

El condimento que faltaba en la educación cibernética en Nigeria: la perspectiva de la seguridad nacional

The missing spice in cyber education in Nigeria: national security perspective

Resumen: Desde el advenimiento de Internet, la cibercrimen se ha convertido en un diezmo periódico en Nigeria. Muchas naciones están luchando para proteger su ciberespacio de los delincuentes, para la seguridad nacional y la integración. Como resultado, los gobiernos están dirigiendo esfuerzos para proteger a sus ciudadanos y su imagen de la delincuencia en línea. Algunos de estos esfuerzos incluyen la educación en ciberseguridad, que implica programas de sensibilización del público en general con el fin de sensibilizarlo sobre el delito cibernético. Se llevaron a cabo varios programas de sensibilización en universidades y otras instituciones educativas e instituciones públicas y privadas. Sin embargo, se ha observado que tales programas nunca se han llevado a cabo al clero, que son agentes fundamentales y quizás uno de los condimentos más importantes que pueden influir en la vida de la mayoría de los nigerianos. Es en este contexto que esta investigación busca utilizar datos cuantitativos para revelar cómo el clero en Nigeria ha sido excluido en la difusión de la conciencia de ciberseguridad entre el público en general. El objetivo del estudio era analizar el papel y la influencia que el clero tiene en su congregación y sugerir formas de usar esta influencia para mejorar la conciencia de ciberseguridad en Nigeria con el fin de aumentar la seguridad nacional en el país.

Abstract: Since the advent of the internet, cybercrime has become a recurring decimal in Nigeria. Many nations are battling to protect their cyber space from criminals, for national security and integration. As a result of this, efforts are being made by governments to protect their citizens and image from online crime. Some of these efforts include cybersecurity education which entails awareness raising programmes to the general public in order to sensitize them about cybercrime. Several awareness raising programmes have been conducted to universities and other educational institutions and public and private institutions. However, it was observed that such programmes have never been conducted to the clergy who are fundamental agent, perhaps one of the most important spice that tends to create influence in the life of most Nigerians. It is against this backdrop that this research seek to utilize quantitative data to reveal how the clergy in Nigeria have been left out in the propagation of cybersecurity awareness among the general public. The objective of the study was to analyze the role and influence the clergy have on their congregation and suggest ways such influence can be utilized to improve cybersecurity awareness in Nigeria for enhanced national security in the country.

Shehu Saidu Shehu 

Nigerian Army.

Abuja, Nigeria.

saidisco@yahoo.com

Recibido: 04 abr. 2020

Aceptado: 12 jul. 2020

COLEÇÃO MEIRA MATTOS

ISSN on-line 2316-4891 / ISSN print 2316-4833

<http://ebrevistas.eb.mil.br/index.php/RMM/index>



1 Introducción

Uno de los fenómenos tecnológicos más significativos que ha afectado positivamente la forma de vida de los seres humanos en todo el mundo es el surgimiento del ciberespacio. El ciberespacio es un dominio global virtual que ha estado impactando cada vez más en casi todos los aspectos de la vida diaria. El dominio está moldeando rápidamente la comunicación, el aprendizaje y la colaboración entre individuos y organizaciones. También está transformando las naciones, eliminando las barreras al comercio y creando oportunidades para las innovaciones (OMODUNBI et al., 2016). Sin embargo, nuevos riesgos y vulnerabilidades que amenazan la economía y la seguridad nacionales están detrás de la creciente dependencia del ciberespacio (TIIRMAA-KLAAR, 2016). Disponer de los conocimientos necesarios sobre las amenazas existentes, lo que conducirá a la gestión de riesgos y a la creación de capacidades adecuadas de prevención y recuperación, son los elementos esenciales de la ciberseguridad. Hoy en día, la ciberseguridad es crucial para el desarrollo económico y la seguridad nacional del país, ya que los delincuentes cibernéticos utilizan el ciberespacio para perpetuar actos nefastos (TIEMO; NELLY, 2016).

El término "delito cibernético" simboliza la inseguridad y el riesgo en línea, siendo ampliamente utilizado hoy en día para describir delitos o daños que se cometen utilizando tecnologías en red (OSHO; ONOJA, 2015). al revés, la ciberseguridad es la protección de los sistemas y redes del ciberespacio contra daños, uso no autorizado o explotación. También es el método utilizado para proteger la fiabilidad de las redes y los sistemas contra amenazas cibernéticas fundamentales, como el ciberterrorismo y la ciberdelincuencia. Dado que los Estados-ación dependen de una amplia gama de redes y sistemas del ciberespacio para el desarrollo económico, la violación de estas redes puede tener graves implicaciones para la seguridad nacional (HILTS, 2018). Además, teniendo en cuenta que la seguridad nacional es la responsabilidad primordial de cada gobierno, las naciones están desarrollando sus esfuerzos de ciberseguridad con el fin de proporcionar un ciberespacio seguro y resiliente para el desarrollo económico. Además, el aumento de la capacidad cibernética de los delincuentes para cometer delitos ha puesto ciertamente en riesgo la seguridad nacional de los Estados (HARE, 2010).

En octubre de 2008, Funcionarios de inteligencia estadounidenses han revelado que las autoridades policiales europeas han descubierto una red de fraude de tarjetas de crédito altamente sofisticada que utiliza tecnología altamente avanzada para enviar datos de cuentas a Pakistán desde cientos de máquinas de tarjetas de supermercados en toda Europa (SIOBHAN, 2018). Del mismo modo, a principios de 2016, un grupo atacante llamado "Lazarus", ubicado en Corea del Norte, robó un total de más de US\$ 100 millones, principalmente de Bangladesh Bank a través de la penetración del Alliance access software utilizado por la red de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT), que realiza transacciones financieras mundiales de manera segura y estandarizada. En la misma línea, un ataque a Maersk por NotPetyransomware más tarde en 2017 costó al gigante del transporte hasta US\$ 300 millones (KOCH; GOLLING, 2018).

En África, Sudáfrica ha experimentado el mayor número de ataques cibernéticos por parte de delincuentes. Según Dahir (2018), Sudáfrica registra un alto número de ataques cibernéticos al

año, ya que el 67% de las empresas fueron supuestamente atacadas. Se estima que estos ataques han costado a la economía sudafricana US\$ 242 millones, aumentando así la tasa de desempleo en el país y afectando los medios de vida (VERMUELEN, 2016). Estimar la pérdida neta generada por la cibercrimen es una tarea difícil. Las cifras oficiales publicadas por organismos gubernamentales o no gubernamentales son indicadores débiles, ya que solo se incluyen los casos que se les presentan. Sin embargo, el último informe indica que el costo total de la cibercrimen es de alrededor de US\$ 600 mil millones, incluidas las ganancias para los delincuentes y los costos de recuperación y defensa para las empresas (LEWIS, 2018).

Nigeria tiene más de 120 millones de usuarios de Internet, lo que representa el 24% de todos los usuarios de Internet en África (INTERNET WORLD STATS, 2019). Este uso de Internet consiste principalmente en el uso de Internet móvil en contraposición al uso de banda ancha fija por suscripción. Sin embargo, esta creciente dependencia del uso de Internet viene con una mayor exposición a amenazas y vulnerabilidades, especialmente en un país popularmente conocido como "yahooyahoo"¹ (TADE; ALIYU, 2011). La encuesta reveló que el 80% de estos "yahooyahoo" son jóvenes y a veces estudiantes de diversas instituciones superiores (ARANSIOLA; ASINDEMADE, 2011). Desde los organismos gubernamentales hasta el público en general ya se han convertido en víctimas de este grupo de personas.

Este grupo de delincuentes sigue prosperando, a pesar de los diversos esfuerzos, severos y leves, realizados por el gobierno de Nigeria para contener la terrible amenaza en el país. El duro esfuerzo se refiere al uso de varias legislaciones de delitos cibernéticos que pueden hacer que los delincuentes sean arrestados, mientras que el esfuerzo leve implica educación, capacitación y habilidades de ciberseguridad. Por invitación de la Oficina del Asesor de Seguridad Nacional (ONSA) en octubre de 2018, el Centro Global de Seguridad Cibernética (GCSCC) realizó una revisión de la madurez de la capacidad de ciberseguridad en Nigeria utilizando el modelo de madurez de ciberseguridad (CMM)² que se compone de 5 dimensiones distintas de la capacidad de ciberseguridad. En la tercera dimensión, el GCSCC analiza la disponibilidad del Programa de Concienciación sobre Ciberseguridad tanto para el público como para los ejecutivos. Sin embargo, se señaló que el Centro no consideró los programas de concientización del clero que son un condimento importante³ el tejido cultural de las comunidades y, como tal, puede influir en la toma de decisiones, las ideologías y los comportamientos morales y éticos de las personas (PINTER et al., 2016).

El objetivo de esta investigación es, por lo tanto, revelar cómo el clero en Nigeria ha sido excluido en la difusión de la conciencia de ciberseguridad al público en general, el grupo más afectado por el delito cibernético. El objetivo del estudio era analizar el papel y la influencia que el clero tiene en su congregación y sugerir formas de usar esta influencia para mejorar la conciencia de ciberseguridad en Nigeria con el fin de aumentar la seguridad nacional en el país. El estudio es significativo, ya que el resultado puede ayudar a mejorar las políticas y agregar al cuerpo existente de conocimiento en ciberseguridad.

1 "YahooYahoo" es una expresión utilizada en Nigeria para referirse a la cibercriminalidad.

2 Ver Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM) edición repasada en: <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition>. Consultado el: 21 Sep. 2019.

3 Condimento se usa aquí para significar "un atributo que hace algo atractivo, interesante o atractivo".

La investigación fue aplicada y se utilizaron datos empíricos que fueron recolectados y analizados. Se utilizó el método de campo de recolección de datos mediante entrevistas y cuestionarios, analizándolos cuantitativamente. Además, el tamaño de la muestra del estudio se realizó utilizando la fórmula de tamaño de la muestra de Taro Yamane. El estudio adoptó una muestra aleatoria por conglomerados y los datos generados se presentaron mediante gráficos para ilustrar las relaciones entre las variables del estudio. El estudio se limita al clero, así como el límite de 6000 a 8000 palabras.

