ODILA

Observatorio de Delitos Informáticos de Latinoamérica

Informe 2017

Contenido

¿Qué es ODILA?

ODILA (Observatorio de Delitos Informáticos de Latinoamérica) nace a partir de la necesidad de dar a conocer el problema de la cifra negra de los delitos informáticos, buscando informar a la sociedad sobre la legislación vigente en la materia y fomentando la realización de denuncias formales ante los organismos competentes.

Misión

Brindar un ámbito virtual donde todas aquellas personas que hayan sido víctimas de algún tipo de un delito informático en Latinoamérica, puedan reportar e informar de manera 100% electrónica sobre el hecho ocurrido, con el fin de recolectar información que permita saber el estado de situación en materia de delitos informáticos en la región.

Visión

Entendemos que la falta de estadísticas oficiales sobre los delitos informáticos ocurridos representa un aspecto sustancialmente problemático que impide desarrollar un trabajo serio de observación, análisis y elaboración de estrategias o planes a mediano o largo plazo orientados a combatir el cibercrimen.

En este marco ODILA busca construir un espacio de investigación y trabajo, especialmente dedicado a relevar y recolectar información sobre delitos informáticos ocurridos en Latinoamérica, con la finalidad de generar, sistematizar y difundir información sobre el problema de la cifra negra y la necesidad de fomentar la realización de denuncias por parte de los particulares que sean víctimas.

Objetivos

- Proponer una alternativa que permita combatir el problema de la cifra negra en materia de delitos informáticos en los países de América Latina.
- Generar, sistematizar y difundir información relevante para estudiar, investigar e incidir en la problemática de los delitos informáticos en países de América Latina.

Objetivos específicos

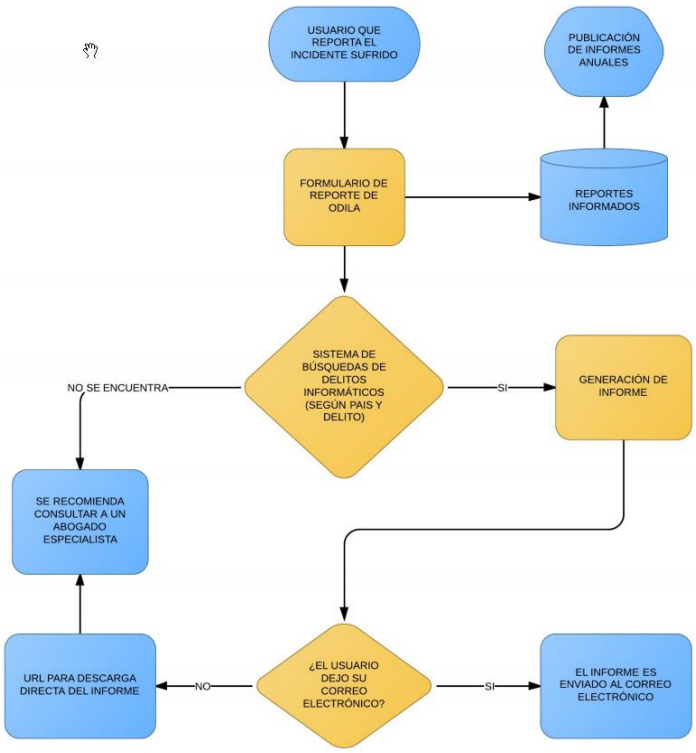
- Informar sobre el problema de la cifra negra en materia de delitos informáticos.
- Difundir consejos e información útil para las víctimas de delitos informáticos.
- Generar informes y estadísticas propias sobre la ciberdelincuencia en Latinoamérica.
- Fomentar en el usuario la realización de denuncias para los casos de delitos informáticos.

Aclaraciones

- ODILA no pretende ser un asesoramiento a medida, razón por la cual se deja en claro que el usuario debe siempre consultar ante un profesional especializado en la materia.
- El sistema ODILA no garantiza la exactitud de los resultados en relación a sobre si el hecho efectivamente puede ser considerado un delito penal en el país indicado por el usuario, sino que simplemente brinda un acercamiento a la materia, destacando que su principal objetivo siempre es la concientización acerca de la importancia de dar conocer la problemática y, sobre todo, fomentar la realización de denuncias que permita un combate eficaz frente al problema de la cifra negra.
- ODILA no requiere que el usuario brinde datos personales para poder utilizar el sistema, es decir que el reporte puede ser realizado de forma totalmente anónima. Opcionalmente el usuario puede informar un correo electrónico a fin de que los resultados y consejos sean enviados a dicha cuenta.

Metodología y Sistema

ODILA funciona a través de su sitio oficial www.ODILA.org, en el cuál el ciudadano puede reportar un incidente que haya sufrido, a fin de poder obtener una guía sobre si el hecho puede ser considerado un delito informático, de acuerdo a la legislación vigente en su país de residencia.



Etapas

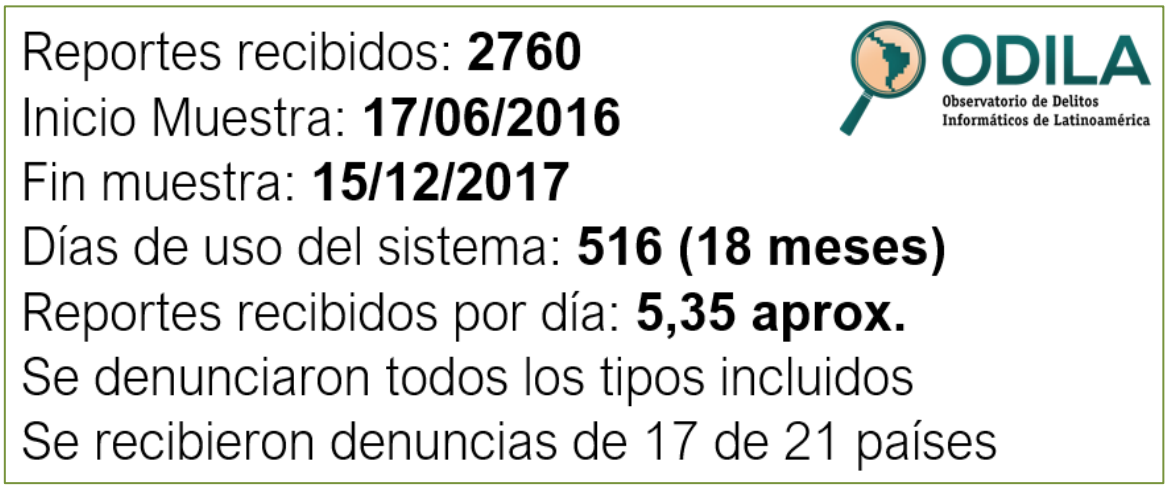
1. Recolección de información a partir del reporte realizado por el usuario a través del formulario de denuncia. Dicha información es recolectada a fines de elaboración de estadísticas y procesada por el sistema de búsquedas de delitos informáticos, de acuerdo al país de residencia y tipo de incidente sufrido.
2. En el caso que el sistema encuentre que en el país indicado ese hecho pueda ser encuadrado en algunos de los tipos penales vigentes, procederá a generar un informe, indicándose dichos artículos y algunas recomendaciones generales a tener en cuenta. También se ofrece información sobre los organismos competentes para que el ciudadano pueda realizar su denuncia formal, a fin de que el hecho pueda ser investigado por parte de las autoridades.
3. En el caso que el sistema no encuentre un tipo penal aplicable de acuerdo a los datos informados por el usuario, devolverá un mensaje informado sobre tal situación, sumado a la legislación vigente en dicho país.

Informes anteriores

- Informe ODILA 2015
- Informe ODILA 2016

Muestra de datos 2017

Este tercer informe de ODILA es generado a partir de **2.760 denuncias** recibidas entre el 17/06/2016 y el 15/12/2017, dando un promedio de **5 reportes diarios.**



Datos opcionales

ODILA es anónimo.

Dentro del formulario disponible para el reporte de incidentes en ODILA, se han incluido algunas preguntas opcionales -cerradas- relacionadas con información afín a las características personales de la víctima del incidente (edad, género, nivel de instrucción, tipo de víctima, etc.).

El fundamento de la inclusión de estas preguntas en el cuestionario tiene relación con la posibilidad de comprender qué tipos de víctimas son las afectadas, qué género, qué rangos etarios y hasta inclusive, que nivel de instrucción tienen las víctimas de la ciberdelincuencia.

