Conciencia Digital

ISSN: **2600-5859**
Vol. 5 No. 1, pp. 238 – 246 , enero – marzo 2022

www.concienciadigital.org

Ciberseguridad influencia en el turismo cubano

Cybersecurity influence on Cuban tourism

[1] Brena Esther Córdova Godoy
Universidad de La Habana, Facultad de Turismo, Licenciatura en Turismo. La Habana, Cuba,
brenaecord@gmail.com
[2] Jeyla Camila Barrera Montané
Universidad de La Habana, Facultad de Turismo, Licenciatura en Turismo. La Habana, Cuba,
jeylacamilabarreramontane@gmail.com
[3] Edgar Nuñez Torres
Universidad de La Habana, Facultad de Turismo, Licenciatura en Turismo. La Habana, Cuba,
enunez8609@gmail.com
[4] Luis Efrain Velastegui Lopez https://orcid.org/0000-0002-7353-5853
Universidad Técnica de Babahoyo, Babahoyo, Ecuador,
evelasteguil@utb.edu.ec

Artículo de Investigación Científica y Tecnológica
Enviado: 17/12/2021
Revisado: 30/12/2021
Aceptado: 06/01/2022
Publicado:26/02/2022
DOI: **https://doi.org/10.33262/concienciadigital.v5i1.2080**

Cítese: Córdova Godoy, B. E., Barrera Montané, J. C., Nuñez Torres , E., & Velastegui Lopez, L. E. (2022). Ciberseguridad influencia en el turismo cubano. ConcienciaDigital, 5(1), 238-245. https://doi.org/10.33262/concienciadigital.v5i1.2080

CONCIENCIA DIGITAL, es una Revista Multidisciplinar, **Trimestral,** que se publicará en soporte electrónico tiene como **misión** contribuir a la formación de profesionales competentes con visión humanística y crítica que sean capaces de exponer sus resultados investigativos y científicos en la misma medida que se promueva mediante su intervención cambios positivos en la sociedad. https://concienciadigital.org
La revista es editada por la Editorial Ciencia Digital (Editorial de prestigio registrada en la Cámara Ecuatoriana de Libro con No de Afiliación 663) www.celibro.org.ec

Conciencia Digital

ISSN: **2600-5859**
Vol. 5 No. 1, pp. 238 – 246 , enero – marzo 2022

www.concienciadigital.org

Palabras claves:
ciberseguridad, cuba, turismo, ciberataques.

A lo largo de la historia, Cuba ha sido víctima constantemente de todo tipo de atentados en contra de la seguridad nacional. Entre ellos, es importante mencionar los ciberataques, los cuales han puesto en riesgo a innumerables entidades cubanas. Uno de los sectores más vulnerables en cuestión de ciberseguridad es el sector del turismo, esto es debido a que, dentro del mismo, la conectividad y los datos personales o confidenciales juegan un papel crucial en procesos como: reservas, compras, alojamientos, recopilación de información de clientes, etc. Por todo lo anterior, el presente trabajo tiene como objetivo principal el estudio de técnicas que permitan elevar los niveles de ciberseguridad en el sector turístico cubano a través del método de investigación lógico-deductivo. Como resultados se relacionan una serie de prácticas que contribuirán a que Cuba tenga un sistema de acción ante las ciber amenazas, basadas en la evaluación de riesgos, que permiten mitigar los ciberataques en las empresas del sector turístico.

Keywords:
typography: cybersecurity, Cuba, tourism, cyber-attack

Abstract

Throughout history, Cuba has constantly been the victim of all kinds of attacks against national security. Among them, it is important to mention cyberattacks, which have put countless Cuban entities at risk. One of the most vulnerable sectors in terms of cybersecurity is the tourism sector, this is because, within it, connectivity and personal or confidential data play a crucial role in processes such as: reservations, purchases, accommodation, collection of customer information. For all the above, the main objective of this work is the study of techniques that allow raising the levels of cybersecurity in the Cuban tourism sector through the logical-deductive research method. The results are a series of practices that will contribute to Cuba having a system of action against cyber threats, based on risk assessment, which allow mitigating cyberattacks in companies in the tourism sector.