2 Revisión de la literatura

2.1 Contexto

El uso de Internet y el número de suscriptores han crecido exponencialmente en Nigeria en los últimos años. De acuerdo con la sección 89, subsección 3 (d), de la Ley de Comunicaciones de Nigeria de 2003 (NCA, 2003)⁴, el informe de la Comisión Nigeriana de Comunicaciones (NIGERIAN COMMUNICATIONS COMMISSION, 2019) afirma que el número de suscriptores activos de Internet móvil y fijo en Nigeria es de alrededor de 175 millones y más de 120 millones, respectivamente. El gran número de suscriptores de Internet son en su mayoría jóvenes que buscan empleo productivo, compromiso social y una mayor conectividad mundial. Sin embargo, con esta creciente prosperidad y digitalización, surgen amenazas, riesgos, vulnerabilidades y delitos informáticos que pueden socavar la seguridad nacional. Los delitos cibernéticos son esencialmente actividades delictivas en las que las computadoras, las redes o los dispositivos electrónicos de tecnología de la información son la fuente, la herramienta, el objetivo o la escena del delito. Los delitos cibernéticos se llevan a cabo a través del acceso ilegal a la base de datos de otra persona, la interceptación ilegal, la interferencia de datos, la interferencia en los sistemas, el uso indebido de dispositivos, la falsificación y el fraude electrónico (BAIDEN, [N. D.]).

2.2 Cibercrimen

En Nigeria, la cibercriminalidad se ha convertido en una de las principales vías para robar dinero y practicar el espionaje comercial. Dentro del ciberespacio nigeriano, Serianu (2016) reveló que el costo de la cibercriminalidad en Nigeria es de alrededor de US\$ 649 millones, con el 81% de los incidentes cibernéticos causados por la proliferación de noticias falsas, ransomware y fraude en Internet, siendo el público en general la categoría más afectada. En agosto de 2019, las autoridades estadounidenses descubrieron y acusaron a 80 personas, la mayoría de las cuales son nigerianas "yahooyahoo" en una estafa de US\$ internet de 46 millones (FARIVAR, 2019). Los estafadores supuestamente victimizaron a individuos de pequeñas y grandes empresas utilizando una táctica llamada "Business Email Compromise (BEC)"⁵.

4 La ley requería que la NCC monitoreara e informara sobre el estado de la industria de las telecomunicaciones de Nigeria, brindara análisis estadístico e identificara las tendencias de la industria en relación con los servicios, tarifas, operadores, tecnología, suscriptores, problemas de competencia, dominio, entre otros, con el fin de identificar áreas donde se necesitaría una intervención regulatoria.

5 BEC es una exploración en el que el atacante obtiene acceso a una cuenta de correo electrónico corporativa y falsifica la identidad del propietario para defraudar a la empresa o a sus empleados, clientes o socios de dinero.

El FBI y la Agencia Anticorrupción de Nigeria, la EFCC⁶, reveló que 167 personas en Nigeria y 74 en los Estados Unidos habían sido víctimas, semanas después de que las autoridades estadounidenses publicaron una lista de sospechosos nigerianos detrás de la estafa en línea. Estos ciberdelincuentes detenidos y varios otros generalmente son procesados por la EFCC de acuerdo con las leyes existentes, para servir como un elemento disuasorio para otros. Por lo tanto, además de la detención y el enjuiciamiento de los delincuentes, el gobierno tiene una sólida iniciativa de educación cibernética centrada en el programa para crear conciencia sobre los riesgos y amenazas de ciberseguridad, y cómo abordarlos, para el público en general y las partes interesadas del gobierno y el sector privado.

2.3 Educación Cibernética

Se observa que la falta de conocimiento de las mejores prácticas de seguridad, la baja educación de los usuarios y la ausencia de programas de sensibilización pueden ser los principales factores atribuidos a la exposición de la mayoría de los nigerianos a las amenazas cibernéticas. Sin embargo, se han notado muchas iniciativas de concientización sobre seguridad cibernética organizadas por algunas instituciones en colaboración con la ONSA, la Agencia Nacional de Desarrollo de Tecnologías de la Información (NITDA), EFCC, el Banco Central de Nigeria (CBN) y NCC, entre otros, dirigidas a sensibilizar a los ejecutivos y al público en general sobre la importancia de la ciberseguridad. Tales iniciativas incluyen el Mes de Concientización sobre Seguridad Cibernética (NCSAM), organizado por el Centro Internacional para el Desarrollo del Liderazgo de Nigeria (ICHDNG). La última NCSAM se celebró en octubre de 2018. Otras iniciativas son la oferta de cursos académicos especializados en ciberseguridad en la Universidad Estatal de Nasarawa (CENTER FOR CYBERSPACE STUDIES, 2019), la Primera Universidad Técnica (TECH-U, [201-]), la Universidad Federal de Tecnología (SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY, c2016) y la Academia Nigeriana de Defensa Kaduna (NIGERIAN DEFENSE ACADEMY, [201-]).

También hay una conferencia anual de seguridad cibernética llamada CyberSecure Nigeria Conference organizada por la Asociación de expertos en seguridad cibernética de Nigeria (CSEAN). La asociación tiene como objetivo reunir la investigación sobre ciberseguridad de la industria y el mundo académico (CYBER SECURITY EXPERTS ASSOCIATION OF NIGERIA, 2019). Además, proveedores de servicios como la Asociación de Proveedores de Pagos Electrónicos de Nigeria (E-PPAN) también han participado en campañas de sensibilización pública, en particular sobre el uso de plataformas de pago electrónico. Además, se observó la aceptación de la certificación internacional de seguridad profesional como ISACA y la Organización Internacional de Normalización (ISO) serie 27000 (GCSCC, 2018). Fuera de las instituciones académicas y oficiales, hay algunos programas comunitarios relacionados con la ciberseguridad para niños. Este programa forma parte de la escuela de verano que se ofrece a estudiantes de primaria y secundaria (DIGITAL PEERS INTERNATIONAL, 2019).

⁶ EFCC significa Comisión de Crímenes Económicos y Financieros.

Estos programas de sensibilización parecen haber sido completos. Sin embargo, GCSCC, que fue invitado por la ONSA para llevar a cabo una revisión de la madurez de la capacidad de ciberseguridad de Nigeria con el objetivo de comprender su capacidad de ciberseguridad con el fin de priorizar la inversión en capacidades de ciberseguridad estratégicamente, señalando que hay una necesidad de una mayor cooperación entre la academia y la industria en la investigación de ciberseguridad. El centro señaló además que se deben proporcionar recursos adecuados para facilitar la educación en materia de ciberseguridad en las universidades y que la membresía de CSEAN solo está abierta a estudiantes, graduados, profesionales de TI y aquellos que no tienen capacitación en TI pero trabajan en instituciones relacionadas. Asimismo, se observó que en lugar de un mes completo, el NCSAM fue llevada a cabo sólo por dos días debido a las restricciones de otras iniciativas que se han producido. Tras el diagnóstico de ciberseguridad de educación de la madurez, la GCSCC hecho algunas recomendaciones encaminadas a proporcionar consejos y pasos a seguir para aumentar la existente en ciberseguridad de la capacidad en Nigeria. Una lectura atenta de la revisión por la GCSCC reveló que no hubo ninguna mención de cualquier campaña de sensibilización organizada por los líderes religiosos en iglesias y mezquitas entre la lista de todos los lugares donde la ciberseguridad de la campaña de sensibilización se ha enumerado. También se observó que la composición de los actores en el diagnóstico realizado por la GSCSS no incluía al clero y no se mencionaban en las recomendaciones del Centro.

2.4 Influencia del Clero en la Población Nigeriana

Nigeria es un país aproximadamente a la mitad entre los cristianos, que viven principalmente en la parte sur del país, y los musulmanes en la parte norte, con una minoría de la población que practica la religión indígena de Nigeria. El escritor y novelista BCC (LETTER..., 2014) reveló que en Nigeria, un país que afirma tener muchas de las celebridades e intelectuales más aclamadas de África, las páginas de Facebook y Twitter con el mayor número de seguidores son las del clero. Ella reveló además que muchos líderes religiosos en Nigeria se consideran superestrellas y desempeñan un papel positivo en el país. Agregó que si los líderes de las cinco iglesias más grandes de Nigeria daban alguna indicación de que nadie debería leer obras del renombrado novelista ChinuaAchebe, la base de fans del autor y las ventas de libros en Nigeria se hundirían instantáneamente, independientemente de lo aclamado que sea en todo el mundo. En Nigeria, la mayoría de los que pertenecen a una u otra religión entienden la espiritualidad como parte de la religión. Sobre este tema, Aja (2019) destacó que:

Tienden a definir la espiritualidad de varias maneras, incluyendo creer o tener fe en lo trascendente, tener esperanza en lo trascendente, tener una relación con lo trascendente y ser religioso, abrir el corazón a lo trascendente, ir a la iglesia, ir a la mezquita, apaciguar a lo trascendente, hacer todo lo que ordena lo trascendente, observar los principios religiosos. Algunos pueden definir la espiritualidad usando una combinación de dos o más de estas definiciones. El trascendente aquí puede ser Dios, Jesús, Allah, o dioses, dependiendo de la tradición religiosa. Los adherentes de la religión islámica, así como los de la religión tradicional, creen en la supremacía de Dios.

La pasión por la religión ha penetrado profundamente en todas las facetas de la vida nigeriana y difícilmente puede ser relegada a un segundo plano. La prohibición religiosa de la planificación familiar ha sido atribuida como el principal factor que inhibe el éxito del programa en Nigeria (LAWANI; IYOKE; EZEONU, 2015). Del mismo modo, Nwaubani (LETTER..., 2014) reveló que cuando los nigerianos estaban convencidos de que sus votos no contarían en las elecciones generales de 2007 a menos que estuvieran registrados, la gente se puso en fila durante horas simplemente porque sus pastores les ordenaron hacerlo. El reportero de la BBC agregó que los líderes religiosos también han desempeñado un papel clave en las batallas contra la poliomielitis, el VIH y la lucha contra el brote de ébola en Nigeria, transmitiendo información relevante y enfatizando la urgencia de la situación desde sus púlpitos. Por lo tanto, el clero podría convertirse en el mayor recurso de Nigeria en la campaña de concientización cibernética si su inmensa influencia fuera aprovechada de maneras más estructuradas y enfocadas.