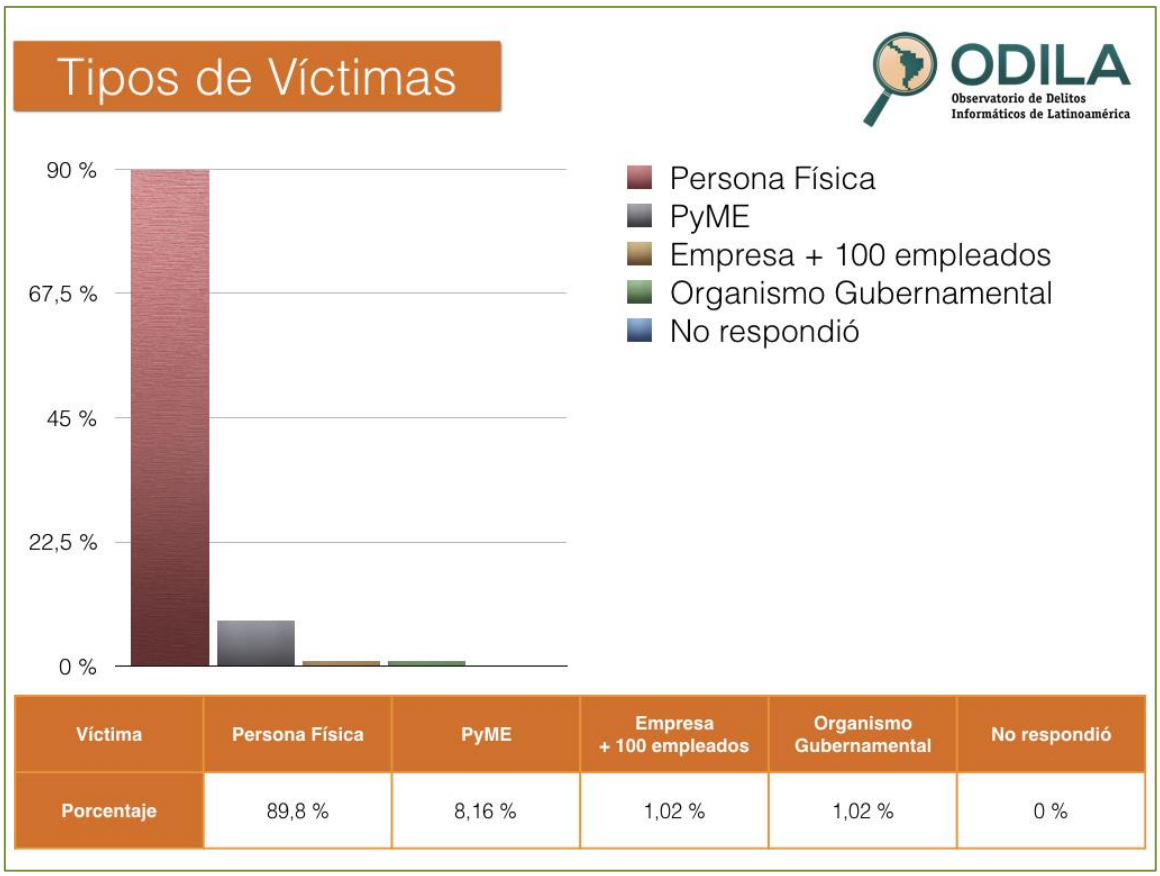
Consideramos que estos datos son de utilidad ya que, al poder determinarse cuáles son las características de los grupos sociales más afectados por los delitos informáticos, más posibilidades existen de pensar y poder trabajar sobre distintas acciones de capacitación y concientización sobre delitos informáticos y el cibercrimen.

Estas preguntas son de carácter opcional para los usuarios, para brindar un espacio de confidencialidad que, entendemos, es de suma importancia para quien decide reportar un caso.

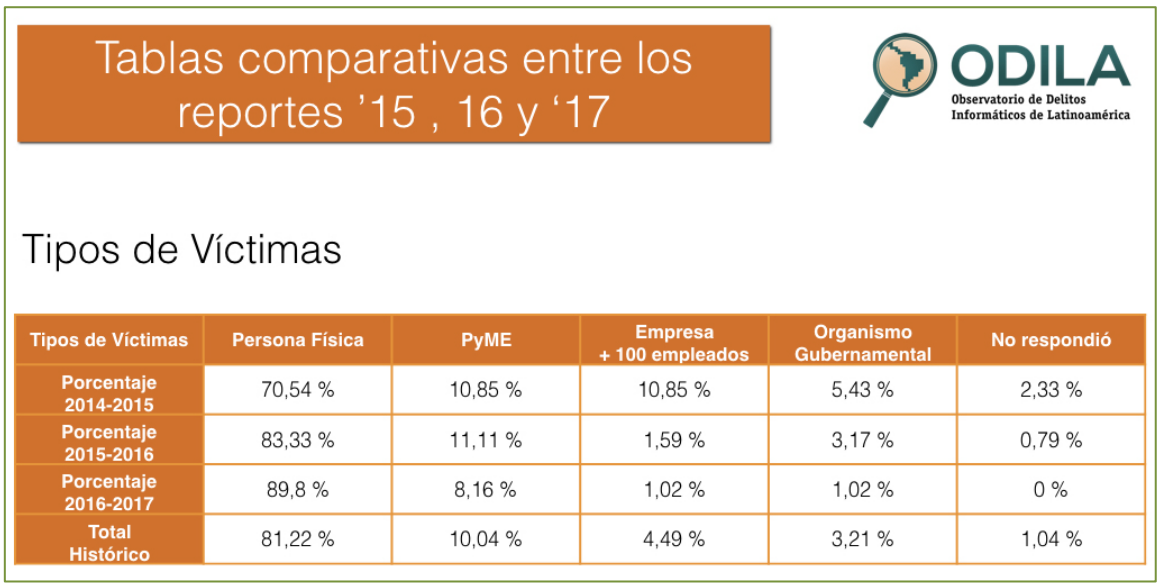
Sin embargo, pese al carácter opcional de estas preguntas, a través de las comparaciones de los últimos 3 informes, puede observarse como patrón en común que los usuarios están cada vez más dispuestos a brindar este tipo de información: este año, casi el 95% de las personas ha decidido brindar estos datos, y esto nos permite seguir trabajando sobre la perfilación de las víctimas de los delitos informáticos.

Tipos de Víctimas

En este tercer informe podemos observar que, nuevamente, el tipo de víctima que más utilizó los servicios del Observatorio son las personas físicas, alcanzando casi un 90 por ciento (89,8%) del total de los reportes recibidos, confirmándose una tendencia que permite concluir que cada vez son más las personas físicas las que deciden utilizar y reportar sus incidentes ante ODILA.



Víctima	Persona Física	PyME	Empresa + 100 empleados	Organismo Gubernamental	No respondió
Porcentaje	89,8 %	8,16 %	1,02 %	1,02 %	0 %



Tipos de Víctimas	Persona Física	PyME	Empresa + 100 empleados	Organismo Gubernamental	No respondió
Porcentaje 2014-2015	70,54 %	10,85 %	10,85 %	5,43 %	2,33 %
Porcentaje 2015-2016	83,33 %	11,11 %	1,59 %	3,17 %	0,79 %
Porcentaje 2016-2017	89,8 %	8,16 %	1,02 %	1,02 %	0 %
Total Histórico	81,22 %	10,04 %	4,49 %	3,21 %	1,04 %

Estos datos confirman uno de los objetivos principales del proyecto ODILA: ser una fuente de consulta e información para las personas, entendiendo que ellas son las que más necesitan contar con información adecuada que les permita poder realizar la denuncia ante los organismos competentes.

