras en línea.

En Costa Rica y El Salvador, datos oficiales permiten ilustrar las tendencias del ciberdelito en la región. Asimismo, los resultados de la Encuesta sobre Ciberdelito, aplicada en los otros países, permiten indagar en la incidencia real, la denuncia y la cifra oculta del ciberdelito en la región.

Es importante tener presente que cada país define los delitos informáticos de acuerdo con su legislación local.

4.1 El Salvador: se duplican los hurtos y estafas informáticas

Cada país define los delitos informáticos de acuerdo con su legislación local. En El Salvador, el cuerpo legal relevante es la Ley Especial contra Delitos Informáticos y Conexos (LDI).

Entre 2019 y 2020, el total de delitos denunciados ante la Fiscalía General de la República (FGR), bajo las tipologías correspondientes a la LDI, aumentó de 822 a 945 casos, es decir, un 15 % (ver cuadro 1).

Los delitos más frecuentes entre los casos denunciados fueron la revelación indebida de información o datos personales, y el hurto de identidad, que sumaron el 49.8 % del total en 2019 y 46.8 % en 2020 (ver cuadro 2).

Las tendencias difieren significativamente por tipo de delito. El crecimiento del hurto de identidad (13.5%) es mayor que el de la revelación indebida de información (5.6%).

Los delitos que más aumentaron en 2020 son la estafa informática y el hurto por medios informáticos. En ambos casos, el total de denuncias creció en más del doble, en 125 % y 114 %, respectivamente. Así, estos dos delitos pasaron de constituir el 8.6 % a ser el 16.4 % de todas las denuncias.

Además, el acoso a través de las TIC creció en 23.7 %, y el acoso a niñas, niños y adolescentes, y a personas con discapacidad, aumentó en 13.3 %, en línea con el aumento general del ciberdelito.

Estas tendencias reflejan el aumento de las transacciones financieras y compras hechas en línea, donde se materializan riesgos de estafa y de sustracción de recursos de las cuentas bancarias o servicios de los usuarios.

Cuadro 2 Número de delitos denunciados ante la Fiscalía General de la República bajo la Ley Especial contra Delitos Informáticos y Conexos en El Salvador (2019-2020)

Delito denunciado	Casos 2019	Casos 2020	Cambio porcentual
Revelación indebida de información o datos personales	284	300	5.6
Hurto de identidad	126	143	13.5
Acoso a través de medios informáticos	59	73	23.7
Utilización de datos personales	58	51	-12.1
Divulgación no autorizada	51	19	-62.7
Hurto por medios informáticos	43	92	114.0
Acoso a niñas, niños, adolescentes o personas con discapacidad	30	34	13.3
Estafa informática	28	63	125.0
Otros	143	170	18.9

Total	822	945	
--------------	------------	------------	--

Fuente: Elaboración propia a partir de datos proporcionados por el Departamento de Estadística, Dirección de Análisis, Técnicas de Investigación e Información, Fiscalía General de la República de El Salvador

Cuadro 3 Distribución porcentual del total de delitos denunciados bajo la LDI en El Salvador (2019-2020)

Delito denunciado	Porcentaje 2019	Porcentaje 2020
Revelación indebida de información o datos personales	34.5	31.7
Hurto de identidad	15.3	15.1
Acoso a través de medios informáticos	7.2	7.7
Utilización de datos personales	7.1	5.4
Divulgación no autorizada	6.2	2.0
Hurto por medios informáticos	5.2	9.7
Acoso a niñas, niños, adolescentes o personas con discapacidad	3.6	3.6
Estafa informática	3.4	6.7
Otros	17.4	18.0
Total	100	100

Fuente: Elaboración propia a partir de datos proporcionados por el Departamento de Estadística, Dirección de Análisis, Técnicas de Investigación e Información, Fiscalía General de la República de El Salvador

4.2 Costa Rica: crecen estafas y suplantación de identidad

Entre 2019 y 2020, el total de delitos informáticos en Costa Rica aumentó en 10.8 %, al pasar de 2091 a 2367, según denuncias realizadas al Organismo de Investigación Judicial (OIJ) de ese país (ver cuadro 3). Al 14 de noviembre de 2021, se tenía ya 2317 denuncias, lo que, de continuar la tendencia, implicaría un aumento de 16 % a fin de ese año respecto al anterior.

Se observa que las estafas informáticas fueron el delito cibernético más denunciado tanto en 2019 como en 2020, y crecieron significativamente entre un año y el otro, a una tasa de 33.1 % anual.

Para 2021, el delito más denunciado fue la suplantación de identidad, con una proyección de crecimiento de 33.2 % con respecto a 2020; además, había sido el segundo con mayor número de denuncias en 2020 y 2019.

Algunos delitos en la lista mostrada, como el espionaje informático o la instalación y propagación de *software* malicioso, crecieron de forma muy importante, ya que aumentaron su representación en el total, al pasar de 2.7 % a 7.8 % entre 2019 y 2021.

Al igual que en otros países, la pandemia impulsó el crecimiento de los delitos informáticos relacionados con el patrimonio.

Es importante notar que entre 2018 y 2019 Costa Rica experimentó un alza muy importante en los delitos informáticos, al pasar de 680 casos denunciados a 2060, es decir, el número registrado esos años se triplicó.

Cuadro 4 Número de delitos informáticos denunciados al Organismo de Investigación Judicial, 2019-2021

Delito denunciado	Casos 2019	Casos 2020	Proyectado 2021
Estafa informática	653	936	806
Suplantación de identidad	618	767	1022
Difusión de información falsa	104	120	154
Espionaje informático	51	122	143
Seducción o encuentro por medios informáticos	55	52	69
Facilitar delitos informáticos	48	48	87
<i>Software</i> malicioso	7	90	69
Suplantación de páginas informáticas	33	36	72
Sabotaje y daño informático	35	58	47
Otros	487	138	264

Total	2091	2367	2733
--------------	-------------	-------------	-------------

Fuente: Datos proporcionados por la Unidad de Análisis Criminal del Organismo de Investigación Judicial de Costa Rica, Solicitud de Información N.º 1894-OPO/UAC/S-2021

Cuadro 5 Distribución porcentual de los delitos informáticos denunciados en Costa Rica, 2019-2021

Delito denunciado	2019	2020	2021
Estafa Informática	31.2	39.5	29.5
Suplantación de identidad	29.6	32.4	37.4
Difusión de información falsa	5.0	5.1	5.6
Espionaje informático	2.4	5.2	5.2
Encuentro con menores por medios informáticos	2.6	2.2	2.5
Facilitar delitos informáticos	2.3	2.0	3.2
<i>Software</i> malicioso	0.3	3.8	2.5
Suplantación de páginas informáticas	1.6	1.5	2.6
Sabotaje y daño informático	1.7	2.5	1.7
Otros	23.3	5.8	9.7
Total	100.0	100.0	100.0

Fuente: Datos proporcionados por la Unidad de Análisis Criminal del Organismo de Investigación Judicial de Costa Rica, Solicitud de Información N.º 1894-OPO/UAC/S-2021

5. La cifra oculta del ciberdelito

Un importante problema para dimensionar las tendencias y la magnitud del ciberdelito en la región es la falta de denuncia, tanto de parte de personas naturales como de empresas e instituciones.