3 Metodología

El método de recolección de datos adoptado en este estudio fue el método de campo. Este método utiliza una combinación de entrevistas y cuestionarios. Los datos primarios para el estudio fueron recopilados de profesionales de ciberseguridad que están asignados a agencias como ONSA, NITDA, NCC, EFCC, Administración de Defensa del Espacio (DSA) y Centro de Ciberseguridad del Ejército de Nigeria Otros son del clero en varios lugares de culto. Dado que la mayoría de la población nigeriana son musulmanes y cristianos, el clero estudiado fue el de las mezquitas y las iglesias. Se enviaron dos series de cuestionarios. Uno se enfocó en el público profesional para averiguar si alguna vez habían considerado al clero como parte de su programa de concientización. El segundo cuestionario estaba destinado al clero para conocer su nivel de conciencia cibernética y si alguna vez habían recibido alguna forma de campaña de conciencia. Cuestionarios cuya fiabilidad era $\alpha = 0,94$ y $0,73$ para el clero y las profesiones de ciberseguridad, respectivamente, en relación con el Alfa recomendado por Cronbach $\alpha = .70$ (UNIVERSITY OF CALIFORNIA, [201 -]) se utilizó para generar datos y los datos recopilados se analizaron cuantitativamente utilizando Microsoft Excel. Como los encuestados estaban en Nigeria, el investigador envió los cuestionarios por WhatsApp al líder de escuadrón Ngulde y al teniente de vuelo Akintunde, quienes ayudaron con la distribución, supervisión y recuperación (BASSIC - RESEARCH, 2019)⁷.

Los datos secundarios se obtuvieron de revistas, seminarios, conferencias y revistas pertinentes. Otros son periódicos en línea, investigaciones inéditas y otros materiales relevantes de Internet. Para calcular el tamaño muestral del estudio se utilizó la fórmula de Taro Yamane con un margen de error del 5% y un nivel de confianza del 95% (QUORA.COM, [S.d.]). Esto resultó en una muestra de 98 y 65 para el clero y profesionales de la ciberseguridad, respectivamente. El estudio adoptó el muestreo aleatorio por conglomerados, ya que los clérigos considerados eran solo aquellos que administraban dentro del área de residencia de los servicios de seguridad. Del mismo modo, los encuestados desde la perspectiva profesional fueron considerados aquellos

⁷ Los cuestionarios pueden consultarse en: <https://drive.google.com/open?id=1LdXeL5f7iCNwCE2xXC9AeEc1HU4PREdR>.
Accesado el: 21 Sep. 2019.

que abordaron profesionalmente la ciberseguridad. Esto se debe a que todas las organizaciones que planifican y ejecutan campañas de sensibilización lo hacen en colaboración con organismos gubernamentales. Los datos generados fueron presentados mediante gráficos para ilustrar las relaciones entre las variables del estudio.

El paradigma teórico utilizado para analizar el uso del clero en la conciencia de ciberseguridad por parte de los profesionales es el de la Teoría del comportamiento Planificado. La premisa principal de esta teoría es que busca predecir la intención conductual, o la probabilidad de que una persona realice un determinado comportamiento. El investigador agregó que una persona es más propensa a realizar un comportamiento específico si el comportamiento se considera importante y si cree que otros aprobarían el comportamiento (AJZEN, 2002; BLOOMFIELD, BOMMARITO, KUHL, 2015).

4 Análisis y presentación de datos

Este capítulo contiene la presentación y el análisis de los datos recogidos de los encuestados. Los datos analizados fueron representados en números absolutos y porcentajes. Además, cada pregunta en su conjunto en el cuestionario fue analizada a través de un gráfico para mostrar los detalles de las respuestas. Se administraron ochenta y nueve cuestionarios al clero, mientras que se enviaron sesenta y cinco a profesionales de la ciberseguridad. Todos los cuestionarios fueron debidamente cumplimentados y devueltos.

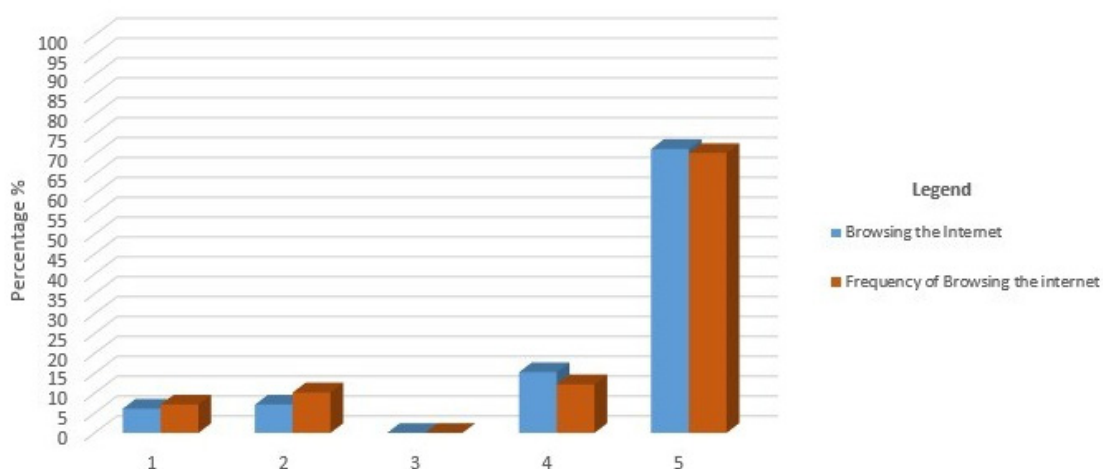
4.1 Análisis de los Datos Obtenidos del Clero

Los datos analizados en esta sección son los del clero. Los datos no fueron analizados en términos de los que ministran en la mezquita o iglesia, sino más bien como representantes de su centro religioso. El cuestionario tenía 16 preguntas en total y cada pregunta tenía una calificación de 1 a 5, siendo 1 la más débil y 5 la más fuerte.

4.1.1 Conocimiento de Internet

El investigador investigó si los encuestados navegan por Internet y con qué frecuencia lo hacen. Las respuestas son las que se muestran en el gráfico 1.

Gráfico 1 – Gráfico del Conocimiento de Internet de los Encuestados



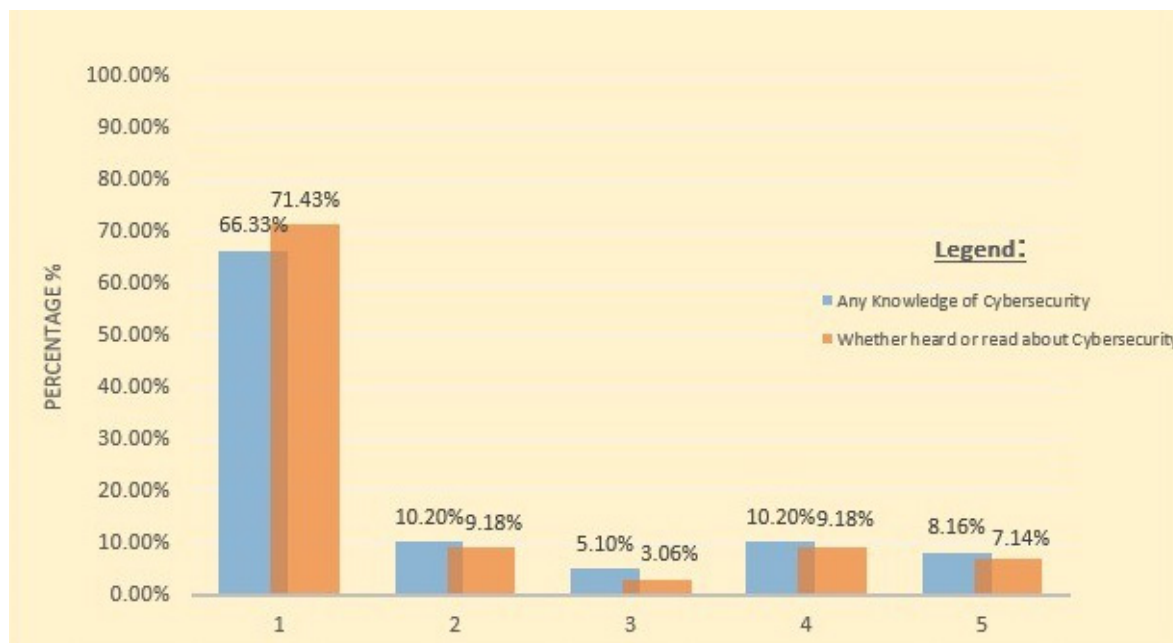
Fuente: Autor (2019).

El Gráfico 1 muestra que el 71,43% de los encuestados navega muy bien por Internet, donde el 15,31% navega bien, mientras que el 6,12% nunca navega por Internet. El alto porcentaje de quienes navegan por Internet contra el bajo porcentaje de quienes no lo hacen, converge con el informe de NCC, que afirma que hay 120 millones de suscriptores de Internet en 2019 (NIGERIAN COMMUNICATIONS COMMISSION, 2019). La cifra también reveló que el 70,41% de los encuestados visita Internet con más frecuencia, frente al 7,14% de los que no visitan Internet. El resultado de la investigación sobre las dos condiciones confirmó la veracidad del informe del NCC.

4.1.2 Conocimiento de la Ciberseguridad

El investigador preguntó si los encuestados tienen algún conocimiento de ciberseguridad, han leído u oído hablar de ella. El resultado de esta encuesta se muestra en el Gráfico 2.