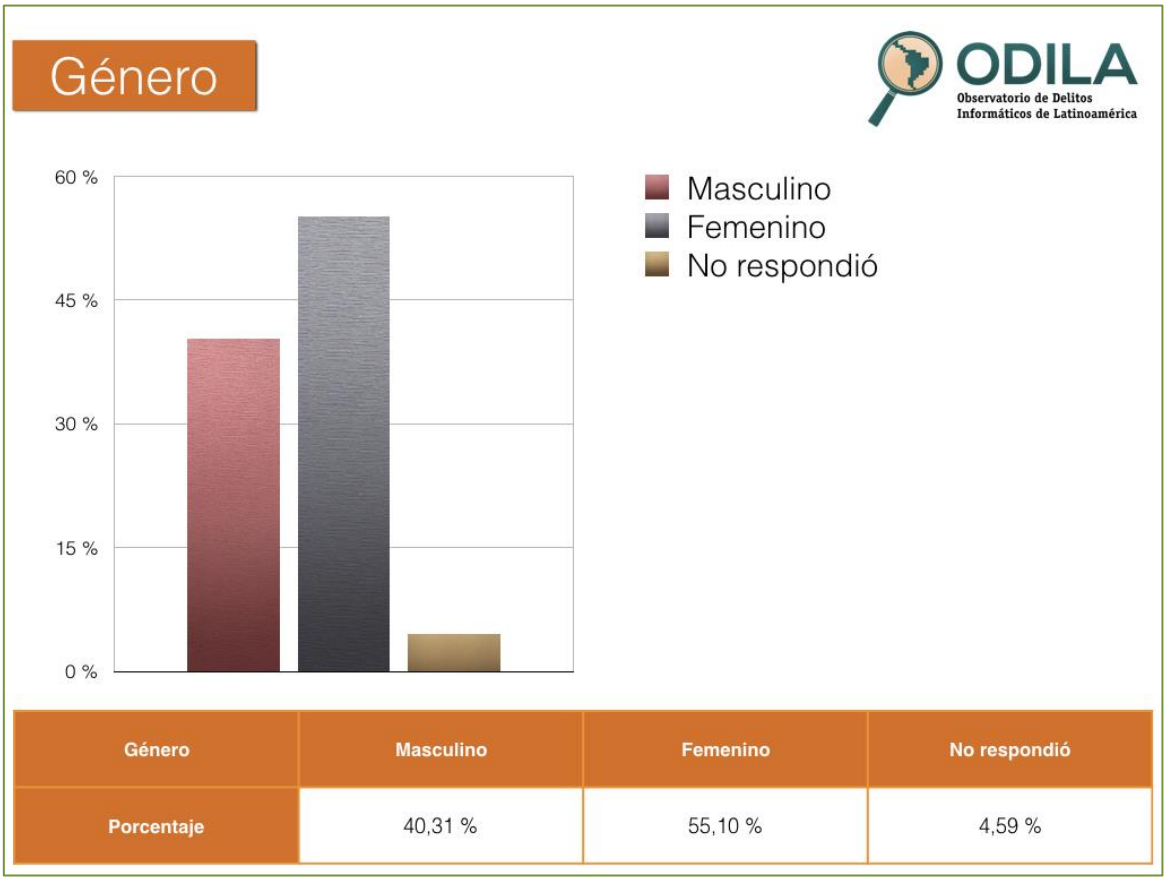
Las personas físicas, en comparación de un organismo -público o privado-, poseen menos recursos y posibilidades de estar adecuadamente informadas. Este hecho tiene consecuencias al momento de realizar las denuncias o al menos, de poder ejercer sus derechos frente a un posible delito informático.

En segundo lugar (8,16%) podemos observar a las Pequeñas y Medianas Empresas, quienes también sufren la falta de recursos y, ante la ocurrencia de incidentes, no saben cuál es la forma adecuada de actuar o de llevar adelante el ejercicio de sus derechos.

Finalmente, con el 1%, comparten el tercer y cuarto lugar las grandes empresas (más de 100 empleados) junto con los organismos públicos, entendiendo que son los tipos de víctimas que más posibilidades tienen de contar un adecuado asesoramiento profesional que les permita, en el caso que así lo decidan, llevar su caso a la justicia. Es también importante remarcar que muchas empresas deciden no denunciar ni hacer público los hechos delictivos porque eso expondría de forma negativa la empresa y/o la marca ante la opinión pública.

Género

En relación al Género de los usuarios de ODILA se puede observar que, por primera vez, los usuarios del género femenino han sido las que más reportes han realizado (55% de reportes).



Género	Masculino	Femenino	No respondió
Porcentaje	40,31 %	55,10 %	4,59 %

Género	Masculino	Femenino	No respondió
Porcentaje 2014-2015	44,96 %	31,01 %	24,03 %
Porcentaje 2015-2016	51,59 %	43,65 %	4,76 %
Porcentaje 2016-2017	40,31 %	55,10 %	4,59 %
Total Histórico	45,62 %	43,25 %	11,13 %

De acuerdo a esta apreciación, y haciendo una interpretación de los resultados en los últimos informes, podemos observar que las diferencias entre un género y otro no son tan marcadas, por lo que no podría concluirse de forma determinante que exista una tendencia de ataques a un género determinado.

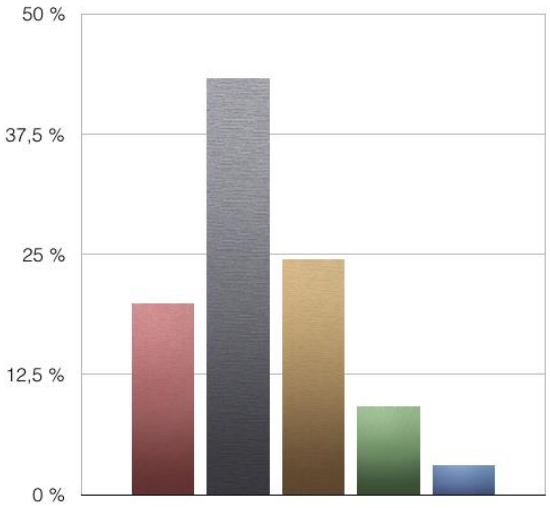
Esta interpretación podría ser compatible con la característica de masividad que tienen la mayoría de los ataques informáticos, donde el delincuente no busca un objetivo determinado -modalidad *spear phishing*- sino que busca aumentar su porcentaje de éxito realizando ataques de forma masiva y aleatoria.

Por otro lado, se observa que sigue bajando la tasa de personas que deciden no informar este dato, expresando lo que podría significar un mayor nivel de confianza de los usuarios con el Observatorio.

Edad

En relación a la Edad de los usuarios de ODILA, podemos observar que la franja etaria más atacada, con un 43,37%, sigue siendo aquella entre 22 y 35 años de edad.

Edad



Menores de 21 años
Entre 22 y 35 años
Entre 36 y 45 años
Más de 45 años
No respondio

Edad	Menores de 21 años	Entre 22 y 35 años	Entre 36 y 45 años	Más de 45 años	No respondio
Porcentaje	19,90 %	43,37 %	24,49 %	9,18 %	3,06 %

Tablas comparativas entre los reportes '15 , 16 y '17

Edad

Edad	Menores de 21 años	Entre 22 y 35 años	Entre 36 y 45 años	Más de 45 años	No respondio
Porcentaje 2014-2015	15,50 %	36,43 %	16,28 %	12,40 %	19,38 %
Porcentaje 2015-2016	23,81 %	34,92 %	19,84 %	16,67 %	4,76 %
Porcentaje 2016-2017	19,90 %	43,37 %	24,49 %	9,18 %	3,06 %
Total Histórico	19,74 %	38,24 %	20,20 %	12,75 %	9,07 %

La interpretación sobre este dato, puede estar relacionada con dos aspectos centrales. En primer lugar, estos jóvenes son, probablemente los adultos que cuenta con mayor nivel de conectividad y dependencia tecnológica, por lo que en definitiva terminan siendo más vulnerables o susceptibles a ser víctimas de los distintos tipos de ataques informáticos.

