Cultura digital sobre Ataques Cibernéticos un estudio exploratorio en personas jóvenes

Carolina Mora Cordero
Universidad Nacional de Costa Rica,
Heredia, Costa Rica.
elena.mora.cordero@est.una.ac.cr

Massiel Mora Rodríguez
Universidad Nacional de Costa Rica,
Heredia, Costa Rica
massiel.mora.rodriguez@est.una.ac.cr

Fulvio Lizano Madriz
Universidad Nacional de Costa Rica,
Heredia Costa Rica
fulvio.lizano.madriz@una.cr

Meribeth Zúñiga Zúñiga
Universidad Nacional de Costa Rica,
Heredia, Costa Rica.
meribeth.zuniga.zuniga@est.una.ac.cr

Lisseth Bolaños Segura
Universidad Nacional de Costa Rica,
Heredia, Costa Rica.
lisseth.bolanos.segura@est.una.ac.cr

ABSTRACT
Hoy en día muchos lugares públicos cuentan con redes Wi-fi gratuitas para que los usuarios se conecten a internet, sin embargo en estos sitios existe un alto grado de posibilidad que ocurra un ataque cibernético. El objetivo principal de esta investigación es conocer ¿Cuáles son las principales características de la cultura digital de las personas jóvenes entre 15 y 24 años acerca del conocimiento que tienen sobre los ataques cibernéticos a los que están expuestos en el Parque Central Nicolás Ulloa, Heredia? Para contestar esta pregunta se realizó una encuesta y observaciones a personas escogidas al azar. Como resultados comprueban la vulnerabilidad que existe ante un ataque cibernético ya que la mayoría de personas no cuentan con medidas de seguridad y reflejan falta de preocupación ante este tema.

Palabras Clave
Ataques cibernéticos, cultura digital, internet.

INTRODUCCIÓN

Las tecnologías de la información han creado una red que se extiende más allá de las fronteras geográficas de los países, éstas han permitido un flujo prácticamente incontrolado de datos. A este nuevo espacio donde millones de personas se conectan, se le denomina ciberespacio [6].

Según el informe de "Estado de la banda ancha en América Latina y el Caribe 2016" emitido por la CEPAL, Costa Rica destaca por el aumento en el acceso a internet mediante dispositivos móviles, siendo el número uno de esa modalidad en América Latina [2].

En América Latina, el acceso a internet por medio de redes inalámbricas, desde hogares, sitios de trabajo, estudios, lugares de acceso públicos como parques y medios de transporte, es cada día más frecuente [2]. El objetivo de nuestra investigación es suplir la carencia de estudios realizados con el tema, la cultura de las personas jóvenes anteriormente delimitada acerca del conocimiento que tienen sobre los ataques cibernéticos. Es por esta razón que se ha formulado la siguiente pregunta de investigación: ¿Cuáles son las principales características de la cultura digital de las personas jóvenes entre 15 y 24 años acerca del conocimiento que tienen sobre los ataques cibernéticos a los que están expuestos en el Parque Central Nicolás Ulloa, Heredia?

El artículo está organizado de la siguiente forma: inicialmente se detallan conceptos básicos de investigaciones previas acerca de los Ataques Cibernéticos, luego, detallamos la metodología realizada para la desarrollar el estudio. Posteriormente se presentan los resultados y su análisis, por último se finaliza con las conclusiones.

ANTECEDENTES

A pesar de que el riesgo de ataques cibernéticos es alto, la investigación en el campo es limitada. Sin embargo, se han realizado trabajos donde explican ciertos conceptos importantes para el presente estudio.

La cultura digital se conoce como un campo de estudio a partir del cual es posible comprender las transformaciones culturales ligadas a la introducción de tecnologías digitales en las sociedades contemporáneas y, en particular, en las del denominado Tercer Mundo, a través de relaciones complejas de entramados tecnosociales, en tres ámbitos a saber: el ejercicio del poder, la acción social colectiva y la experiencia estética [1].