Gráfico 2 – Gráfico sobre el Conocimiento de Ciberseguridad de los Encuestados



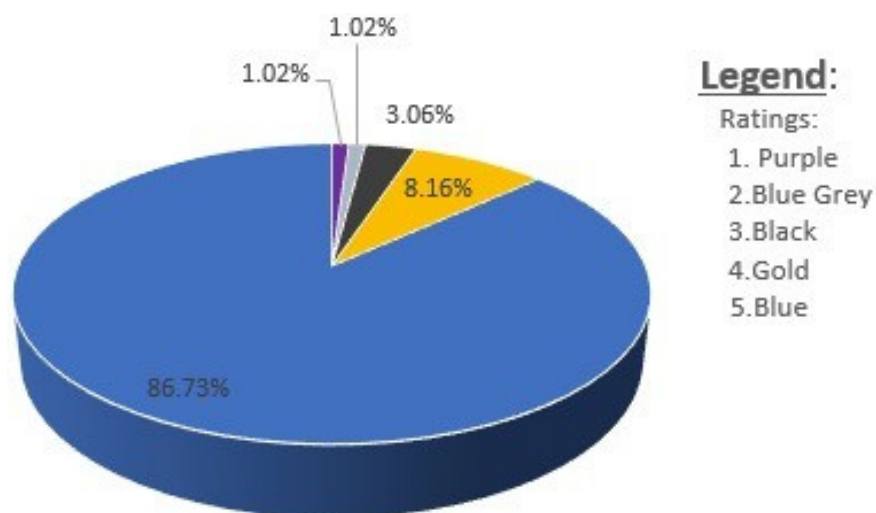
Fuente: Autor (2019).

El gráfico 2 reveló que el 66.33% del clero afirmó no tener conocimiento sobre ciberseguridad. El informe también reveló que el 71,43% de ellos no había leído ni oído hablar de ciberseguridad. La cifra también reveló que el 8,16% de los encuestados dijo tener un conocimiento muy bueno de la ciberseguridad, mientras que el 10,20% dijo que tenía conocimiento de ella. Por otro lado, el 7,14% de los encuestados indicó tener un muy buen conocimiento de ciberseguridad a través de la lectura o conferencias, mientras que el 9,18% reveló un buen conocimiento a través del mismo medio. La gran diferencia entre los encuestados que no tienen conocimiento de ciberseguridad y los que tenían conocimiento de ella puede indicar que aquellos que ya han oído hablar del tema no necesariamente lo hicieron a través de campañas de sensibilización cibernética organizadas en el lugar de culto.

4.1.3 Conocimiento de cualquier Campaña de Sensibilización sobre Ciberseguridad organizada en un lugar de culto.

Se les preguntó si se había organizado alguna campaña de sensibilización sobre ciberseguridad en los lugares de culto de los encuestados y los resultados de la encuesta de campo se muestran en el Gráfico 3 a continuación:

Gráfico 3 – Gráfico del Conocimiento de las Campañas de Sensibilización sobre Ciberseguridad Organizadas en un Lugar de Culto



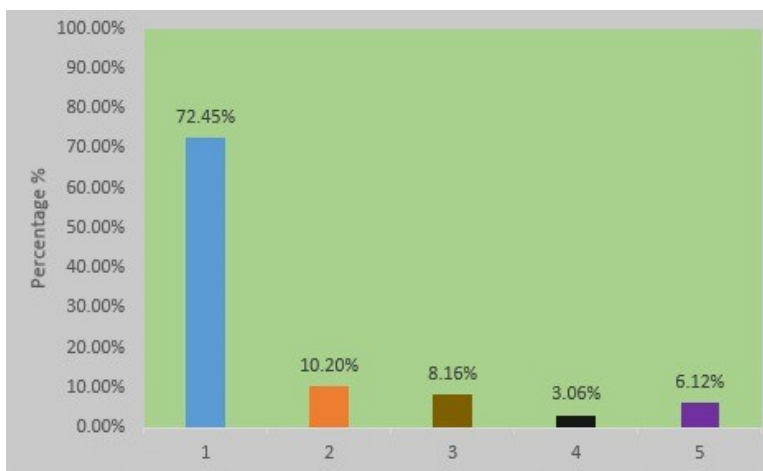
Fuente: Autor (2019).

En el Gráfico 3 anterior, se puede ver que el 86.73% de los encuestados desconocían cualquier campaña de concientización sobre seguridad cibernética realizada en su lugar de culto. Por lo tanto, se puede deducir que el alto porcentaje obtenido aquí dio credibilidad al análisis del investigador en la sección 4.1.2 que el pequeño porcentaje de encuestados que tienen conocimiento de ciberseguridad lo tienen por sí solo y no como resultado de una campaña organizada de sensibilización sobre ciberseguridad.

4.1.4 Conocimiento de Ciberseguridad

El investigador preguntó si los encuestados son conscientes de la ciberdelincuencia y el resultado de la encuesta se muestra en el Gráfico 4 a continuación.

Gráfico 4 – Evolución del Conocimiento de la Cibercrimen



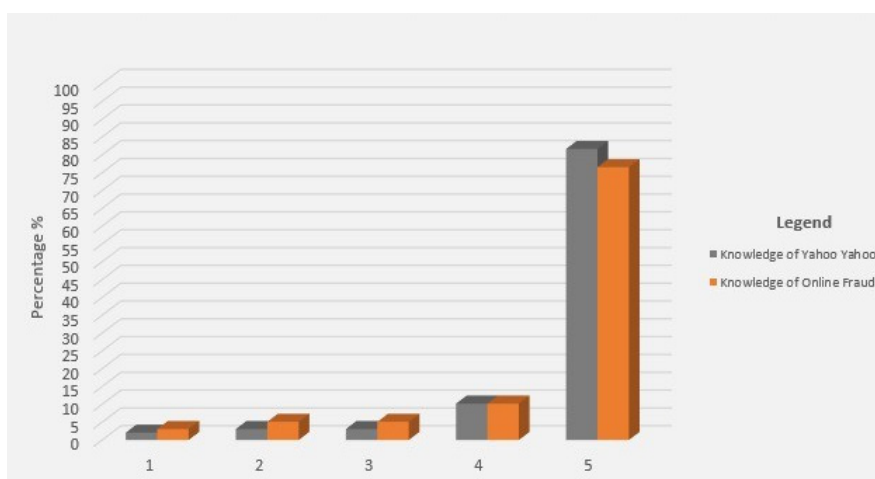
Fuente: Autor (2019).

El Gráfico 4 reveló que el 72,45% de los encuestados no son conscientes de la cibercrimen. El resultado aquí es potencialmente preocupante si se considera en el contexto de lo demostrado en la Sección 4.1.1 y lo revelado por Business Day (AKIYODE-LAWANSON, 2019) que Nigeria ocupa el tercer lugar en usuarios atacados por malware móvil, con un 37.72%.

4.1.5 Conocimiento de Yahoo Yahooe 419⁸

El investigador preguntó si los encuestados tienen conocimiento de YahooYahoo y 419 en Nigeria y el resultado de la encuesta se muestra en el Gráfico 5 a continuación.

Gráfico 5 – Gráfico del Conocimiento sobre Yahoo Yahoo y 419 de los Encuestados



Fuente: Autor (2019).

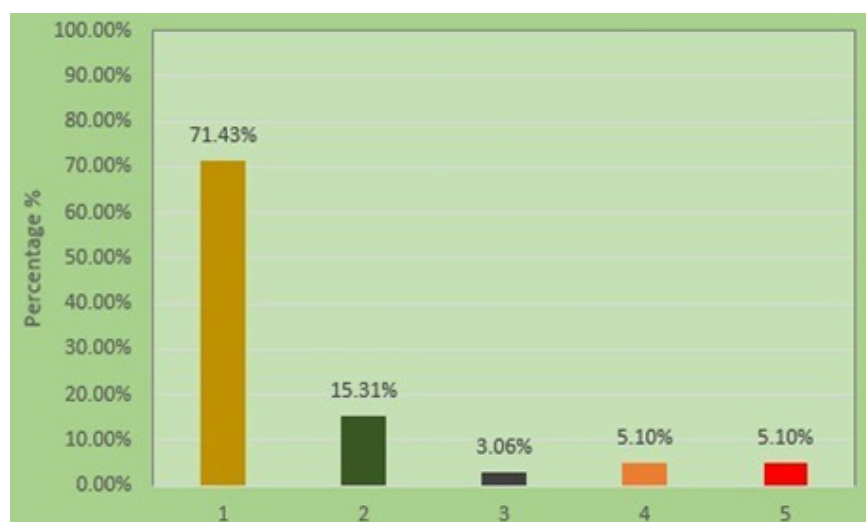
8 Plazo 419 se utiliza generalmente para describir actividades fraudulentas. Se originó en la sección 419 de las leyes en vigor en Nigeria, que penaliza el fraude financiero y el fraude en Internet o el fraude cibernético en Nigeria.

En el gráfico 5, se puede observar que el 81,63% y el 76,3% de los encuestados conocen YahooYahoo y 419, respectivamente. El alto porcentaje obtenido aquí puede ser el resultado de una práctica popular de YahooYahoo de enviar mensajes fraudulentos para engañar a los suscriptores de la red GSM. Tade y Aliyu (2011) revelaron que los criminales, teniendo conocimiento del funcionamiento del sistema de promoción de las telecomunicaciones, lo clonaron y explotaron para defraudar a los nigerianos enviando mensajes fraudulentos en sus teléfonos sobre una gran cantidad de dinero que ganaron. Los investigadores muestran además que los delincuentes luego pidieron a la víctima que enviara una cierta cantidad de crédito a un cierto número antes de hacer la llamada para negociar cómo se entregaría el premio. Tales actos han hecho YahooYahoo y 419 muy popular en Nigeria.

4.1.6 Conocimiento de la relación entre cibercrimen, YahooYahoo y fraude en línea

El investigador verificó si los encuestados son conscientes de que el cibercrimen es el mismo que YahooYahoo y 419. Los resultados se muestran en el gráfico 6 a continuación.

