¿Son útiles las TIC para combatir la ciberdelincuencia? La relación entre la denuncia de delitos informáticos y el equipamiento tecnológico de las comisarías

Does ICT Curb Cybercrimes? The Association between Cybercrime Charges and the Police Station Technological Apparatus

Submetido(*submitted*): 08/07/2018
Parecer(*revised*): 05/08/2018
Aceito(*accepted*): 14/08/2018

William Fernández[*]
Carmen Vargas[**]

Abstract

Purpose – *Computer crimes are serious and recent problems in Peru. The easy access to technology and the socioeconomic conditions of the country have made it a favorable place to commit cybercrimes. On the other hand, the agents involved, such as the police, are often at a disadvantage, as they do not have the necessary skills to combat those crimes. It is relevant to ask whether the ability of the police to use Information and Communication Technologies (ICT) works as a marker that serves to deter criminals from committing crimes.*

Methodology/approach/design – *A database was constructed from sources of information on police stations and crimes in Peru. With this, a probit model was estimated in which the dependent variable is the probability of the occurrence of computer crimes. The marginal effects of three indices constructed from variables indicating the use of ICT were calculated.*

Findings – *The results obtained show that two of our three indices explain that, the greater the use of ICT in Peruvian police stations, there is a lower probability of the occurrence of cybercrimes.*

Keywords: Criminality, cybercrime, citizen security, information and communication technologies, Peru.

Resumen

Propósito – La ocurrencia de delitos informáticos es una problemática bastante grave y reciente en el Perú. El fácil acceso a la tecnología y las condiciones socioeconómicas del país han dado pie a que se convierta en un lugar propicio para cometer ciberdelitos. Por otro lado, los agentes involucrados como la policía muchas veces se encuentran en desventaja, ya que no cuentan con las habilidades necesarias para combatir este tipo de

[*]Bachiller en economía de la Universidad del Pacífico. Se desempeña como asistente de investigación en el Centro de Investigación de la Universidad del Pacífico. Email: w.fernandeztinoco@up.edu.pe.
[**]Bachiller en economía de la Pontificia Universidad Católica del Perú. Se desempeña como consultora del Ministerio de Economía y Finanzas del Perú. Email: carmen.vargas@pucp.pe.

FERNÁNDEZ, W; VARGAS, C. *¿Son útiles las TIC para combatir la ciberdelincuencia? La relación entre la denuncia de delitos informáticos y el equipamiento tecnológico de las comisarías*. **The Law, State and Telecommunications Review**, Brasilia, v. 10, n. 2, p. 37-52, October 2018. [DOI: https://doi.org/10.26512/lstr.v10i2.21492]

crímenes. En ese sentido, es relevante preguntarnos si es que la capacidad del personal de la comisaría para utilizar las Tecnologías de Información y Comunicación (TIC) funciona como señal de seguridad que sirve para disuadir a los criminales de delinquir.
Metodología – De esta manera, se construyó una base de datos a partir de fuentes de información sobre comisarías y delitos en el Perú. Con ello, se estimó un modelo probit en el cual la variable dependiente es la probabilidad de ocurrencia de delitos informáticos. Se obtuvo los efectos marginales de tres índices construidos a partir de variables que indican el uso de las TIC.
Resultados – Los resultados obtenidos muestran que dos de nuestros tres índices explican que, a mayor uso de las TIC en las comisarías peruanas, existe una menor probabilidad de ocurrencia de delitos informáticos.

Palabras clave: Criminalidad, ciberdelincuencia, seguridad ciudadana, tecnologías de información y comunicación, Peru.

Introducción

Un delito informático se define como toda aquella acción ilegal que se comete a través de las vías informáticas o que tiene como propósito causar daños a los instrumentos electrónicos o redes de comunicación. Así, se valen mucho del uso de las diferentes Tecnologías de Información y Comunicación (TIC) para cometerse. Este tipo de delincuencia comenzó a proliferar a inicios del siglo XXI, junto con el proceso de digitalización de los sistemas de información y la globalización que se dio entre las naciones del mundo. Al hacerse más barata la producción de sistemas informáticos, las TIC se hicieron más accesibles para la población en general. En este sentido, la problemática de los delitos informáticos no es ajena para los países en vías de desarrollo, puesto que, en dichos países, la ocurrencia de este tipo de crímenes se ha incrementado y, al mismo tiempo, se han visto considerablemente sofisticados (KSHETRI, 2010). Esto puede deberse a que la probabilidad de cometer un crimen y ser detectado es menor si se compara con la de las naciones de ingresos altos. Aun así, lo más preocupante de esto es que el impacto económico que los cibercrímenes generan ha sido muchas veces mayor que el que originan los crímenes convencionales, y esto es algo que puede impactar de manera negativa en la población del mundo en desarrollo.