Por otra parte, el término ciberespacio fue acuñado por el escritor William Gibson en su novela Neuromante. Sin embargo, fue John Perry Barlow quien se apropió del término para referirse al ciberespacio como un lugar donde se establecen interrelaciones entre personas libres de ataduras físicas [8]. Así pues, definimos Ciberespacio como el conjunto de posibles comunicaciones que se desarrollan en el ámbito digital, a través de los diferentes dispositivos, canales y medios, y que permiten la interactividad entre usuarios. Como se mencionó anteriormente, las tecnologías de investigación han creado todo un ciberespacio donde las personas en el día a día se conectan para realizar distintas actividades, tanto de trabajo como las cotidianas que con anterioridad se realizaban de diversa manera, como son las transacciones bancarias [6].

La cifra de personas conectadas a la Internet aumenta cada vez más. El uso de internet por medio de teléfonos inteligentes, tabletas o computadoras es más común hoy en día [4]. En Costa Rica, el gobierno intenta incrementar los proyectos para habilitar el Wi-Fi libre en más de 50 puntos del territorio nacional bajo el Programa de RACSA para el Acceso Gratuito de Internet.

Ya que el crecimiento de usuarios conectados ha sido muy rápido, no se ha podido crear una buena resistencia cibernética por factores de limitación de jueces y fiscales en los casos informáticos, lo que limita que la Fuerza Pública del país no esté preparada a estos nuevos crímenes [4].

El Cibercrimen es un nuevo tipo de delito que se comete en el ciberespacio para realizar actos delictivos. Según el artículo de Pedro Rodríguez, "el concepto de cibercrimen abarca desde el delito económico, como el fraude informático, el robo, la falsificación, el computer hacking, el espionaje informático, el sabotaje, la extorsión informática, la piratería comercial y otros crímenes contra la propiedad intelectual, la invasión de la intimidad, la distribución de contenidos ilegales y dañosos, la incitación a la prostitución y otros crímenes contra la moralidad y el crimen organizado" (Rodríguez, 2006) [5].

Según el informe ESET, los ataques cibernéticos, se dan más por vulnerabilidades de software y sistemas como debilidades en el protocolo de cifrado HTTPS o fallas en bibliotecas de desarrollo. Otra de las causas es el Malware o los códigos maliciosos son una preocupación hoy en día. Esta problemática se ha vuelto una preocupación, ya que se dejó de lidiar con incipientes amenazas como los virus, para tener que enfrentar software malicioso cada vez más sofisticado, que tiene un único fin generar ganancias económicas para sus creadores [3]. En Costa Rica el OIJ cuenta desde 1997 con la Sección de Delitos Informáticos, la cual es la encargada de investigar las infracciones de esta índole y otros actos delictivos en donde la informática fue utilizada para la realización de éstos o pueda ser útil para esclarecer la verdad de los hechos [7].

METODOLOGÍA

En esta investigación se utilizaron una encuesta y una observación para la recolección de datos.

Variables	Detalle/ N° / %
Género	Hombre 42 (51.9%) Mujer 39 (48.1%)
Edad	De 15 a 17 años 22 (27.2%) De 18 a 20 años 15 (18.5%) De 21 a 24 años 44 (54.3%)
Ocupación	Trabaja 13 16% Estudia 51 63% Ambas 13 16% Ninguna 4 5%

Tabla 1. Información Demográfica de la encuesta

Variables	Detalle/ N° / %
Género	Hombre 11 (55%) Mujer 9 (45%)
Edad	De 18 a 20 años 8 (40%) De 21 a 24 años 12 (60%)
Ocupación	Trabaja 7 35% Estudia 13 65%

Tabla 2. Información Demográfica de las observaciones

Participantes:

La muestra del estudio utilizada en la encuesta está conformada por ochenta y un participantes de manera aleatoria con las características que se muestran en la tabla1. De estos ochenta y un encuestados se observaron veinte participantes con las características que se muestran en la tabla 2.

Colección de datos

Se elaboró un formulario para la encuesta a través de Google Forms, así mismo, se utilizó el análisis estadístico generado por esta aplicación. Dividimos la encuesta en cuatro secciones: datos demográficos, información sobre dispositivo móviles, conocimiento de redes wi-fi publica y conocimientos teóricos de ataques cibernéticos.

Además, una guía de observación que viene a ayudar al observador en recopilar los datos necesarios para aplicarle un estudio adecuado. Se realizó una guía, en la que se presentan aspectos específicos tales como:

Obs1. Su dispositivo contaba con un antivirus instalado

Obs2. Sabe el nombre del antivirus que posee el dispositivo.

Obs3. Tiene conocimiento sobre la utilización del antivirus.