El término “cifra oculta” es el usual para denotar los delitos que ocurren y no son denunciados por diversas razones, desde el temor y la vergüenza de la víctima hasta la falta de confianza en las autoridades. En cuanto al ciberdelito, es difícil estimar el tamaño de la cifra oculta, que puede ser muy alta debido a la dificultad de investigar este tipo de crimen, la posibilidad de que el victimario se encuentre fuera de la jurisdicción de las autoridades locales, las amenazas a las víctimas y la naturaleza confidencial de la información que puede haber sido revelada. Por otro lado, durante la

pandemia, el auge del teletrabajo en 2020 y 2021 aumentaron la conectividad de las personas, volviéndolas más vulnerables al ciberdelito.

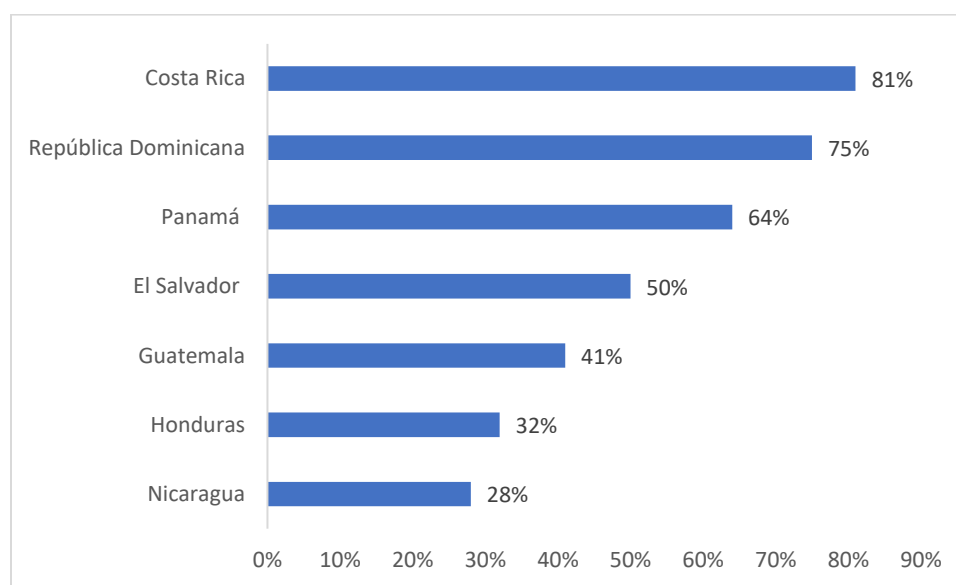
Para dimensionar la magnitud y el alcance de los delitos informáticos, es necesario mirar el acceso a los servicios de Internet y su conectividad en Centroamérica y República Dominicana.

5.1 Contexto: conectividad en Centroamérica y República Dominicana

El acceso a Internet se ha incrementado significativamente en la región en la última década. Según datos de la Unión Internacional de Telecomunicaciones (UIT), se observa que, entre 2010 y 2020, la población con accesibilidad pasó de ser un 20 % a constituir un 53 %. Costa Rica, República Dominicana y Panamá poseen las mayores tasas de uso.

Aunque en la región existe todavía un porcentaje importante de la población que no utiliza Internet de manera regular, la tendencia ha sido hacia un crecimiento rápido, y se espera que continúe aumentando, sobre todo en los países donde el grado de adopción es menor a la media latinoamericana que es de 62 %, es decir, en El Salvador, Guatemala, Honduras y Nicaragua (ver gráfico 1).

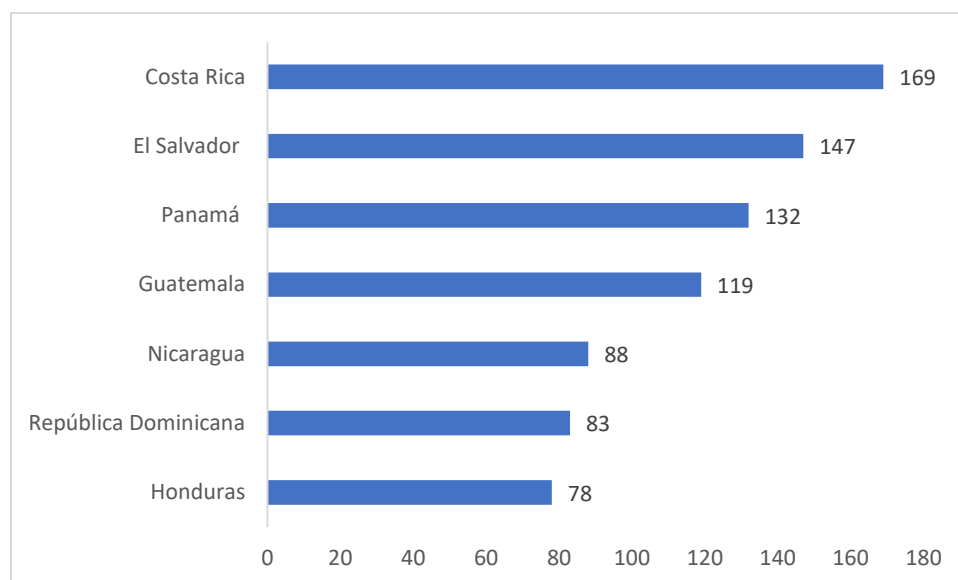
Gráfico 1 Distribución porcentual de usuarios de Internet en Centroamérica y República Dominicana, 2020



Fuente: Estadísticas de la Unión Internacional de Telecomunicaciones (2020a).

Asimismo, el acceso a conectividad a través de telefonía celular ha alcanzado niveles relativamente altos en la región, en algunos países, y ha superado el número de suscripciones por cada 100 personas al valor que se observa en los países desarrollados. Costa Rica (169 suscripciones por cada 100 personas) y El Salvador (147) sobresalen en este indicador (ver gráfico 2).

Gráfico 2 Suscripciones a telefonía móvil por cada 100 personas en Centroamérica y República Dominicana, 2020



Fuente: Estadísticas de la Unión Internacional de Telecomunicaciones (2020b).

5.2 Principales resultados de la “Encuesta sobre ciberdelito en Centroamérica y República Dominicana”

Una manera de obtener información más cercana a la incidencia de los delitos informáticos es preguntar directamente a las personas si han sido víctimas de estos y si los han denunciado. Aun cuando en este caso siempre es posible que exista un subregistro debido a que algunas víctimas podrían no revelar los incidentes sufridos, este valor tiende a ser mayor, en especial dadas las características de anonimato de la encuesta y de neutralidad del cuestionario.

En esta sección se presentan los resultados de la encuesta sobre ciberdelito conducida a mediados de 2021 en cinco países de la región de Centroamérica y República Dominicana, implementada por CID Gallup para el proyecto regional Infosegura, con apoyo de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID).

La consulta se realizó entre abril y mayo de 2021, con el objetivo de indagar sobre la victimización por ciberdelito en la región durante la pandemia de COVID-19, así como respecto a otras situaciones asociadas a la calamidad sanitaria.

La indagación se basó en el módulo estandarizado sobre ciberdelito de la Iniciativa para la encuesta de victimización delictiva en Latinoamérica y el Caribe (VICLAC), el cual, a su vez, retoma los conceptos de la clasificación internacional del delito con fines estadísticos (*International Classification of Crime for Statistical Purposes* [ICCS]).

Los datos de la encuesta indican una elevada incidencia del ciberdelito entre toda la población, con la mayoría (80 %) expuesta a algún tipo de delito informático en el último año.