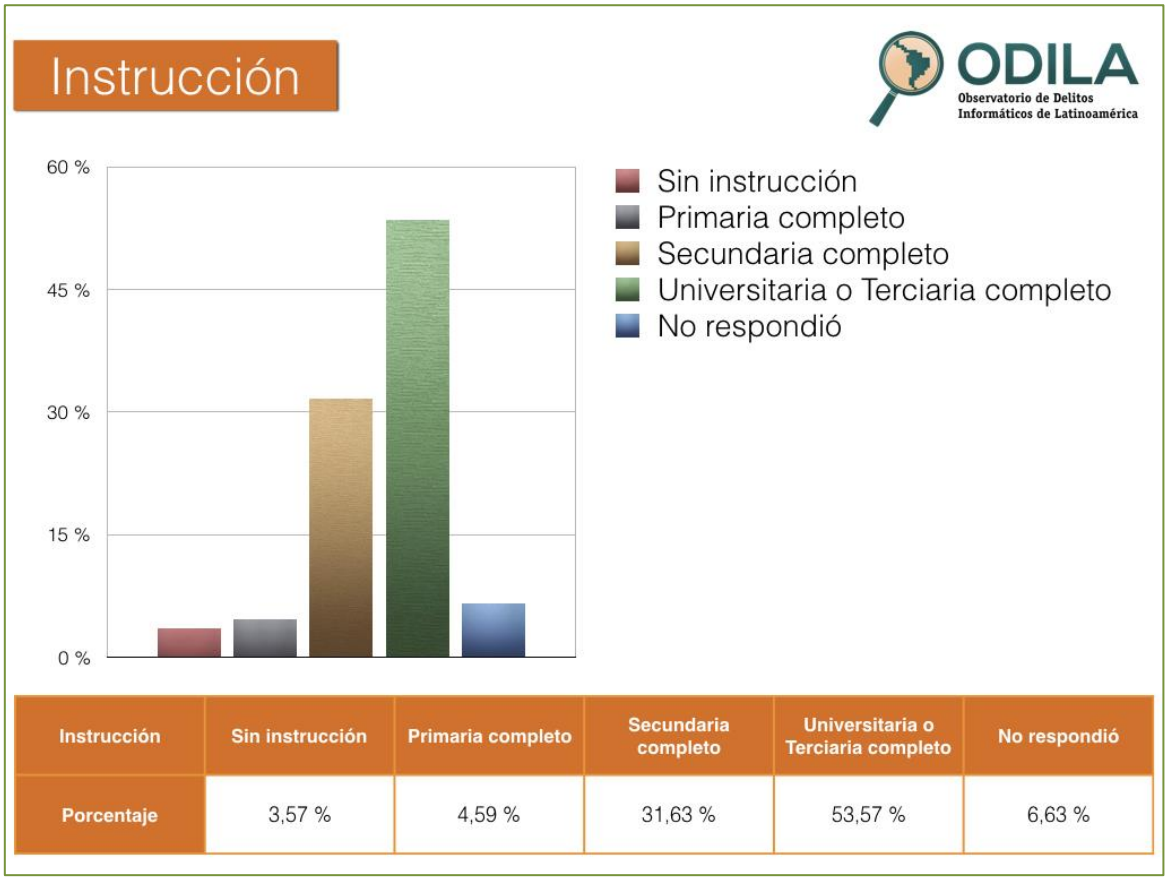
En segundo lugar, no debemos descartar que la difusión realizada sobre ODILA, de acuerdo a las posibilidades de quienes llevamos adelante esta iniciativa, ha tenido como foco distintos tipos de eventos, congresos, jornadas y seminarios relacionados a la Seguridad Informática y el Derecho Informático, así como eventuales jornadas en ámbitos universitarios. En todos ellos, los principales destinatarios de este tipo de difusión personal, justamente han sido personas en esta franja etaria.

Volviendo a los números obtenidos, en segundo lugar, con un 24,49% encontramos usuarios entre 36 y 45 años, seguidos por los menores de 21 años de edad (19,90). Finalmente, encontramos a los usuarios mayores de 45 años (9,18%).

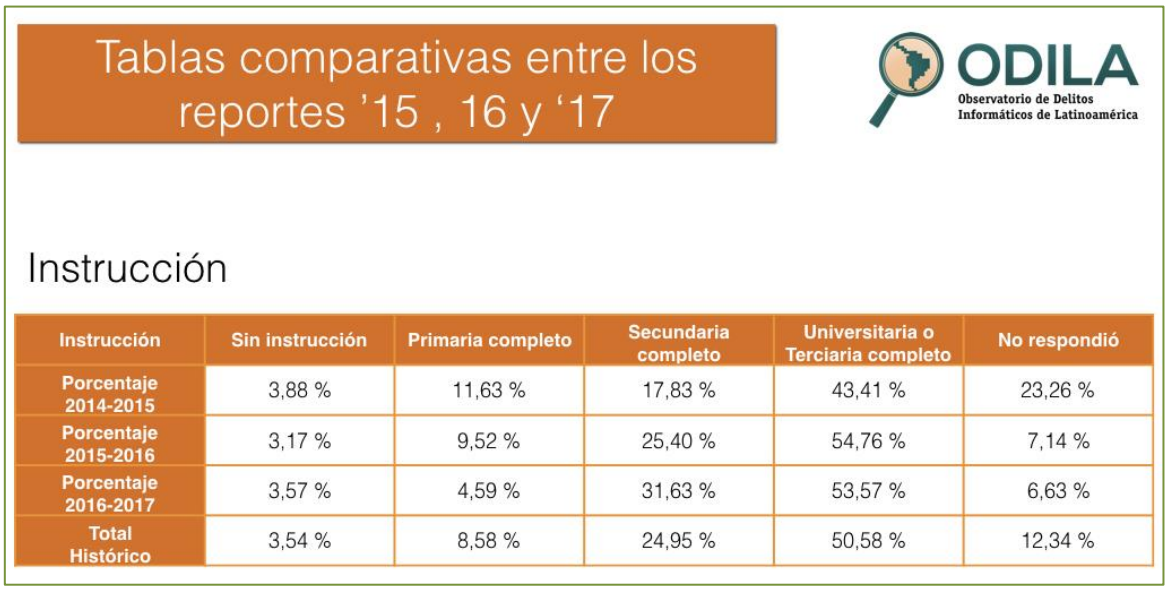
Como se observó en los otros datos opcionales, el porcentaje de los usuarios que han decidido no brindar información personal ha disminuido, siendo sólo de un 3%. Nuevamente, interpretamos que este descenso está relacionado con el aumento de confianza de los usuarios con respecto al Observatorio.

Instrucción

En relación a la Instrucción de los usuarios de ODILA, podemos observar que el grupo más atacado (y/o los que más reportan) posee estudios universitarios o terciarios completos, con un 50,6%. En segundo lugar, con el 25% se encuentran los usuarios con estudios secundarios completos.



Instrucción	Sin instrucción	Primaria completo	Secundaria completo	Universitaria o Terciaria completo	No respondió
Porcentaje	3,57 %	4,59 %	31,63 %	53,57 %	6,63 %



Instrucción

Instrucción	Sin instrucción	Primaria completo	Secundaria completo	Universitaria o Terciaria completo	No respondió
Porcentaje 2014-2015	3,88 %	11,63 %	17,83 %	43,41 %	23,26 %
Porcentaje 2015-2016	3,17 %	9,52 %	25,40 %	54,76 %	7,14 %
Porcentaje 2016-2017	3,57 %	4,59 %	31,63 %	53,57 %	6,63 %
Total Histórico	3,54 %	8,58 %	24,95 %	50,58 %	12,34 %

Al igual que se observó en los otros datos opcionales, el porcentaje de los usuarios que han decidido no brindar información personal ha disminuido (6,63%).