Introducción

El avance en el desarrollo de las Tecnologías de la Información y la Comunicación (TIC) y su influencia en prácticamente todas las esferas de la vida económica, política y social, propició la aparición de comportamientos ilícitos, dirigidos contra las redes y sistemas informáticos, como pudieran ser ataques a servidores, desfiguración de sitios web,

denegación de servicios, introducción de códigos maliciosos y envío masivo de correo no deseado (spam), por citar algunos ejemplos, y aquellos que utilizan las redes y sistemas como medio para cometer ilegalidades, tales como el fraude, robo, espionaje, pornografía infantil, entre otros. Por tanto, uno de los temas que más debate y polémica suscita a nivel internacional es la ciberseguridad; más aún en el contexto actual, ya que según Kaspersky empresa líder en ciberseguridad, durante la pandemia el número de ciberataques incrementaron en un 25% (Antón, 2021).

El pueblo cubano, históricamente, ha sido blanco de todo tipo de atentados contra la seguridad nacional. Los ciberataques forman parte de esta amenaza constante y se puede considerar que el sector turístico es uno de los más vulnerables en este sentido. Esto es debido a que dentro del mismo la conectividad y los datos personales o confidenciales juegan un papel crucial en procesos como: reservas, compras, alojamientos, recopilación de información de clientes, etc. y no se debe olvidar que a mayor conectividad mayor exposición, por lo tanto, mayor grado de peligrosidad y riesgo de recibir un ataque (Deloitte, 2017).

Según Miguel Gutiérrez Rodríguez, director general de informática del Ministerio de Comunicaciones de Cuba, en su entrevista "Hablando de ciberseguridad en Cuba" consultada en Pérez (2019), la falta de una cultura de ciberseguridad en directivos, especialistas y la población en general; insuficiente percepción de riesgos; la tendencia a rechazar cambios; la inexistencia de un repositorio de aplicaciones nacionales en software libre que cubra las necesidades existentes; la obsolescencia tecnológica, la diversidad de dispositivos (impresoras, lectores de código de barra, escáner) de una parte de los medios de cómputo del país, son algunos de los problemas que facilitan los ciberataques en el sistema empresarial cubano.

Por tanto, es indispensable proteger el ciberespacio nacional y preservar la soberanía sobre su utilización; organizar la seguridad de las TIC y los servicios y aplicaciones que soportan y establecer la seguridad de las infraestructuras críticas, con la finalidad de contar con una estrategia de fortalecimiento y sostenibilidad. El objetivo general de la investigación fue estudiar técnicas que permitan elevar los niveles de ciberseguridad en el sector turístico cubano (Pérez & Gardey, 2017).

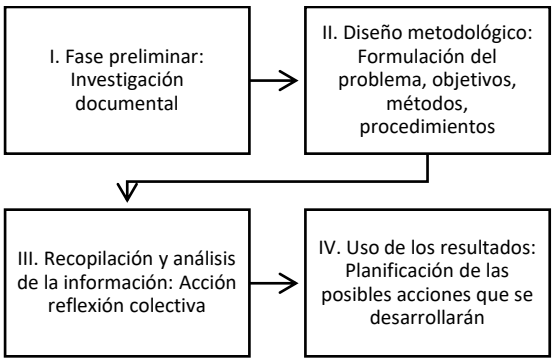
Metodología

Para la realización de la investigación se ejecutaron seis fases como se muestra en la figura 1, la primera fase se realiza una investigación documental sobre el tema de ciberseguridad, en la fase 2 se plantea el diseño metodológico de la investigación, después en la fase tres se recopila toda la información para así en la fase cuatro planificar las posibles acciones que se desarrollarán.

Conciencia Digital
ISSN: **2600-5859**
Vol. 5 No. 1, pp. 238 – 246 , enero – marzo 2022
www.concienciadigital.org

Figura 1

Fases de la investigación



Métodos utilizados

Tras la razón de que un método de investigación científica es una receta efectiva ante cualquier problema, el equipo de autores consideró necesario para llevar a cabo el proyecto, la utilización de métodos de investigación científica de tipo teórico y empíricos.

Análisis-síntesis cuyo empleo permitió el estudio de los diferentes ciberataques y conocer en qué medida influyen en el nivel de manejo de la información, así como las relaciones que entre ellos se establecen, manifestando los efectos de cada uno sobre el sector turístico.