El Perú, país de ingreso medio que experimentó un crecimiento económico importante durante la primera década del siglo XXI, no se encuentra ajeno a este fenómeno. Este país se ha convertido en un lugar propicio para la creación de *malware* (virus informáticos), el cual es uno de los tipos de ciberdelitos más comunes en países de ingreso medio. Por ejemplo, el trabajo de KSHETRI (2013) habla sobre la creación del Sistema de Administración de PCs Zombi (SAPZ), un virus presuntamente creado en el Perú, que infectaba la computadora del usuario

mediante *phishing*[1] y, una vez instalado, redirigía a la víctima a una versión falsa de la página del Banco de Crédito del Perú, para robarse las credenciales del usuario. Esto solo es un ejemplo para poner en contexto la magnitud del problema, puesto que el Perú se ubica en el cuarto lugar en cuanto al número de ataques cibernéticos por cada 10,000 usuarios de Internet, y primero del mundo en actividad maliciosa por usuario de banda ancha (KSHETRI, 2013).

Ante esta situación, las autoridades peruanas comenzaron a actuar para hacerle frente a la ciberdelincuencia. Así, desde el año 2005, la Dirección de Investigación Criminal de la Policía Nacional del Perú (DIRINCRI) cuenta con la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), cuya principal función es luchar contra los delitos informáticos, realizando una tarea especializada de investigación, para la que su personal cuenta con las mismas o mejores condiciones que las de los delincuentes. Desde el campo normativo, la legislación peruana condena los delitos informáticos desde el 22 de octubre de 2013, con la promulgación de la Ley 30096 ("Ley de delitos informáticos"). En dicha ley, se penan las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de las TIC.

A pesar de lo mencionado en el párrafo anterior, la lucha contra el cibercrimen no puede depender únicamente de un área de la policía nacional. Todas las comisarías necesitan tener el número adecuado de equipos de comunicación e informática, y su personal debe estar debidamente capacitado, con el objetivo de poder identificar o detectar delitos que utilicen como principal medio las TIC, para que los culpables puedan ser sancionados. Tal como establece la literatura, los delitos informáticos suelen quedar impunes en países en vías de desarrollo, y esto sucede porque los culpables no pueden ser identificados, dado el poco conocimiento que tienen las mismas autoridades policiales sobre el tema. En otras palabras, no basta únicamente con contar con los mejores equipos informáticos o de comunicación, sino también saber cómo utilizarlos para poder hacer frente al cibercrimen.

Bajo este contexto, la pregunta de investigación que se plantea en este documento es la siguiente *"¿el hecho de que el personal de una comisaría maneje mejor las TIC sirve para disuadir a los criminales de cometer ciberdelitos?"* Para responder a esta interrogante, nos valemos principalmente de dos fuentes de información: el Censo Nacional de Comisarías y el Registro Nacional de Delitos en las Dependencias Policiales. Ambas bases de datos tienen como unidad de análisis a las comisarías peruanas, y contamos con información de los años 2015 y 2016.

[1] Se refiere a las técnicas que utilizan los estafadores para tomar la identidad de una empresa o persona confiable, ya sea vía correo electrónico o llamadas telefónicas. Esto se hace con el fin de adueñarse de contraseñas e información personal de las víctimas.

FERNÁNDEZ, W; VARGAS, C. *¿Son útiles las TIC para combatir la ciberdelincuencia? La relación entre la denuncia de delitos informáticos y el equipamiento tecnológico de las comisarías*. **The Law, State and Telecommunications Review**, Brasilia, v. 10, n. 2, p. 37-52, October 2018. [DOI: https://doi.org/10.26512/lstr.v10i2.21492]

Marco Teórico

La relación entre el uso de las TIC en una comisaría y la ocurrencia de delitos informáticos

El estudio de la problemática de la ciberdelincuencia en países en vías de desarrollo se encuentra en sus inicios. Tal como la literatura indica, esto puede deberse a que todavía se conserva la percepción de que, en muchas de estas naciones, la brecha digital aún es bastante amplia o que la penetración de los servicios de Internet entre la población es parcial. Esto lo señala KSHETRI (2010). La poca importancia ha dado pie a que se destinen muy pocos recursos a combatir el cibercrimen, puesto que por mucho tiempo estos no se han percibido como una amenaza real. Sin embargo, justamente los altos índices de pobreza, sumados a las altas tasas de desempleo de estas naciones, han funcionado como incentivos para que los individuos se vean atraídos para cometer este tipo de crímenes, dado que pueden investigar sobre estas nuevas maneras de delinquir a un relativo bajo costo. Por ejemplo, un *hacker* puede aprender a robar contraseñas únicamente con una computadora y una conexión estable a Internet.