Obs4. Muestra preocupación respecto a los ataques cibernéticos.

Obs5. Muestra interés en aprender sobre el qué son los ataques cibernéticos.

Obs6. Este informado (a) sobre recientes ataques cibernéticos.

Obs7. Cuenta alguna historia de un ataque cibernético de él mismo o de algún conocido.

Procedimiento

Se centró en las respuestas de los participantes. Se encuestaron y observaron a personas que se encontraban en el parque central de Heredia y que hubieran utilizado la red wifi pública del parque central al menos una vez, además, se tomó en cuenta la disposición voluntaria a participar y que estuvieran en un rango de edad entre 15 y 24 años.

RESULTADOS Y ANÁLISIS

A continuación se presentan los resultados obtenidos en este estudio con su respectivo análisis.

I Parte. Encuestas

Sección 1. Dispositivos móviles

Se les preguntó a los jóvenes qué dispositivo utilizaban para conectarse a la red wifi pública se obtuvo que 80 personas (98.8%) respondieron que utilizaban el teléfono celular. Del total de personas encuestadas 39 personas (48.1%) respondieron que sí tenían un antivirus instalado en su dispositivo, de estas 39 personas, 34 afirmaron mantenerlo actualizado y la frecuencia con que cambian las contraseñas de sus cuentas de usuario solo 77 personas brindaron dicha información de las cuales 32 (41.6%) respondieron que "nunca", 23 (29.9%) dijeron que "muy poco", 15 respondieron que "algunas veces" y solo 7 personas respondieron que "todo el tiempo", además, si al crear una nueva cuenta de usuario utilizaban una contraseña ya empleada anteriormente o creaban una nueva, 37 (45.7%) personas respondieron que sí.

Sección 2. Conocimiento de Red Wifi Pública

En la tabla 3 se incluyó una lista algunos de los usos más utilizados por las personas mientras se esté usando una red wifi pública, la población encuestada encuentra el entretenimiento y las redes sociales como los principales factores al momento de utilizar el dispositivo móvil, destacando que 70 encuestados de los 81 en total utilizan la

red wifi pública para las redes sociales; el segundo uso de importancia fue el entretenimiento con un 60.5% de los encuestados, equivalente a 49 personas. Sin embargo, el uso de la red wifi pública para transacciones bancarias y pagos electrónicos fueron los que tienen menos índice de uso, equivalente a un 12.3% entre los dos. Obteniendo como resultado que, de las personas encuestadas, dedican más tiempo a actividades sociales o de entretenimiento, dejando de último lugar la utilización de la red wifi pública para el movimiento de dinero que sin duda esta es una buena práctica realizada porque es una forma de evitar que nos roben información.

Ante la pregunta si conocen el significado de red wifi pública, 65 personas (80.2%) respondieron que sí de manera firme y si conoce acerca de los riesgos que está expuesto al utilizar puntos de acceso gratuitos a wifi, 42 personas (51.9%) respondieron que sí. Estos datos han sido inesperados ya que casi es la mitad de personas encuestadas las que conocen el término y la otra mitad no, y a como se han popularizado últimamente éstas redes Wifi gratuitas deberían ser más conocidas por la población. Además, la pregunta realizada al participante de que, si conocen el significado de red wifi pública, 65 personas (80.2%) respondieron que sí. Por otra lado se preguntó si conoce acerca de los riesgos que está expuesto al utilizar puntos de acceso gratuitos a wifi, solo 42 personas (51.9%) respondieron que sí.

Usos de dispositivo móvil	**Población**
Entretenimiento	49 (60.5%)
Actividades laborales	9 (11.1%)
Educación	20 (24.7%)
Redes Sociales	70 (86.4%)
Revisa y/o envía correos electrónicos	18 (22.2%)
Transacciones bancarias	6 (7.4%)
Pagos electrónicos	4 (4.9%)

Tabla 3. Uso del dispositivo móvil cuando se está conectado a la red

Sección 3. Conocimientos teóricos

3.1 Conocimiento Básico

Cuando se les preguntó a los encuestados si sabían que es un ataque cibernético solo 23 (32.5%) dijeron que sí. A las personas que respondieron afirmativamente se les preguntó si podían dar alguna definición de ataque cibernético, entre las respuestas más interesantes se obtuvieron las siguientes:

- Es un tipo de intromisión por medio de la red con el fin de robar información o denegar servicios.
- Le roban información personal y hasta dinero por ingresar a sitios inseguros y desde ahí le roban toda la información de la computadora o móvil.
- Robo de información personal, producida por hackers y otras personas.