Inducción-deducción que permitió la exploración de elementos que denotan cierta particularidad y su posterior análisis en un campo más general permitieron la identificación de puntos comunes en los fenómenos y variables utilizados en el desarrollo de la investigación.

Hipotético-deductivo: Fue de gran utilización debido a que esta investigación partió de una hipótesis sustentada en el conocimiento previo de las constantes amenazas de Estados Unidos hacia Cuba, que, siguiendo reglas lógicas de la deducción, permitió llegar a nuevas conclusiones y predicciones empíricas, verificando la validez de dicha hipótesis.

Histórico-lógico: Se empleó para profundizar en los criterios de diferentes autores acerca del proceso evolutivo de las TIC y las relaciones entre Estados Unidos y Cuba.

Revisión bibliográfica de varios volúmenes, por ejemplo, referentes a la ciberseguridad en el sector turístico, lo que permitió arribar a resultados y conclusiones sobre las características de la relación que se establece entre estos en Cuba.

Resultados

Pese a que estos ataques crecen exponencialmente, muchos de estos riesgos pueden ser evitados, o al menos controlados, si aplicamos las siguientes medidas de seguridad:

Cada entidad del sector que haga uso de las TIC debe diseñar, implantar, gestionar y mantener actualizado un sistema de seguridad en correspondencia con los elementos a proteger y los riesgos a los que estos se exponen. El diseño del plan de seguridad de las TIC debe ser resiliente, garantizar integridad, confidencialidad, métodos de vigilancia, detección y notificación de incidentes. Además, debe tomar como base la metodología establecida por el Ministerio de Comunicaciones en la Resolución No. 129/2019, como parte de las normas jurídicas recientemente puestas en vigor (Suárez, 2020).

Proceso de capacitación del personal sobre el desarrollo, implantación, administración, despliegue del soporte técnico y utilización de aplicaciones seguras, ya utilizadas en varias entidades, como el sistema operativo NOVA, el paquete ofimático OpenOffice, Navegador Firefox y cliente de correo *Thunderbird*, o sus similares, entre otros. Así como la formación de estos para que tomen conciencia de los riesgos y amenazas presentes en Internet y sepan detectarlos o mitigarlos si fuese necesario. Los empleados deben convertirse en la primera línea de defensa frente a un ciberataque (Jiménez, 2021).

Establecer un control de uso de herramientas corporativas. Es decir, determinar y controlar qué software estará autorizado para el tratamiento de la información dentro de la empresa; así como controlar los accesos desde el exterior por parte del personal ajeno a la organización.

Contar con una política de seguridad en la que se defina y clasifique la información, dejando claro quién y en qué condiciones accederá. Impidiendo fugas de información y acceso de personal no autorizado a información personal o confidencial (Arevich, 2021).

Reunir la información necesaria y limitar su acceso a terceros (*partners*, agencias de marketing, etc.).

Estar al día en cuanto a actualizaciones y parches de seguridad para evitar ser víctimas de ataques a través de vulnerabilidades. Esto se debe a que todo software es susceptible de mejorar, ya sea por motivos de seguridad o por añadir nuevas funcionalidades. Esto incluye al firmware de los equipos electrónicos, sistemas operativos y aplicaciones informáticas, incluidos los productos antimalware (IBERDROLA S.A., 2020).

Exigir medidas de seguridad a proveedores de servicios. Por ejemplo, exigir seguridad de aplicaciones desarrolladas por terceros y confidencialidad en la contratación de servicios.

Realizar copias de seguridad periódicas, asegurándose que albergan toda la información relevante para evitar su perdida ante ciberataques o fallos de los sistemas de almacenamiento. De igual forma, es necesario tener conocimiento de cómo recuperar los datos en caso necesario.

Monitorizar continuamente la huella digital en Internet para poder detectar estafas, fugas de información y vulnerabilidades que puedan afectar a la reputación del negocio o a sus clientes. Es habitual hoy en día los ataques que suplantan la identidad de establecimientos turísticos con la finalidad de engañar a clientes y hacerse con datos tan sensibles como cuentas bancarias, números de tarjetas de crédito, etc. (Universidad Internacional de Valencia, 2021), perjudicando gravemente tanto a dichos clientes como también al establecimiento turístico.