Aún no existir claras medidas de lucha contra el cibercrimen, se torna más difícil que el culpable de un delito informático sea identificado y posteriormente castigado (KSHETRI, 2010), con lo que los criminales ven incrementado su retorno esperado de delinquir. En un país en vías de desarrollo (tal como el Perú) hay, además, grandes oportunidades para los ciberdelincuentes, puesto que recién se están digitalizando todas las transacciones, por lo que los consumidores y los negocios aún no adoptan las medidas de ciberseguridad necesarias para estar protegidos contra este tipo de delitos (la inexistencia de mecanismos de defensa eleva el retorno esperado del criminal). Por si esto fuera poco, MORA (2015) señala que hay una importante falta de personal calificado para el manejo o uso de las TIC en las comisarías peruanas, por lo que es evidente que los oficiales se encuentran en una clara desventaja con respecto a los delincuentes. Esta situación se torna incluso más delicada para las comisarías del interior del país.

Asimismo, también es importante analizar la decisión de denunciar o no un ciberdelito en un país como el Perú. De acuerdo con LEUKFELDT (2017), hay factores económicos asociados a la decisión de reportar un cibercrimen (costos y beneficios), por lo que, para el contexto peruano, denunciar un delito informático podría acarrear muchos costos (como la transacción) y traer muy pocos beneficios, dado que la probabilidad de encontrar al culpable y castigarlo es casi nula. Este mismo estudio señala que la policía de países de ingresos medios no cuenta con las habilidades ni conocimiento para manejar los casos de cibercrímenes de manera efectiva.

El retorno esperado del delincuente

En vista de lo descrito previamente, es necesario plantear el retorno esperado del delincuente, para poder determinar en qué medida la utilización de las TIC en las comisarías pueden influir en el mismo. Tal como dice (NGAFEESON, 2010), al momento de cometer un delito informático, los culpables enfrentan una barrera de seguridad, que influye directamente sobre la probabilidad de ser detenidos o salir impunes. Dicha barrera de seguridad se vale tanto de las medidas de ciberseguridad que puedan adoptar las empresas o individuos, como también de la capacidad tecnológica de la comisaría. En tal sentido, ORTIZ (2013) señala que la tecnología brinda la capacidad de amplificar abrumadoramente las capacidades de los agentes policiales en sus tareas de aprehensión, análisis e investigación, y esto se vuelve más relevante para el caso de los ciberdelitos, puesto que se cometen valiéndose principalmente de las TIC.

Así, se plantea la siguiente función de retorno esperado:

$$E(R) = (1 - \alpha) * (M_b + P_b) + \alpha * (\partial * O_c) - c$$

Donde:

α =Probabilidad de ser detenido.

M_b =Beneficios monetarios de cometer el delito.

P_b =Beneficios psicológicos de cometer el delito (existen personas que crean *malware* sin fines económicos, únicamente para robar información).

∂ =Probabilidad de ser condenado.

O_c =Costo de oportunidad de ser condenado.

c =Todos los costos asociados a cometer el delito informático (tiempo, dinero, etc.).

Teniendo esta función en mente, es importante ver dónde puede influir la comisaría. Naturalmente, el parámetro que puede afectar es α, puesto que esa es la probabilidad de ser detenido. Tal como establece KSHETRI (2010), el valor de esta probabilidad en el Perú debería ser muy bajo, por lo que el retorno esperado finalmente sería positivo. Si se busca disuadir a los delincuentes, entonces se debe subir α, para que el retorno esperado sea cada vez menor. La mejor manera de disminuir este retorno esperado sería crear *Computer Incidence Response Teams* (CIR), tal como GERCKE (2011) señala. Sin embargo, esta es una alternativa muy costosa. Por ello, lo mejor para un país como el Perú es que cada comisaría tenga la capacidad de detectar, analizar e investigar cibercrímenes. Lo que se busca probar en este estudio es que esto efectivamente disminuye la probabilidad de ocurrencia de un delito informático.

Fuentes de Información

Para poder responder a la pregunta de investigación, nos valemos de dos bases de datos que conformaran un *pool* de observaciones que comprende dos periodos de análisis. La primera fuente es el Censo Nacional de Comisarías del Perú (CNC) 2015 y 2016, elaborado por el INEI (Instituto Nacional de Estadística e Informática). Esta base tiene como unidad de análisis a las dependencias policiales del país, que suman un total de 1,471 al año 2016 y 1,469, para el 2015. La parte más relevante de la misma es el módulo 300, que cuenta con datos acerca del equipamiento informático que existe dentro de cada comisaría. La segunda base de datos de la que se vale el presente estudio es el Registro Nacional de Denuncias de Delitos en las Dependencias Policiales (RENADDEP) 2015 y 2016. La unidad de análisis de esta base son las comisarías básicas y unidades especializadas de investigación criminal de la Policía Nacional del Perú (PNP). Al año 2016, se identificaron en total 1,290 comisarías entre las básicas y las especializadas en investigación criminal; mientras que, para el 2015, se cuenta con 1,241 comisarías.