Frente a la alta prevalencia y dada la limitada cantidad de denuncias realizadas en cada país, se vuelve evidente la necesidad de educar a la población sobre las maneras de

prevenir este crimen, comprender su naturaleza y denunciarlo, así como de proveer plataformas de uso sencillo para la denuncia de las situaciones de victimización experimentadas.

5.3 Resultados regionales

La gran mayoría de las personas consultadas (80 %) fue víctima de alguna de las situaciones descritas en el cuadro 5, en los doce meses anteriores a la encuesta, período que corresponde al primer año de la pandemia de COVID-19. La tasa de incidencia va de 76.8 % (Costa Rica) a 83.7 % (El Salvador), aunque las diferencias entre países no son significativas, ya que están dentro del margen de error de la encuesta (4 %).

Las situaciones más comunes fueron el ciberacoso y el hackeo de una cuenta de red social, aunque también son muy prevalentes la propagación de *software* malicioso (*malware*) y el hackeo de cuentas de correo electrónico (*email*).

En Guatemala, Honduras y República Dominicana, el delito más prevalente es el hackeo de redes sociales; mientras que, en El Salvador, es el ciberacoso; y en Costa Rica, la difusión de *malware*. A pesar de estas diferencias locales, en todos los países el porcentaje de personas que ha sufrido una o más de estas situaciones es elevado.

Ficha técnica de la encuesta

Trabajo de campo: del 29 de abril al 12 de mayo de 2021

Modalidad de la encuesta: teléfonos celulares activos

Países donde se condujo: Costa Rica, El Salvador, Guatemala, Honduras y República Dominicana

Muestra total: 3000 personas, 600 por país

Margen de error: +- 4 %

Nivel de confianza: 95 %

Población urbana en la muestra: 82 %

Participación por sexo: 49 % hombres, 51 % mujeres

Cuadro 5 Porcentaje de personas que han experimentado alguna de las situaciones descritas en los últimos 12 meses, 2020¹

Delito/país	Guatemala	El Salvador	Honduras	Costa Rica	República Dominicana	Valor regional
Ciberacoso	39.0	38.8	26.2	21.8	19.2	29.0
<i>Malware</i>	30.3	32.7	27.0	33.2	23.2	29.3
Hackeo de <i>email</i>	37.3	20.0	19.5	15.8	23.8	23.3
Hackeo de red social	48.7	34.2	33.5	23.2	47.8	37.5
<i>Ransomware</i>	8.3	5.3	5.2	2.8	6.0	5.5
Robo de información de tarjeta de débito o crédito	18.5	8.8	12.5	22.8	16.3	15.8
Secuestro de información	15.0	7.0	5.7	10	4.8	8.5
Al menos un delito informático	78.3	83.7	79.3	76.8	83.0	80.2

Fuente: Elaboración propia a partir de los datos de la Encuesta sobre ciberdelito en Centroamérica y República Dominicana

5.4 Todas las personas son víctimas del ciberdelito

Dada la gran incidencia del ciberdelito en la región, todos los grupos de personas están expuestos. La encuesta de ciberdelito permite revelar los patrones de incidencia en diferentes grupos de

¹ Pregunta P11. Usted mencionó que en los últimos tres (3) años ha experimentado personalmente alguna de las situaciones descritas en la tarjeta. Ahora bien, ¿podría decirme cuál(es) situación(es) ha sufrido durante los últimos doce (12) meses, es decir, entre mayo 2020 y mayo 2021?

población definidos por nivel educativo, sexo y rango de edad. Aunque no se observan diferencias significativas en los valores regionales, existen diferencias por país, por ejemplo:

- En Guatemala y Honduras, la incidencia del ciberdelito es mayor entre las personas con un nivel educativo más bajo; lo contrario ocurre en El Salvador. Mientras, en Costa Rica, la incidencia más alta es entre las personas con educación secundaria; asimismo, en República Dominicana (ver cuadro 6). Aunque se observan diferencias entre grupos, no superan el margen de error.
- No se notan diferencias significativas en el promedio de hombres y mujeres que han sido víctimas de, al menos, una situación de ciberdelito en el último año, salvo en Guatemala, donde la incidencia es menor entre las mujeres.
- Solo en Costa Rica se observan diferencias significativas por edad, con menor incidencia entre las personas mayores de 35 años. En el resto de los países, las diferencias observadas no superan el margen de error.

Cuadro 6 Prevalencia del ciberdelito en los últimos 12 meses, en porcentajes y por grupo de población, 2021

Categoría/país	Guatemala	El Salvador	Honduras	Costa Rica	República Dominicana	Valor regional
Nivel educativo						
Primaria	82.4	68.0	83.1	74.4	83.9	78.4
Secundaria	79.0	84.3	79.4	80.8	81.2	80.9
Superior	74.8	84.4	77.2	72.2	86.2	79.0
Sexo						
Mujer	76.6	84.3	79.8	76.6	82.6	80.0
Hombre	80.5	83.0	78.9	77.1	83.4	80.6
Rango de edad						
De 18 a 34 años	78.4	84.0	79.7	83.7	83.8	81.9

De 35 años y más	78.0	82.9	78.5	71.5	81.5	78.5
------------------	------	------	------	------	------	------

Fuente: Elaboración propia a partir de los datos de la Encuesta sobre cibercriminología en Centroamérica y República Dominicana

5.5 Ciberacoso

En el plano regional, el ciberacoso es el delito informático más frecuentemente reportado por las personas encuestadas. Al analizar por nivel educativo, sexo y edad, se puede observar algunas tendencias.

- La victimización es mayor para las personas con educación secundaria o menos, al compararlas con las que cuentan con educación superior. La tendencia anterior es evidente en cuatro de los países analizados. La excepción es República Dominicana, que reporta tasas mayores para las personas con mayor nivel educativo.
- La victimización por ciberacoso es mayor para las mujeres que para los hombres, particularmente en El Salvador. Solo en República Dominicana se reportan tasas similares para hombres y mujeres.
- En el ámbito regional, no hay diferencias en la victimización por edad. Sin embargo, a nivel de país, Costa Rica presenta un grado muy superior de incidencia entre las personas más jóvenes, mientras que El Salvador y Honduras se muestra entre las mayores de 35 años (ver cuadro 7). Al examinar en detalle, se observa que los grupos muy victimizados por el ciberacoso son las mujeres más jóvenes (de 19 a 24 años), con una tasa de 35.7 %, seguidas de los hombres de 35 a 44, con 32.7 % (PNUD-Infosegura, 2021).

Cuadro 7 Prevalencia del ciberacoso en los últimos 12 meses, en porcentaje y por grupo de población, 2021

Categoría/país	Guatemala	El Salvador	Honduras	Costa Rica	República Dominicana	Valor regional
Nivel educativo						
Secundaria o menos	40.4	43.1	27.0	26.0	17.1	30.7
Superior	33.9	34.3	24.0	14.8	23.5	26.1
Sexo						
Mujer	41.3	43.3	28.0	23.8	18.7	31.0

Hombre	36.1	34.3	24.5	20.0	19.7	26.9
Rango de edad						
De 18 a 34 años	38.9	37.3	25.2	29.3	18.8	29.9
De 35 años y más	39.3	42.0	28.5	16.0	20.0	29.2

Fuente: Elaboración propia a partir de los datos de la Encuesta sobre cibercriminología en Centroamérica y República Dominicana.