Uso de credenciales y cifrado para los datos, dispositivos y sistemas que contengan información sensible y confidencial. De tal manera que además de un nombre de usuario haya que introducir una contraseña lo más robusta posible (haciendo uso de minúsculas, mayúsculas, números y caracteres especiales), que deberá ser actualizada periódicamente y eliminada de forma segura cuando sea necesario. Las contraseñas deficientes o mal custodiadas pueden provocar accesos no autorizados a los datos y servicios de una organización (Red Global de Conocimientos en Auditoría y Control Interno, 2021).

Eliminación segura de la información. Una vez que la información llega a la última fase de su ciclo de vida, se vuelve necesaria una eliminación de forma segura para que ésta no vuelva a ser accesible, evitando así posibles difusiones accidentales o indeseadas.

Siguiendo este tipo de pautas básicas, es posible proteger la información que gestiona una entidad turística cubana, y de esta forma transmitir una imagen positiva, generando confianza tanto en clientes como proveedores. Proteger y gestionar correctamente la información en cualquier empresa debe ser una de las principales prioridades, ya que conforman la base del negocio del sector turístico.

Conclusiones

- Cuba tiene un sistema de acción ante los ciberataques bastante desarrollado. Siempre que se detecta un incidente de ciberseguridad, se inicia una acción coordinada en la que participan múltiples actores, incluyendo las entidades que son afectadas.
- Este sistema de acción no disminuye los peligros que enfrenta el sector turístico ante los ciberataques. Por lo cual, es necesario complementar el protocolo con una serie de medidas de seguridad, basadas en la evaluación de riesgos, que permiten mitigar los ciberataques en las empresas del sector turístico.

- Si las empresas mantienen buenas prácticas en cuanto a ciberseguridad, en conjunto con las autoridades nacionales competentes, es más sencillo proteger la confidencialidad, integridad y disponibilidad de estas. De esta forma se garantiza elevar los niveles de ciberseguridad en las empresas que tributan al sector turístico.
- Es de gran importancia que este tema se mantenga en constante estudio, puesto que la tecnología evoluciona cada minuto y con ello las formas de desarrollar su uso ilícito.

Referencias bibliográficas

Antón Rodríguez, S. (24 de julio de 2021). ¿Cuándo empezaron y qué pretenden los ciberataques contra Cuba? *Granma, pág. 8.*

Arevich Marín, M. (2021). *Gaceta Oficial de la República de Cuba*. Ministerio de Justicia.

Deloitte. (2017). *La ciberseguridad en el sector turístico*. Deloitte. https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/ciberseguridad-sector.turistico.html

IBERDROLA S.A. (2020). *Ciberataques: Qué son y qué tipos existen*. IBERDROLA S.A: https://www.iberdrola.com/innovacion/ciberataques

Jiménez, D. (2021). Herramientas de ciberseguridad que apuntan a ser tendencia en el 2022. Cointelegraph. https://es.cointelegraph.com/news/cybersegurity-tools-that-point-to-be-a-trend-in-2022

Pérez Porto, J., & Gardey, A. (2017). *Definición de Ciberespacio*. https://definicion.de/ciberspacio/

Pérez Salomón, O. (2019). Hablando de ciberseguridad en Cuba. Cubadebate.

Red Global de Conocimientos en Auditoría y Control Interno. (16 de diciembre de 2021). Los 10 hallazgos más comunes en una auditoría de ciberseguridad. AUDITOOL: https://www.auditool.org/blog/auditoria-de-ti/8241-los-10-hallazgos-mas-comunes-en-una-auditoria-de-ciberseguridad

Suárez Pérez, E. (1 de enero de 2020). Así comenzamos: Una aproximación. Presidencia y Gobierno de Cuba: httpps://www.presidencia.gob.cu/es/noticias/asi-comenzamos-una-aproximacion/

Conciencia Digital

ISSN: **2600-5859**
Vol. 5 No. 1, pp. 238 – 246 , enero – marzo 2022

www.concienciadigital.org

Universidad Internacional de Valencia. (10 de marzo de 2021). Ciber amenazas en 2021: ¿cómo identificarlas? Universidad Internacional de Valencia. https://www.universidadviu.com/pe/actualidad/nuestros-expertos/ciberamenazas-en-2021-como-identificarlas

El artículo que se publica es de exclusiva responsabilidad de los autores y no necesariamente reflejan el pensamiento de la **Revista Conciencia Digital.**

Indexaciones