Cabe resaltar que este tipo de establecimientos son también dependencias policiales, por lo que la información de esta última base se puede juntar fácilmente con la de la primera. La información relevante que se consigue de esta base es si se ha reportado la ocurrencia de algún tipo de delito informático dentro de cada dependencia policial o no. Dada la naturaleza de nuestras bases de datos, al realizar la unión de ambas bases quedaron cerca de 811 observaciones con información incompleta sobre el uso de los equipos informáticos que emplean o que no tienen datos de las denuncias de delitos informáticos. Por lo tanto, la base con la cual se estimaron los resultados tiene como unidad de análisis a 2,230 dependencias policiales del 2015 y 2016, tal como se puede observar en el cuadro 1. Asimismo, para tener un mejor entendimiento de las variables utilizadas en el cuadro 2 se expone el resumen y descripción de cada una de estas, así como la fuente de la cual fueron obtenidas.

Cuadro 1: Estadísticas descriptivas de las principales variables

	Total		No ocurrió delito		Ocurrió delito	
Variables	N	Promedio	N	Promedio	N	Promedio
TIC_1	2,330	0.36	2,249	0.36	81	0.32
TIC_2	2,330	0.26	2,249	0.27	81	0.09
TIC_3	2,330	0.39	2,249	0.40	81	0.20
Distrito urbano	2,330	0.61	2,249	0.60	81	0.72
Usuario	2,330	0.46	2,249	0.46	81	0.56

computadora						
Población atendida por comisaría	2,330	3.17	2,249	3.15	81	3.60
Operaciones estadísticas	2,330	0.49	2,249	0.49	81	0.56
Equipos comunicación	2,330	5.15	2,249	5.20	81	3.93
Equipos informáticos	2,330	12.51	2,249	12.44	81	14.44

Fuente: Censo Nacional de Comisarías del Perú y Registro Nacional de Delitos en las Dependencias Policiales 2015-2016. Elaboración propia.

Cuadro 2: Resumen y descripción de variables utilizadas

Variable	Descripción	Fuente
Ocurrió delito	Toma el valor de 1 si se registró la denuncia de un delito informático en la dependencia policial. Se considera "delito informático" a todo aquel crimen que se cometió utilizando como medio las herramientas informáticas.	Registro Nacional de Denuncias de Delitos en las Dependencias Policiales, 2015-2016
Región	Variable que indica a cuál de las 25 regiones del país pertenece la comisaría.	Censo Nacional de Comisarías, 2015-2016
Distrito urbano	Toma el valor de 1 si la comisaría se encuentra en un distrito considerado "urbano" según el INEI.	INEI, 2015-2016
Usuario computadora	Toma el valor de 1 si la persona autorizada para usar las computadoras dentro de la comisaría es únicamente el comisario	Censo Nacional de Comisarías, 2015-2016
Población atendida por comisaría	Variable que toma valores del 1 al 6 de acuerdo al rango de población que la comisaría debe atender aproximadamente. Los rangos son los siguientes: 1 (menos de 5,000 habitantes), 2 (entre 5,000 y 10,000 habitantes), 3 (entre 10,001 y 20,000 habitantes), 4 (entre 20,001 y 40,000 habitantes), 5 (entre 40,001 y 80,000 habitantes) y 6 (de 80,0001 a más habitantes).	Censo Nacional de Comisarías, 2015-2016
Operaciones estadísticas	Toma el valor de 1 si la comisaría cuenta con un ambiente dedicado a realizar operaciones estadísticas.	Censo Nacional de Comisarías, 2015-2016

Equipos comunicación	Número de teléfonos fijos, celulares y otros equipos de comunicación con los que cuenta la comisaría.	Censo Nacional de Comisarías, 2015-2016
Equipos informáticos	Número de computadoras, laptops, impresoras, escáner, proyectores y otros equipos informáticos con los que cuenta la comisaría.	Censo Nacional de Comisarías, 2015-2016

Elaboración propia.