Como se puede observar a modo genérico en los últimos 3 informes, los más afectados son los usuarios de mayor nivel de instrucción. En relación a la interpretación de estos datos, es posible dar tres interpretaciones como mínimo:

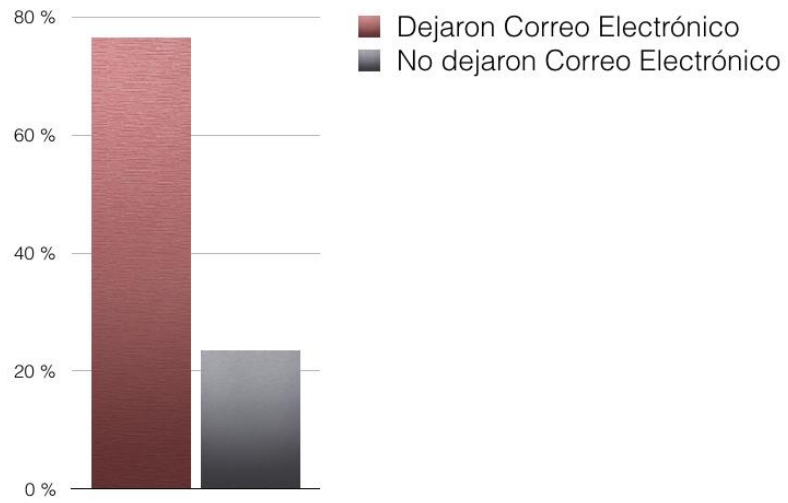
- En principio, la más sencilla y directa sería interpretar que, a mayor nivel de educación del usuario, más posibilidades hay de que sea atacado porque se vuelve un "objetivo" más apreciado por los delincuentes. Creemos que en principio esta interpretación debe ser moderada, considerando que el nivel de instrucción, por lo general, está ligado al nivel de utilización de las nuevas tecnologías y, por lo tanto, de la dependencia tecnológica. En este sentido, como ya hemos visto con relación a la edad, a mayor nivel de dependencia y utilización de las TICs, mayores posibilidades de ser víctima de un ataque informático.
- Una segunda lectura podría ser que, en realidad, el nivel de instrucción del usuario lo lleva a buscar información sobre el ataque del que ha sido víctima, y de esta forma llega a ODILA y completa su denuncia.
- La tercera lectura tiene que ver con la difusión de ODILA, que en general ha sido realizada en ambientes de seminarios, congresos y Universidades, donde promedian los usuarios de alto nivel de instrucción.

Correo electrónico

En relación al correo electrónico, como hemos explicado anteriormente, el mismo es un dato opcional que sólo tiene por finalidad que el resultado del informe realizado sea enviado a la cuenta de correo electrónico indicada.

Correo electrónico

ODILA
Observatorio de Delitos Informáticos de Latinoamérica



Correo Electrónico	Dejaron Correo Electrónico	No dejaron Correo Electrónico
Porcentaje	76,53 %	23,47 %

Tablas comparativas entre los reportes '15 , 16 y '17

ODILA
Observatorio de Delitos Informáticos de Latinoamérica

Correo Electrónico

Correo Electrónico	Dejaron Correo Electrónico	No dejaron Correo Electrónico
Porcentaje 2014-2015	62,79 %	36,43 %
Porcentaje 2015-2016	69,05 %	30,95 %
Porcentaje 2016-2017	76,53 %	23,47 %
Total Histórico	69,45 %	30,28 %

En este último año hemos podemos observar un incremento en el número de usuarios que han decidido utilizar esta opción (76,53%), algo que interpretamos -en coherencia con el resto de los datos opcionales analizados- como un aumento en el nivel de confianza de los usuarios con respecto al Observatorio.

También puede interpretarse como la necesidad de realizar o establecer algún contacto para mayor asesoramiento que demandan las víctimas: parte de la problemática observada en relación a la cifra negra de los ciberdelitos, se encuentra relacionada con que las víctimas no se sienten seguras para ir a denunciar, no saben dónde dirigirse y, en algunos casos, cuando se animan y se acercan a algún organismo público, no reciben el asesoramiento adecuado como para poder canalizar su caso.

Esto último es reflejado a través de la cantidad de correos electrónicos directos que nos llegan a través del formulario de contacto de ODILA, de personas que inicialmente completan el formulario recibiendo sus resultados, pero que se quedan demandando mayor nivel de información para sus situaciones particulares.

Lamentablemente, muchas de las consultas recibidas sobre casos particulares no pueden ser respondidas, porque implicaría una acción de asesoramiento al caso concreto, aspectos que exceden a las finalidades y objetivos de ODILA.

A continuación, compartimos -de forma anónima-, algunas de las consultas recibidas:

> *Una amiga que es una figura pública ha sufrido un acceso indebido a su teléfono móvil y le fueron extraídas fotografías y conversaciones privadas, además de apropiarse de sus cuentas de correo y redes sociales modificando las contraseñas, y también las configuraciones de correos y teléfono para recuperación. En Paraguay no hay mucho de esto por lo que nos sentimos desamparados para saber cómo proceder. El daño que está causando este delincuente informático es muy grave para esta persona y su familia. Aguardamos contacto. Saludos.*

> *Hola, me comunico con ustedes porque estoy siendo víctima de difamación, daño moral, extorsión, hackeo y suplantación de identidad en la web, desde el día 18 de julio del presente año, por seguridad no escribo mi nombre real y me gustaría saber a dónde puedo llamar o contactarme directamente para dar más detalles e información. No sé qué hacer esta persona me está destruyendo. Quedo atenta a sus respuestas lo antes posible. Gracias.*

> *Buen día, el día de hoy alguien filtró vía Facebook unas fotos mías desnuda las cuales solo las tenía una ex-pareja a través de un perfil falso, yo no di permiso de publicarlas, mucho menos pasarlas a mis familiares, necesito de su ayuda para llevar los trámites jurídicos yo nunca las hice públicas y tampoco si mi consentimiento para pasarlas a mis familiares, soy de México, gracias.*

> *Consulta: Conozco alguien que fue abusado de manera sexual. El agresor tomó fotos de ello y las publicó en varios sitios, pero el problema es que el afectado no es menor de edad, tiene 19 años, ¿Aun así se puede hacer una denuncia?*

> *Consulta: Estoy pasando por un momento complicado en el cual estoy siendo amenazada con subir imágenes mías a páginas de citas sin mi consentimiento de carácter íntimo por favor estoy desesperada no sé qué hacer me gustaría saber si pueden ayudarme darme información de que hacer donde denunciar.*

Denuncia

Entre los datos más importantes de ODILA se encuentra el indicador sobre si el usuario ha realizado la denuncia formal sobre el hecho del cuál (supone) ha sido víctima.

¿Ha denunciado?

¿Ha Denunciado?	No, no denuncié porque... (ver siguiente pregunta)	Si, ya denuncie y la investigación está en curso	Si, denuncie pero la investigación no avanzó	Sí, denuncié y ya se ha condenado al o los culpables.
Porcentaje	83,67 %	6,12 %	9,18 %	1,02 %

Tablas comparativas entre los reportes '15 , 16 y '17

¿Ha denunciado?

¿Ha Denunciado?	No, no denuncié porque...	Si, ya denuncie y la investigación está en	Si, denuncie pero la investigación no	Sí, denuncié y ya se ha condenado al o los
Porcentaje 2014-2015	68,22 %	16,28 %	15,5 %	0 %
Porcentaje 2015-2016	82,54 %	5,56 %	11,11 %	0,79 %
Porcentaje 2016-2017	83,67 %	6,12 %	9,18 %	1,02 %
Total Histórico	78,14 %	9,32 %	11,93 %	0,60 %

Es precisamente este indicador el que nos permite observar de forma directa el nivel de la cifra negra, es decir, la cantidad de delitos que realmente ocurren pero que no son tratados ni conocidos por el segmento penal y, en consecuencia, a los cuales el Estado no da respuesta alguna.

En este tercer informe puede observarse que el 83,67% de los usuarios ha reconocido que no ha denunciado el delito, observándose un leve incremento en relación al número obtenido en el período 2015-2016, lo cual nos permite confirmar nuevamente la existencia de la cifra negra, superior al 80%. Podríamos entonces afirmar que 8 de cada 10 delitos informáticos que ocurren, no llegan a ser conocidos por el Estado y, por lo tanto, no tienen ningún tipo de consecuencia penal.

Este número, confirma precisamente parte de la hipótesis de trabajo del Observatorio, donde se afirma que, en su gran mayoría, los delitos informáticos no son denunciados, existiendo un alto nivel de cifra negra de este tipo de incidentes.

Por otro lado, un 6,12% de los usuarios, ha reconocido haber hecho la denuncia formal y afirma que investigación del hecho se encuentra en curso. En cambio, el 9,18% restante que ha denunciado formalmente el hecho, dice que la investigación no avanzó (por distintos motivos).

Finalmente, sólo un 1% ha realizado la denuncia formal y dice que investigación ha finalizado y se ha logrado conseguir una condena efectiva sobre el imputado. Es decir, de cada cien delitos informáticos, sólo uno lograría llegar a obtener condena efectiva (sin tener en consideración el tipo de condena logrado).