5.6 Hackeo de cuentas de redes sociales

En la región, el segundo delito más reportado por las personas que respondieron la encuesta es el hackeo de redes sociales.

- Al igual que con el ciberacoso, en este caso la victimización es mayor para las personas con educación secundaria o menos, al compararlas con las que cuentan con educación superior. Esta tendencia se evidencia particularmente en Guatemala, Honduras y Costa Rica. En cambio, en El Salvador, no hay mayor diferencia por nivel educativo (ver cuadro 8).
- La victimización por hackeo es levemente mayor para las mujeres que para los hombres, si se observa el promedio regional. Sin embargo, en la mayoría de los países no hay diferencias significativas por sexo. La excepción es El Salvador, donde hay una diferencia importante (del 9 %) que señala mayor victimización de las mujeres.
- Se da un claro patrón para todos los países analizados donde la gente más joven es la que más sufre este tipo de cibercriminología. De hecho, la incidencia es más alta entre las personas de 18 a 34 años, de las que 41.9 % ha sufrido esta situación en el último año.

Cuadro 8 Prevalencia del hackeo de redes sociales en los últimos 12 meses, en porcentajes y por grupo de población, 2021

Nivel educativo/país	Guatemala	El Salvador	Honduras	Costa Rica	República Dominicana	Valor regional
Secundaria o menos	53.1	35.6	35.4	31.7	49.9	41.1

Superior	33.1	35.5	28.7	11.7	46.9	31.2
Sexo						
Mujer	48.5	38.7	33.6	22.8	48.9	38.5
Hombre	48.9	29.7	33.3	23.5	46.8	36.4
Rango de edad						
De 18 a 34 años	51.1	34.9	35.3	35.7	52.5	41.9
De 35 años y más	41.3	32.6	29.1	13.4	38.5	31.0

Fuente: Elaboración propia a partir de los datos de la Encuesta sobre ciberdelito en Centroamérica y República Dominicana

5.7 Robo de información de tarjeta de crédito

Aunque el robo de información de tarjeta de crédito o débito es el quinto ciberdelito más frecuente, es revelador analizar el perfil de las víctimas, ya que el patrón difiere del observado en los delitos relacionados con ciberacoso, la información personal y las cuentas de red social o correo electrónico.

- En todos los países de la región, las personas más educadas y de mayor edad son las que con más frecuencia son víctimas de este tipo de delito (ver cuadro 9). La prevalencia es mayor para los hombres en tres de los países (Guatemala, Honduras y Costa Rica).
- La incidencia de este delito está relacionada con la inclusión financiera de las personas en cada país. El Salvador es el que presenta la menor inclusión financiera de la región, donde solo el 30 % de los adultos posee cuenta bancaria. Según el índice Findex del Banco Mundial (Demigürç-Kunt et ál., 2018), la nación salvadoreña presenta también la menor afectación, mientras que Costa Rica, que goza de mayor bancarización (68 % de la población adulta), también es el lugar donde más se produce esta clase de contravención.

El mayor acceso a servicios financieros en línea y compras a través de Internet continuará siendo un elemento que lleve al alza esta clase de actos.

Cuadro 9 Prevalencia del robo de información de tarjeta de crédito o débito en los últimos 12 meses, en porcentajes y por grupo de población, 2021

Nivel educativo	Guatemala	El Salvador	Honduras	Costa Rica	República Dominicana	Promedio
Secundaria o menos	17.8	7.4	11.3	19.1	13.6	13.8
Superior	21.3	10.4	15.6	29.1	21.9	19.7
Sexo						
Mujer	13.8	8.7	10.3	20.3	19.3	14.5
Hombre	24.4	9.0	14.5	25.2	13.2	17.3
Rango de edad						
De 18 a 34 años	17.1	7.1	12.4	16.3	12.0	13.0
De 35 años y más	22.7	12.4	12.8	27.9	25.0	20.2

Fuente: Elaboración propia a partir de los datos de la Encuesta sobre ciberdelito en Centroamérica y República Dominicana

5.8 Denuncias por ciberdelito

Los datos oficiales sobre denuncias, presentados para Costa Rica y El Salvador, muestran una incidencia relativamente baja del ciberdelito, lo que contrasta fuertemente con los datos mostrados por la Encuesta de Ciberdelito en Centroamérica y República Dominicana.

Al igual que con otros tipos de delito, un porcentaje importante de casos no son denunciados. En los delitos informáticos, puede ser mayor por diferentes razones, incluida la falta de conocimiento sobre su tipificación, la consideración de que no fue una situación grave, la vergüenza o el temor, la falta de confianza en las autoridades, etc.

En la Encuesta sobre Ciberdelito, solo el 18.3 % de los casos fue denunciado de manera formal ante alguna entidad externa; en tanto, un porcentaje menor (10.9 %) planteó la denuncia ante alguna entidad oficial encargada de investigar (policía, ministerio público o fiscalía, o sistema judicial). El resto de las denuncias fue puesto ante instituciones privadas, en especial, ante bancos y servicios de redes sociales.

Si apenas uno de cada nueve casos de ciberdelito es denunciado, se tiene una cifra oculta significativa, que limita de manera importante su detección y persecución. Aumentar la tasa de denuncia es uno de los retos de la política pública en materia de ciberseguridad.

En el siguiente apartado, se analiza con mayor detalle el comportamiento de la denuncia, a partir de los datos de la Encuesta sobre Ciberdelito.

5.9 Tasa de reporte para diferentes tipos de ciberdelito

De acuerdo con la Encuesta sobre Ciberdelito en Centroamérica y República Dominicana 2021, la tasa de reporte del ciberdelito varía significativamente entre países y por tipo de delito. Los datos mostrados en esta página incluyen tanto denuncias ante autoridades oficiales como ante empresas privadas u organizaciones de la sociedad civil. Las principales tendencias son:

- El país donde existe mayor tasa de denuncia es Costa Rica, que alcanza el 23.2 % de los delitos cometidos. Le siguen Guatemala y República Dominicana, con 20.7 % y 20 % respectivamente (ver cuadro 10).
- El Salvador es donde hay menos porcentaje de víctimas que denuncia: solo un 12.5 %.
- Los delitos con mayor tasa promedio de denuncia son el robo de información de tarjeta de crédito, con poco más de la mitad de los casos (51.4 %), y el secuestro de información (44.7 %). Esto se explicaría por las implicancias financieras de esta clase de transgresión.
- Delitos como el hackeo de redes sociales o la difusión de *software* malicioso poseen muy bajas tasas de denuncia.

Cuadro 10 Porcentaje de víctimas que reporta de manera formal el ciberdelito, incluidas autoridades de justicia y empresas privadas, 2021

Hecho experimentado	Guatemala	El Salvador	Honduras	Costa Rica	República Dominicana	Valor regional
Ciberacoso	23.0	12.5	18.3	28.6	15.6	19.6
<i>Malware</i>	4.2	2.4	6.3	7.2	9.6	5.9
Hackeo de email	10.8	6.8	14.8	20.0	15.5	13.6

Hackeo de red social	11.9	6.2	9.2	7.2	10.9	9.1
Robo de información de tarjeta de débito o crédito	58.7	40.5	51.5	47.3	59.1	51.4
Secuestro de información	62.2	31.2	46.7	37.2	46.2	44.7
Al menos un delito informático	20.7	10.3	17.5	23.2	20.0	18.3

Nota: No se incluye información sobre *ransomware*, ya que el número de casos es bajo y no es posible establecer comparaciones válidas entre países.