Metodología

De acuerdo con la teoría econométrica, para procesar datos en forma de variables dicotómicas de corte transversal, la mejor alternativa es utilizar modelos *logit* o *probit* (GREENE, 2003). En ese sentido, dado que la variable dependiente de la especificación que estimaremos es una dicotómica, que toma el valor de 1 si se denunció la ocurrencia de un delito informático en la dependencia policial y 0 de cualquier otra forma, lo mejor para la presente investigación es utilizar la metodología del modelo de probabilidad de variable dependiente limitada (*probit*). Este explica la probabilidad de ocurrencia de un delito informático en la dependencia policial, y está expresada en la siguiente ecuación:

$$y_i^* = x_i\beta + \varepsilon_i$$

A partir de la ecuación, la variable y_i^* es la ocurrencia del delito informático en la i-ésima comisaría, x_i es el conjunto de variables de control que explican la ocurrencia de los cibercrímenes. El vector de coeficientes de las variables es β y ε_i es una variable continua con distribución normal. Para y_i, la probabilidad de observar la denuncia del delito informático tiene la siguiente forma:

$$y_i = \begin{cases} 1, si\ y_i^* > \tau \\ 0, si\ y_i^* \leq \tau \end{cases}$$

Cuando existen denuncias sobre los delitos informáticos $(y_i = 1)$, asumiendo que el umbral es $\tau = 0$, se puede obtener la siguiente expresión:

$$\Pr(y_i = 1|x_i) = \Pr(\varepsilon_i < x_i\beta|x_i) = F(x_i\beta)$$

Debido a la ecuación anterior, que es la distribución de la probabilidad acumulada normal, estimamos el modelo *probit* utilizando la siguiente ecuación:

$$y_i = \beta_o + \delta TIC_i + \beta_1 dist_i + \beta_2 policial_2 + u_i$$

La variable de interés es TIC_i, el cual se refiere a una serie de índices cuya construcción será explicada en la siguiente sección, pero que reflejan el uso de las TIC en la comisaría. Por otro lado, $distdist_i$ se refiere a los efectos fijos por el distrito en el que se ubica la comisaría, que serán utilizados como variables de control; mientras que $policialpolicial_i$ se refiere al conjunto de características

propias de cada dependencia policial, y que también explican la ocurrencia de delitos informáticos. Finalmente, μ_i es el error de la estimación.

Análisis Factorial Exploratorio

La construcción de las variables TIC se realizó a partir del análisis factorial exploratorio, técnica estadística que consiste en encontrar grupos homogéneos a partir de un conjunto grande de variables que se correlacionan altamente entre sí. Este es un enfoque impulsado por los datos, de modo tal que no se realizan especificaciones con respecto al número de variables latentes ni las relaciones entre los factores comunes (FERNÁNDEZ, 2015). En ese sentido, se emplea esta metodología para construir tres diferentes índices: TIC_1, que se refiere al acceso de la comisaría a sistemas de información digital; TIC_2, que se compone de variables que indican si la comisaría realiza el registro de las ocurrencias de manera digital, y TIC_3, que se construye a partir de variables que funcionan como *proxy* del uso de las TIC. Es necesario resaltar que los tres índices fueron estandarizados para que únicamente presentaran valores entre 0 y 1. A continuación, se presentan las variables que componen cada índice:

Cuadro 3. Descripción de las variables de interés (índices TIC)

Índice	Descripción
TIC_1	Se refiere al acceso a sistemas de información. Lo componen las variables: Acceso a información del RENIEC, requisitorias policiales, registros públicos, procesos judiciales, movimientos migratorios y al sistema de denuncias.
TIC_2	Se refiere al registro digital de las ocurrencias. Lo componen las variables: registro digital de accidentes de tránsito, denuncias directas y reservadas, registros operativos y patrullas.
TIC_3	Se refiere al uso de las TIC. Lo componen las variables: registro digital de denuncias en general, horas de uso promedio de las computadoras, acceso al sistema de denuncias, y registro total de las denuncias en el Sistema de Denuncia Policial (SIDPOL).

Elaboración propia.

Análisis de resultados

Se estimó la ecuación especificada en la sección anterior en tres versiones del modelo *probit*, en las que se van insertando las variables de interés TIC_1, TIC_2 y TIC_3. De esta manera, en el cuadro 4 se puede observar el efecto marginal de cada índice TIC sobre la probabilidad de ocurrencia de delitos informáticos. El modelo 1 contiene la variable TIC_1, de acceso a sistemas de información en la