Gráfico 6 – Gráfico del Conocimiento de los Encuestados sobre la Relación entre el Cibercrimen, YahooYahoo y el Fraude en Línea



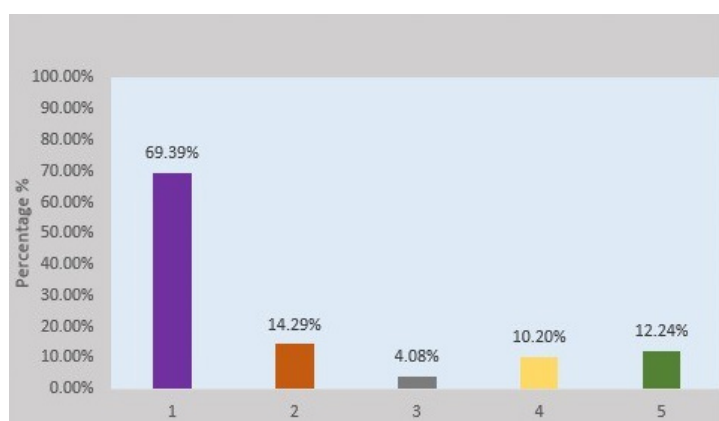
Fuente: Autor (2019).

En el gráfico 6 anterior, se puede ver que el 71,43% de los encuestados no son conscientes de ninguna relación entre el cibercrimen, YahooYahoo y 419. De los resultados obtenidos en la sección 4.1.4 y la sección 4.1.5, se puede ver que los encuestados tienen un amplio conocimiento de YahooYahoo y 419, pero no tienen idea de lo que significa el cibercrimen. Por lo tanto, el hecho de que no sean conscientes de que YahooYahoo, 419 y cibercrimen significan lo mismo, indica que ven YahooYahoo y 419 desde el prisma de engañar a un individuo y no necesariamente tener que ver con el ciberespacio.

4.1.7 Conocimiento de las medidas que deben adoptarse cuando son víctimas del crimen cibernético

El investigador preguntó si los encuestados tenían algún conocimiento de las acciones que se deben tomar cuando son víctimas del delito cibernético. Los resultados se muestran en el Gráfico 6 a continuación.

Gráfico 7 – Gráfico del Resultado sobre las Medidas que Deben Adoptarse Cuando son Víctimas del Crimen Cibernético



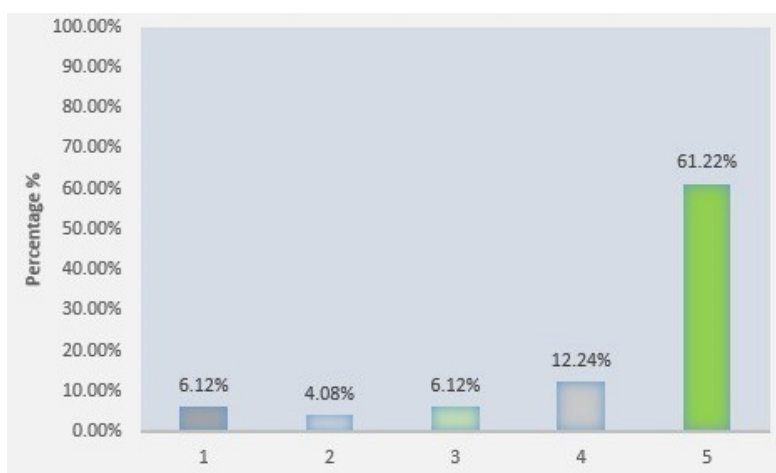
Fuente: Autor (2019).

El gráfico 7 revela que el 69,39% de los encuestados no son conscientes de las medidas que deben tomarse cuando son víctimas de la cibercriminalidad. El gráfico también reveló que solo el 12,24% conocía las medidas a tomar. El alto porcentaje de personas que no eran conscientes de las acciones a tomar no es sorprendente debido a la falta de conocimiento de ciberseguridad por parte de los encuestados. Se puede decir que esta falta de conocimiento por parte de los encuestados es de particular preocupación con la circular de CBN (CENTRAL BANK OF NIGERIA, 2019) para que todos los bancos de dinero de depósito nos informen de su política de implementar la recolección de retiros y depósitos de personas físicas y jurídicas para que se haga cumplir la campaña del gobierno por una sociedad sin dinero físico. La circular indicaba que las tasas eran del 3% y el 2% a cobrar a los particulares por retiros de efectivo y depósitos, respectivamente, mientras que el 5% y el 3% se aplicaban a las empresas. El hecho de que los cargos entren en vigor el 31 de marzo de 2020 significa que todas las actividades financieras en el país estarán en línea a partir de esa fecha. Por lo tanto, existe la necesidad de una campaña agresiva de concienciación sobre ciberseguridad para mitigar el riesgo inherente al ciberespacio.

4.1.8 Conocimiento sobre cómo ser afectado por YahooYahoo

El investigador preguntó si los encuestados ya habían sido afectados por YahooYahoo y el resultado de la encuesta de campo se muestra en el Gráfico 8 a continuación:

Gráfico 8 – Gráfico sobre el Conocimiento de Haber Sido Afectado por YahooYahoo



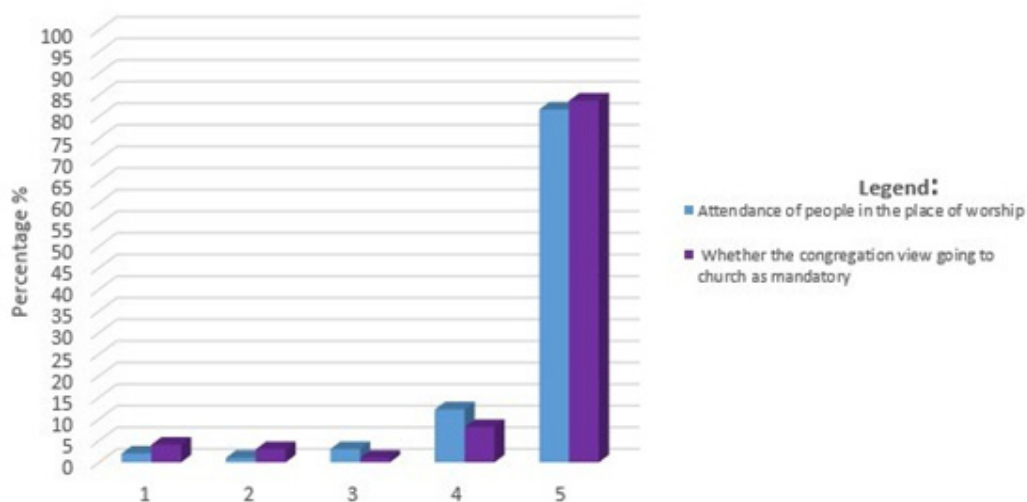
Fuente: Autor (2019).

El Gráfico 8 reveló que el 61.22% de los encuestados fueron bien golpeados por YahooYahoo, mientras que el 12.24% fueron moderadamente golpeados. La alta respuesta observada aquí puede ser el resultado del esquema GSM o de una reunión con el "viajero angustiado". El fenómeno del "viajero angustiado" es un tipo de estafa en Nigeria donde un criminal, bien vestido y de aspecto respetable, pinta un escenario de estar atascado y sin dinero para la tarifa del autobús y pide ayuda para llegar a su destino, cuando en realidad, es solo un estafador que emplea tácticas para engañar a la gente por su dinero.

4.1.9 Conocimiento Sobre el Culto Religioso

El investigador preguntó acerca de la asistencia de la congregación a los lugares de culto y si veían su asistencia como obligatoria. Las respuestas se muestran en el Gráfico 9:

Gráfico 9 – Gráficos con Resultados sobre el Culto Religioso



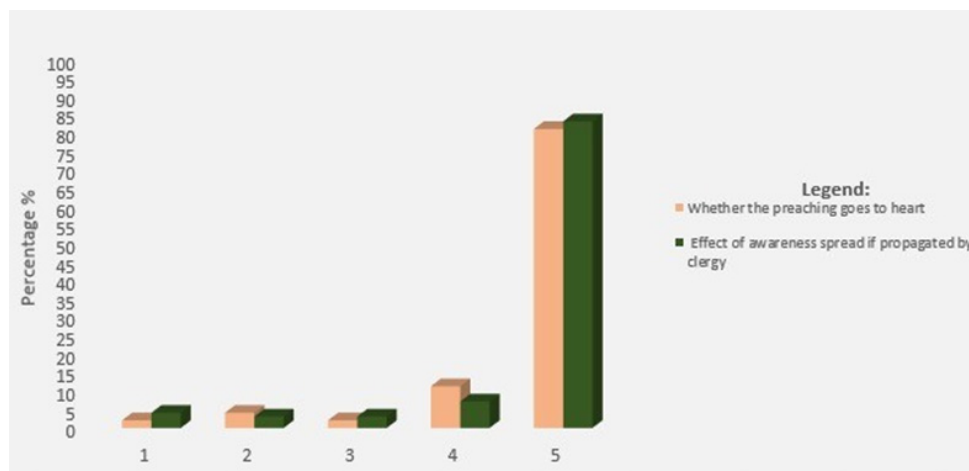
Fuente: Autor (2019).

De la Gráfico 9 anterior, se puede ver que el 81,63% de los encuestados cree que la población asiste muy bien a los diversos cultos. Del mismo modo, el 83,61% de los encuestados cree que la congregación ve que ir al culto es obligatorio para ellos. Por lo tanto, esto está correlacionado con la revelación de Ajah (2019) de que la mayoría de las personas que pertenecen a una religión u otra en Nigeria perciben la espiritualidad como parte de la religión. O resultado obtenido también correlacionou-se com uma pesquisa da BBC 2010, que revelou que 87% dos nigerianos disseram que a religião era muito importante para suas vidas. Otro informe de la BBC de 2014 también reveló cómo las reuniones de las mega-iglesias de Nigeria atraen a los estadios de fútbol.

4.1.10 Influencia de la Palabra del Clero en la Congregación

El investigador cuestionó la visión de los encuestados de cómo su predicación es llevada al corazón por su congregación y el efecto resultante. Los resultados se muestran en el Gráfico 10 a continuación.

Figura 10 – Gráfico con el Resultado de la Influencia de la Palabra del Clero en la Congregación



Fuente: Autor (2019).