Fuente: Elaboración propia a partir de los datos de la Encuesta sobre ciberdelito en Centroamérica y República Dominicana

5.10 Denuncias de ciberdelito ante las autoridades oficiales

El valor regional promedio de ciberdelitos que son denunciados ante las autoridades oficiales de cada país es de solamente 10.9 % porque las denuncias de algunos delitos, en particular el robo de información financiera y el hackeo de redes sociales, son interpuestas a las instituciones financieras o a las empresas proveedoras de redes sociales, es decir, menos de la mitad de los reportes sobre ciberdelito son dirigidos hacia las autoridades oficiales:

- Los países donde existe mayor tasa de denuncia son Guatemala y Honduras, con 16.3 % y 13 % respectivamente (ver cuadro 11).
- El Salvador es el país donde hay menos porcentaje de víctimas que denuncia ante las autoridades: solo un 4.5 %.
- Los delitos con mayor tasa de denuncia son el secuestro de información y el robo de información de tarjeta de crédito, con porcentajes de reportes ante las autoridades de 47.7 % y 34.9 %, respectivamente. Al comparar con el cuadro 10, se observa que alrededor del 60 % de las denuncias de robo de información bancaria y el 40 % de las denuncias de secuestro de información se dirigen a los bancos o empresas privadas.

Cuadro 11 Porcentaje de víctimas que denuncia de manera formal el ciberdelito ante las autoridades de justicia, 2021

Hecho experimentado	Guatemala	El Salvador	Honduras	Costa Rica	República Dominicana	Valor regional
Ciberacoso	21.0	8.9	15.3	21.4	9.1	15.1
<i>Malware</i>	4.2	1.6	4.7	4.6	6.8	4.4
Hackeo de email	9.7	3.4	10.2	16.0	7.1	9.3
Hackeo de red social	11.0	2.2	5.5	3.6	6.2	5.7
Robo de información de tarjeta de débito o crédito	30.4	4.8	34.9	17.8	14.7	20.5
Secuestro de información	46.0	6.2	47.7	20.9	23.1	28.8
Al menos un delito informático	16.3	4.5	13.0	12.5	8.8	11.0

Nota: No se incluye información sobre *ransomware* ya que el número de casos es bajo y no es posible establecer comparaciones válidas entre países.

Fuente: Elaboración propia a partir de los datos de la Encuesta sobre ciberdelito en Centroamérica y República Dominicana

5.11 Denuncias de ciberdelito ante las autoridades de justicia

Cuando se analiza el comportamiento de las denuncias por ciberdelito presentadas ante las autoridades de justicia o seguridad pública, se observan diferencias sobre todo en cuanto al sexo de la víctima y en relación con ciertos delitos. Las tendencias más notables son:

- Los hombres tienden a denunciar más que las mujeres, en la mayoría de los delitos. Las excepciones son el hackeo de red social y el *software* malicioso. La brecha de denuncias entre hombres y mujeres es mayor es el delito de secuestro de información, para el cual los hombres denuncian en el 41.2 % de los casos y las mujeres solo en el 16.1 % (ver cuadro 12).
- No hay diferencias significativas en la denuncia entre grupos de diferente nivel educativo.

- Tampoco se observa grandes diferencias en la denuncia entre las personas más jóvenes y las de mayor edad, salvo para el caso del robo de información de tarjetas de crédito o débito, y del secuestro de información, donde la gente más joven denuncia con mayor frecuencia.

Cuadro 12 Porcentaje de víctimas que denuncia de manera formal el ciberdelito ante las autoridades de justicia, 2021

Hecho experimentado	Sexo		Educación		Edad	
	Mujeres	Hombres	Secundaria o menor	Superior	De 18 a 34 años	35 años o más
Ciberacoso	14.5	16.4	15.7	14.2	15.4	15.0
<i>Malware</i>	5.3	3.4	3.6	4.9	3.8	4.8
Hackeo de email	7.3	10.7	8.6	10.5	9.2	8.9
Hackeo de red social	6.5	5.8	6.1	6.4	5.5	7.9
Robo de información de tarjeta de débito o crédito	17.1	23.0	21.8	18.3	27.0	14.7
Secuestro de información	16.1	41.2	28.8	31.7	32.8	26.7
Al menos un delito informático	10.0	12.0	10.8	11.3	10.8	11.2

Nota: No se incluye información sobre *ransomware*, ya que el número de casos es bajo y no es posible establecer comparaciones válidas entre grupos.

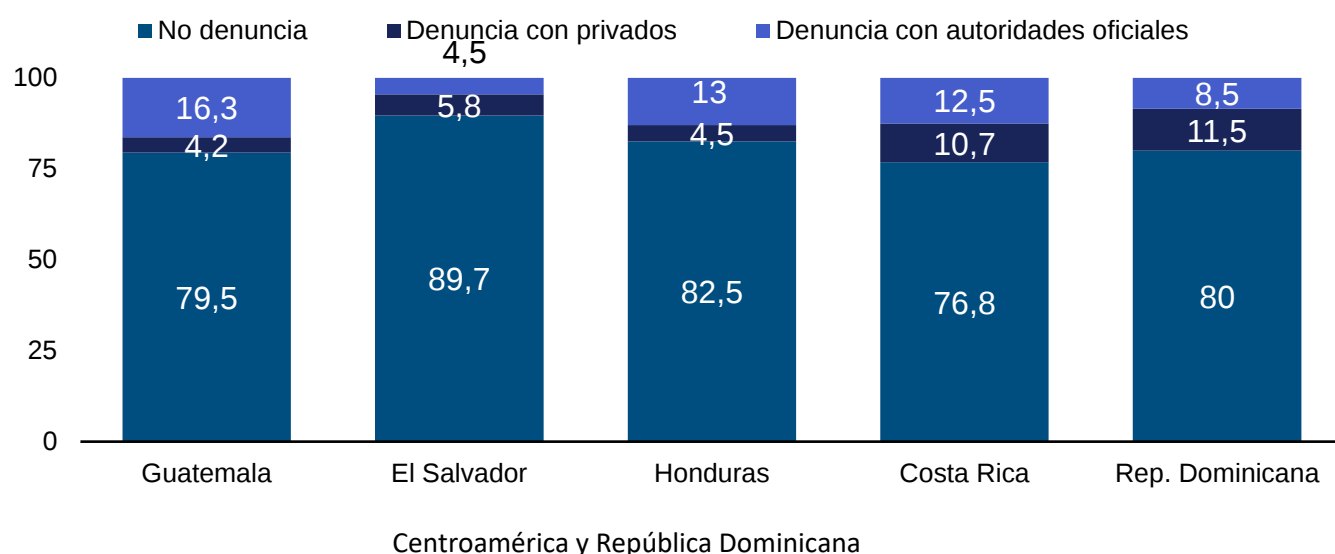
Fuente: Elaboración propia a partir de los datos de la Encuesta sobre ciberdelito en Centroamérica y República Dominicana

5.12 Denuncia y cifra oculta para el ciberdelito

- En países como Costa Rica y El Salvador, la comparación de los datos oficiales con los datos de la encuesta permite pensar que el número de casos reales de ciberdelito es 8 veces lo reportado para el primer país y 22 veces lo indicado para el segundo.