dependencia policial. Esta variable no es significativa; sin embargo, sí se obtienen resultados significativos para algunas de las variables de control. Tanto el número de equipos informáticos, equipos de comunicación, usuario de la computadora, la población atendida por la comisaría y si esta cuenta con un ambiente designado a tareas de estadística, tienen efectos significativos sobre la probabilidad de ocurrencia de un delito. Si únicamente el comisario está autorizado para utilizar las computadoras, entonces la probabilidad se incrementa en casi 2 pp. (puntos porcentuales). Esto tiene sentido, puesto que solo habría una persona con el conocimiento y permiso necesarios para manejar los sistemas informáticos, por lo que las medidas de ciberseguridad implementadas no podrán ser muy potentes. Otra variable que presenta un resultado interesante es la de la población atendida por la comisaría, dado que se obtiene que, a mayor población, mayor probabilidad de delito. En el Perú, los lugares más poblados son las zonas urbanas o las ciudades más grandes, donde la penetración del Internet es mayor y en general existe mayor acceso a las TIC. La variable de equipos de comunicación presenta un coeficiente negativo, es decir, el tener un mayor número de equipos está asociado a una menor probabilidad de que ocurra un cibercrimen (-0.3 pp.). No obstante, lo que este estudio busca demostrar es que el uso (y no la tenencia) de las TIC impacta negativamente sobre la probabilidad de ocurrencia de un delito informático, por lo que esta variable no funcionaría como buen *proxy* (al igual que la de equipos informáticos).

El modelo 2 incluye como variable a TIC_2. Este índice consiste en el registro digital de las ocurrencias dentro de la comisaría, y es significativo al 1%. En ese sentido, ante un aumento de 0.1 en nuestro índice, la probabilidad de ocurrencia de un delito informático disminuye en 6 pp., aproximadamente. Asimismo, las variables de control mantienen su significancia y signo. Por último, el modelo 3 presenta el efecto marginal de la variable TIC_3, que se convierte en nuestro índice más poderoso, puesto que, ante un aumento de este en 0.1, la probabilidad de que ocurra un delito informático se reduce en 10 pp. Algo curioso de esta estimación es que la variable de distrito urbano presenta un coeficiente positivo y significativo por primera vez. Así, si la comisaría se ubica en un distrito clasificado como "urbano", entonces la probabilidad de ocurrencia de un delito informático se incrementa en 2 pp. En las tres estimaciones, las tres regiones que no presentan delitos informáticos (Tacna, Callao y Moquegua) son omitidas, puesto que no se podría estimar la probabilidad si es que no hay información sobre las denuncias. Esto no afecta la consistencia de la estimación de los efectos de las otras variables, ya que no se utilizan dichas observaciones en la regresión.

Cuadro 4: Efectos marginales (dy/dx) de la estimación de la probabilidad de ocurrencia de delitos informáticos

Probabilidad de ocurrencia de delito informático	(1) TIC_1	(2) TIC_2	(3) TIC_3
TIC_1	-0.0243		
	(0.0195)		
TIC_2		-0.0569***	
		(0.0140)	
TIC_3			-0.102***
			(0.0197)
Distrito urbano	0.0121	0.0133	0.0188**
	(0.0106)	(0.00987)	(0.00925)
Usuario computadora (comisario==1)	0.0187**	0.0188**	0.0195**
	(0.00786)	(0.00791)	(0.00802)
Población atendida por comisaría	0.00616**	0.00734**	0.00914***
	(0.00308)	(0.00309)	(0.00306)
Operaciones estadísticas	0.0163**	0.0143*	0.0139*
	(0.00802)	(0.00778)	(0.00770)
Equipos comunicación (número)	-0.00363**	-0.00308**	-0.00262**
	(0.00143)	(0.00134)	(0.00129)
Equipos informáticos (número)	0.00219***	0.00208***	0.00216***
	(0.000560)	(0.000553)	(0.000535)
Observaciones	2,211	2,211	2,211

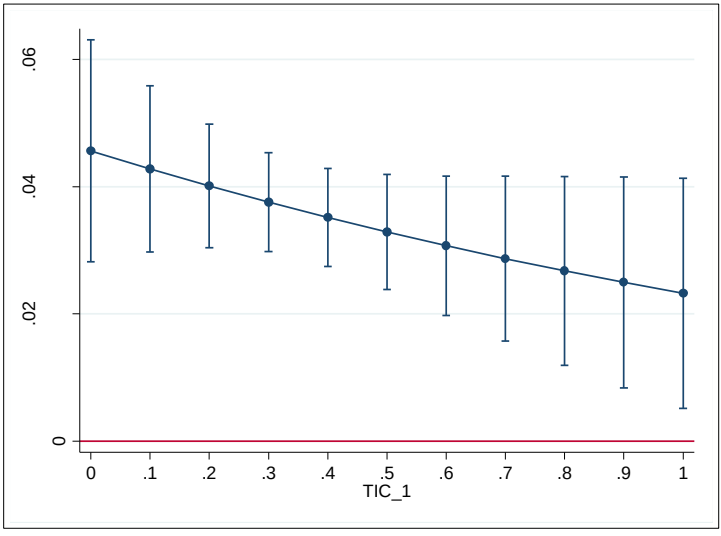
Notas: Errores estándar entre paréntesis. *** p<0.01, ** p<0.05, * p<0.1. En todas las estimaciones se incluyen variables de control por región.