Del Gráfico 10 anterior, se puede ver que el 80.61% de los encuestados cree que la congregación es totalmente sumisa a su predicación. Además, la encuesta reveló que el 82,65% de los encuestados también opina que la difusión de la conciencia de ciberseguridad será amplia si utilizan su púlpito para propagarla. Los dos resultados obtenidos en esta encuesta van en conjunto con la encuesta de la BBC 2010, según lo revelado por Nwaubani (CARTA..., 2014) que la mayoría de las personas en Nigeria están profundamente comprometidas con las prácticas y los principios tanto del Cristianismo como del Islam. El resultado obtenido de la investigación también puede haber enfatizado la posición de Nwaubani de que los libros publicados por los clérigos son campeones de ventas en una sociedad que a menudo se acusa de tener una cultura de lectura pobre. El informe reveló además que las instrucciones en los mensajes de texto de clérigos de renombre generalmente se toman en serio en Nigeria, y la mayoría de las veces se vuelven virales.

4.1.11 Efecto de la Campaña de Sensibilización sobre Ciberseguridad en la mitigación de la Cibercriminalidad

El investigador preguntó a los encuestados si creen que las actividades de los delincuentes cibernéticos podrían reducirse drásticamente si hay una gran conciencia sobre la seguridad cibernética y la criminalidad. Los resultados se muestran en el Gráfico 11 a continuación.

Gráfico 11 – Gráfico del Efecto de la Campaña de Sensibilización sobre Ciberseguridad en la mitigación de la Cibercriminalidad



Fuente: Autor (2019).

El Gráfico 11 muestra que el 68,37% de los encuestados son optimistas de que una mayor conciencia de la ciberseguridad podría ayudar a reducir las actividades de los ciberdelincuentes. Esta revelación es apoyada por el 10,20% que también cree que la campaña de sensibilización podría tener un efecto preventivo sobre las actividades de los delincuentes cibernéticos. El resultado obtenido aquí es similar a la revelación de Johnson y Bowers (2003) de que la publicidad puede mejorar enormemente la efectividad de la reducción del crimen. El investigador añadió que una campaña de sensibilización cuidadosamente organizada podía representar un instrumento poderoso y eficaz en función de los costos para la prevención del delito.

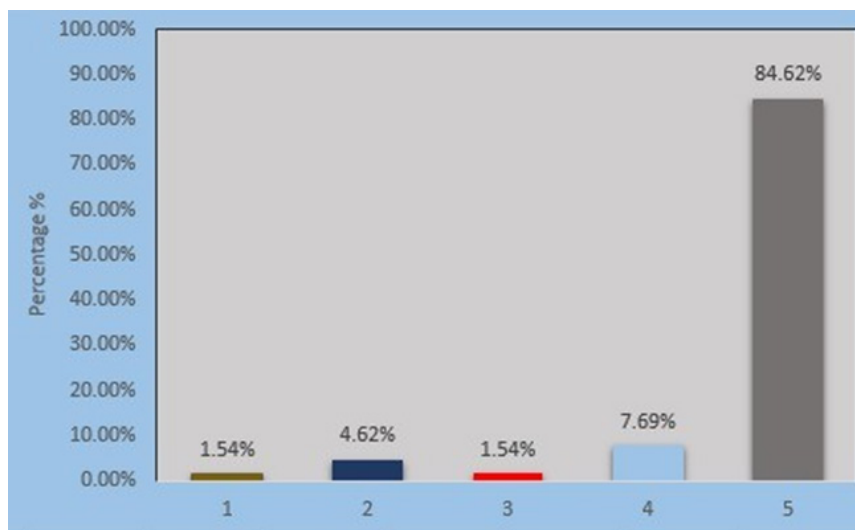
4.2 Análisis de datos obtenidos de profesionales de ciberseguridad

En esta sección se analizan los datos obtenidos de los encuestados que se asignan en áreas relacionadas con la ciberseguridad dentro de las diversas agencias gubernamentales. Estos organismos incluyen ONSA, NITDA, EFCC, DSA y Comando Espacial del Ejército. Los encuestados de organizaciones privadas no fueron considerados porque siempre organizan campañas de sensibilización sobre ciberseguridad en colaboración con agencias gubernamentales. Los datos no se analizaron en términos de los obtenidos de cada agencia individual, sino como datos de agencias profesionales. El cuestionario tenía 16 preguntas en total y cada pregunta tenía una calificación de 1 a 5, siendo 1 la más débil y 5 la más fuerte.

4.2.1 Realización de la Campaña de Sensibilización sobre Ciberseguridad

El investigador preguntó a los encuestados si alguna vez han participado en la realización de campañas de sensibilización cibernética y el resultado de la encuesta se muestra en el gráfico 12 a continuación:

Gráfico 12 – Gráfico de Resultados sobre la Realización de Campañas de Sensibilización en Ciberseguridad



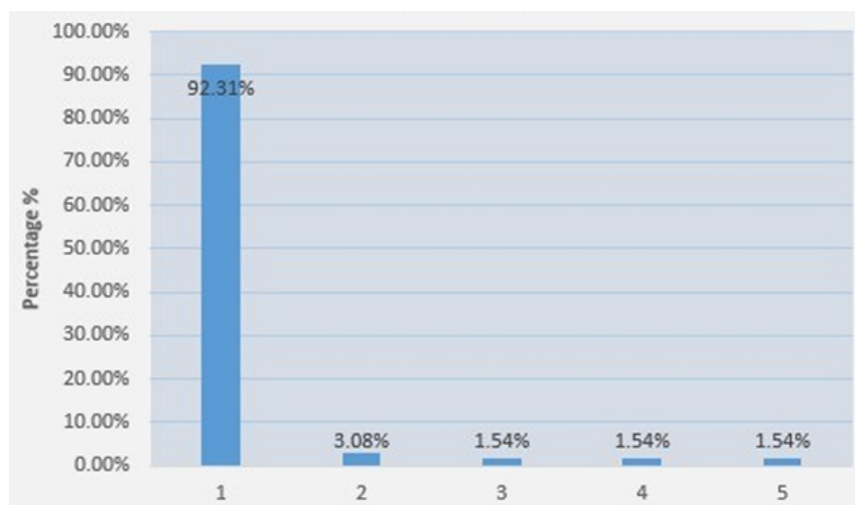
Fuente: Autor (2019).

En el gráfico 12, se puede ver que el 84,62% de los encuestados informaron haber participado en gran medida en campañas de sensibilización sobre ciberseguridad. El fuerte contraste entre las personas que afirman haber participado en gran medida en campañas de sensibilización y el 7,69% de los encuestados que afirman haber participado ya reveló que casi todo el personal de la agencia estaba, de una manera u otra, involucrado en campañas de sensibilización sobre ciberseguridad. Este hallazgo coincidió con el descubrimiento de la Revisión de gcsc (2018) sobre la madurez de la capacidad de ciberseguridad en Nigeria, que reveló que las iniciativas nacionales para la Conciencia de Ciberseguridad efectivamente ocurren en Nigeria. El informe destacó además que octubre de 2018 fue NCSAM representando un esfuerzo adicional de actividades de concientización que se llevan a cabo en la nación. La revisión también destacó la participación de organizaciones como CSEAN, (E-PPAN) en la conciencia pública, mientras que varias universidades nigerianas ofrecen cursos de ciberseguridad junto con algunas investigaciones sobre ciberseguridad.

4.2.2 Realización de Campañas de Sensibilización sobre Ciberseguridad en Lugares de Culto

El investigador preguntó a los encuestados si alguna vez habían organizado alguna campaña de concientización sobre ciberseguridad en cualquier lugar de culto y el resultado de la encuesta se muestra en el Gráfico 13 a continuación.

Gráfico 13 – Gráfico de Resultados de Campañas de Sensibilización Sobre Ciberseguridad en Cualquier Lugar de Culto



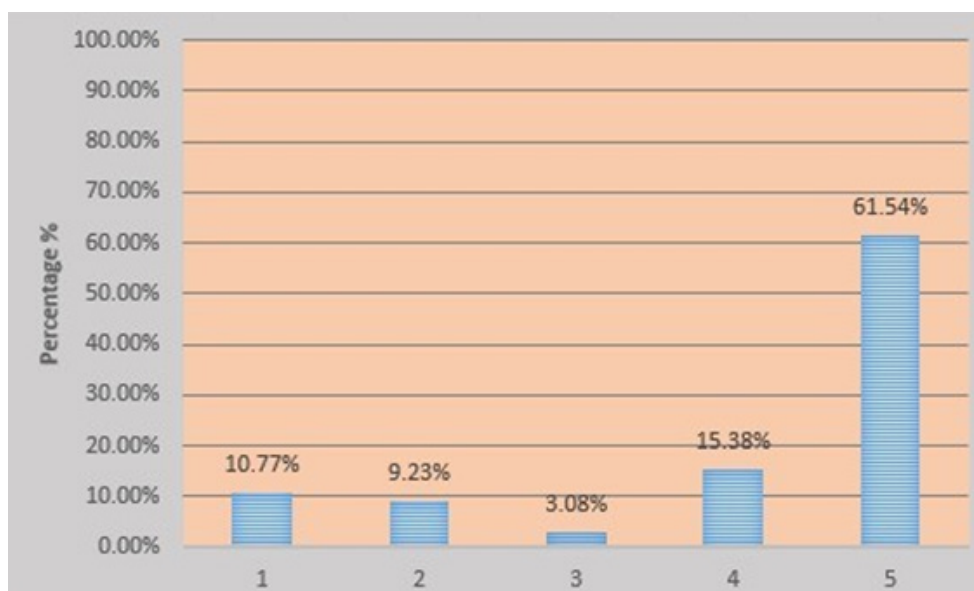
Fuente: Autor (2019).

El gráfico 13 reveló que el 92,31% de los encuestados estaban firmemente de acuerdo en que nunca habían organizado ninguna forma de campaña de sensibilización en ningún centro de culto religioso. El alto porcentaje obtenido de la investigación corrobora el informe del teniente coronel M. B. Fakandu, Subdirector, Protección de la Infraestructura de Información Crítica (CIIP), ONSA, al ser entrevistado por teléfono, afirmó que su oficina nunca había llevado a cabo ninguna campaña de ciberseguridad para una institución religiosa desde su nombramiento para el cargo. Agregó que un análisis del archivo oficial tampoco reveló ninguna evidencia de una actividad anterior de esta naturaleza. Además, el Señor Sa'adAbubakar, jefe de la Unidad de Ciberdelincuencia de la EFCC, hizo el mismo relato cuando fue entrevistado por teléfono. El dúo también declaró que no estaban al tanto de las campañas de concienciación sobre ciberseguridad organizadas por otras agencias de seguridad, ya que nunca se habían mencionado en el Consejo Asesor Nacional de Ciberseguridad ni en las reuniones rutinarias del Equipo de Respuesta a Emergencias Informáticas de Nigeria (ngCERT) (BASSIC-RESEARCH, 2019).