- Así, Costa Rica estaría experimentando más de 18 000 casos de ciberdelito, y El Salvador, más de 22 000 por año².
- La cifra oculta es especialmente preocupante en El Salvador, ya que a pesar de contar con un marco legal especializado en ciberdelito (la Ley Especial contra Delitos Informáticos y Conexos o LDI), recibe pocas denuncias. Eso puede deberse a un conjunto de factores que se exploran más adelante.
- En Costa Rica y República Dominicana, se observa que las empresas privadas reciben una parte muy importante de las denuncias (ver gráfico 3). Esto se debe a que un tipo de ciberdelito muy prevalente en estos países, el robo de información de tarjeta de crédito o débito se denuncia principalmente a la misma institución financiera.

Gráfico 3 Distribución porcentual según condición de denuncia y cifra oculta del ciberdelito en



Fuente: Elaboración propia a partir de los datos de la Encuesta sobre ciberdelito en Centroamérica y República Dominicana

² Para calcular la cifra de casos reales de ciberdelito en Costa Rica y El Salvador, se divide el total de casos para cada país entre el número de veces. En Costa Rica, se divide 18 000 casos entre 8 veces lo reportado; en El Salvador, 22 000 entre 22 veces lo reportado.

5.13 Razones para no denunciar

La elevada cifra oculta del ciberdelito tiene múltiples razones, incluida la percepción individual de que no se trata de un hecho importante o de que no es necesario que intervenga una autoridad oficial. También es relevante la falta de confianza en las autoridades de justicia y seguridad pública, así como el temor a represalias.

El motivo más común por el cual no se denuncia es que las víctimas consideran que el hecho no tuvo gran importancia. A esto puede sumarse el porcentaje de víctimas que dice no saber que la situación constituye delito o afirma que no lo es.

Por otro lado, un porcentaje de víctimas no denunció y dice haberlo resuelto a su manera (13.9 %), lo cual incluye diversas situaciones, desde medidas para prevenir la recurrencia hasta cerrar cuentas o cambiar claves.

Por último, un porcentaje relevante de personas (12.3 %) no cree que sirviera de algo denunciar; asimismo, un 2.9 % menciona que no habría sido apropiado o necesario que la policía o autoridad interviniera (ver gráfico 4).

Gráfico 4 Distribución porcentual de las razones para no denunciar el último caso de ciberdelito, 2021



Fuente: Elaboración propia a partir de los datos de la Encuesta sobre ciberdelito en Centroamérica y República Dominicana

6. Monitoreo de redes sociales

Entre el 1 de junio y el 19 de agosto de 2021, a través del servicio Social Listening de la plataforma Digimind, se realizó un ejercicio de recopilación y análisis de mensajes y contenidos de las redes sociales para descubrir tendencias y temas importantes relacionados con la ciberseguridad y el ciberdelito en los países de Centroamérica y República Dominicana que participaron en la Encuesta de Ciberdelito (Guatemala, Honduras, El Salvador, Costa Rica y República Dominicana).

Las tendencias identificadas en este ejercicio son consistentes entre países, aunque existen algunos acentos particulares en cada uno. Entre las tendencias más importantes están:

- Publicación de muchos mensajes sobre perfiles e información falsos difundidos en redes sociales.
- Publicaciones y comentarios sobre los ciberataques contra el gobierno de Estados Unidos y empresas de ese país, que ocurrieron en el período de observación.
- Comentarios sobre pornografía, en especial infantil, motivados por el arresto de una *youtuber* muy conocida por posesión de pornografía infantil.
- Mensajes sobre posible *software* malicioso y cómo protegerse del hackeo de dispositivos o cuentas de correo electrónico y redes sociales.
- En el caso de El Salvador, se difundieron muchos mensajes sobre delitos relacionados con robo o hurto de criptomonedas, en el contexto del anuncio de la adopción del *bitcoin* como moneda de curso legal en ese país.
- En Guatemala, se enviaron mensajes sobre estafas en línea, extorsiones y otros delitos, a través de tecnologías de la información y la comunicación.

Las conversaciones y la discusión sobre delitos informáticos están presentes en redes sociales. Sin embargo, el conjunto de mensajes y publicaciones que se revisaron en el ejercicio mencionado muestra que lo que se difunde no siempre es preciso y no aporta información concreta de cómo protegerse de las amenazas del ciberdelito.

Los datos de la encuesta indican una incidencia casi universal del ciberdelito y las amenazas informáticas. Efectivamente, al estar la mayor parte de la población cada vez conectada a Internet usando diversos servicios, que van de redes sociales a plataformas financieras digitales, la exposición es constante.

Al mismo tiempo, el grado de denuncia contra el ciberdelito es bajo. Además, en muchos casos, las personas desestiman el hecho sufrido y la posibilidad de contar con apoyo de parte de las autoridades.

Todos los grupos poblacionales están expuestos al ciberdelito. Ciertos tipos de delito afectan más a algunos grupos, como es el caso del ciberacoso, donde la victimización hacia las mujeres es más frecuente.

No todas las denuncias son canalizadas hacia las autoridades oficiales de seguridad pública y justicia. En repetidas ocasiones, especialmente en cuanto a robo de información financiera, las personas denuncian con los bancos y empresas.

El análisis de las redes sociales muestra que existe la difusión de noticias sobre ciberataques, perfiles falsos y casos de pornografía infantil y otros delitos cometidos a través de la Internet. Sin embargo, no aportan de manera concreta a la prevención o detección de los ataques informáticos.

7. Hacer frente al ciberdelito

Enfrentar la amenaza del ciberdelito, que es ubicua para toda la población, requiere de una estrategia con múltiples frentes, que fortalezca las capacidades de las personas y organizaciones para conocer, prevenir y protegerse frente a los riesgos cibernéticos, que refuerce la capacidad de las autoridades para recibir y procesar las denuncias recibidas, y que permita a la ciudadanía confiar para acudir a las autoridades de manera fácil y que sus derechos y privacidad no sean vulnerados de nuevo.

A continuación, se delinean cinco ejes principales para una estrategia de contención del ciberdelito para la región. Estos contienen múltiples elementos que debieran ser desarrollados en cada país, para alcanzar las competencias necesarias para un combate eficaz a la ciberdelincuencia. Estos cinco ejes son:

1. Educación, prevención y protección, que se enfoca en fortalecer los conocimientos y herramientas de las personas para no ser víctimas de ciberdelitos.

2. Plataformas de atención y denuncia: con el fin de brindar a la ciudadanía herramientas sencillas y confiables para acudir a las autoridades y buscar protección frente al ciberdelito.
3. Ajuste del marco legal que permita la medición del ciberdelito en los códigos penales.
4. Mejora de las capacidades de las autoridades para investigar el ciberdelito y atender a las víctimas; incluye el marco legal, las capacidades técnicas y las alianzas estratégicas.
5. Tránsito hacia una medición uniforme de los ciberdelitos en los códigos penales.

8. Educación, prevención y protección

Es innegable que las herramientas digitales e Internet ofrecen oportunidades únicas de información, entretenimiento y negocios para las personas. Desafortunadamente, la exposición al crimen informático crece junto con el uso de los servicios digitales. Por tal razón, las personas y organizaciones deben estar bien informadas y comprender la magnitud de los riesgos generados por el ciberdelito, así como conocer y ser capaces de utilizar medidas de protección de sus datos y cómo reaccionar frente a las amenazas.