Nuestros resultados también se pueden mostrar de manera gráfica. En la Figura 1, se observa que los efectos marginales que miden el cambio en la probabilidad de ocurrencia de un delito informático a medida que TIC_1 cambia de 0 a 1, no son significativos (manteniendo todas las demás variables en sus valores promedio). En cambio, en la Figura 2, se observa el cambio en la probabilidad de ocurrencia de un delito a medida que el factor TIC_2 se acerca a 1. En este caso, la probabilidad de que ocurra un delito puede llegar a disminuir hasta ubicarse entre 0 y 20%. De este resultado se puede concluir que, para combatir la ciberdelincuencia, no basta con contar con equipos informáticos de alta calidad ni acceso a la información digital, la verdadera diferencia radica en poder utilizar estas herramientas informáticas para manejar de manera efectiva los casos de ciberdelincuencia.

Por otro lado, en la Figura 3 se puede apreciar que, mientras más uso hagan las comisarías de las tecnologías de la información, la probabilidad de que ocurra un delito informático se acerca a 0. Una de las teorías presentadas en el marco teórico que explica este resultado se basa en que una manera de hacer uso de las

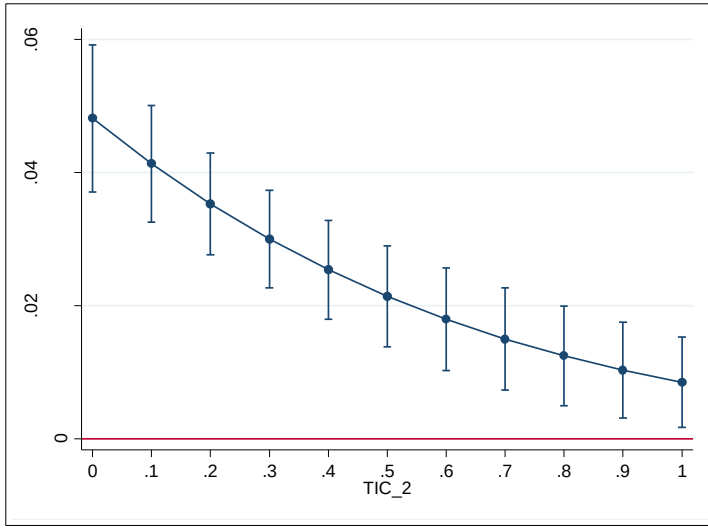
tecnologías es creando mayores medidas de ciberseguridad. Esto se traduce en mayores costos para el delincuente al momento de cometer el crimen, ya que será detectado fácilmente. Además, el uso de las tecnologías de manera adecuada a las comisarías no solo genera eficiencia en el desarrollo de sus actividades, sino que también aumenta el bienestar de las personas al vivir en una sociedad más segura y de menor probabilidad de ser atacados por *hackers* o estafadores.

Figura 1. Cambio en la probabilidad de ocurrencia de un delito informático: TIC_1



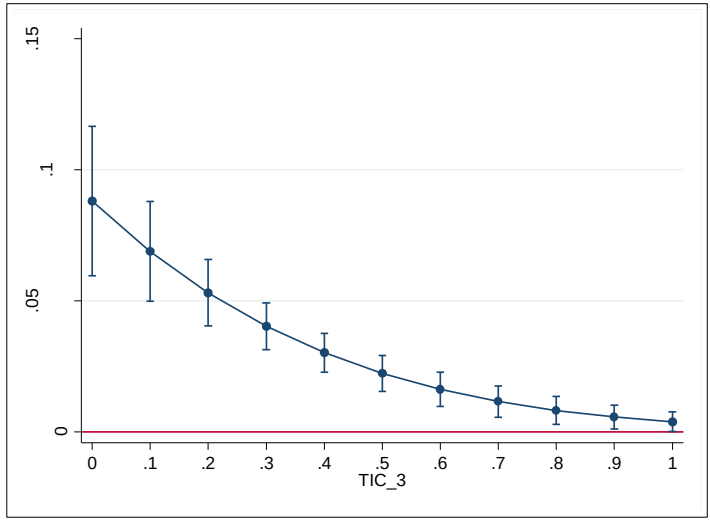
Notas: Se analiza únicamente el efecto de la variable TIC_1 sobre la probabilidad de ocurrencia de delito informático, manteniendo el resto de las variables en sus valores promedio. Elaboración propia.

Figura 2. Cambio en la probabilidad de ocurrencia de un delito informático: TIC_2



Notas: Se analiza únicamente el efecto de la variable TIC_2 sobre la probabilidad de ocurrencia de delito informático, manteniendo el resto de las variables en sus valores promedio. Elaboración propia.