A los encuestados se les preguntó si podían decir algún método utilizado por los delincuentes para ataques cibernéticos que ellos conocieran, a esta pregunta, solo 18 dijeron conocer alguna.

3.2 Conocimiento específico

En la tabla 4 se muestra el conocimiento de los participantes de alguno(s) de los términos relacionados con ataques cibernéticos. Se representa los resultados según la población (P) representada por ochenta y un participantes y el porcentaje (%) equivalente a un 100% por cada término. Se obtuvo que falsificación es el término más conocido con un 77% equivalente a 63 encuestados, mientras que crímenes contra la propiedad intelectual fue el término menos conocido con un 29.6% equivalente a 24 personas del total encuestados. Se puede comprobar que muchos de estos términos son desconocidos por la población. Ante la pregunta de si el participante sabe qué técnicas de seguridad se pueden usar para prevenir un ataque cibernético, solo un 66.7% (20 de 30) indicaron conocer alguna técnica y sobre el conocimiento del riesgo al dar información personal como correo electrónico o nombre completo podría estar expuesto a un ataque cibernético un 63% (51 de los 81) respondieron que sí conocían el riesgo.

Término	**Si**		**No**	
	P	**%**	**P**	**%**
Falsificación	63	77	18	23
Crímenes contra la integridad intelectual	24	29.6	57	70.4
Invasión a la intimidad	54	66.7	27	33.3
Computer hacking	49	60.5	32	39.5
Espionaje informático	44	54.3	37	45.7
Sabotaje	41	50.6	40	49.4
Fraude Informático	33	40.7	48	59.3
Extorsión	30	37	51	63

Tabla 4. Términos relacionados con ataques cibernéticos.

Pregunta	**Sí**	**No**
Obs1	14	6
Obs2	13	7
Obs3	13	7
Obs4	6	14
Obs5	8	12
Obs6	14	6
Obs7	5	15

Tabla 5. Resultados de la observación

3.3 ¿Cómo proceder ante un ataque?

Cuando se les preguntó a los participantes encuestados si conocen algún caso de ataque cibernético un 36.7% (11 de 30) respondieron de manera afirmativa de las cuales solo un 20% (6 de 30) confirmo que el caso había sido denunciado. Aparte, se obtuvo también que, de un 81 encuestados solo 15 personas (18.4%) respondieron que sí conocían el ente encargado de resolver los delitos

informáticos. Son pocas las personas que denuncian estos delitos, muchos de ellos debido a que no conocen cual es el ente que se encarga en nuestro país de resolverlos. Esto se demuestra en el 81.6% de personas (66 de 81) que negaron conocer este dato.

Observaciones

Los resultados de la observación se reflejan en el resumen realizado en la Tabla 5, donde el acrónimo Obs se define en la metodología.

ANALISIS

Según los resultados podemos inferir que la vulnerabilidad a ser víctimas de un ataque cibernético que presentan las personas al conectarse a una red Wifi gratuita es grande, ya que se pudo observar que aunque si hay personas con antivirus instalados en sus teléfonos, algunos no saben cómo utilizarlos o no los mantienen actualizados. A este factor se suma el hecho de que a la mayoría de personas no les preocupa el tema de los ataques cibernéticos.