Las recomendaciones se hacen en tres categorías: conocimiento, prevención y reacción.

a. Conocimiento

Los usuarios deben conocer las amenazas existentes, las formas en las que se producen, el impacto de ser víctima de una de ellas y cuáles de estas constituyen ciberdelito.

Esta es una responsabilidad compartida por todos, donde las autoridades pueden generar campañas de difusión de conocimiento que expliciten la manera en que los atacantes vulneran la información y los servicios de los usuarios, y visibilizar la prevalencia y la relevancia de las amenazas existentes.

b. Prevención

Muchos de los delitos informáticos cometidos se facilitan porque los usuarios no implementan las medidas de protección y prevención disponibles. El conjunto de estas es amplio e incluye el uso de contraseñas seguras que se renuevan frecuentemente, la utilización de mecanismos de doble verificación, la activación de controles de privacidad en redes sociales, la evitación de acciones inseguras (como seguir vínculos de correos electrónicos sospechosos) o la instalación de *software* de fuentes poco seguras. Incluso en el caso de las organizaciones, las principales vulnerabilidades están en acciones tomadas por individuos sin pleno conocimiento de sus consecuencias. Estas

también deben tomar medidas para encriptar y respaldar sus datos y contar con mecanismos de recuperación ante ataques.

c. Reacción

Si bien el conocimiento y la prevención permiten reducir el número de amenazas que se materializan, la sofisticación de los atacantes siempre va en aumento. Por tal razón, es importante que las personas conozcan cómo reaccionar frente a estos casos, ante quién denunciar y cuáles son los mecanismos a su disposición para minimizar el daño causado.

9. Plataformas y mecanismos de atención y ayuda

Los datos de la encuesta sobre ciberdelito en la región, así como otros datos disponibles a nivel internacional, señalan la gran magnitud de la cifra oculta del ciberdelito.

Para reducir la magnitud de la cifra oculta, el primer paso es la educación ciudadana, por un lado, para reducir los casos de ciberdelito; por el otro, concienciar sobre los riesgos existentes y los canales para reaccionar ante incidentes. Sin embargo, una vez hecho esto, es importante también poder recibir y canalizar las denuncias y consultas ciudadanas de manera ágil y minimizar los costos para las víctimas.

Para abordar este reto de manera concreta, se proponen tres ejes:

a. Plataforma accesible para denuncia

Uno de los primeros contactos de la autoridad con el ciberdelito puede hacerse a través de una plataforma amigable con las víctimas y otros usuarios que buscan información. Estas plataformas ya han sido implementadas en el ámbito internacional, e incluye el Internet Crime Complaint Center del FBI en Estados Unidos (<https://www.ic3.gov/>) y ReportCyber en Australia (<https://www.cyber.gov.au/acsc/report>).

b. Seguimiento

Si bien la existencia de una plataforma es importante como primer paso para la recepción de consultas y denuncias, estas deben recibir un seguimiento adecuado para generar confianza en la ciudadanía y proporcionar apoyo y atención a las víctimas. Por tanto, se requiere también de un equipo humano calificado para atender y priorizar las quejas recabadas.

c. Formar en uso y relevancia de la plataforma

Al mismo tiempo que la ciudadanía debe comprender la naturaleza de las amenazas del ciberdelito, sus mecanismos de acción y las maneras de protegerse, también es importante que conozca en qué casos sus derechos se han vulnerado, y la legislación le permite acudir para denunciar y buscar apoyo ante las autoridades o ante las empresas que prestan servicios canalizados a través de herramientas informáticas.

Se requerirá de una campaña constante de formación sobre la existencia y el uso de la plataforma de denuncia y otros canales de atención, los derechos de las personas frente a las amenazas informáticas y la manera en que las denuncias se procesan e investigan.

10. Investigación del ciberdelito y atención a víctimas

Además de la educación y las plataformas técnicas, el combate al ciberdelito también involucra la capacidad de las autoridades para detectar, combatir y perseguir el ciberdelito.

Debido al grado de sofisticación de los creadores de amenazas informáticas y su posible ubicación en jurisdicciones difíciles de alcanzar, la estrategia de combate al ciberdelito debe abrir frentes diversos que incluyen:

a. Definición de responsabilidades

Debe definirse la responsabilidad de los proveedores de servicios (plataformas de servicios de *software* y servicios de conectividad) para incentivar la adopción de medidas de prevención, detección y reacción frente a las actividades informáticas criminales. Asimismo, se requiere explicitar a los usuarios cuál es su nivel de responsabilidad individual y cómo minimizar su exposición al ciberdelito.

b. Marco legal

Aunque algunos países en la región han avanzado en generar marcos legales vinculados al delito informático (ver anexo), queda mucho camino por andar en la adecuación de los marcos legales, en particular en temas relacionados con la privacidad y el uso de los datos. El Banco Interamericano de Desarrollo (BID, 2020) califica a tres países de la región: Guatemala, Honduras y El Salvador, con puntajes muy bajos (entre 1 y 2 de 5 puntos en las dimensiones relacionadas con el marco regulatorio para el ciberdelito, y a Costa Rica y República Dominicana, con un mayor avance: entre 2 y 3 puntos).

c. Capacidad técnica

La persecución efectiva del ciberdelito exige contar con equipos humanos altamente calificados, capaces de rastrear e identificar a los autores de las amenazas cibernéticas y de proteger o recuperar los recursos vulnerados a las víctimas. A su vez, esto exige de una estrategia proactiva de reclutamiento y capacitación de los equipos de atención. También, es importante la competencia en atender a las víctimas y proteger sus derechos.

d. Colaboración interinstitucional y con el sector privado

Finalmente, la amenaza del ciberdelito es demasiado compleja para ser abordada por un único agente. Por tanto, se requiere de la colaboración activa de los proveedores de servicios informáticos y plataformas digitales, del sistema financiero y de las agencias internacionales, para potenciar los esfuerzos de las autoridades por frenar y perseguir el ciberdelito.

11. Enfrentar el ciberdelito desde lo público y a través de la colaboración internacional

a. Participación en iniciativas internacionales

Una de las características definitorias del ciberdelito es su carácter remoto. Esto supone que personas o redes pueden cometer ilícitos desde otras jurisdicciones y hacer uso de infraestructuras tecnológicas multinacionales. Por ello, el combate al ciberdelito no puede realizarse desde un solo país, sino que debe formar parte de una estrategia concertada a nivel internacional, lo que implica tanto hacer uso de iniciativas globales para potenciar las capacidades de cada país con el fin de detectar y combatir el ciberdelito como tomar parte activa en iniciativas y grupos de tarea donde se investigan, promueven y adoptan enfoques actualizados para el combate del cibercrimen. Esto incluye el aprovechamiento de los recursos de agencias como la INTERPOL y la AMERIPOL, para desarrollar esos enfoques y mejorar las capacidades de las entidades de persecución del delito en cada país de la región.

Debido a que la tecnología informática avanza en forma continua y acelerada, el abordaje del ciberdelito debe tener un enfoque similar ágil, capaz de reconocer y reaccionar ante las nuevas amenazas.

b. El ciberdelito en lo público

La mayor visibilidad del ciberdelito ocurre cuando este afecta a grandes números de personas o cuando se vulneran los sistemas de grandes empresas. Sin embargo, al mismo tiempo, el ciberdelito también ataca y se infiltra en los sistemas de las instituciones oficiales, tanto vulnerando los

sistemas y la información pública como estableciendo mecanismos para fraudes informáticos y esquemas de corrupción.