Figura 3. Cambio en la probabilidad de ocurrencia de un delito informático: TIC_3



Notas: Se analiza únicamente el efecto de la variable TIC_3 sobre la probabilidad de ocurrencia de delito informático, manteniendo el resto de las variables en sus valores promedio. Elaboración propia.

Conclusiones

Los resultados encontrados confirman la hipótesis, es decir, el uso de las tecnologías de información y comunicación en las dependencias policiales sí funciona como una señal significativa para disuadir a los delincuentes de cometer delitos informáticos. Si bien la variable dependiente únicamente se basa en la denuncia de algún delito informático en las comisarías (que solo sucede en 81 casos), las pérdidas registradas por ciberdelitos en el 2016 ascienden a U$ 4,072 millones para el país, según cifras de la firma *Digiware* (ROJAS, 2016). A partir de las estimaciones de los tres modelos propuestos, se encuentra que TIC_3 es el índice más potente al momento de reducir la probabilidad de que ocurra un delito informático. Por ello, las comisarías peruanas deberían enfocarse en potenciar las variables que componen dicho índice (horas de uso de la computadora, registro digital de denuncias, etc.). Es muy costoso para el Estado crear unidades como la DIVINDAT en todo el Perú, pero lo que sí puede hacer es potenciar el uso de las TIC en las comisarías, mediante la compra de equipo, pero, lo que es igual o más importante, es la correcta capacitación del personal.

No se debe sub-dimensionar el problema. Si bien es cierto nosotros establecemos que solo en 81 comisarías ocurrió algún delito informático, en muchas de estas el número de delitos es bastante alto, y esto representa un altísimo costo social. Por este motivo, es evidente que el Perú aún enfrenta muchos desafíos en términos de la prevención y erradicación del cibercrimen. Nuestro estudio investiga este tema, que ha sido bastante dejado de lado en la literatura y definitivamente necesita atención. Más aún, se ha comprobado la capacidad de la comisaría en luchar contra el cibercrimen. Así, las investigaciones futuras en este campo deberían esbozar un perfil de los criminales dedicados a cometer ciberdelitos o de las víctimas, para que la policía tenga aún mayores probabilidades de capturarlos.

Referencias

ANDEME, D.; FOSSO, S.; KALA, J. R. Determinants of Cyber Security Use and Behavioral Intention: Case of the Cameroonian Public Administration. ***Springer Nature 2018***, n. 746, p. 1087–1096, 2018.

BMI RESEARCH. Peru: crime and security risk report includes the bmi operational risk index. ***London: Business Monitor International***, 2017.

CHUNG, W. et al. Fighting cybercrime: a review and the Taiwan experience. ***Decision Support Systems***, v. 41, p. 669–682, 2004.

FERNÁNDEZ, A. Aplicación del análisis factorial confirmatorio a un modelo de medición del rendimiento académico en lectura. ***Ciencias Económicas***, San José, Costa Rica, v. 33, n. 0252-9521, p. 39-66, 17 Noviembre 2015.

GERCKE, M. Understanding cybercrime: a guide for developing countries, Switzerland, 2011.

GREENE, W. H. Econometric Analysis. International. ed. [S.l.]: ***Pearson Education***, 2003.

KIGERL, A. Routine Activity Theory and the Determinants of High Cybercrime Countries. ***Social Science Computer Review***, v. 30, p. 470-486, 2012.

KSHETRI, N. Diffusion and effects of cyber-crime in developing economies. ***Third World Quarterly***, Greensboro, v. 31, n. 7, p. 1057-1079, January 2010.

KSHETRI, N. Cybercrime and cybersecurity in the global south. Greensboro: ***International Political Economy***, 2013.

KUNDI, G. M.; NAWAZ, ; AKHTAR, R. Digital Revolution, Cyber-Crimes And Cyber Legislation: A Challenge To Governments In Developing Countries. ***Journal of Information Engineering and Applications***, v. 4, n. 4, 2014.

LEUKFELDT, R. Research agenda the human factor in cybercrime and cybersecurity. [S.l.]: ***Eleven International Publishing***, 2017.

MORA, P. N. Uso de tecnologías para sistematización de la información sobre el crimen (usos, problemas de georreferencia y demás). Lima: Pontificia Universidad Católica del Perú, 2015.

NGAFEESON, M. Cybercrime Classification: A Motivational Model. ***College of Business Administration***, n. 1201, 2010.

ORTIZ, J. C. La investigación del delito en la era digital: Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación. ***Fundación Alternativas***, n. 74, 2013.

OVERVEST, B.; STRAATHOF, B. What drives cybercrime? Empirical evidence from DDoS attacks, 24 April 2015.

ROJAS, W. Cibercrimen en Perú va en aumento. [S.l.]: Canal Ti, 2016.

SALAZAR, M. Peru: new cybercrime law undermines transparency legislation. New York: ***Global Information Network***, 2013.