En relación a la interpretación de estas cifras, cabría hacer una consideración en relación a los usuarios y, por lo tanto, a la información recolectada: es posible que una importante cantidad de los usuarios del Observatorio que completan las encuestas, sean aquellos que están en la etapa de “búsqueda de información”, es decir, aquellas víctimas de algún incidente de seguridad de la información que no saben si han sido víctima de un delito informático en particular, o dónde debe dirigirse para denunciarlo, por ejemplo. Por lo tanto, si los usuarios se encuentran en esta etapa, lo más probable es que afirmen que aún no han realizado sus respectivas denuncias

ante los organismos competentes. De hecho, ODILA pretende ser efectivamente una fuente de información para que los usuarios identifiquen si han sido víctimas, se informen sobre las dependencias estatales habilitadas y puedan ir a realizar allí sus denuncias. Esta interpretación, parte de la presunción que muchos de los usuarios del Observatorio, llegan al mismo a través de búsquedas voluntarias en Internet, intentando obtener información que les brinde una guía acerca de qué deberían hacer, o cuáles serían los pasos a seguir para denunciar un delito informático.

Para poder explicarlo de otra manera, es posible que quien ya haya realizado una denuncia formal, esté menos interesado en buscar información y, por lo tanto, en utilizar y aportar datos en ODILA. Incluso, el bajo interés de un usuario en aportar datos al Observatorio, se hace más evidente en aquellos casos en la víctima de algún delito, haya realizado una denuncia formal con resultados (o condena) positivos.

Causas de la No Denuncia

Los usuarios que han optado por indicar que aún no han realizado la denuncia formal correspondiente, tienen en este punto la posibilidad de indicar una o más causas por las cuáles aún no han denunciado.

Causas de la no denuncia

ODILA Observatorio de Delitos Informáticos de Latinoamérica

Causas	No creo que la denuncia sea útil, porque el sistema penal no es apto para combatir el cibercrimen	No quiero difundir públicamente el incidente (pérdida de confidencialidad)	No sé donde denunciar	No creo que la investigación tenga éxito	Tengo temor de futuras represalias de parte del autor	No creo en la Policía ni en la Justicia Penal	No estoy seguro de haber sido víctima de un delito penal	En parte me siento culpable por el incidente	Otros	No me considero víctima de un delito
%	16,94 %	16,12 %	14,88 %	14,05 %	14,05 %	9,09 %	6,20 %	3,31 %	3,31 %	2,07 %

Tablas comparativas entre los reportes '15 , 16 y '17

ODILA Observatorio de Delitos Informáticos de Latinoamérica

Causas de no denuncia

Causas	No creo que la investigación tenga éxito	No quiero difundir públicamente	No creo en la Policía ni en la Justicia Penal	No creo que la denuncia sea útil, porque el	Tengo temor de futuras represalias de	No sé donde denunciar	No me tomaron la denuncia	En parte me siento culpable por	No me considero víctima de un	Otros
Porcentaje 2014-2015	17,00 %	17,00 %	12,00 %	12,00 %	10,00 %	9,00 %	7,00 %	7,00 %	5,00 %	4,00 %
Porcentaje 2015-2016	16,19 %	12,38 %	8,57 %	5,71 %	16,19 %	19,05 %	4,76 %	0,95 %	13,33 %	2,86 %
Porcentaje 2016-2017	14,05 %	16,12 %	9,09 %	16,94 %	14,05 %	14,88 %	2,07 %	3,31 %	6,20 %	3,31 %
Total Histórico	15,75 %	15,17 %	9,89 %	11,55 %	13,41 %	14,31 %	4,61 %	3,75 %	8,18 %	3,39 %

En esta tercera etapa 2016-2017 se puede observar que el valor más alto (16,94%) ha sido el de aquellos que no creen que la denuncia sea útil porque piensan que el sistema penal no es apto para combatir la ciberdelincuencia.

Esta causa no se refiere a la falta de confianza hacia la justicia como servicio a la sociedad, que es otra de las opciones que se pueden seleccionar, sino una falta de expectativa a que la denuncia del delito sirva para lograr un cambio sobre el conflicto social base, incluso teniendo la posibilidad de llegar a una condena para el delincuente.

Es decir, de alguna forma la víctima piensa que incluso haciendo que el delincuente se haga responsable penalmente por la acción realizada, ello no aportará al cambio social necesario para que nuevos delitos sigan ocurriendo, considerando que el conflicto social base responde a otros factores.

En segundo lugar, con un porcentaje bastante similar (16,12%) se encuentran aquellos que deciden no realizar la denuncia porque no quieren difundir públicamente el hecho ocurrido. Es decir, el sistema no ofrece las condiciones de privacidad o confidencialidad para resguardar el nombre, honor o imagen de la víctima, ya sea una persona física o jurídica.

Muchas víctimas de distintos tipos de delitos informáticos deciden voluntariamente no denunciar sus casos, bajo el razonamiento que la posibilidad de difusión pública ocasionaría un daño peor al ya efectivamente sufrido. Es decir, las personas priorizan el requisito de la confidencialidad por sobre la necesidad de que dicho incidente sea investigado penalmente por las autoridades competentes.

En el caso de las organizaciones, este hecho también está asociado a que la exposición del incidente implicaría el reconocimiento público de haber sufrido el problema de seguridad, revelando la falta de medidas al respecto en algún caso, y generando, sobre todo, pérdidas de imagen sobre la organización. La difusión de la noticia sobre el incidente rápidamente podría transformarse en un perjuicio mayor para la víctima.

En tercer lugar (14,88%) se advierte la falta de información sobre el lugar en donde realizar la denuncia formal, y queda en evidencia uno de los aspectos más problemáticos que ODILA intenta combatir: la falta de información. Este índice, implica que la víctima está dispuesta a realizar la

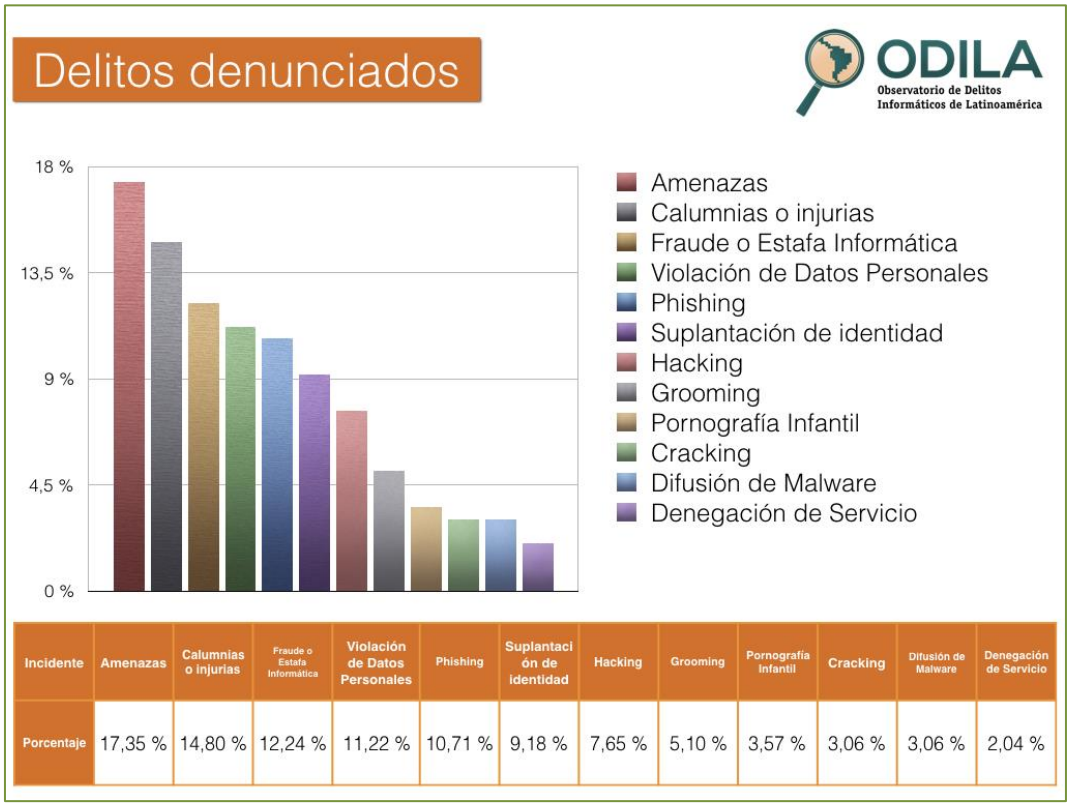
denuncia, pero que no encuentran en el Estado (del país que corresponda) una respuesta adecuada en cuanto a brindarle información oficial, o bien en un centro de respuesta o de atención a las víctimas de la ciberdelincuencia. Independientemente del organismo u oficina que se trate, cabe destacar la importancia que debería tener el acceso real para las víctimas.