Por esta razón, los gobiernos deben establecer también mecanismos de control y detección de este tipo de esquemas, por un lado, creando resiliencia en los sistemas informáticos para repeler y recuperarse de los ataques, por otro, estableciendo instancias de detección de irregularidades cometidas a través de los sistemas de información.

Por último, corresponde también al gobierno establecer marcos regulatorios que establezcan mínimos de seguridad para los sistemas financieros, el comercio electrónico y otras actividades que ocurren a través de sistemas informáticos, para proteger la seguridad de empresas y personas frente al ciberdelito. Esto es especialmente importante dadas las todavía limitadas capacidades instaladas para reconocer y enfrentar estas amenazas.

Reflexión final

El mundo tiende hacia la virtualización y el trabajo remoto, a un uso cada vez mayor de plataformas digitales y a conducir los negocios y la vida privada de las personas a través de estas herramientas.

En este contexto, proteger los derechos de las personas y organizaciones es un reto enorme que requiere de una estrategia activa y de la actualización constante, así como de una amplia colaboración interinstitucional que vincule también al sector público y privado.

La estrategia delineada sobre cinco ejes —educación, recursos para la ciudadanía y capacidad de investigación del ciberdelito— resalta áreas fundamentales para el combate de las amenazas informáticas, que seguirán estando presentes y crecerán en sofisticación. Por este motivo, las autoridades tendrán que actualizar y diseñar nuevas estrategias a medida surjan nuevos riesgos.

Centroamérica y República Dominicana han alcanzado un elevado grado de digitalización que, combinado con las limitadas capacidades institucionales y un marco legal que avanza con cierto rezago, implica una gran exposición a las amenazas del ciberdelito. Para la región, actualizar sus estrategias y mejorar las capacidades de respuesta de sus autoridades adquieren un grado de urgencia.

Se espera que este informe, que resume tendencias y datos recolectados durante 2020 y 2021, sirva para motivar la reflexión y conducir a la acción frente a estas amenazas.

Referencias

- Banco Interamericano de Desarrollo. (2020). *Reporte Ciberseguridad 2020*. <https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf>
- Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S. y Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies, Volumen(23)*: sup1, S47-S59. <https://doi.org/10.1080/14616696.2020.1804973>
- Cyber Security Agency of Singapore. (2021). *Singapore Cyber Landscape 2020*. <https://www.csa.gov.sg/News/Publications/singapore-cyber-landscape-2020>
- Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., and Hess, J. (2018). *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. Overview booklet*. World Bank. <https://openknowledge.worldbank.org/bitstream/handle/10986/29510/211259ov.pdf>
- Federal Bureau of Investigation. (2020). *Internet Crime Report 2020*. Internet Crime Complaint Center, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- Goddard, W. (27 de mayo de 2021). *Cyber Security Statistics 2020*. IT Chronicles. <https://itchronicles.com/information-security/cyber-security-statistics-2020/>
- Help Net Security. (14 de abril de 2021). *330 million people across 10 countries were victims of cybercrime in 2020*. <https://www.helpnetsecurity.com/2021/04/14/victims-of-cybercrime/>
- IPANDETEC Centroamérica. (2020). *Centroamerica cibersegura*. https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/04/CIBERSEGURIDAD_IPANDETEC.pdf
- Lucas, G. (2020). *Cybersecurity: A brief analysis on the Central American Context*. <https://www.a-id.org/cybersecurity-a-brief-analysis-on-the-central-american-context/>
- Mahadevan, P. (2020). *Cybercrime Threats during the COVID-19 Pandemic*. Global Initiative Against Transnational Organized Crime. <https://globalinitiative.net/wp-content/uploads/2020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf>

- Morgan, S. (Ed.) (s. f.). *2019 Official Annual Cybercrime Report*. Cybersecurity Ventures.
<https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>
- Morgan, S. (2020) *Cybercrime to Cost the World \$10.5 Trillion Annually by 2025*.
<https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>
- Oficina de las Naciones Unidas contra la Droga y el Delito. (Febrero de 2020). *La ciberdelincuencia en resumen*. <https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-in-brief.html#:~:text=La%20ciberdelincuencia%20es%20un%20acto,%2C%202012%3B%20Maras%2C%202014%3B>
- Programa de las Naciones Unidas para el Desarrollo. (2021). *América Latina y el Caribe: Gobernanza Efectiva, más allá de la recuperación*.
- Programa de las Naciones Unidas para el Desarrollo-Infosegura. (2021). *Encuesta sobre ciberdelito en Centroamérica y República Dominicana*.
- Radoini, A. (2020). *Cyber-crime during the COVID-19 Pandemic*. *Freedom From Fear Magazine, Issue 16*. United Nations Interregional Crime and Justice Research Institute.
<http://f3magazine.unicri.it/?p=2085>
- Unión Internacional de Telecomunicaciones (2021a). Porcentaje de personas que utilizan Internet.
<https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2021/December/PercentIndividualsUsingInternet.xlsx>
- Unión Internacional de Telecomunicaciones (2021b). Suscripciones de banda ancha móvil.
https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2021/December/MobileBroadbandSubscriptions_2007-2020.xlsx
- Verizon (2021). Data Breach Investigations Report. <https://vigitrust.com/wp-content/uploads/2021/05/John-Grim-Insights-from-the-2021-Data-Breach-Investigations-Report.pdf>

Anexo: Marcos legales para el combate contra el ciberdelito en la región de Centroamérica y República Dominicana

- Costa Rica: Decreto Legislativo 9048, que reformó el Código Penal para introducir formalmente disposiciones para el delito cibernético, y Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Ley 8968).
- El Salvador: Ley Especial contra los Delitos Informáticos y Conexos (Decreto Legislativo 260 del 4 de febrero de 2016, publicada en el Diario Oficial No. 40, Tomo 210 y reformada el 7 de diciembre de 2021) y Decreto 133 de la Ley de Firma Electrónica del 1 de octubre de 2015, publicada en el Diario Oficial No. 196, Tomo 409 y reformada el 20 de julio de 2021.
- Guatemala: Código Penal, Decreto 17-73, artículo 274, literales del (a) al (h). La legislación sobre una Ley de Combate a la Ciberdelincuencia y una Ley de Protección de Datos Personales se encuentran en discusión ya por varios años.
- Honduras: no existe una legislación específica, aunque en 2021 se debatió en el Congreso la Ley Nacional de Ciberseguridad y Medidas de Protección ante los Actos de Odio y Discriminación en Internet y Redes Sociales, y la Ley de Protección de Datos Personales.
- Nicaragua cuenta con varios cuerpos legales relacionados con la ciberseguridad, incluidas la Ley 787 (Ley de Protección de Datos Personales) y la Ley 919 (Ley de Seguridad Soberana), además del Código Penal.
- Panamá tampoco cuenta con una ley específica, si bien el Código Penal ha sido reformado para incluir conductas asociadas al ciberdelito.
- República Dominicana: la Ley 53-07301 sobre Crímenes y Delitos de Alta Tecnología y la 172-13, que tiene por objeto “la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados”.

Fuente: BID (2020) e IPANDETEC (2020)



*info*SEGURA

**Forma
ción**