Además, viene a afirmar los cambios culturales ligados la tecnología digital, además se pudo comprobar los estudios emitidos por el CEPAL donde se destaca que Costa Rica destaca el aumento de internet mediante dispositivos móviles [2]. Por otro lado, se puede comprobar que menos de la mitad de los encuestados cuentan con antivirus, incluso según los resultados obtenidos la mayoría de las personas no cambian las contraseñas de sus cuentas de usuario con frecuencia, incluso al crear nuevas cuentas utilizan la misma contraseña produciendo un fácil acceso a los delitos informáticos según definido con anterioridad por Pedro Rodríguez ya que Costa Rica no ha podido crear buenas resistencias para evitar estos delitos por el aumento del uso del internet [5]. Es claro que las mayoría de la población conoce el término "internet" y lo que implica estar conectado a él por medio de algún teléfono inteligente u otro dispositivo electrónico afirmando el aumento de conectados a las redes de wifi [4], de aquí también se puede deducir que las personas que utilizan este tipo de acceso libre al internet, la mayoría tiene conciencia de los riesgos que corre al conectarse a esto tipo de redes, correspondiendo al aumento de delitos informáticos en Costa Rica [4,5]. Adicional se evidenciaron los resultados antes investigados según el informe realizado por la compañía de seguridad Symantec, sin embargo existe una diferencia de resultados en el uso de este servicio para las cuentas de correo electrónico ya que en nuestra investigación el uso de las redes wifi públicas para acceder a estos servicios es muy poco, sin obviar que la diferencia de tiempo entre los estudios y esta investigación es de un año aproximadamente. Lastimosamente un porcentaje muy pequeño de esta población muestra preocupación e interés acerca del tema de Ataques Cibernéticos. Por otra parte, la mayor parte de las personas a las que les han realizado algún tipo de estafa, extorción o cualquier otro tipo de estos delitos por medio de la red, no han realizado la denuncia.

CONCLUSIONES

En esta investigación se logró conocer las principales características de la cultura digital presente en las personas jóvenes, se encontró que la cultura digital ha progresado considerablemente en materia del uso de dispositivos electrónicos especialmente el teléfono celular, a pesar de ello existe una carencia de conocimiento con respecto a lo que es un ataque cibernético y todo lo que este conlleva. Asimismo fue evidente la falta de interés y preocupación a la hora de tomar medidas para prevenir ser víctima de algún tipo de ataque cibernético. Afortunadamente ante el gran desconocimiento y desinterés sobre este tema pudimos confirmar que son muy pocas las personas las que utilizan el servicio de wifi gratuito lo cual ya es una ventaja debido a que el estar conectado(a) a este tipo de red implica estar expuesto a cualquier ataque cibernético.

Se tuvo como limitante los factores climáticos, ya que en el mes de mayo hubieron abundantes lluvia provocando que hubiera muy pocas personas en el Parque Central; también, la mayor de las limitantes era el desconocimiento de la población sobre la existencia de esta red wifi o el mal servicio de conexión que brindaba la municipalidad de Heredia, provocando que no se pudiera realizar de manera efectiva la investigación.

REFERENCIAS

1. R.(2008, April). Cibercultura: metáforas, prácticas sociales y colectivos en red [PDF]. Universidad Central de Colombia. Recuperado de http://nomadas.ucentral.edu.co/nomadas/pdf/nomadas_28/28_1R_Ciberculturametaforaspracticas.pdf
2. Edwin Fernando Rojas, L. P. y N. G. (2016, October). Estado de la banda ancha en América Latina y el Caribe 2016. CEPAL, 5–35. Retrieved from http://repositorio.cepal.org/bitstream/handle/11362/40528/S1601049_es.pdf?sequence=6&isAllowed=y
3. ESET. (2014). Eset Security Report Latinoamérica 2014. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2016/04/eset-security-report-latam-2016.pdf
4. Lemieux, F., & Lavinder, K. (2016). Ataques Cibernéticos ¿Está preparada América Latina ? The Cipher Brief, 39–45. Retrieved from http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2016/2016-4/2016_4_05_lavinder_s.pdf
5. Rodríguez, A. P. (2006). Los cibercrímenes en el espacio de libertad, seguridad y justicia., 5–10.
6. Sánchez Medero, G. (2012, April). CIBERESPACIO Y EL CRIMEN ORGANIZADO. LOS NUEVOS DESAFÍOS DEL SIGLO XXI. Revista Enfoques: Ciencia Política Y Administración Pública, 71–87. Retrieved from http://www.redalyc.org/pdf/960/96024266004.pdf
7. Bolaños Diaz, A. y Narvaez Narvaez, T. (2014). Análisis Comparativo Sobre Delitos Informáticos En Colombia Con Relación A Seis Países De Latinoamérica. Colombia: Recuperado de: http://hdl.handle.net/10596/2728
8. Aparici, R. (2014). Conectados en el ciberespacio. Madrid: UNED. Recuperado de https://books.google.co.cr/books?id=EuprFDxMY0UC&pg=PT10&dq=ciberespacio#v=onepage&q=ciberespacio&f=false