En relación a las comparaciones de los resultados con los años anteriores, podemos observar algunas diferencias. Por ejemplo, en la etapa 2015-2016: las víctimas no sabían dónde ir a realizar las denuncias (19,05%), no creían que la investigación tenga éxito (16,19%) y tenían temor a futuras represalias por parte del autor del delito (también 16,19%). Esto demuestra por un lado la falta de confianza en la justicia, y por otro, el hecho que las víctimas se sienten indefensas frente a un victimario "invisible", que desconocen y que, por lo tanto, no saben si podría volver a atacarlos y provocarles un daño mayor como forma de represalia.

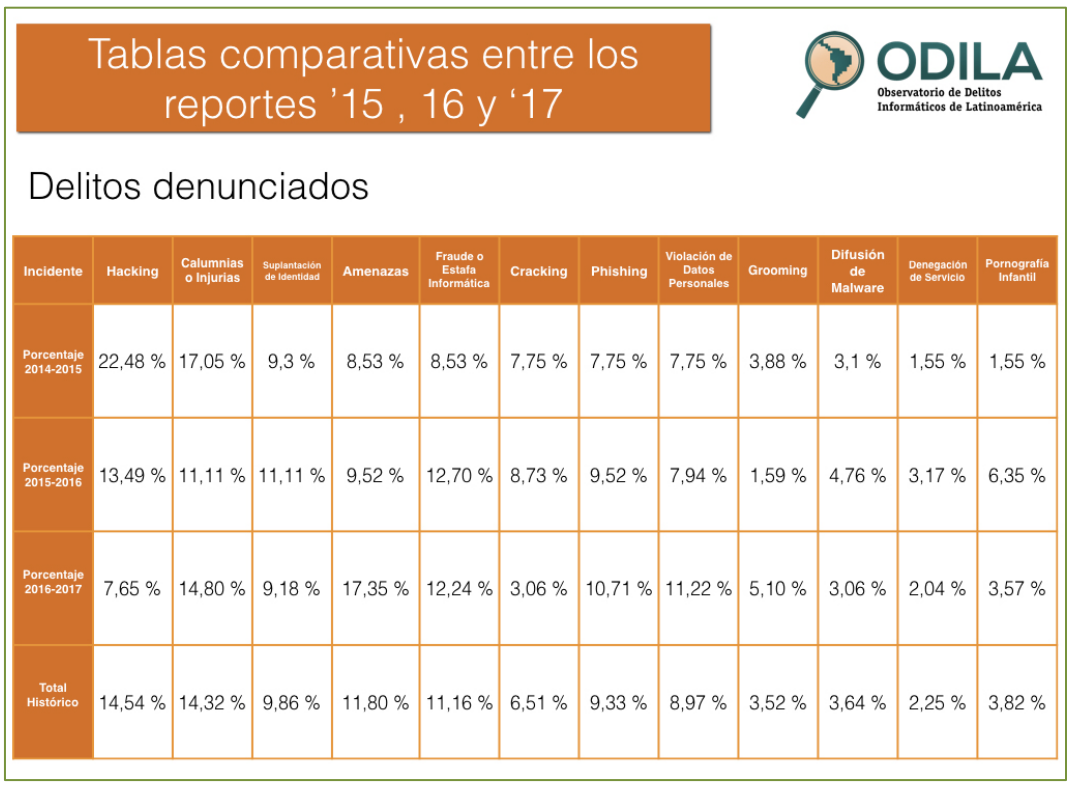
Es interesante analizar que al menos un ocho por ciento de las personas dicen que no se consideran víctimas y, en razón de ello, deciden no realizar la denuncia formal. Este dato podría ser analizado también por la falta de información por parte de los usuarios, ya que en general existe una situación de duda sobre si lo que están sufriendo configura o no un delito penal en el país donde se encuentran.

Delitos más denunciados

En relación a los delitos más denunciados por los usuarios, en este tercer informe se ha vuelto a modificar la posición en el *ranking* confeccionado por el Observatorio.



Incidente	Amenazas	Calumnias o injurias	Fraude o Estafa Informática	Violación de Datos Personales	Phishing	Suplantación de identidad	Hacking	Grooming	Pornografía Infantil	Cracking	Difusión de Malware	Denegación de Servicio
Porcentaje	17,35 %	14,80 %	12,24 %	11,22 %	10,71 %	9,18 %	7,65 %	5,10 %	3,57 %	3,06 %	3,06 %	2,04 %



Incidente	Hacking	Calumnias o injurias	Suplantación de Identidad	Amenazas	Fraude o Estafa Informática	Cracking	Phishing	Violación de Datos Personales	Grooming	Difusión de Malware	Denegación de Servicio	Pornografía Infantil
Porcentaje 2014-2015	22,48 %	17,05 %	9,3 %	8,53 %	8,53 %	7,75 %	7,75 %	7,75 %	3,88 %	3,1 %	1,55 %	1,55 %
Porcentaje 2015-2016	13,49 %	11,11 %	11,11 %	9,52 %	12,70 %	8,73 %	9,52 %	7,94 %	1,59 %	4,76 %	3,17 %	6,35 %
Porcentaje 2016-2017	7,65 %	14,80 %	9,18 %	17,35 %	12,24 %	3,06 %	10,71 %	11,22 %	5,10 %	3,06 %	2,04 %	3,57 %
Total Histórico	14,54 %	14,32 %	9,86 %	11,80 %	11,16 %	6,51 %	9,33 %	8,97 %	3,52 %	3,64 %	2,25 %	3,82 %

Este año encontramos que las amenazas a través de medios electrónicos han sido el problema más reportado por los usuarios (17,35%), siendo un 7% superior a lo observado en dos años anteriores (8,53 y 9,52 respectivamente). Con respecto a este delito en particular, debemos mencionar que es posible que el incremento de herramientas y medidas que permiten brindar un alto nivel de anonimato para el emisor de una comunicación electrónica, terminen dando como consecuencia un incremento en este tipo de delitos. Adicionalmente es necesario mencionar, que cabe realizar un análisis particular sobre cada uno de los casos (tarea que excede a las misiones del Observatorio) para poder conocer si realmente se encuentran dados todos los elementos jurídicos que se necesitan para que pueda ser considerado como amenaza.

También esbozamos como hipótesis que el incremento de este tipo de denuncia, puede haberse visto afectado por el crecimiento masivo de los casos de *ransomware* en el mundo (fenómeno de Wanancry en mayo y NotPetya en julio de 2017). Entre los tipos penales disponibles por ODILA, no se encuentra aún disponible alguno dedicado a este tipo particular de incidente informático; por lo cual es posible que los usuarios víctimas del mismo, hayan seleccionado la opción "amenazas", entendiéndolo como sinónimo de "extorsión".

En segundo lugar (con un 14,80%), encontramos a las calumnias e injurias a través de medios electrónicos, uno de los delitos más comunes que se ha vuelto cada vez más grave (con distintos niveles de daño al honor y reputación de las personas. La utilización masiva de las redes sociales, combinada con la sensación de "impunidad" y la exacerbación de la libertad de expresión, podrían determinar el crecimiento de esta actividad delictiva. Como apreciación adicional, en muchos casos las víctimas consideran que los dichos (a través de medios electrónicos) de una persona (determinada o indeterminada) son lo suficientemente graves como para calificar y ser considerados como injurias o calumnias. Dicha apreciación de las víctimas, posteriormente debe ser analizada por el fiscal o autoridad correspondiente, que deberá realizar un análisis de ponderación sobre la viabilidad del caso.

En tercer lugar, con un leve descenso con respecto el año anterior (0,45%), encontramos a los fraudes y estafas informática (12,25%) que, durante

estos tres años del Observatorio, siempre han estado dentro del *ranking* de los cinco delitos más reportados. Las estafas y fraudes a través de medios electrónicos no dejan de seguir estando vigentes, porque terminan siendo para los delincuentes, la forma más sencilla y directa de acceder a un beneficio económico.