4.2.3 Influencia de la Religión en la Sociedad

Se preguntó a los encuestados sobre la influencia de la religión en la sociedad y sus respuestas se muestran en el gráfico 14 a continuación:

Gráfico 14 – Gráfico del Resultado sobre la Influencia de la Religión en la Sociedad



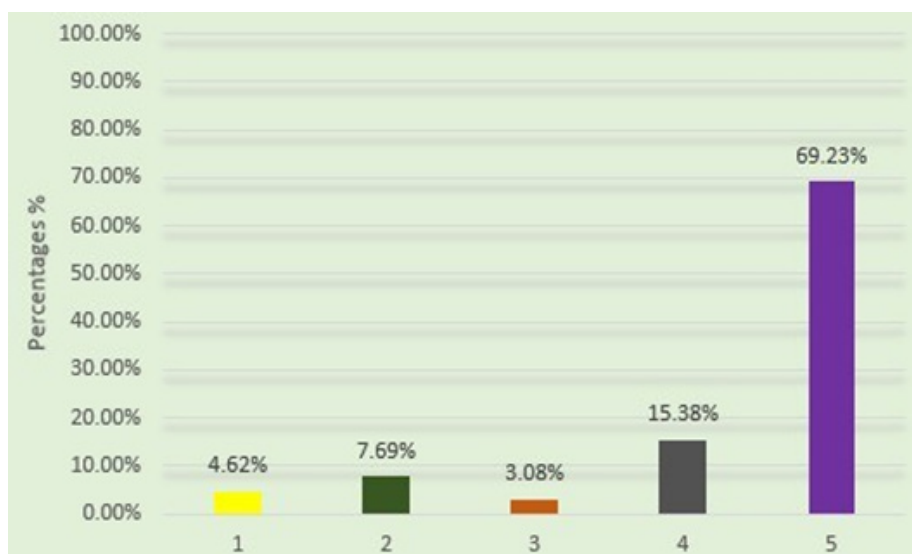
Fuente: Autor (2019).

El gráfico 14 reveló que el 61,54% de los encuestados cree que la religión tiene una enorme influencia en la sociedad de Nigeria. el 15,38% también cree que la religión tiene influencia en la población nigeriana. El resultado obtenido en esta investigación puede considerarse congruente con Ojonemi et al. (2014) que la religión en Nigeria y la fe son aspectos críticos de la vida cotidiana e influyen en las leyes, pensamientos y actitudes. Los investigadores afirmaron además que la religión desempeña un papel importante en la formulación de políticas y grandes proyectos públicos, debido a la importancia que se le atribuye.

4.2.4 Impacto de los líderes religiosos en la difusión de la Conciencia de Ciberseguridad

El investigador cuestionó sobre el impacto que los líderes religiosos pueden tener en la difusión de la conciencia de ciberseguridad y el resultado obtenido se muestra en el Gráfico 15 a continuación:

Gráfico15 – Gráfico con el Resultado sobre el Impacto de los Líderes Religiosos en la Difusión de la Conciencia de Ciberseguridad



Fuente: Autor (2019).

Del gráfico 15 resulta que el 69,23% de los encuestados cree que los líderes religiosos pueden tener un gran impacto en la difusión de la conciencia de ciberseguridad. El gráfico también reveló que el 15,38% de los encuestados cree que el clero puede tener un efecto en la difusión de la conciencia de ciberseguridad. La revelación puede considerarse cierta, teniendo en cuenta que el punto de vista religioso sobre la Planificación Familiar había inhibido el éxito de todas las intervenciones organizadas destinadas a aumentar la adopción de anticonceptivos en Nigeria, dejando al país con una de las tasas de prevalencia más bajas de anticonceptivos modernos (mCPRP) estimada en 9,8% (COMISIÓN NACIONAL de POBLACIÓN; ICF INTERNATIONAL, 2014). Sin embargo, sabiendo que los líderes religiosos en Nigeria pueden influir sustancialmente y dar forma a las ideas y opiniones de las personas sobre el tema, la Iniciativa de Salud Reproductiva Urbana de Nigeria (NURHI) decidió asociarse con líderes religiosos para promover la conciencia sobre el uso de anticonceptivos. Adedini et al. (2018), quienes documentaron la investigación, revelaron que la decisión del 66.4% de las mujeres que aceptaron la planificación familiar fue influenciada por las continuas declaraciones inspiradoras a favor de la planificación familiar en reuniones públicas y a través de los medios por parte del clero.

5 Resumen de las conclusiones

El condimento que faltaba en la educación cibernética en Nigeria: la perspectiva de la seguridad nacional Para ello, se realizaron dieciséis y cuatro preguntas de investigación para clérigos y profesionales de ciberseguridad, respectivamente, además de entrevistas, para el estudio. Los datos generados fueron presentados mediante gráficos para ilustrar las relaciones entre las variables del estudio. En consecuencia, los resúmenes de las conclusiones son:

- a. El clero tiene un amplio conocimiento de Internet y visita Internet con frecuencia.
- b. El clero no tiene conocimiento de ciberseguridad.
- c. El clero nunca ha organizado ninguna campaña de concienciación sobre ciberseguridad en su lugar de culto.
- d. El clero no tiene conocimiento de ciberseguridad.
- e. El clero es consciente de YahooYahoo y 419, pero no tienen idea de que es lo mismo que el crimen cibernético.
- f. El clero, en un momento u otro, se vio afectado por la ciberdelincuencia.
- g. El clero no conoce las medidas a tomar en caso de ciberataque.
- h. Un gran número de personas asisten a los servicios en diversos lugares de culto.
- i. Los mensajes desde el púlpito tienen una gran influencia en las masas nigerianas.
- j. La campaña de concienciación sobre la seguridad cibernética tendrá un gran efecto preventivo sobre la delincuencia cibernética.
- k. Los profesionales de la ciberseguridad han llevado a cabo muchas campañas de sensibilización sobre la ciberseguridad.
- l. Los profesionales de la ciberseguridad nunca han organizado ninguna campaña de sensibilización sobre la ciberseguridad en los lugares de culto.
- m. La religión tiene un enorme efecto en la sociedad nigeriana.
- n. La inclusión del clero en la campaña de concienciación sobre seguridad cibernética tendrá un gran efecto en la Educación Cibernética en la sociedad nigeriana.

De acuerdo con los resultados del estudio, se recomienda que la futura campaña de concienciación sobre ciberseguridad se organice con el clero con el fin de impulsar el máximo beneficio inherente a su influencia en la sociedad nigeriana.

6 Conclusión

Durante la última década, Internet ha experimentado un crecimiento explosivo en el número de usuarios conectados, aumentando diariamente a un ritmo exponencial. A medida que Internet se hace más accesible y más servicios se vuelven dependientes de ella para su operación diaria, también lo hace el horizonte de amenazas. Los Estados gradualmente llegan a un acuerdo con los peligros cibernéticos y establecen directrices, políticas e instituciones para hacerles frente. A pesar de esto, definitivamente se espera que el fraude en Internet aumente a medida que aumenta la presencia del comercio electrónico en Internet y el actual impulso del gobierno nigeriano para presionar su política de "sociedad sin efectivo". En vista de este hecho, el gobierno ha diseñado varios programas para aumentar la conciencia pública sobre los riesgos y amenazas de ciberseguridad, así como la forma de abordarlos, con el fin de servir como una verdadera herramienta para mitigar los peligros de la ciberdelincuencia y fortalecer la seguridad nacional. Sin embargo, es posible que el esfuerzo del gobierno no se haya sentido debido al hecho de que todas las campañas de sensibilización sobre ciberseguridad organizadas estaban dirigidas a instituciones de capacitación y oficiales, mientras que la población más grande del país está desempleada. En consecuencia, siendo la religión un agente fundamental y quizás uno de los factores más importantes que tienden a crear influencia en las vidas de la mayoría de los nigerianos, el uso del clero podría ser el mayor activo de los gobiernos en su campaña de concienciación sobre ciberseguridad.

Agradecimientos

Gloria a Allah SWT, cuya misericordia eterna me ha permitido llevar a cabo este proyecto. Me gustaría expresar mi profunda gratitud a mi ilustre supervisor, el Coronel Marcelo Gomes. Junto a mi supervisor, me gustaría extender mi más profunda gratitud a mi país por darme la oportunidad de ser parte de BASSIC 2019. También quiero agradecer a mi familia por su apoyo sin fin, a mis instructores por su orientación y a sus colegas por su gran ayuda.

Referencias

ADEDINI, S. A. et al. Role of religious leaders in promoting contraceptive use in Nigeria: Evidence from the Nigerian Urban reproductive health initiative. **Global Health Science and Practice**, [Baltimore], v. 6, n. 3, p. 500-514, 2018.

AJA, V. T. The relevance of patients' spiritual care in the Nigerian cultural context: a health care chaplain's perspective. **The Journal of Pastoral Care & Counseling: JPCC**, [Thousand Oaks], v. 73, n. 2, p. 82-87, 2019.

AJZEN, I. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. **Journal of Applied Social Psychology**, [S. l.], v. 32, n. 4, p. 665-683, Apr 2002.

AKIYODE-LAWANSON, J. Cybercrime: Nigeria ranks 3rd most attacked country in Africa. **BusinessDay**, Lagos, Nigeria, Mar 9, 2019. Disponible en: <https://businessday.ng/technology/article/cybercrime-nigeria-ranks-3rd-most-attacked-country-in-africa/>. Accesado el: Set. 21, 2019.

ARANSIOLA, J. O.; ASINDEMADE, S. O. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. **Cyberpsychology, Behavior, and Social Networking**, [New Rochelle, NY], v. 14, n. 12, p. 759-763, Dec 2011.

BAIDEN, J. **John Baiden, BSc., MBA., M.Sc., (distinction) JD, LL.M (distinction) 1.** [s. d.]. p. 1-14.

BASSIC-RESEARCH. **BrazilWarCollege - Google Drive**. [S. l.: s. n.], 2019. Disponible en: <https://drive.google.com/drive/folders/1LdXeL5f7iCNwCE2xXC9AeEc1HU4PREdR>. Accesado el: Set. 21, 2019.

BLOOMFIELD, C.; BOMMARITO, R. K.; KUHL, M. **Supporting military families through research and outreach public awareness campaigns**. In: SEMANTIC SCHOLAR. [S. l.]: Allen Institute for AI, July 2015. Disponible en: <https://pdfs.semanticscholar.org/7432/6da820ae48d452f08754e8b7d3cef0de969d.pdf>. Accesado el: Junio 6, 2020.

CENTRAL BANK OF NIGERIA. **Cash-less Nigeria**. Abuja: Central Bank of Nigeria, 2019. Disponible en: [https://www.cbn.gov.ng/cashless/#targetText=The Central Bank of Nigeria,N3%2C000%2C000 for Corporate bodies](https://www.cbn.gov.ng/cashless/#targetText=The%20Central%20Bank%20of%20Nigeria,N3%2C000%2C000%20for%20Corporate%20bodies). Accesado el: Set. 21, 2019.

CENTRE FOR CYBERSPACE STUDIES. **Keffi, Nigeria: CCS-NUSUK**, 2019. Disponible en: <https://www.ccs-nsuk.net/>. Accesado el: Set. 21, 2019.

CYBER SECURITY EXPERTS ASSOCIATION OF NIGERIA. **Lagos, Nigeria: CSEAN**, 2019. Disponible en: <https://csean.org.ng/>. Accesado el: Set. 21, 2019.

DAHIR, A. L. Cybercrime is costing Africa's business billions. **QuartzAfrica**, [S. l.], Junio 2018. Disponible en: <https://qz.com/africa/1303532/cybercrime-costs-businesses-in-kenya-south-africa-nigeria-billions/>. Accesado el: Set. 21, 2019.

DIGITAL PEERS INTERNATIONAL. **Programs**. Abuja, Nigeria: Digital Peers International, 2019. Disponible en: <http://www.digitalpeers.org/programs.html>. Accesado el: Set. 21, 2019.

FARIVAR, M. How dozens of nigerian scammers stole millions from people, businesses. **Voice of America**, [S. l.], Aug 24, 2019. Disponible en: <https://www.voanews.com/usa/how-dozens-nigerian-scammers-stole-millions-people-businesses>. Accesado el: Set. 21, 2019.

HARE, F. The cyber threat to national security: why can't we agree?. In: CZOSSECK, C.; PODINS, K. (ed.). **Conference on cyber conflict: proceedings 2010**. Tallinn, Estonia: CCD COE Publications, 2010. Disponible en: https://ccdcoe.org/uploads/2018/10/1_Proceedings2010FullBook.pdf. Accesado el: Junio 10, 2020.

HILTS, S. A perspective on cyber security from the Canadian nuclear private sector. In: LEUPRECHT, C.; MACLELLAN, S. **Governing cyber security in Canada, Australia and the United States: special report**. Ontario, Canada: Centre for International Governance Innovation, 2018. p. 19-21. Disponible en: <https://www.cigionline.org/sites/default/files/documents/SERENE-RISCweb.pdf>. Accesado el: Set. 21, 2019.

INTERNATIONAL CENTRE FOR LEADERSHIP DEVELOPMENT NIGERIA. **Cyber Security Awareness Month in Nigeria**. Abuja: ICLDNG, 2018. Disponible en: <https://icldng.org/cyber-security-awareness-month-ng/>. Accesado el: Set. 21, 2019.

INTERNET WORLD STATES. **Africa Internet Users, 2019 Population and Facebook Statistics**. [MadiPradexe]: Miniwatts Marketing Group, 2019. Disponible en: <https://www.internetworldstats.com/stats1.htm>. Accesado el: Set. 21, 2019.

JOHNSON, S. D; BOWERS, K. J. Opportunity is in the eye of the beholder: the role of publicity in crime prevention. **Criminology Public Policy**, [S. l.], v. 2, n. 3, p. 497-524, July 2003.

KOCH, R.; GOLLING, M. **The cyber decade: cyber defence at a X-ing point**. In: MINÁRIK, T.; JAKSCHIS, R.; LINDSTRÖM, L. (ed.) **10th International Conference on Cyber Conflict: CyCon X: maximizing effects**. Tallinn, Estonia: NATO CCD COE Publications, 2018. p. 159-185, 2018. Disponible en: https://ccdcoe.org/uploads/2018/10/CyCon_2018_Full_Book.pdf. Accesado el: Junio 10, 2020.

LAWANI, L. O.; IYOKE, C. A.; EZEONU, P. O. Contraceptive practice after surgical repair of obstetric fistula in southeast Nigeria. **International Journal of Gynecology and Obstetrics**, [Malden, MA], v. 129, n. 3, p. 256-259, Feb 2015.

LETTER from Africa: the power of religion. **BBC News**, [London], Nov 7, 2014. Disponible en: <https://www.bbc.com/news/world-africa-29692580>. Accesado el: Set. 21, 2019.

LEWIS, J. **Economic impact of cybercrime – no slowing down**. Washington: Center for Strategic and International Studies (CSIS), Feb 2018. Report. Disponible en: https://assets.website-files.com/5bd672d1924b9893a632c807/5c171d5e85ed62697a79e351_economic-impact-cybercrime.pdf. Accesado el: Junio 10, 2020.

NATIONAL POPULATION COMMISSION; ICF INTERNATIONAL. **Nigeria demographic and health survey 2013**. Abuja: NPC; Rockville, Maryland: ICF International, 2014. Disponible en: <https://dhsprogram.com/pubs/pdf/FR293/FR293.pdf>. Accesado el: Junio 10, 2020.

NIGERIAN COMMUNICATIONS COMMISSION. **Industry Statistics**. Abuja: NCC, 2019. Disponible en: <https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#view-graphs-tables-6>. Accesado el: Set. 21, 2019.

NIGERIAN DEFENSE ACADEMY. **Intelligence and cyber security**: academic branch. Kaduna: NDA [201-]. Disponible en: <https://academics.nda.edu.ng/faculties/military-science-and-interdisciplinary-studies/intelligence-and-cyber-security/>. Accesado el: Set. 21, 2019.

OJONEMI, S. et al. Deficit in religious practice in Nigeria: implications for national development. **Developing Country Studies**, [S. l.], v. 4, n. 4, p. 184-194, 2014. Disponible en: <https://core.ac.uk/download/pdf/234681546.pdf>. Accesado el: Junio 10, 2021.

OMODUNBI, B. et al. Cybercrimes in Nigeria: analysis, detection and prevention. **FUOYE: Journal of Engineering and Technology**, [Oye Ekiti], v. 1, n. 1, 2016. Disponible en: <https://engineering.fuoye.edu.ng/journal/index.php/engineer/article/view/16>. Accesado el: Junio 10, 2020.

OSHO, O.; ONOJA, A. D. National cyber security policy and strategy of Nigeria: a qualitative analysis. **International Journal of Cyber Criminology**, [Gujarat], v. 9, n. 1, p. 120-143, Aug 2015. Disponible en: <https://www.cybercrimejournal.com/Osho&Onoja2015vol9issue1.pdf>. Accesado el: Junio 10, 2021.

PINTER, B. et al. Religion and family planning. **European Journal of Contraception and Reproductive Health Care**, [London], v. 21, n. 6, p. 486-495, Dec 2016.

SERIANU. **Africa cybersecurity report 2016**. Kenya: Serianu, 2016. Disponible en: <http://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf>. Accesado el: Junio 10, 2021.

SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY. **Minna, Niger State**: Federal University of Tecnology, c2016. Disponible en: <https://sict.futminna.edu.ng/>. Accesado el: Set. 21, 2019.

SIOBHAN, G. Fraud ring funnels data from cards to Pakistan. **The Wall Street Journal**, New York, Oct 11, 2018. Disponible en: <https://www.wsj.com/articles/SB12236699999723871>. Accesado el: Set., 20, 2019.

TADE, O.; ALIYU, I. Social Organization of Internet Fraud among University Undergraduates in Nigeria. **International Journal of Cyber Criminology**, [Gujarat], v. 5, n. 2, p. 860, 2011. Disponible en: <https://www.cybercrimejournal.com/tadealiyui2011julyijcc.pdf>. Accesado el: Junio 10, 2020

TECH-U. Faculty of natural and applied sciences. Ibadan, Oyo State: **First Technical University**, [201-]. Disponible en: <https://tech-u.edu.ng/faculty-of-natural-and-applied-sciences/#>. Accesado el: Set. 21, 2019.

TIEMO, P. A.; NELLY, D. B. Efforts in combating cyber crime and criminality in Nigeria. **Information and Knowledge Management**, [S.l.], v. 6, n. 3, p. 23-28, 2016. Disponible en: <https://www.iiste.org/Journals/index.php/IKM/article/view/29271/30060>. Accesado el: Junio 10, 2020.

TIIRMAA-KLAAR, H. Building national cyber resilience and protecting critical information infrastructure. **Journal of Cyber Policy**, [London], v. 1, n. 1, p. 94-106, 2016.

UNIVESITY OF CALIFORNIA. Institute for Digital Research & Education Statistical Consulting. SPSS. Frequently asked questions. **What does Cronbach's alpha mean?**. Los Angeles: UCLA, [201-]. Disponible en: <https://stats.oarc.ucla.edu/spss/faq/what-does-cronbachs-alpha-mean/>. Accesado el: Set. 21, 2019.

VERMUELEN, J. Anonymous hacks SA government database. **MyBroadband**, Olifantsfontein, South Africa, Feb 12, 2016. Disponible en: <https://mybroadband.co.za/news/security/155030-anonymous-hacks-sa-government-database.html>. Accesado el: Set. 21, 2019.

WHAT is Yamane sample calculation?. In: QUORA. [S. l.: s. n., 2017?]. Disponible en: <https://www.quora.com/What-is-Yamane-sample-calculation>. Accesado el: Set. 21, 2019.