De acuerdo a la tabla comparativa expuesta de los tres años, podemos observar que en las dos primeras etapas el delito informático más denunciado había sido el acceso indebido a datos o sistemas restringidos (hacking) con un 22,5% en la etapa 2014-2015 y 13,5% en la etapa 2015-2016. Este año, el acceso indebido a datos o sistemas restringidos ha bajado nuevamente (5,85%), pasando a estar en el séptimo puesto.

De una lectura general, podemos observar que los delitos menos reportados en estos tres años han sido la pornografía infantil, la denegación de servicio (DoS) y la difusión de malware. En relación al primero, interpretamos que la baja tasa de reportes en ODILA se debe a que en este tipo de delitos sí existe mayor confianza en el sistema penal y predisposición del sistema a perseguirlos; siguen siendo los más investigados y, se utilizan los recursos judiciales existentes. Debido a lo mencionado, creemos que ODILA no fue el lugar elegido por las víctimas para denunciar el caso.

En contraste a esto y a modo de apuntalamiento de esta hipótesis, se puede observar que los más denunciados, sí suelen ser aquellos delitos que no reciben una adecuada atención o respuesta por parte del "sistema penal" del Estado, dejando en gran parte a las víctimas en una situación de desamparo frente al hecho sufrido.

En relación a los otros dos delitos menos denunciados, DoS y difusión de malware, tiene conexión en que ambos se encuentran directamente relacionados con incidentes de seguridad de la información a nivel corporativo. Bajo el razonamiento que la difusión pública ocasionaría un daño mayor, este hecho es coherente con las causas por las cuáles no se denuncian los ciberdelitos. Es decir, se prioriza el requisito de la confidencialidad por sobre la necesidad de que dicho incidente sea investigado penalmente por las autoridades competentes.

Denuncias por país

En relación a este dato, en esta tercera etapa se observa un incremento de la participación de otros países latinoamericanos distintos a la Argentina.

Pais	Ar	Mx	Co	Br	Ve	Bo	Pe	Ch	Gt	Hn	Pa	Ni	Cr	Cu	Ht	Py	Pr	Do	Ec	Sv	Uy
% 2014 al 2015	51,94 %	10,85 %	6,2 %	5,43 %	3,88 %	3,1 %	3,1 %	2,33 %	2,33 %	2,33 %	2,33 %	1,55 %	0,78 %	0,78 %	0,78 %	0,78 %	0,78 %	1,59 %	0 %	0 %	0 %
% 2015 al 2016	54,76 %	4,76 %	8,73 %	0,79 %	1,59 %	2,38 %	2,38 %	0,79 %	3,17 %	7,94 %	0,79 %	0,79 %	0,79 %	0 %	0,79 %	0 %	0,79 %	0,79 %	4,76 %	0 %	2,38 %
% 2016 al 2017	41,33 %	17,86 %	11,22 %	1,02 %	2,55 %	1,02 %	6,12 %	4,59 %	5,10 %	2,04 %	0,51 %	1,02 %	1,02 %	0,00 %	0,00 %	0,51 %	0,00 %	0,00 %	2,04 %	1,02 %	1,02 %
Total Histórico	49,34 %	11,16 %	8,72 %	2,41 %	2,67 %	2,17 %	3,87 %	2,57 %	3,53 %	4,10 %	1,21 %	1,12 %	0,86 %	0,26 %	0,52 %	0,43 %	0,52 %	0,79 %	2,27 %	0,34 %	1,13 %

En los dos primeros informes, se observó el liderazgo absoluto de Argentina como país fuente de los reportes recibidos (52% y 55% respectivamente), encontrando explicación en que la difusión a los cuáles se ha tenido alcance desde el Observatorio, sólo han podido ser canales de alcance nacional, considerando que el proyecto es gestionado desde Argentina, con casi nula difusión internacional (sólo a través de redes sociales).

Recién a partir del tercer año, se puede empezar a visualizar un leve incremento de la participación de otros países latinoamericanos, como México y Colombia que, de a poco, van sumando información al Observatorio.

Desde nuestro lugar, consideramos que este cambio tiene que ver básicamente con el tiempo de vida del Observatorio, que implica la posibilidad de mayor llegada y conocimiento hacia las víctimas de distintos países.

Conclusiones

Puntualmente y en relación a la existencia de una "plataforma adecuada para abordar con éxito" una investigación, es menester hacer notar que, en los casos de delitos informáticos, para poder realizar una investigación eficaz tendiente a determinar el verdadero autor y reunir la evidencia suficiente y necesaria para lograr una condena, es necesario poseer una infraestructura técnica y humana que se encuentre apta para llevar adelante este tipo de investigaciones complejas.

Es decir, por un lado, se precisa contar con los recursos técnicos adecuados, sumado a la existencia de un personal disponible y capacitado. Por otro, se necesita trabajar con cierta agilidad en cuanto a coordinación y cooperación de distintos entes (Communications Service Provider - CSP / Justicia).

El paso de los años demuestra que el problema de los delitos informáticos sigue creciendo y cada vez a pasos más acelerados. Si bien en la mayoría de los países latinoamericanos ya se ha dado el primer paso, sancionando penalmente en mayor o menor medida a los delitos informáticos, esto no es suficiente.

Desde ODILA creemos que una legislación procesal más adecuada y flexible permitirá una mejor recolección de la evidencia digital, elemento vital y necesario para avanzar sobre la problemática.

Expresamos nuestra preocupación sobre la falta de estadísticas oficiales (cifra blanca) emitidas por cada país sobre delitos informáticos, la cual impide, por ejemplo, determinar qué tipo de delitos son los más cometidos, los bienes jurídicos más afectados, determinar los tipos de objetivos de los delincuentes (empresas financieras, bases de datos personales, etc.), entre otros datos de interés para el momento de tomar decisiones serias de política criminal.

A nuestro entender, la cifra negra existente representa un aspecto sustancialmente problemático que impide desarrollar un trabajo serio de observación, análisis y elaboración de estrategias o planes a mediano o largo plazo orientados a combatir el cibercrimen.

Los resultados publicados obtenidos a partir del funcionamiento del Observatorio Latinoamericano de Delitos Informáticos (ODILA), han sido más que satisfactorios, toda vez que por un lado el número de reportes ha superado las expectativas, y por otro, los resultados obtenidos confirman y reafirman los objetivos del propio proyecto.

Los números de las víctimas que confirman que no han realizados las denuncias formales ante los organismos competentes se ha visto incrementado en relación al primer informe, ascendiendo a un 82% sobre el total de los reportes recibidos, evidenciando nuestra hipótesis sobre la existencia de una cifra negra, es decir, de una importante cantidad de incidentes que ocurren a diario en nuestra sociedad pero que pasan desapercibidos para el sistema penal.

Por otro lado, entre las causas, observamos que en mayor grado las personas que no han realizado las denuncias, responden a una falta de confianza sobre la eficacia en las investigaciones por un lado (no se cree en la justicia), no saben dónde denunciar (falta de información por parte de la víctima, o bien falta de trabajo por parte del Estado para facilitar el acceso a la justicia por parte de las víctimas). Sigue estando entre los más altos índices, el problema de la confidencialidad para el denunciante, que teme que su incidente se haga de público conocimiento al realizar la denuncia formal.

Por último, destacamos que los autores de esta iniciativa, somos conscientes de las limitaciones y errores que pueden darse en el proceso de recolección de reportes planteados, algunas de ellas ya desarrolladas en entre las aclaraciones importantes del Observatorio, otras que seguramente se irán develando con el pasar del tiempo en el funcionamiento del mismo.

Aun así, los directores de ODILA asumen el riesgo de equivocarse intentando llevar adelante un proceso de recolección de datos, pero convencidos de estar aportando una idea y un lugar de trabajo que, más allá de la precisión o calidad de los datos que puedan llegar a obtenerse con el paso del tiempo, siempre tendrá como finalidad última una intención de difusión y concientización hacia la sociedad sobre la problemática de los delitos informáticos.

Otros Informes de Referencias

- 2016 - ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA
- http://www.interior.gob.es/documents/10180/5791067/Estudio+Cibercriminalidad+2016.pdf/456576b2-9ce8-4f3c-bbcc-ca0dbf3bb3cf
- IOCTA 2016 INTERNET ORGANISED CRIME THREAT ASSESSMENT
https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016
https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf