ANÁLISIS DE LAS AMENAZAS Y RIESGOS CIBERNÉTICOS QUE AFRONTAN LOS USUARIOS Y LAS ORGANIZACIONES EN LA CONSULTA Y/O ADQUISICIÓN DE SERVICIOS TURÍSTICOS A TRAVÉS DE MEDIOS ELECTRÓNICOS

JULIÁN ERNESTO ALMARIO PEÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

IBAGUÉ

2022

ANÁLISIS DE LAS AMENAZAS Y RIESGOS CIBERNÉTICOS QUE AFRONTAN LOS USUARIOS Y LAS ORGANIZACIONES EN LA CONSULTA Y/O ADQUISICIÓN DE SERVICIOS TURÍSTICOS A TRAVÉS DE MEDIOS ELECTRÓNICOS

JULIÁN ERNESTO ALMARIO PEÑA

Proyecto de Grado – Monografía presentado para optar por el título de

ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director:

MIGUEL ANDRES AVILA GUALDRON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

IBAGUÉ

2022

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ibagué, 2022

DEDICATORIA

Con amor dedico este trabajo a mi hijo, que con su carisma y comprensión me acompañó en cada etapa vivida, colaborándome de manera indirecta, minimizando mis preocupaciones de padre, también lo dedico a mi mamá que con su apoyo, consagración y paciencia disminuyo mis tareas en el hogar permitiéndome una entrega más tranquila en el estudio y trabajo.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

pág.

GLOSARIO

CAI VIRTUAL: El Centro Atención Inmediata virtual es un servicio que ha dispuesto la Policía Nacional para la atención de delitos informáticos o de incidentes cibernéticos que afectan a los ciudadanos: Allí los ciudadanos víctimas de delitos que se realizan a través de la web, pueden poner en conocimiento de las autoridades de manera gratuita y las 24 horas el caso y podrán recibir orientación sobre qué tipo de medidas podrán tomar.[1]

CARDING: es una modalidad de fraude electrónico: "En la cual las personas detectan cargos no reconocidos en sus tarjetas de crédito o de débito. Los delincuentes acceden de forma ilegal, a través de un software de manera aleatoria, a la información de tarjetas de crédito o débito".[2] Una vez que obtienen la información realizan pagos con ellas, que en primera instancia pueden pasar desapercibidos, ya que no son montos muy poco significativos, esto ocurre hasta el momento en el que los tarjetahabientes perciben cargos que desconocen

CIBERDELINCUENCIA: es aquella actividad que por medio de la red (sea pública o privada) o a través de un sistema informático "tenga como objetivo atentar a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y los datos, así como el uso fraudulento de tales sistemas, redes y datos".[3]

CIBERSEGURIDAD: "Es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques

---

[1] CAI VIRTUAL. Conoce como funciona el CAI VIRTUAL de la Policía. [Sitio WEB]. Bogotá. 2020. (19 de octubre de 2020). Disponible en: https://bogota.gov.co/mi-ciudad/seguridad/conoce-como-funciona-el-cai-virtual-de-la-policia

[2] KUESKI STAFF. ¿Qué es el Carding y los Bineros?. [Sitio WEB]. Bogotá. 2020. (18 de mayo de 2020). Disponible en: https://kueski.com/blog/finanzas-personales/diccionario-finanzas/que-es-carding/

[3] SISTEMIUS. Ciberdelincuencia: Los 4 delitos informáticos más comunes. [Sitio WEB]. Santiago de Compostela (24 de abril de 2020). Disponible en Internet: https://www.sistemius.com/ciberdelincuencia-4-tipos-de-delitos-informaticos/

maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica” [4]

CONTRASEÑA: es una clave que permite acceder a un lugar, ya sea en el mundo real o en el virtual. “Las contraseñas se utilizan por varios motivos: para preservar la intimidad, para mantener un secreto, como una medida de seguridad o como una combinación de todo ello”[5]

COPIA DE SEGURIDAD: “también llamada respaldo o backup, se refiere a la copia de archivos físicos o virtuales o bases de datos a un sitio secundario para su preservación en caso de falla del equipo u otra catástrofe. El proceso de copia de seguridad de los datos es fundamental para un plan de recuperación de desastres (DRP) exitoso”[6]

DELITO CIBERNÉTICO: “Son todos aquellos que se cometen haciendo uso equipos informáticos, internet y en ocasiones, también software malicioso o malware del tipo troyano”[7]

DISPOSITIVO MÓVIL: se puede definir como: “Un aparato de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales”[8]

---

[4] KASPERSKY. ¿Qué es la Ciberseguridad? [Sitio WEB]. AO Kaspersky Lab. [2022]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[5] DEFINICION ABC. Definición de Contraseña. [Sitio WEB]. Definición ABC. [Diciembre de 2015]. Disponible en internet: https://www.definicionabc.com/tecnologia/contrasena.php

[6] ROUSE, M. Copia de Seguridad o Respaldo. [Sitio WEB]. ComputerWeekly. [2018]. Disponible en internet: https://www.computerweekly.com/es/definicion/Copia-de-seguridad-o-respaldo

[7] LEGADOO. El Delito Cibernético: [Sitio WEB]. Legadoo. [28 Diciembre de 2016].. . Disponible en: http://legadoo.com/legal/index.php/delitos/delitos-ciberneticos/delito-cibernetico-concepto-clasificaciones/

[8] DELGADILLO, P. Revista Iberoamericana de Producción Académica y Gestión Educativa. [en línea]. México: 2015. [Consultado 19, julio,2022]. Disponible en: https://www.pag.org.mx

RED: “Es la interconexión de un número determinado de computadores (o de redes, a su vez) mediante dispositivos alámbricos o inalámbricos que, mediante impulsos eléctricos, ondas electromagnéticas u otros medios físicos, les permiten enviar y recibir información en paquetes de datos, compartir sus recursos y actuar como un conjunto organizado”[9]

SEGURIDAD INFORMÁTICA: “Es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema”[10]

SERVIDOR: “Es un sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, conocidos como clientes, a través de una red. En teoría, se consideran servidores aquellos ordenadores que comparten recursos con máquinas cliente. La computación real se efectuaba en el servidor”[11]

SISTEMA ELECTRÓNICO: “Es un conjunto de circuitos que interactúan entre sí para obtener un resultado, Entradas o Inputs – Sensores (o transductores) electrónicos o mecánicos que toman las señales (en forma de temperatura, presión, etc.) del mundo físico y las convierten en señales de corriente o voltaje”[12]

SUPLANTACIÓN DE IDENTIDAD: “Es una actividad malintencionada que consiste en hacerse pasar por otra persona por diversos motivos: cometer algún tipo de fraude, obtener datos de manera ilegal, cometer ciberbullying o grooming (conseguir la confianza de un menor para poder abusar sexualmente de él). El ejemplo más

---

[9] Dirección General de Sistemas y Tecnologías de la Información. (s.f). *Redes.* Gobierno del Estado de México. https://normas-apa.org/referencias/citar-pagina-web/comment-page-1/

[10] SOLICIT. Seguridad Informática. [Sitio WEB]. Solicit S.R.L. [2022]. Disponible en: http://www.solicit.com.bo/en-us/Productos/Infraestructura-TI/Software/Seguridad-informatica

[11] PAESSLER. ¿Qué es un servidor? [Sitio WEB]. Paessler AG. [2022]. Disponible en: https://www.paessler.com/es/it-explained/server

[12] El Santuario de la Electrónica. Sistemas electrónicos. [Sitio WEB]. El Santuario de la Electrónica. [2011]. Disponible en: https://elsanturariodelaelectronica.webnode.es/sistemas-electronicos/

típico de suplantación es crear un perfil falso en las redes sociales para poder comunicarse con otras personas haciéndose pasar por ella”[13]

TURISMO: “Comprende las actividades que realizan las personas durante sus viajes y estancias en lugares distintos al de su entorno habitual, por un período de tiempo consecutivo inferior a un año, con fines de ocio, por negocios y por otros motivos turísticos, siempre y cuando no sea desarrollar una actividad remunerada en el lugar visitado”[14]

[13] ATICO 34. Suplantación de Identidad ¿Qué es? ¿Cómo Evitarlo? [Sitio WEB]. Madrid. Grupo Atico 34. [28 de febrero de 2020].. Disponible en: https://protecciondatos-lopd.com/empresas/suplantacion-de-identidad/

[14] INDEC. Turismo, concepto y definiciones.. Disponible en: https://www.indec.gob.ar/ftp/cuadros/economia/turismo_cyd.pdf

RESUMEN

En la presente monografía, se identifican algunos de los ataques más recurrentes que presentan las empresas de turismo, el modo en que los ciberdelincuentes acceden a la información confidencial y los efectos negativos que este tipo de situaciones puede traer para la productividad y credibilidad de los servicios prestados.

En ella, se expone un análisis sobre las amenazas y riesgos cibernéticos que afrontan los usuarios y las organizaciones en la consulta y/o adquisición de servicios turísticos a través de medios electrónicos, como aporte en la prevención de brechas de seguridad de la información. Por otra parte, se comparten algunas herramientas, técnicas y estrategias que permiten proporcionar mecanismos de seguridad de la información, recomendaciones y buenas prácticas cibernéticas para coadyuvar en la mitigación de incidentes cibernéticos.

Palabras Clave: ataque cibernético, ciberdelincuente, ciberseguridad, recomendaciones cibernéticas.

ABSTRACT

In this monograph, some of the most recurrent attacks presented by tourism companies are identified, the way in which cybercriminals access confidential information and the negative effects that this type of situation can bring to the productivity and credibility of the services provided.

In it, an analysis of the cybernetic threats and risks faced by users and organizations in the consultation and/or acquisition of tourist services through electronic means is presented, as a contribution to the prevention of information security breaches. On the other hand, some tools, techniques and strategies are shared that allow providing information security mechanisms, recommendations and good cyber practices to help mitigate cyber incidents.

Keywords: cyber attack, cyber criminal, cyber security, cyber recommendations.

INTRODUCCIÓN

La ciberseguridad se ha convertido en una de las practicas que más está siendo utilizada en las empresas para proteger y defender las redes, los procesos de comercio electrónico, computadores, dispositivos móviles y servidores de ataques cibernéticos. En la actualidad es un hecho que las empresas turísticas al igual que todas las organizaciones tienen que enfrentar a diario cientos de amenazas como el robo de información confidencial, la denegación de servicio, suplantación o engaño, entre otros, degradando la experiencia de los usuarios y desmejorando la calidad del servicio ofrecido.

Este documento se enfoca principalmente en las empresas de turismo, en las cuales la ciberdelincuencia ha centrado su atención para efectuar ataques que permitan el robo de información confidencial, como los datos financieros de los clientes, utilizando diferentes técnicas, tácticas y procedimientos en el desarrollo de sus delitos.

Adicional a lo anterior, se abordan antecedentes relacionados con la ciberseguridad, destacando el inicio de uno de los primeros hackers de la historia como Nevil Maskelyne, el cual “En 1903, interceptó la primera transmisión de telégrafo inalámbrico, mostrando las vulnerabilidades de este sistema desarrollado por Marconi”; al igual que, John Draper que fue denominado como “el primer ciberdelincuente”, mejor conocido como “Captain Crunch” quien descubrió que el sonido emitido por un silbato que se obsequiaba en las cajas de cereal de “Cap’n Crunch”, podía engañar a la señal de la central telefónica y así poder realizar llamadas gratis” [15]

Por otra parte, también se destacan antecedentes relacionados con ataques cibernéticos que afectaron profundamente la economía mundial, como, en el año 1.999 el denominado “Melisso” que fue el primer malware que se propagaba por correo electrónico y en el 2.000 el popular “I Love You” en el que las víctimas

[15] INFOSECURITY. Ciberseguridad. Una guía completa del concepto, tipos, amenazas y estrategias, [Sitio WEB]. México. Infosecurity México. [6 de octubre de 2022]. Disponible en Internet: https://www.infosecuritymexico.com/es/ciberseguridad.html

recibían en su bandeja de entrada una presunta carta de amor, pero en realidad, lo que estaban abriendo era un sofisticado virus que sobrescribía los archivos del ordenador. [16] También se resalta en el 2.004 el nombrado “Sasser y Netsky” que no necesitaba de los correos electrónicos para poder propagarse, si no que, era un tipo de gusano que rastreaba la red en busca de dispositivos conectados con vulnerabilidades conocidas.[17]

Estos ejemplos destacan un inicio de lo que hoy conocemos como ataques cibernéticos, los cuales, con el tiempo han aumentado su complejidad para sobrepasar las barreras de seguridad que se establecen y afectar no solo a las organizaciones, si no, a los consumidores finales de los servicios consultados y/o adquiridos a través de medios electrónicos, como es el caso del sector turístico.

Por tal razón, es importante realizar una contribución en el aumento y diversificación de conocimientos sobre cómo identificar y disminuir amenazas cibernéticas en las empresas de turismo, así como, en los usuarios, acerca de los tipos de ataques que se realizan con mayor frecuencia, sus repercusiones a nivel interno y externo, incluyendo amenazas y vulnerabilidades, para de esta forma, proponer recomendaciones que permitan minimizar la ocurrencia de incidentes cibernéticos.

[16] DATTA. 11 ataques Informáticos que cambiaron para siempre la ciberseguridad [Sitio WEB]. [28, noviembre, 2018]. Disponible en Internet: https://datta.com.ec/articulo/11-ataques-informaticos-que-cambiaron-para-siempre-la-ciberseguridad

[17] Ibid. 2 p.1

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En la historia de la ciberseguridad existen muchos eventos que fueron transformando el mundo digital, conocido actualmente como la principal herramienta para movilizar las economías de los países, es por esto que, su influencia en la productividad ha sido notoria, a pesar de ello, han surgido riesgos en el manejo de la información confidencial de las empresas. Los antecedentes de las vulnerabilidades cibernéticas son amplios y variados, sin embargo, vale la pena mencionar algunos que dieron inicio a la búsqueda de fallas en los sistemas, como lo fue en el año 1986 la creación de un virus que infectaba el sector de arranque, denominado “Brain”, siendo conocido como el primer virus creado para PC y con el cual, se inició la infección de los disquetes de 5.2: “Según el informe de Securelist, este virus se atribuye a los hermanos Basit y Amjad Farooq Alvi, que regentaban una tienda informática en Pakistán. Cansados de que los clientes realizaran copias ilegales de su software, desarrollaron Brain, que reemplazaba el sector de arranque de un disquete por un virus” [18]

El gusano creado por Robert Morris en el año 1988 ocasiono: “Que se infectaran casi todos los computadores conectados al internet de los cuales muchos permanecieron infectados durante casi 72 horas, descargo archivos inusuales en los directorios y los hizo funcionar más lento”[19]

Otro caso relevante, fue un pirata informático llamado: Jonathan James, el cual con tan solo 15 años infiltró repetidamente el Departamento de Defensa de Estados Unidos y la Administración Nacional de Aeronáutica y del Espacio (NASA) en 1999,

[18] KASPERSKY. (2021). Una breve historia de los virus informáticos y lo que nos depara el futuro. [Sitio WEB]. Kaspersky. [11 de mayo de 2021]. Disponible en: https://latam.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds

[19] WELIVESECURITY (2016). Martes de Retrospectiva: el gusano Morris. [Sitio WEB]. Welivesecurity. [1 de Agosto de 2022]. Disponible en: https://www.welivesecurity.com/la-es/2016/11/08/retrospectiva-gusano-morris/

extrayendo nombres de usuario y contraseñas de más de 3.000 correos electrónicos.[20]

Una de las epidemias más graves de esta nueva era fue LoveLetter, que apareció el 4 de mayo de 2000 y presentaba forma de archivo VBS: “La línea de asunto era "I Love You" (Te amo) y el correo electrónico contenía un archivo adjunto, "LOVE-LETTER-FOR-YOU-TXT.vbs". El creador de ILOVEYOU, Onel de Guzmán, diseñó este gusano para que sobrescribiera archivos existentes y los reemplazara por copias de sí mismo, que luego se usaban para transmitir el gusano a todos los contactos de correo electrónico de las víctimas.[21]

En los años siguientes al 2000: Desde el 2001 hasta el 2004, inicio una oleada de malware que azoto el internet naciente fue causada por la primera versión del gusano de correos electrónicos Mydoom. “La epidemia se disparó al instante, lo cual sugería que su propagación se efectuaba mediante el envío masivo de mensajes infectados a través de redes zombi. El número de correos electrónicos generados automáticamente era tan grande que muchos servidores de correo corporativo fallaron o vieron drásticamente reducidas sus salidas, incapaces de manejar el abrumador flujo del tráfico”[22]

En años recientes, más específicamente durante el año 2014, se popularizo “Heartbleed” un virus que puso en bastante riesgo los servidores que trabajan con Open SSL, que es una biblioteca criptográfica la cual contiene un código abierto que “Envía "pulsaciones" para comprobar que los endpoints seguros sigan conectados. Los usuarios pueden enviar a OpenSSL una cantidad específica de datos y solicitar la devolución de la misma cantidad; por ejemplo, un byte. Si los usuarios afirman que están enviando el máximo permitido, 64 kilobytes, pero solo envían un byte, el servidor responde con los últimos 64 kilobytes de datos almacenados en la RAM”.[23]

Es un hecho que con el trascurrir de los años la información de la red ha ido aumentando de forma considerable y consigo los avances tecnológicos, han adquirido un papel prioritario en la sociedad, que hoy visualiza este escenario como

---

[20] DW Made for minds. Periódico. [en línea]. 2019. [Consultado 28, noviembre,2018]. Disponible en: https://www.dw.com/es/seis-ataques-cibern%C3%A9ticos-que-sacudieron-el-mundo/a-46967214

[21] Ibid. 6. P. 1

[22] KASPERSKY. (2004). Historia de Ciberataques. [Sitio WEB]. AO Kaspersky Lab. [07 de octubre 2022]. Disponible en: https://encyclopedia.kaspersky.es/knowledge/year-2004/

[23] Ibid. 6. P.1

un espacio fundamental para el desarrollo económico de un país, sin embargo, mencionado progreso también se ha visto permeado por las acciones delictivas de algunas personas que buscan una ventaja en el denominado, ciberespacio.

En la actualidad, se utilizan plataformas avanzadas de detección y respuesta de endpoint (EDR) para proteger los equipos ante un ataque cibernético, sin embargo, a finales de esta década, Kevin Mitnick utilizó ingeniería social para tener acceso a información personal y confidencial; este tipo de ciberataque, que comenzó a tener mayor uso en aquella época y sigue siendo uno de los métodos más populares para vulnerar los activos de una empresa, por tal razón, no solo es importante implementar dispositivos de seguridad perimetral, si no, elaborar una buena estrategia de formación para los colaboradores y usuarios finales.[24]

De acuerdo con lo anterior, y ante la constante evolución de los sistemas informáticos, es importante mencionar que a nivel mundial ha surgido la necesidad de proponer regulaciones y debates acerca del ámbito cibernético, con el fin de sugerir medidas de seguridad en el ciberespacio, teniendo en cuenta que este tipo de afectaciones puede perturbar la economía y estabilidad de los países. Algunas de las acciones que se han tomado iniciaron en el año 1986, en Estados Unidos se creó la Computer Fraud and Abuse Act, sin embargo, su capacidad se vio sobrepasada por la transformación tecnológica. En el año 1995, surgió un comité que se encontraba conformado por profesionales especializados en delitos informáticos ubicados en Europa cuyo objetivo principal era disminuir y crear estrategias para disminuir estos ataques digitales. Dentro de sus premisas determinaron que hacía falta una política de tipo penal que protegiera a todas las sociedades frente a los ataques cibernéticos, a la vez de poder fortalecer los vínculos internacionales, por esto se crea durante el año 2001 el Convenio de Budapest que actualmente se encuentra conformado por 56 países” [25]

En Colombia se han creado normas y leyes relacionadas con los delitos informáticos, entre las cuales se pueden destacar:

La Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la Ley de Delitos Informáticos, tuvo sus propios antecedentes jurídicos, además de las condiciones de contexto analizadas en el numeral anterior. El primero de ellos se remite veinte años atrás, cuando mediante el Decreto 1360 de 1989 se reglamenta la inscripción

[24] Ibid. 1.pag 1

[25] Ibid. 15. pág. 1

del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas.[26]

En lo que respecta a la defensa de los derechos de autor se creó el Decreto 1360 del año 1989 y la Ley 444 de 1993 que son normas que establecen las penas y sanciones cuando se violan los derechos de autor.

Por otra parte, las estadísticas en cuanto a las dinámicas del cibercrimen en Colombia van creciendo pues según reportes de la Policía Nacional: "En el año 2019 se registraron un total de 28.827 casos, de estos 15.948 las victimas efectuaron las respectivas denuncias teniendo en cuenta lo estipulado en la ley 1273 de 2009, obteniendo un porcentaje del 57% de la totalidad de los casos que fueron informados, en cuanto las denuncias que se presentaron durante el año 2018 se presentó una disminución del 5.8% y una variación que fue negativa de 983 casos" [27]

Figura 1. Conducta de delitos informáticos en Colombia

Fuente: CCIT. Tendencias Cibercrimen en Colombia 2019-2020. [En línea]. Bogotá D.C.: 2019. (Recuperado el 25 de abril del 2021) Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

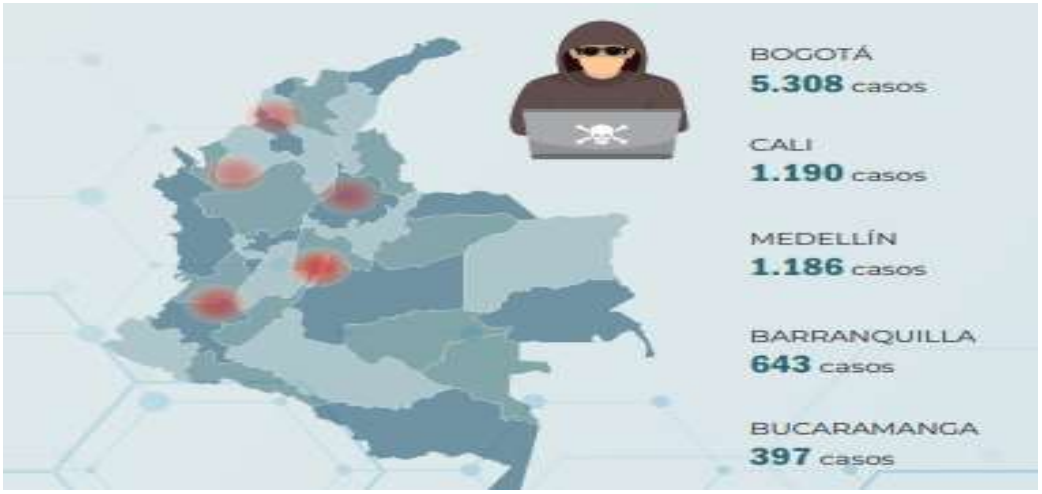
[26]OJEDA PEREZ, Jorge Eliecer. Delitos informáticos y entorno jurídico vigente en Colombia. [en línea]. Articulo. Universidad Santo Tomas, Bogotá D.C.: 2010. [Consultado 28, noviembre,2018]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

[27] CCIT. Tendencias Cibercrimen en Colombia 2019-2020 (29 de octubre 2019, Bogotá D.C.) Tendencias Cibercrimen en Colombia. 2019. 36p

Durante el año 2017: “El número de hurtos que se presentaron por medios informáticos fue de 31.058 casos, ocupando de esta manera el primer lugar”[28]. El interés de los cibercriminales se encuentra directamente relacionado con el dinero que tienen los usuarios en sus cuentas bancarias y por eso comprometen los dispositivos que se utilizan regularmente para realizar las transacciones. “En cuanto a la violación de los datos personales ocupo una segunda posición con un total de 8.037 casos, incluyendo a los ciudadanos y empresas dentro del total, otra de las categorías que ocupo la tercera posición es el acceso de forma abusiva a los sistemas informáticos con un total de 7.994 casos. La cuarta y quinta posición la ocuparon las trasferencias no consentidas de los activos con un total de 4.325 casos y la utilización de softwares maliciosos con un total de 2.387 casos”[29]

Así mismo, si se tiene en cuenta los delitos informáticos por ciudades se puede indicar que: “La concentración del fenómeno criminal en 2019 sitúa a Bogotá, Cali, Medellín, Barranquilla y Bucaramanga como las ciudades con mayor afectación por esta problemática con un 55% de los casos registrados”[30]

Figura 2. Delitos Informáticos por Ciudades



Fuente: CCIT. Tendencias Cibercrimen en Colombia 2019-2020. [En línea]. Bogotá D.C.: 2019. (Recuperado el 25 de abril del 2021) Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[28] TicTac. Tendencias del Cibercrimen en Colombia 2019-2020. [en línea]. Articulo. CCIT Bogotá D.C.: 2019. [Consultado 4, octubre,2022]. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

[29] Ibid. 28. Pag 1

[30] Ibid. 5. Pág 8

En lo que respecta a los ataques cibernéticos más destacados en Latinoamérica en la tabla 1 se muestra un resumen de los sucesos más relevantes desde el año 2009 hasta el 2017.

Tabla 1. Ciberataques y Ciberdefensas en América Latina

AÑO	SUCESO
2009	Robos cibernéticos a cuentas bancarias en Colombia superaron los 50 millones de dólares.
2011	UNASUR incluye en sus planes de acción del 2012, 2013 y 2014 tópicos concernientes a defensa contra ataques cibernéticos
2012	Jorge Maximiliano Pachón es capturado con más de 8000 tarjetas de crédito clonadas y un monto superior a 9 millones de dólares repartido entre 5 países de América Latina
2013	Assange advierte de espionaje de Estados Unidos a América Latina y el Caribe. El 4.2% de los ataques cibernéticos a América Latina y el Caribe corresponden a Venezuela. El 23% de las computadoras de Venezuela tuvieron infección por malware.
2014	Hackeo de más de 500 millones de cuentas en Yahoo. Hackeo de cuentas de Microsoft, Facebook, Google
2015	OEA presenta su programa de seguridad cibernética para los países del Caribe y América Latina
2016	Grupo Anonymous México hackea la página del Sistema de Administración Tributaria de ese país. Más de un tercio de la población de Colombia reporta haber sido víctima de fraude electrónico en distintas organizaciones. Pokémon GO deja sus primeras víctimas por aplicaciones no originales
2017	Los usuarios de Pokémon GO dejan de ser víctimas exclusivamente por delitos cibernéticos, sino que se pasa al modelo de robo de equipos

Fuente: IZAGUIRRE OLMEDO, Jorge. Análisis de los Ciberataques Realizados en América Latina [En línea]. Articulo. Universidad Internacional del Ecuador. Ecuador D.C.: 2018. (Consultado el 11 de octubre del 2021) Disponible en: https://repositorio.uide.edu.ec/bitstream/37000/3782/13/An%C3%A1lisis%20de%20los%20Ciberataques%20Realizados%20en%20Am%C3%A9rica%20Latina.pdf

1.2 FORMULACIÓN DEL PROBLEMA

La ciberseguridad se ha convertido en una de las practicas que más están siendo utilizadas en las empresas con el fin de proteger y defender las redes, los sistemas electrónicos, los computadores, los dispositivos móviles y los servidores de ataques

es un hecho que las empresas turísticas se tienen que enfrentar a diario a amenazas importantes en ciberseguridad entre las que se pueden destacar, el robo de información confidencial, degradando la experiencia de los usuarios y desmejorando la calidad del servicio ofrecido.

En las empresas de turismo, la ciberdelincuencia se ha enfocado principalmente a robar información confidencial, específicamente sus intereses se dirigen hacia los datos de carácter financiero de los clientes y el método que utilizan más regularmente es la red Wi-Fi que en algunos casos no cuentan con ningún tipo de protección. “Los hoteles suelen ser una de las víctimas más frecuentes de las estafas, y las ofertas falsas representan el 40% de los fraudes en este ámbito, de esta forma la ciberdelincuencia y los fallos informáticos se han colocado por primera vez, entre las cinco mayores preocupaciones de las empresas en todo el mundo, según el Barómetro del Riesgo 2015 de Allianz Global”.[31]

Existen una clase de ataques que se denominan carding y que cuentan con varias modalidades como el cambio de tarjetas de los clientes, las clonan, suplantan su identidad en las páginas web todo con el objetivo de obtener sus datos de orden personal, crean call center que son ficticios, esto se puede confirmar con estadísticas presentadas por la policía nacional que crearon una herramienta denominada @caivirtual y que durante el año 2017, tuvieron 328 denuncias motivadas por eventos de carding, identificándose que los sectores donde se presentó más esta problemática fue el turismo, los hoteles, locales de comercio y entidades donde se desarrolla los pagos de servicios públicos.[32]

De lo anterior, nace el planteamiento del presente proyecto enfocado en:

---

[31] ACIS. Hotelería y Turismo el Tercer Sector más afectado por ataques informáticas. [Sitio WEB]. Bogotá D.C. ACIS. [28, noviembre, 2018]. Disponible en internet: https://acis.org.co/portal/content/hoteler%C3%ADa-y-turismo-tercer-sector-m%C3%A1s-afectado-por-ataques-inform%C3%A1ticos

[32] VALOYES MOSQUERA, Avancio. Ciberseguridad en Colombia. [En línea]. Articulo. Universidad Piloto de Colombia. Colombia. (Consultado el 25 de Abril de 2021. Disponible: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

¿Qué beneficios se obtienen al realizar un análisis de las amenazas y riesgos cibernéticos sobre la prevención de la seguridad de la información que necesitan los usuarios y organizaciones de servicios turísticos a través de medios electrónicos?

2 JUSTIFICACIÓN

“Los antecedentes históricos del comercio electrónico en Colombia tuvieron sus inicios durante los años 2000 y el año 2004 con el nacimiento de las primeras tiendas que se crearon online”[33]. Este proceso de posicionamiento fue lento pues los colombianos no confiaban totalmente de las compras que se efectuaban por internet, a pesar de estos inconvenientes este país ha presentado crecimientos considerables en los desarrollos tecnológicos.

El crecimiento de la sociedad ha hecho que el comercio electrónico esté a la vanguardia de todos los procesos que se realizan a nivel empresarial. Por este motivo, cobra importancia la ciberseguridad a través de la protección de los sistemas informáticos, aplicando medidas preventivas de protección para evitar ataques cibernéticos que pueden ocasionar pérdidas económicas; en este caso en las empresas de turismo colombianas.

Además que las empresas de turismo obtienen muchos beneficios al implementar planes de ciberseguridad, por ejemplo, proteger la propiedad intelectual pues trabajan constantemente con datos personales de los clientes, mejoran la competitividad en el mercado actualizándose constantemente con los cambios que va requiriendo la era digital, también permite realizar un control efectivo al acceso de la información, gestionar contraseñas, actualizaciones, copias de seguridad y la eliminación segura de información.

En lo académico, la oportunidad que brinda este escrito es pertinente en el sentido de poder abordar los conocimientos que están relacionados con la aplicación de medidas de ciberseguridad en el sector turístico colombiano y a nivel internacional si se ha mejorado la seguridad de las organizaciones del sector turístico

.

Con la presente monografía se quiere estudiar el papel fundamental que cumple la ciberseguridad en organizaciones de turismo, debido a los recientes cambios

[33] VENDES FACIL. La historia del ecommerce en Colombia. [Sitio WEB]. Medellín. Vendes facil. [03, octubre, 2022]. Disponible en internet: https://www.vendesfacil.com/ecommerce/la-historia-del-ecommerce-en-colombia/

tecnológicos en los clientes y empresarios, surge la necesidad de aplicar medidas de seguridad básicas, como la capacitación del personal en este sentido ayudando a que el turismo cuente con organizaciones más seguras, colaborativas y eficientes.

En definitiva, con la realización de esta monografía se contribuirá en el aumento y diversificación de conocimientos sobre cómo identificar y disminuir amenazas cibernéticas en las empresas de turismo colombianas, los tipos de ataques que se realizan con mayor frecuencia, sus repercusiones a nivel interno y externo de las compañías, incluyendo amenazas y vulnerabilidades añadiendo las recomendaciones que se deben seguir para evitar estos tipos de ataques.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar las amenazas y riesgos cibernéticos que afrontan los usuarios y las organizaciones en la consulta y/o adquisición de servicios turísticos a través de medios electrónicos, como aporte en la prevención de brechas de seguridad de la información.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar las amenazas y riesgos cibernéticos asociados a la adquisición de servicios turísticos a través de medios electrónicos que permita un reconocimiento del estado actual en este sector de la economía.

- Esquematizar las herramientas, técnicas y estrategias que proporcionen mecanismos de seguridad de la información a usuarios y organizaciones de servicios turísticos que utilizan medios electrónicos para su consulta y/o adquisición.

- Proponer recomendaciones de buenas prácticas cibernéticas para la consulta y/o adquisición de servicios turísticos por medios electrónicos que contribuyan en la prevención de incidentes cibernéticos en este sector de la economía.

4 MARCO REFERENCIAL

4.1. ESTADO DEL ARTE

4.1.1 Investigaciones nacionales e internacionales

Las investigaciones que se han elaborado partiendo de temáticas que guardan cierta relación con la de la presente monografía son variadas pues han abordado la ciberseguridad desde varias perspectivas buscando una solución eficaz a los ataques cibernéticos que se puedan presentar.

En este sentido se tendrán en cuenta proyectos de grado e investigaciones que se han realizado a nivel nacional e internacional, una de ellas es la titulada “Modelo experimental de Ciberseguridad y Ciberdefensa para Colombia” presentada ante la Universidad Libre durante el año 2015 y cuyos autores son Nicolás Alfredo Arias Torres y Jorge Alberto Celis Jutinico, se plantea desarrollar un modelo para la Ciberseguridad y Ciberdefensa colombiana (MCCPC), se configuran luego de segmentar espacialmente los marcos de acción logística tanto de los estamentos militares, de policía, como las unidades asesoras de gobierno previa validación de los documentos y referentes existentes que han liberado y difundido estados de trascendental importancia en la lucha contra el terrorismo cibernético.

Se concluye que el MCCPC, establece los valoradores de acción logística, como resultado de la interpretación analítica de los ejes de referenciación organizacional para controlar y formular procedimientos para la Ciberseguridad y para la Ciberdefensa, fundamentados en la significancia de la administración moderna (P=planeación, O=organización, D=dirección, E=ejecución, R=revisión o control), significando que para implementar el modelo convencionalmente, el programa debe acercarse como consultor al MINTIC y MINDEFENSA.

La segunda investigación es un trabajo de grado de maestría cuyo título es: “Impacto del Riesgo Cibernético en el Bienestar del Segmento Mipyme” presentada ante la Universidad EAFIT durante el año 2018 en la ciudad de Medellín y cuya autora es Sara Villa Mesa, el propósito de este trabajo es: “Analizar el impacto del seguro de riesgo cibernético en la protección de las utilidades para el segmento

Mipyme en Colombia, mediante el estudio de un grupo de empresas pertenecientes al segmento, las cuales experimentaron pérdidas debido a incidentes cibernéticos"[34]

Para el cálculo de la Utilidad Esperada EU: "Se utiliza la función de aversión al riesgo CRRA, donde a partir del análisis de datos de 50 empresas afectadas, se comprueba como el seguro es un mecanismo de transferencia de riesgo que apalanca el bienestar de las empresas Mipyme"[35]

La tercera investigación es un proyecto de grado para optar a la especialización en seguridad informática su título es: "Diseño de un plan de gestión de riesgos y vulnerabilidades del caso de estudio de la empresa QWERTY S.A., basados en los estándar NTC-ISO/IEC 27001 Y NTC-ISO/IEC 27032" presentada ante la Universidad Nacional Abierta y a Distancia UNAD durante el año 2020 en la ciudad de Tunja y cuyo autor es Jorge Emilio Saavedra Agudelo. En este proyecto se plantea: "Utilizar procedimientos, técnicas y métodos en donde se implemente un Sistema de Gestión de Seguridad de la Información (SGSI), como así mismo la administración y gestión de la ciberseguridad y todo esto con el fin de llevar a cabo su implantación, monitoreo, procedimiento, operación, verificación, mantenimiento, sostenimiento y mejora del sistema mencionado, fortaleciendo el sistema de seguridad, identificando y gestionando los riesgos posibles en el sistema de información, basándonos en la información propuesta en el caso de estudio de la empresa QWERTY S.A, utilizando como referencia las normas internacionales ISO/IEC 27001 y ISO/IEC 27032"[36]

---

[34] MESA, Sara. Impacto del Riesgo Cibernético en el Bienestar del Segmento Mipyme. [En línea]. Trabajo de Grado. Universidad EAFIT. Medellín. 2018. p. 6. Consultado el 6 de mayo de 2022. Disponible en: https://repository.eafit.edu.co/bitstream/handle/10784/12890/Sara_VillaMesa_2018.pdf?sequence=2&isAllowed=y

[35] Ibid. 34.p.20

[36] SAAVEDRA, Jorge Emilio. Diseño de un plan de gestión de riesgos y vulnerabilidades del caso de estudio de la empresa QWERTY S.A., basados en los estándar NTC-ISO/IEC 27001 Y NTC-ISO/IEC 27032. [En línea]. Proyecto de Especialización. Universidad Nacional Abierta y a Distancia UNAD. Boyacá. 2020. p. 21. Consultado el 6 de julio de 2022. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/36866/jsaavedraag.pdf?sequence=3&isAllowed=y

Dentro de las conclusiones se menciona que con la implementación del SGSI en el caso de estudio de la empresa QWERTY S.A., de acuerdo con el estándar de calidad ISO 27001:2013, se concluye que cualquier tipo de entidad, pymes u organización que implemente estas normas, proporcionará seguridad en cada uno de los activos de la información y prolongará la existencia y valoración de los mismos. Mediante el análisis de las amenazas, riesgos, vulnerabilidades y la aplicación de procedimientos o controles se puede garantizar una mayor vida útil a los activos de información tanto físicos como del ciberespacio y todo esto a partir de las estrategias de protección tanto físicos como virtuales basándonos en los principios de confidencialidad, integridad, disponibilidad y no repudio de la información.

La cuarta investigación es una tesis doctoral que se denomina: “La Ciberseguridad en España 2011 – 2015 una Propuesta de Modelo de Organización” presentada ante la Universidad Nacional de Educación a Distancia durante el año 2018 en la ciudad de Madrid y cuyo autor es Aníbal Villalba Fernández, Este trabajo de investigación: “Se ha construido como un estudio de caso sobre la ciberseguridad en España, estimando su relevancia y su naturaleza en relación con la propuesta de un modelo de organización de la ciberseguridad en España, el cual pueda ser realizable y tenga un impacto positivo en el incremento de los niveles de la seguridad nacional”[37]

Se concluye que después de revisarse el modelo de gobernanza actual en España, se ha realizado una propuesta de modelo de organización nacional de la ciberseguridad. "En el nivel político estratégico se propone mantener el Consejo Nacional de Ciberseguridad con su composición y misión de planeamiento político estratégico, pero incorporando a este CNCS una capacidad ejecutiva para realizar el seguimiento de la implementación del Plan Nacional de Ciberseguridad y de sus Planes Derivados. Tras detectar la inexistencia de un nivel operacional de carácter nacional que pueda continuar el proceso de planeamiento a ese nivel de modo integral, así como realizar la implementación de estos planes y su control en los organismos subordinados, se propone la creación de un Centro de Ciberseguridad Nacional, directamente dependiente del Consejo Nacional de Ciberseguridad. Por último, tras valorarse positivamente el diseño del nivel táctico y técnico de la

[37] FERNANDEZ, Anibal. La ciberseguridad en España 2011–2015 una propuesta de modelo de organización. [En línea]. Tesis Doctoral. Universidad Nacional de Educación a Distancia España. . 2015. p. 20. Consultado el 6 de julio de 2022. Disponible en: http://e-spacio.uned.es/fez/eserv/tesisuned:CiencPolSoc-Avillalba/VILLALBA_FERNANDEZ_Anibal_Tesis.pdf

ciberseguridad en España, se propone que el CERT Gubernamental Nacional actual (CCN-CERT) realice funciones de coordinación nacional en el ámbito de la prevención y respuesta a ciberataques, para los tres niveles de las administraciones públicas y para empresas de carácter estratégico, y que se constituya además en centro de referencia para el sector privado"[38]

4.2 MARCO TEÓRICO

En el presente marco teórico se incluyen varias teorías que están relacionadas con la consulta y adquisición de servicios turísticos y las amenazas y riesgos cibernéticos que afrontan estas empresas.

Uno de los primeros autores que se trae a colación es Raymundo Cuervo quien propuso un análisis del turismo teniendo en cuenta la teoría de sistemas, su teoría se titula "El turismo como medio de comunicación humana", definiendo el turismo como: "Un conjunto bien definido de relaciones, instalaciones y servicios que se generan en virtud de ciertos desplazamientos humanos"[39]

Este autor analiza el turismo como un sistema de comunicación que se puede transmitir de forma positiva o negativa, pero que debe conservarse como un operador que trasmite comunicaciones de forma positiva. Esta teoría reafirma el tema principal de esta monografía pues en la consulta y adquisición de servicios turísticos necesariamente debe existir una comunicación entre el personal que hace parte de las agencias, hoteles y las organizaciones turísticas con los clientes para poder llegar a acuerdos comerciales.

De igual manera las teorías que han sido postuladas por autores sobre las amenazas y riesgos cibernéticos que afrontan las empresas, una de ellas es la postulada por el filósofo y profesor Marshall Mc Luhan y los peligros que afrontan las comunidades virtuales: "Actualmente las guerras ya no se ganan en el campo de batalla tradicional, como fueron las trincheras; sino que ahora se obtienen en los medios de comunicación. En este sentido, es cada vez más el espacio simbólico que construyen los canales de comunicación y sus ampliaciones, donde se

[38] Ibid. 37.p.20

[39] PANOSSO, Alexandre. Teorías, Sistemas y Modelos. En; Teoría del Turismo. México. Editorial Trillas.2012.9-38

reconstruye y destruye los procesos de la vida cotidiana, particularmente en las ciudades”[40]

Esta teoría es importante en el desarrollo de esta monografía pues las comunidades turísticas virtuales presentan peligros, amenazas y vulnerabilidades al manejar la información personal de sus clientes que utilizan los medios de comunicación del internet para realizar sus transacciones y requerimientos comerciales lo que requiere de la puesta en marcha de estrategias y técnicas que impidan el robo de esta información por parte de los ciber atacantes.

Otra de las teorías fue la formulada por el matemático estadounidense Norbert Wiener, quien propuso su teoría del control y la comunicación en máquinas y animales que denomino la cibernética, basa sus postulados en que: “Dentro de nuestras sociedades, es imposible conseguir los objetivos principales de la vida en común sin la información necesaria en el momento y lugar precisos”[41]

Según este autor, las sociedades tienden al fracaso sino se encuentran ligadas con la entrega de la información de una forma oportuna, los seres humanos deben comunicarse continuamente y es que el comercio electrónico ha permitido que las comunicaciones se extiendan a cualquier lugar del mundo.

Dentro de las teorías que se destacan en esta investigación se incluye la formulada por Héctor Luis Saint-Pierre en el año 2016 sobre el concepto que tiene acerca de lo que significa una amenaza pues la analiza como un fenómeno perceptivo y no objetivo: “La percepción depende del sujeto perceptor, de sus características psicológicas, su estructura física, su formación cultural y académica, la estructuración de su familia”. [42]

Si se efectúa la consideración de la amenaza como un tipo de percepción, es fundamental realizar un análisis sobre sus vulnerabilidades, potencialidades, características y su naturaleza, puesto que influirá de una forma directa en el

---

[40] RIVEROS, Fredy. Administración del Riesgo Cibernético un enfoque desde la alta gerencia empresarial en Colombia. [en línea]. Articulo. Universidad Militar Nueva Granada, Bogotá D.C.: 2016. [Consultado 28, noviembre,2020]. Disponible en internet: https://repository.unimilitar.edu.co/bitstream/handle/10654/15837/RiverosCardenasFredyOrlando2017.pdf?sequence=1&isAllowed=y

[41] Ibid. 29. p. 9

[42] YEPES, H. Las Teorías de la Seguridad. Revista de Ciencias de Seguridad y Defensa. [en línea]. Articulo. Academia de Guerra del Ejercito, Ecuador.: 2018. [Consultado 28, noviembre,2020] Disponible en: https://www.researchgate.net/publication/325023212_LAS_TEORIAS_DE_LA_SEGURIDAD

perceptor provocando la reacción del mismo y la debida orientación que tome para poder enfrentarlo.

4.2.1 Estado Actual del Cibercrimen en Comercio Electrónico

Según el Informe de tendencias del Cibercrimen del primer trimestre del año 2020 presentado por el Tanque de Análisis y Creatividad de las TIC - TicTac y su programa SAFE en asocio con la Policía Nacional y su Centro Cibernético Policial los ciberataques van en aumento:

Durante los meses de enero hasta la tercera semana de marzo de 2020, las denuncias por ciberdelitos en Colombia reportaban un incremento de 6.082 casos, es decir, un 8% más respecto al mismo periodo del 2019. Sin embargo, en la última semana de marzo y la primera de abril los ciberataques aumentaron hasta en un 37% debido a la coyuntura del COVID-19, según la Policía Nacional se ha detectado 195 páginas web para robar y estafar.[43]

Según las estadísticas presentadas durante el primer trimestre del año 2020 el Cibercrimen que tiene más auge es el de suplantación de sitios web para capturar datos personales y las empresas colombianas han reportado que se presentan diferentes modos en que operan en este sentido entre los que se pueden mencionar: envío de correos electrónicos fraudulentos, envió de mensajes de texto y cadenas de WhatsApp con enlaces maliciosos, también lo realizan por medio de aplicaciones falsas fuera de las tiendas virtuales que son normalmente conocidas.

El segundo Cibercrimen que ha tenido un crecimiento significativo durante el año 2020 fue la violación de datos personales pues se registraron 958 casos por medio de denuncias que hicieron los usuarios con lo cual se presentó un aumento significativo del 13.5% con relación al año 2019.

---

[43] INFORME TENDENCIAS DE CIBERCRIMEN PRIMER TRIMESTRE DE 2020. (Abril del 2020 , Bogotá D.C.). Informe Tendencias del Cibercrimen en Colombia. Bogotá. Policía Nacional. 2021. 14p.

A nivel internacional, distintos organismos emitieron alertas a lo largo de este 2020 advirtiendo acerca del incremento de los engaños y estafas en compras online. “En España, a mediados de abril las estafas por Internet habían aumentado en un 70%, afirman datos de la Guardia Civil, mientras que, en Argentina, en julio el aumento de los delitos por Internet era del 50%, aseguran datos de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)”[44]

Como decíamos, las estrategias y técnicas utilizadas por los criminales a nivel global no son nuevas. El FBI, por ejemplo, en agosto publicó una alerta en la que explica que registraron un aumento en la cantidad de denuncias. Por ejemplo, de víctimas a las que no le llegaron los productos que compraron, personas que reportan que fueron dirigidas a sitios a través de anuncios en redes sociales luego de buscar en sitios de compras online.

4.3 MARCO CONCEPTUAL

4.3.1 Ciberseguridad

La definición que se tiene de ciberseguridad es que forma parte del: “Conjunto de herramientas y procedimientos que se utilizan con el fin de proteger toda la información que se procesa y genera utilizando las computadoras, redes, dispositivos móviles y sistemas que son electrónicos”[45]

4.3.2 Elementos de la Ciberseguridad

[44] WELIVESECURITY. Crece el ecommerce y aumentan las estafas y los incidentes de seguridad. [Sitio WEB]. Welivesecurity. [25, noviembre, 2020]. Disponible en: https://www.welivesecurity.com/la-es/2020/11/25/crece-ecommerce-aumentan-estafas-incidentes-seguridad/

[45] Ibid. 1 pág. 1

Son tres los elementos fundamentales de la ciberseguridad como se puede apreciar en la figura 3 en la cual se especifica que son: “La confidencialidad, la integridad y la disponibilidad”[46]

Figura 3. Elementos Fundamentales de la Ciberseguridad

Fuente: PÉREZ, Yuly. Importancia de la Ciberseguridad en Colombia. [En línea]. Articulo. Universidad Piloto de Colombia. Bogotá D.C. (Consultado el 03 de Mayo del 2021) Disponible en: http://polux.unipiloto.edu.co:8080/00003620.pdf

El primer elemento es la confidencialidad que tiene la propiedad de que la información no tenga una divulgación o acceso a procesos, personas o entidades que no se encuentran autorizados, el segundo elemento es la integridad que se trata de conservar los activos que tienen la información con la exactitud que vienen originalmente y el tercer elemento es la disponibilidad es una de las propiedades que consiste en estar utilizable y disponible cuando se hagan requerimientos por las entidades autorizadas.

También se incluyen otros elementos como son el riesgo de seguridad digital que tiene que ver con el desarrollo de actividades en los entornos digitales.

Así mismo está la Gestión de riesgos de seguridad digital: “Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. [47]

[46] PÉREZ, Yuly. Importancia de la Ciberseguridad en Colombia. [En línea]. Articulo. Universidad Piloto de Colombia. Bogotá D.C. (Consultado el 03 de Mayo del 2021) Disponible en: http://polux.unipiloto.edu.co:8080/00003620.pdf

[47] Ibid. 35. p.3

Dentro de los elementos se incluyen los delitos informáticos y los ciberdelitos que lo constituyen los actos ilegales que no están autorizados e impiden el procesamiento de los datos en los sistemas informáticos, además que utilizan tecnologías de internet para su desarrollo en los ciberespacios.

4.3.3 Características de los Ciberataques

4.3.3.1 Apropiación de Credenciales

Algunas de las formas que utilizan los cibercriminales para explotar los diferentes tipos de vulnerabilidades que se pueden encontrar es por medio del internet y lo realizan de la siguiente forma:

Obtención directa: el usuario entrega directamente sus datos al atacante. Obtención por engaño al usuario: el atacante se hace pasar por administrador y solicita credenciales al usuario con motivo de soporte técnico. Obtención por escucha de tráfico: el atacante intercepta los datos trasmitidos por medios no seguros, sin cifrado o monitoreo de tráfico. Obtención por medio de aplicaciones: uso de virus en los equipos de los usuarios, guardan sus parámetros de conexión a sistemas. Obtención por acceso a archivos de credenciales. Obtención por descifrado de credenciales cifradas y obtención por observación a los usuarios.[48]

4.3.3.2 Ataques de Denegación de Servicios

“Este tipo de ataque es el más usado regularmente, abusando de los recursos que tienen disponibles los usuarios, la forma de actuar es que sobrecargan de solicitudes los respectivos sistemas informáticos, denegando accesos y disponibilidades por medio de overflow, buffer o inundando mensajes”[49]

---

[48] Ibid 9.p 2

[49] Ibid. 9 p. 3

4.3.3.3 Ataque por cambio de la página web

Este ataque se relaciona con el término defacement, donde el contenido de la página es alterado. “Una variedad de este tipo de ataques es cuando se redirige al usuario a un sitio falto, pero es copia exacta del sitio deseado, se realiza con el fin de obtener datos como los de las tarjetas de crédito, de aquí la palabra phishing”[50]

4.3.3.4 Alteración de Protocolos de Comunicación

Este procedimiento solo lo pueden hacer los ciberatacantes que tienen conocimientos en los diferentes protocolos que existen como: “El Icmp, Tcp/Ip y el Udp y cuáles son las limitantes con las que cuentan, por eso pueden realizar acciones como aumentar la carga de los respectivos sistemas, impedir las comunicaciones entre los emisores y los receptores, paralizar las redes, hacer direcciones de paquetes hacia Ip que contienen destinos falsos”[51]

4.3.4 Modelo del Ciberataque

En el modelo de desarrollo de los ciberataques se ejecuta en cuatro fases: la fase 1 se encarga de la obtención de la información y la respectiva investigación, la técnica utilizada es la ingeniería social, en esta fase se pueden identificar los mecanismos que utilizan los usuarios como son sus niveles de seguridad y las autenticaciones. Por su parte, en las fases 2 y 3 los ciberatacantes ponen a prueba sus conocimientos técnicos utilizan los elementos de la fase 1 para ingresar ilegalmente a los sistemas: “En la fase 4, su objetivo es evitar que sea detectado el origen del ataque, por eso es común el uso de alias o el uso de identidades digitales falsas, incluso el borrado de rastros que impidan la llegada al atacante”[52]

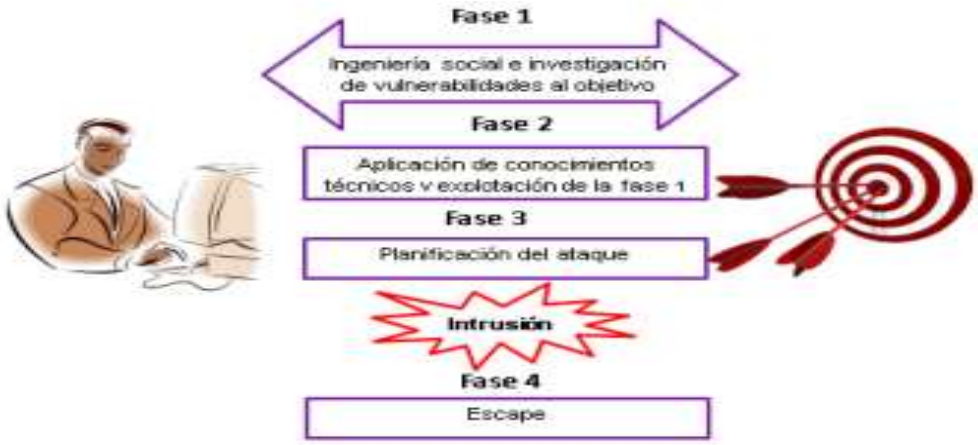
Figura 4. Fases del Ciberataque

---

[50] Ibid 9. p. 3

[51] ibid. 9. Pag 3

[52] Ibid. 9. p 3



Fuente: PÉREZ, Yuly. Importancia de la Ciberseguridad en Colombia. [En línea]. Articulo. Universidad Piloto de Colombia. Bogotá D.C. (Consultado el 03 de Mayo del 2021) Disponible en: http://polux.unipiloto.edu.co:8080/00003620.pdf

4.3.5 Ciberseguridad y sus riesgos

La ciberseguridad y la seguridad informática son dos aspectos que han cobrado una relevancia fundamental en los últimos años, a pesar de esto se nota que no ha avanzado lo que se cree suficiente para poder crear una cultura colectiva en este sentido: “Las Tic en estos últimos años han generado una conducta delictiva, debido a su fácil anonimato, se trata de nuevas formas penales que han exigido una normativa penal concreta, en la práctica se observa que el uso incorrecto de las Tic facilita la comisión de delitos virtuales”[53]

La UIT (Unión Internacional de Telecomunicaciones) define en su recomendación UIT-T X.1205 Unión Internacional de Telecomunicaciones (2008) a la ciberseguridad como:

El conjunto de herramientas políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación,

[53] ZAMBRANO MACIAS, María. Ciberseguridad, riesgo y amenazas de los jóvenes en las redes sociales caso: Colegio Fiscal Mixto Camilo Ponce. [en línea]. Proyecto de Investigación. Universidad Laica “Eloy Alfaro”, Ecuador: 2018. [Consultado 28, noviembre,2020]. Disponible en: https://repositorio.uleam.edu.ec/bitstream/123456789/1756/1/ULEAM-PER-0031.pdf

prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y lo usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios y la totalidad de la información transmitida y/o almacenada en el ciberentorno[54]

La ciberseguridad tiene una función principal y es la de garantizar los alcances y mantenimiento de las propiedades con las que cuenta la seguridad de los activos de la empresa, además que los usuarios se protegen contra riesgos de seguridad del ciberentorno. Dentro de las propiedades con las que cuenta la seguridad se incluyen: la confidencialidad y disponibilidad incluyendo los procesos de integridad dentro de los cuales se destacan el no repudio y la autenticidad.

4.3.6 Tipos de ciberataques

Existe una gran cantidad de agente de tipo malicioso que pueden utilizar los cibercriminales para ingresar ilegalmente a los sistemas informáticos, entre los más frecuentes y comunes se encuentran:

4.3.6.1 Malware

Este procedimiento solo lo pueden hacer los ciberatacantes que tienen conocimientos en los diferentes protocolos que existen como: “El Icmp, Tcp/Ip y el Udp y cuáles son las limitantes con las que cuentan, por eso pueden realizar acciones como aumentar la carga de los respectivos sistemas, impedir las comunicaciones entre los emisores y los receptores, paralizar las redes, hacer direcciones de paquetes hacia Ip que contienen destinos falsos”[55]

Los más comunes son los virus, troyanos, spyware, Rasomware, Adware y Botnets.

---

[54] Ibid. 9. p 16

[55] ibid. 9. Pag 3

4.3.6.2 Phishing

Es un programa malicioso enviado a las víctimas o usuarios a través de correos electrónicos que parecen ser de una empresa legítima, bancos u otra organización, solicitando información personal o confidencial. “En muchas ocasiones dichos correos poseen enlaces a sitios web preparados por los cibercriminales. Estos ataques se utilizan a menudo para inducir a que las personas entreguen datos bancarios, de tarjetas de crédito, de débito u otra información personal”[56]

4.3.6.3 Ataque de Inyección SQL

Es un ataque que utiliza códigos maliciosos con lenguajes de programación de consulta que se encuentran estructurados y se utilizan para lograr comunicarse con las bases de datos que se encuentran en los servidores que realizan almacenamientos de información crítica de servicios y sitios web todo con el fin de extraer datos confidenciales de los clientes y tomar el control, esto sucede mucho en los bancos, cuando se manejan los usuarios, contraseñas, números de cuentas bancarias, tarjetas de crédito, etc.[57]

4.3.6.4 Ataque de Denegación de Servicio

Este tipo se puede realizar a la vez en muchos ordenadores y se trata de causar saturaciones de tráfico en los sistemas informáticos o sitios web produciendo sobrecargas en los servidores y redes, con esto se impide que se puedan satisfacer

---

[56] GAMBOA, José Luis. Importancia de la seguridad Informática y ciberseguridad en el Mundo actual. [En línea]. Articulo. Universidad Piloto de Colombia. Bogotá D.C. (Consultado el 03 de Mayo del 2021) Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8668/IMPORTANCIA%20DE%20LA%20SEGURIDAD%20INFORM%C3%81TICA%20Y%20CIBERSEGURIDAD%20EN%20EL%20MUNDO%20ACTUAL.pdf?sequence=1&isAllowed=y

[57] ibid. 30. p 3

las solicitudes y que sean legítimas, inutilizando e impidiendo que las empresas puedan realizar sus actividades básicas como dar respuesta a las solicitudes de los usuarios o publicar contenidos en sus páginas web.[58]

4.3.7 Comercio Electrónico

El e-commerce, o comercio electrónico, es un sistema de compra y venta de productos o servicios que se realiza exclusivamente a través de Internet. Se refiere a las transacciones entre compradores y vendedores mediante una plataforma online que gestiona los cobros y los pagos de manera completamente electrónica.[59]

4.3.8 Aspectos científicos y tecnológicos de la ciberseguridad

La ciberseguridad y la seguridad informática desde su aparición han tenido que sobrepasar retos desde el manejo de grandes computadores y sus conexiones a las redes de las comunicaciones, a pesar de ello, los avances tecnológicos como el internet, los dispositivos móviles, las redes eléctricas inteligentes, el internet de las cosas han cobrado una relevancia significativa.[60] “La ciberseguridad es una de las áreas de la computación que tiene como función la implementación y desarrollo de los mecanismos que existen para proteger la información incluyendo las clases de infraestructuras tecnológicas, estas acciones se efectúan con el objetivo de mantener sistemas más seguros y garantizar a los usuarios la disponibilidad, integridad y confidencialidad de sus datos, por este motivo se proponen herramientas, métodos y prácticas que evalúen las amenazas cibernéticas, sistemas de seguridad y hardware”[61]

---

[58] ibid. 30. p 3

[59] ESERP. ¿Qué es e-commerce o comercio electrónico? [Sitio WEB]. España. Eserp Business & Law School. [28, noviembre, 2020]. Disponible en: https://es.eserp.com/articulos/e-commerce-o-comercio-electronico/?_adin=02021864894

[60] ibid. 35. Pag 2

[61] URCUQUI, Cristian Camilo. Ciberseguridad un enfoque desde la ciencia de datos.1 ed. Cali. Editorial Universidad ICESI.2018.90p. ISBN: 978-958-8936-55-0

La ciencia de datos tiene su relación con la ciberseguridad pues tiene la capacidad de brindar soluciones que pueden ser aproximadas a problemas que normalmente no tienen una solución viable utilizando los sistemas convencionales, es útil debido a que puede manejar altos volúmenes de información y fuertes capacidades de la computación.

La ciencia de datos surge como una opción para mejorar los mecanismos de análisis que requieren los sistemas cibernéticos para hacerle frente a los diferentes tipos de riesgos de seguridad que existen en la actualidad. “La ciencia de datos, si bien puede ayudar a mejorar la seguridad, también puede servir para erosionarla, por lo que es importante mantener la dinámica de análisis y desarrollo de nuevas estrategias que garanticen el mejoramiento continuo de la seguridad informática”[62]

4.3.9 Aplicación de la Ciencia de Datos al Análisis de Ciberamenazas

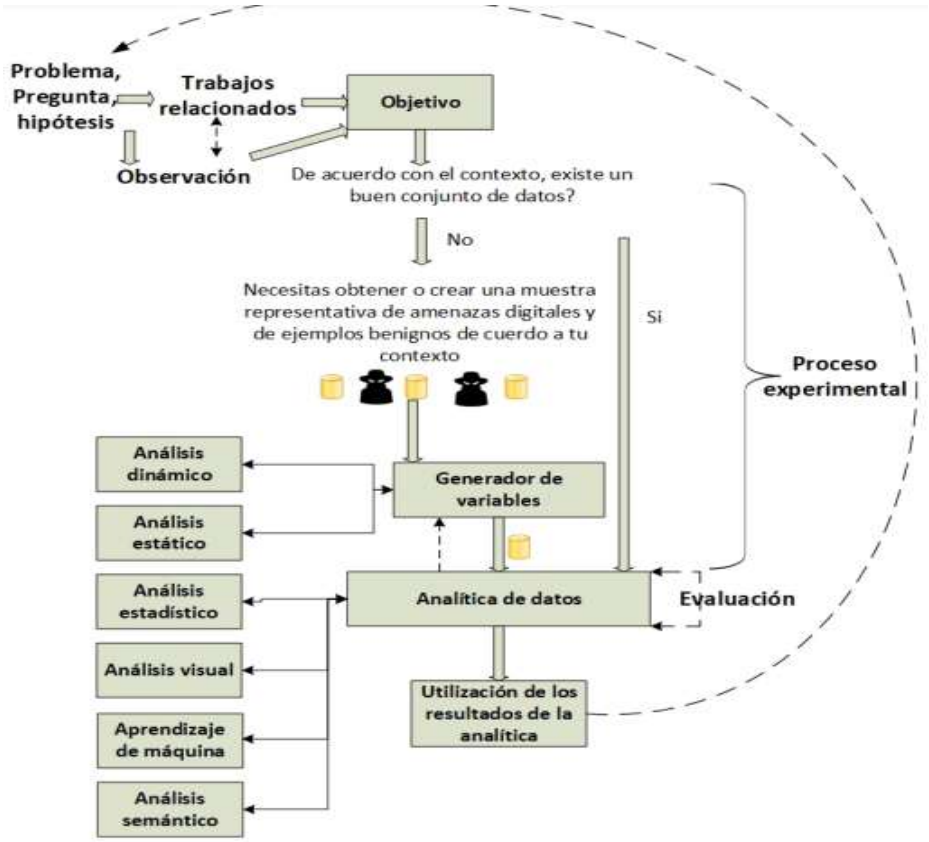
La aplicación de la ciencia de datos en los análisis de ciberamenazas es un procedimiento que puede servir de base para la formulación futura de un framework para realizar los entrenamientos de modelos de machine learning que pueden aplicarse para detectar amenazas cibernéticas en diferentes contextos de una investigación. [63]

En la figura se realiza el desarrollo de un método científico en el que se identifica una problemática, se plantea un objetivo o una pregunta de la respectiva investigación, estableciendo una hipótesis y buscando su refutación o aceptación.

Figura 5. Proceso de Aplicación de la Ciencia de Datos en Ciberseguridad

[62] Ibid. 34 p 21

[63] Ibid 35. Pag 5



Fuente: URCUQUI, Cristian Camilo. Ciberseguridad un enfoque desde la ciencia de datos.1 ed. Cali. Editorial Universidad ICESI.2018.90p. ISBN: 978-958-8936-55-0

4.3.10 Clasificación del turismo

El turismo se clasifica en muchas categorías como son en el campo vacacional, deportivo, convenciones, negocios, científico, cultural, religioso, familiar, de aventura, se definirán algunas de estos tipos de turismo. [64]

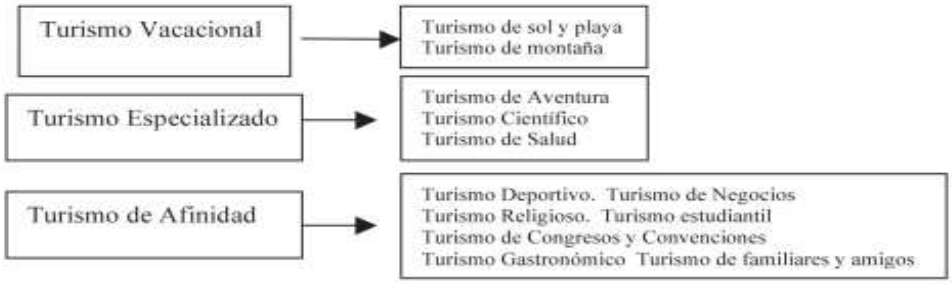
El turismo de vacaciones es el que se encarga del ocio y descanso de las personas que van encaminadas a cambiar las actividades de rutina durante el tiempo que no

[64] Ibid. 9 p 146

se labora y está relacionado con otros tipos de turismo como el de naturaleza, estudiantil y cultural.

A continuación, se presenta en la figura 1 en la que se clasifica el turismo cuando existen motivos de viaje

Figura 6. Clasificación del Turismo según el Motivo de Viaje



Fuente: MORILLO, Moreno. Turismo y producto turístico, evolución, conceptos, componentes y clasificación

El turismo que es de aventura se enfoca en realizar viajes a lugares o regiones que son poco conocidas y visitadas como es el caso del Desierto del Sahara, la Antártida, etc. [65]

En este tipo de turismo se puede realizar la práctica de deportes, entornos de viajes donde predomine la naturaleza y la observación de la fauna y flora.

El turismo deportivo comprende los viajes que se hacen para participar en eventos deportivos de índole mundial que son organizaciones por asociaciones e instituciones de actividades recreativas. Dentro de los deportes que incluye que se encuentran la natación, pesca, velerismo, alpinismo, esquí y demás deportes que son de riesgo.

[65] Ibid 9 p 146

En el turismo de negocios se: “contempla los viajes efectuados por ejecutivos, comerciantes y funcionarios del gobierno con algún incentivo laboral o económico, con excepción de aquellos desplazamientos efectuados por inmigrantes cuyo principal propósito es lograr empleo y mejores remuneraciones”[66]

El turismo religioso por su parte se basa en el interés que tienen los viajeros por conocer templos, monumentos en los que se practica cierto tipo de denominación religiosa, sus creencias, se hace normalmente bajo la programación de las iglesias que hacen peregrinaciones a estos lugares y cuya acogida se encuentra en mayor tendencia por las personas de la tercera edad.

En general el turismo que es cultural esta: “motivado por los deseos del viajero de aumentar sus conocimientos y disfrutar de emociones artísticas en monumentos, museos, zonas arqueológicas y otros, que procuran conocimientos, satisfacción y contemplación directa (no lograda con reproducciones) de forma superficial o rápida mediante la formación de imágenes de los valores y lugares visitados”[67]

Así mismo se encuentra en turismo estudiantil cuyo interés fundamental radica en el deseo de los alumnos de ampliar sus conocimientos intelectuales haciendo intercambios con otros países para aprender más acerca de su cultura, costumbres, etc., normalmente se organizan en grupos bajo la supervisión de los docentes, en el que se encuentran beneficios como tener un efecto multiplicador de las experiencias de los estudiantes hacia sus familias y amigos.

Finalmente, el turismo de salud y de tipo científico incluye viajes que se realizan para apoyar la investigación de centros de investigación, bibliotecas y universidades todo con el objetivo de probar el carácter científico e intelectual en cuestión.

4.3.11 Turismo en Colombia

[66] Ibid. 9 p 147

[67] Ibid. 9 p 148

El turismo en Colombia genera ganancias considerables y está ligado a muchos sectores que aportan a la economía un balance positivo según estadísticas: “En el trimestre comprendido entre noviembre 2013 y enero 2014 el sector Comercio, Hoteles y restaurantes participó con el 27,7 % (5.895 miles de personas) del total de la población ocupada en el país (21.253) siendo el sector que más participa porcentualmente en el total de ocupados, según informe del CITUR”[68]

Según estas estadísticas el turismo impulsa de forma importante la economía y competitividad colombiana pues la diversidad natural lo hace un destino turístico muy atractivo, pues cuenta con playas en los dos océanos más grandes del mundo, diversidad de ecosistemas que se encuentran en las cosas y en el fondo de los mares, además que cuenta con tres mil especies diferentes de peces, millones de bosques, hectáreas, sabanas, zonas áridas, lagos, humedales.

Lo más impactante es que: “El 14 % del territorio nacional es área protegida en las que se encuentran parques nacionales, parques naturales y santuarios. Los datos y las cifras encontradas alrededor de la naturaleza de Colombia no dejan de sorprender: Contamos con el 20% de especies de aves en el mundo, el 17 % de anfibios, el 8% de peces dulceacuícolas, el 8 % de reptiles, el 16 % de mariposas diurnas y el 10 % de mamíferos entre otros”[69]

Ahora bien, el alcance de las Tics en el sector turístico colombiano es evidente según el estudio hecho en el año 2016 que se pueden visualizar en la figura 2.

En general se observa el manejo de las tecnologías en las Agencias de viajes, en lo que tiene que ver con la tenencia de página web se puede analizar que en el total de las agencias el 54% afirmaron que si cuentan con esta página web mientras que las Agencias de la Asociación Colombiana de Agencias de Viajes y Turismo se

[68] FANDIÑO, Jesús Rafael. Marketing digital en las empresas de Turismo de Naturaleza del Departamento de Magdalena. [En Línea]. Articulo. Universidad Nacional Abierta y a Distancia. Santa Marta. (Consultado el 6 de mayo de 2021). Disponible en internet: https://www.researchgate.net/publication/330295536_Marketing_digital_en_las_empresas_de_Turismo_de_Naturaleza_del_Departamento_de_Magdalena

[69] Ibid 15 p 291

obtuvo un porcentaje del 86% lo que indica que estas agencias cuentan con la página web mientras que el 14% restante optaron por la opción no.

De acuerdo con el segundo ítem de las redes sociales y su grado de utilización, en el total de las agencias 79% opto por la opción si mientras que el 21% restante se inclinó por la opción de no utilizar las redes sociales, en las Agencias ANATO por su parte el 82% se inclinó por la opción si y el 14% opto por la opción de no utilizar las redes sociales.

Se presenta otro aspecto y es el que se relaciona con servicios que se prestaron en las páginas web, se puede observar que en el total de Agencias los cuatro aspectos que más presentaron porcentaje son que es utilizada para la venta de paquetes con el 48%, informativo 43%, reserva no aérea el 32%, la venta de tiquetes de tipo aéreo con el 24%, de igual manera en las Agencias ANATO se obtiene que también son utilizadas en estos cuatro aspectos prioritarios variando un poco en los porcentajes obtenidos de cada ítem.

Figura 7. Tecnología en las Agencias de Viajes

Fuente: FANDIÑO, Jesús Rafael. Marketing digital en las empresas de Turismo de Naturaleza del Departamento de Magdalena. [En Línea]. Articulo. Universidad Nacional Abierta y a Distancia. Santa Marta. (Consultado el 6 de mayo de 2021). Disponible en internet: https://www.researchgate.net/publication/330295536_Marketing_digital_en_las_empresas_de_Turismo_de_Naturaleza_del_Departamento_de_Magdalena

4.3.12 Métodos de protección de ciberseguridad

En todo proceso de Ciberseguridad se debe pasar por las siguientes fases:

La primera es proteger todas las superficies de ataque: “En la práctica, proteger aplicaciones en la nube basadas en SaaS, como Office 365, requiere una solución completa diseñada para gestionar de forma centralizada esas redes híbridas”[70]

De igual forma corresponde a las empresas capacitar a los usuarios a que aprendan a protegerse de ciberataques, guardar información que sea sensible, detectar emails falsos, comprobar las fuentes, la utilización y configuración correcta de contraseñas, mantener los sistemas actualizados, certificados de seguridad, buenas soluciones de copias de seguridad, etc.

4.3.13 Plataforma integral de ciberseguridad

Es necesario que en las empresas de turismo colombianas se desarrollen plataformas integrales de seguridad que permitan generar ventajas competitivas pues se puede conocer a más detalle las necesidades de los clientes y brindarles la mejorar asesoría en el momento que lo requieran con una plataforma y conectividad seguras.

De esta manera para que esta plataforma sea efectiva para las organizaciones de turismo: “Debe contar con una social wifi, ser visible en la red durante todo el tiempo, contar con unas administraciones sencillas en la red, un acceso a wifi que sea seguro y rápido, también poseer una analítica de presencia” [71]

---

[70] RAMOS, Camino. La Ciberseguridad de los datos en mi Hotel. 2021. En: Entorno Turístico. 21 de enero de 2021. Sec.3. p.3. Disponible en internet: https://www.entornoturistico.com/la-ciberseguridad-de-los-datos-en-mi-hotel/

[71] Ibid. 44. p 1

4.4 MARCO HISTÓRICO

Es una realidad que los medios de comunicación de Colombia no le dan un despliegue significativo a los ataques cibernéticos que ha sufrido esta nación a lo largo de las últimas décadas, aunque las circunstancias sean de este tipo se ha reportado que diariamente se presentan ciberataques de formas pasivas y activas abarcando un sinnúmero de entidades que se han afectado por estas circunstancias como las privadas, publicas, financieras, instituciones educativas lo que ha causado pérdidas millonarias debido a que no han previsto con antelación estas problemáticas.

Algunos casos que se han presentado en Colombia de ciberataques en los últimos años se describen a continuación:

En el ámbito internacional durante el año 2010 la guardia civil española desmantelo una de las más grandes redes de computadores de tipo “Zombie” que se conocía con el nombre de “BootNet Mariposa” que se encontraba compuesto por una cantidad de más de trece millones de direcciones IP que se encontraban infectadas y se distribuyeron alrededor del mundo aproximadamente en 190 países, Colombia no escapo a este ataque y ocupo el quinto lugar entre los países más afectados por este motivo, como se puede apreciar en la tabla.

Tabla 2. Top de 20 países afectados por BootNet Mariposa

País	%
INDIA	19.14
MÉJICO	12.85
BRASIL	7.74
COREA	7.24
COLOMBIA	4.94
RUSIA	3.14
EGIPTO	2.99
MALASIA	2.86
UCRANIA	2.69
PAKISTÁN	2.55
PERÚ	2.42
IRÁN	2.07
ARABIA SAUDÍ	1.85
CHILE	1.74
KAZAKHSTÁN	1.38
EMIRATOS ÁRABES UNIDOS	1.15
MARRUECOS	1.13
ARGENTINA	1.10
ESTADOS UNIDOS	1.05

Fuente: CAMACHO, Reinerio. Ciberseguridad y Ciberdefensa en Colombia. [En línea]. Articulo. Universidad Piloto de Colombia. Bogotá D.C.: 2013. (Recuperado el 04 de mayo del 2021) Disponible en: http://polux.unipiloto.edu.co:8080/00001172.pdf

"En el año 2011, el conocido grupo Anonymous atacó los sitios web del Ministerio de educación, Senado, Ministerio de Defensa, Presidencia de la República y el sitio de Juan Manuel Santos. En el año 2012, nuevamente este grupo se atribuye el ataque al sitio web de la policía"[72]

En el año 2016 por su parte la Registradora Nacional del Estado Civil sufrió un ataque unos días antes de que se realizará el plebiscito. Según noticias publicadas por el diario el Tiempo en el mes de julio de este mismo año, presento un reporte que, en Latinoamérica, Colombia ocupa el tercer lugar dentro de los países que ha presentado mayores ataques cibernéticos.

[72] Ibid. 9 p 4

Durante el periodo del 2014 al 2016 se recibieron cerca de 13.774 denuncias de violación a la ley 1273 de 2009, en el transcurso del año 2017 aumento este número a 15.565.

En el 2016 fueron capturados 18 personas de nacionalidad extranjera por delitos cibernéticos realizados en Colombia. Según el Centro Cibernético Policial y en alianza con la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), las denuncias más frecuentes son las del ciudadano común con un porcentaje 66% de los incidentes siendo una modalidad que afecta fuertemente a Colombia. `12 La estafa que más se presenta es la que se realiza a nivel de ofertas publicadas en una página web o plataformas ecomerce, estas denuncias son originadas por el incumplimiento del algunas de las partes involucradas en la compra del producto.73

4.5 MARCO LEGAL

El marco legal referente a la ciberseguridad es muy amplio en Colombia, a continuación, se incluye en la tabla algunas leyes y decretos que ha implementado el gobierno colombiano en esta materia.

Dentro de las leyes y Decretos que se encuentran vigentes en Colombia y que soportan la temática principal de esta monografía se pueden destacar:

Ley 527 de 1999

Mediante esta ley: “Se hizo la reglamentación del comercio electrónico, su uso y los accesos a los mensajes de datos, y las firmas digitales; además que se crearon las

[73] MARIN, Ana Milena. Estudio monográfico sobre casos más comunes de cibercrimen en las pymes colombianas. [En línea]. Monografía. Universidad Nacional Abierta y a Distancia UNAD. Bogotá. 2018. p. 19. Consultado el 6 de mayo de 2021. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/30322/1098663077.pdf?sequence=1&isAllowed=y

entidades que son llamadas de certificación y se dictaron otras disposiciones al respecto”[74].

Esta ley es fundamental pues reglamenta el marco jurídico integral que le brinda autorización a los mensajes de datos en las actividades que se realizan en el sector público y privado, información que normalmente es vulnerada por los ciber atacantes que ingresan a las organizaciones turísticas utilizando los medios electrónicos.

Decreto 2364 de 2012

En este decreto se: “Definen algunas características que benefician el uso de los medios electrónicos en mecanismos de autenticación se hace necesario reglamentar la firma electrónica para generar mayor entendimiento sobre la misma, dar seguridad jurídica a los negocios que se realicen a través de medios electrónicos, así como facilitar y promover el uso masivo de la firma electrónica en todo tipo de transacciones”[75]

El Decreto 2364 les brinda seguridad a los usuarios, en este caso los que adquieren servicios y viajes turísticos sobre la utilización de la firma electrónica que representa un medio de identificación electrónico tecnológico, flexible y neutro que se puede adecuar a las necesidades que presentan los usuarios en cuanto a la seguridad de la información de sus datos personales.

Decreto 1377 de 2013

El presente Decreto tiene como objeto: “Reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales”[76]

---

[74] Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. (18 de agosto de 1999). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

[75] Decreto 2364 de 2012. La firma electrónica y se dictan otras disposiciones. (22 de noviembre de 2012). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=50583

[76] Decreto 1377 de 2013. Proteccion de datos personales. (27 de junio de 2013). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Este decreto permite en general a todos los usuarios que presentan requerimientos ante las empresas, en especial los que solicitan información sobre planes turísticos y las respectivas solicitudes por medios electrónicos que se les protejan sus datos personales ante posibles amenazas y ataques que generen perdidas irremediables de los mismos. Al respecto se tienen en cuenta los avisos de privacidad, los datos públicos y sensibles, como también su trasferencia y transmisión.

Ley de Comercio Electrónico

Se establece la validez jurídica y probatoria de la información electrónica: "Se encuentra la definición y reglamentación del acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales"[77]

Esta ley se utiliza en la presente investigación porque reglamenta el acceso y el respectivo uso de los mensajes que se tramitan por comercio electrónico como los realizados por los usuarios de las empresas turísticas que normalmente envían sus documentos y firmas por estos medios que de no ser confiables pueden ocurrir perdidas que afecten su integridad económica y personal.

Ley 599 de 2000.

Esta ley: "Es penal e incluye aspectos como la violación que se hace de forma ilícita de las comunicaciones se relaciona indirectamente con los delitos informáticos"[78], en los artículos que se mencionan a continuación:

- Artículo 192. Trata la violación ilícita que se realiza de las comunicaciones.
- Artículo 193. Incluye el ofrecimiento, venta o compra de los instrumentos que son aptos para poder interceptar las comunicaciones privadas entre personas.
- Artículo 194. Determina la divulgación y empleo de los documentos que son de carácter reservado.

---

[77] Ley 527 de 1999. Comercio Electrónico. (1999). http://www.sice.oas.org/e-comm/legislation/col2.asp

[78] Ley 599 de 2000. Por la cual se expide el Código Penal. (24 de Julio de 2000). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

- Artículo 195. Accesos abusivos a los sistemas informáticos; derogado por el artículo 4 de la Ley 1273 de 2009
- Artículo 196. La violación ilícita de comunicaciones o la correspondencia que es de carácter oficial.

De acuerdo con esta Ley el acceso ilícito en las comunicaciones tiene efectos penales, esto ocurre cuando se generan accesos no autorizados a las cuentas o correos electrónicos de los usuarios que requieren información sobre planes turísticos, envían documentación y demás inquietudes por medios electrónicos, por eso es fundamental conocer las sanciones que estipula esta norma al respecto.

Ley 1266 de 2008 Habeas Data.

Por medio de la cual: "Se dictan las disposiciones generales del hábeas data y se hace la regulación del manejo de la información que se encuentra contenida en bases de datos personales, específicamente las de tipo financiero, crediticio, comercial, de servicios y la que proviene de terceros países"[79]

En relación con esta ley que regula el habeas data que es un derecho que tienen todas las personas de rectificar, actualizar y conocer la información que se encuentra en archivos y bases de datos en las organizaciones públicas o privadas vinculadas con el sector turístico, es importante para esta investigación pues los usuarios muchas veces desconocen estos derechos que regulan de una manera clara su información de carácter personal.

Ley 1273 de 2009.

Por medio de la cual: "Se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado" de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[80]

• Artículo 269A: Acceso abusivo a un sistema informático.

[79] Ley 1266 de 2008. Habeas data e información contenida en bases de datos personales. (31 de diciembre de 2008). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

[80] Ley 1273 de 2009. Por medio del cual se modifica el Código Penal. (5 de enero de 2009). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

• Artículo 269B: Obstaculización ilegitima de un sistema informático o red de telecomunicación.

• Artículo 269C: Intercepción de datos informáticos.

Con respecto a esta ley es fundamental para el desarrollo de este proyecto pues los usuarios de las empresas turísticas deben conocer que leyes los protegen en caso de que los ciber atacantes ingresen a sus medios electrónicos de forma ilícita y las penas que se encuentran determinadas que pueden tener prisión de cuarenta y ocho a noventa y seis meses y multas que oscilan entre 100 a 1000 salarios mínimos legales vigentes.

Ley 1480 de 2011

Esta ley tiene como objetivos: “Proteger, promover y garantizar la efectividad' y el libre ejercicio de los derechos de los consumidores, así como amparar el respeto a su dignidad y a sus intereses económicos”[81] en especial, lo referente a:

1. La protección de los consumidores frente a los riesgos para su salud y seguridad.

2. El acceso de los consumidores a una información adecuada, de acuerdo con los términos de esta ley, que les permita hacer elecciones bien fundadas

Esta ley es importante en el desarrollo de este proyecto debido a que les brinda protección y garantía a los consumidores, en este caso, los usuarios de las empresas turísticas de Colombia en cuanto al manejo de la información de una manera adecuada y el respeto a sus derechos y dignidad.

Ley Estatutaria 1581 de 2012 y reglamentada parcialmente por el decreto nacional 1377 de 2013. La presente ley tiene por objeto: “Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las

[81] Ley 1480 de 2011. Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones. (12 de octubre de 2011). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=44306#:~:text=Esta%20ley%20tiene%20como%20objetivos,para%20su%20salud%20y%20seguridad.

informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma"[82]

El objeto principal de estas leyes es que regulan las obligaciones y los derechos que se originan entre los consumidores, proveedores y productores, proveedores, sus responsabilidades, información que es fundamental para la realización de esta investigación pues todas las partes involucradas en los procesos comerciales de las empresas turísticas tienen sus derechos y obligaciones con respecto al acceso y seguridad de la información suministrada.

Legislación internacional

UNCITRAL (1985). "Recomendación sobre el valor jurídico de los documentos informáticos"[83]

UNCITRAL (1996). "Ley modelo sobre comercio electrónico"[84]

UNCITRAL (2001). Ley modelo de firmas electrónicas.

UNCITRAL (2005). "Convención de las naciones unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales"[85]

---

[82] Ley Estatutaria 1581 de 2012. Protección de datos personales. (17 de octubre de 2012). https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf

[83] CNUDMI. Naciones Unidas. (2013). Guía de la CNUDMI. Datos básicos y funciones de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/12-57494-guide-to-uncitral-s.pdf

[84] Ibid. 72.pag 24

[85] Ibid. 72. Pag 23

UNCITRAL (2007). “Documento de fomento de confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de auténticas y firmas electrónicas”[86]

Finalmente se incluyen algunas normas internacionales que se encuentran relacionadas con el comercio electrónico, las firmas electrónicas, marco jurídico, aspectos que son esenciales para este proyecto pues tanto los usuarios como los empresarios de turismo deben tener claro este marco legal, no solo a nivel nacional sino el que existe a nivel internacional para que puedan defender sus derechos ante vulnerabilidades de la información confidencial.

En relación con el marco legal relacionado con la temática de esta monografía se incluye en el Anexo B que se denomina: “Normativa Internacional relacionada con asuntos de seguridad digital”

[86] Ibid. 72. Pag.69

5 DESARROLLO DE LOS CAPÍTULOS

5.1 AMENAZAS Y RIESGOS CIBERNÉTICOS EN ADQUISICIÓN DE SERVICIOS TURÍSTICOS POR MEDIOS ELECTRÓNICOS

Este capítulo está encaminado a la identificación de las amenazas y riesgos cibernéticos asociados a la adquisición de servicios turísticos a través de medios electrónicos con el fin de efectuar un reconocimiento del estado actual en este sector de la economía.

5.1.1. Estadísticas de Comercio Electrónico en Empresas de Turismo Colombianas

Por ese motivo en el presente capitulo se incluyen informes y estadísticas del comportamiento del comercio electrónico en las empresas de turismo colombianas, de igual manera informes que se han presentado por entidades de policía y la incidencia de los ciberdelitos que más se han presentado en el sector turismo de Colombia.

Para empezar, se incluye la información de un artículo publicado por la Cámara de Comercio de Bogotá en el que se asegura que el turismo mueve más de un billón de pesos en comercio electrónico en Colombia: “Según un informe publicado por Place To Pay que es conocida como una de las más famosas pasarelas para realizar pagos y que tiene una cobertura mundial en agencias de viajes como Atrápalo, Aviatur, entre otras, se afirma que este sector logro un posicionamiento significativo lo que aporte positivamente al crecimiento económico en Colombia en lo relacionado al comercio electrónico”[87]

[87] CÁMARA DE COMERCIO DE BOGOTÁ. [sitio web]. Bogotá: CCB. El turismo mueve más de $1 billón en comercio electrónico en el país. [12-03-2021]. Disponible en: https://www.ccb.org.co/Clusters/Cluster-de-Turismo-de-Negocios-y-Eventos/Noticias/2017/Marzo-2017/El-turismo-mueve-mas-de-1-billon-en-comercio-electronico-en-el-pais

”.[88]

Según estadísticas que se presentaron durante el año 2016, Place To Pay es una pasarela que ha obtenido millonarias ganancias que se encuentran vinculadas con el sector turístico, estas originadas por el uso de medios de pago como PSE, MasterCard y Visa con las que se pueden efectuar transacciones comerciales por internet desde las cuentas de ahorros y las corrientes de los usuarios.

Es de anotar que el factor fundamental para este crecimiento del sector turístico han sido las transacciones hechas por las plataformas de pago lo que aumenta la eficacia del comercio electrónico para este tipo de reservas pues se tiene estimado que durante al año 2016 la Compañía Place to Pay uvo un crecimiento del 55% debido al número de transacciones que se realizaron desde la pasarela de pagos.

El primer informe fue publicado por la Asociación Colombiana de Ingenieros de Sistemas durante el año 2015 en el que se especifica que la hotelería y turismo ocupa el tercer sector de los más afectados por ataques de tipo informático.

Es una realidad que este sector alberga una gran cantidad de información que es sumamente atractiva para los ciberdelincuentes que pueden robar datos, ransomware o los ataques DDoS con los cuales se hace denegación de los servicios entre otros.

> Dentro del sector turístico, el delito más frecuente es el robo de información, con especial interés en los datos financieros y la vía más habitual para hacerlo son las redes Wi-Fi no protegidas. Los hoteles suelen ser una de las víctimas más frecuentes de las estafas, y las ofertas falsas representan el 40% de los fraudes en este ámbito, de esta forma la ciberdelincuencia y los fallos informáticos se han colocado por primera vez, entre las cinco mayores preocupaciones de las empresas en todo el mundo, según el Barómetro del Riesgo 2015 de Allianz Global.[89]

El segundo informe corresponde a las amenazas del Cibercrimen en Colombia presentado durante el periodo 2016 y 2017 del centro cibernético de la policía, dentro de la caracterización que hacen del Cibercrimen incluyen como quinta causa

[88] Ibid. 28.p.1

[89] Ibid.. 7. p 5

de este delito la vinculación cada vez más frecuente de ciudadanos extranjeros en las organizaciones criminales con injerencia en Colombia.

En las entidades financieras los fraudes en los cajeros automáticos tipo ATM en Colombia es el más usado por los ciberdelincuentes, su modo de operar es que realizan copias de los chips o bandas magnéticas a las tarjetas débito o crédito, pudiendo retirar dinero y realizar compras con estas tarjetas.

Esta modalidad conocida como skimming:

> Registró 84 incidentes en el 2016, y 23 en lo corrido del año 2017, teniendo una creciente injerencia de bandas internacionales de países como Rumania, que llegan a Colombia, principalmente a ciudades con gran afluencia de turistas, instalan dispositivos de alta tecnología con microcámaras, micrófonos y otros elementos en cajeros electrónicos, que permite almacenar la información y posteriormente ser magnetizada[90]

.

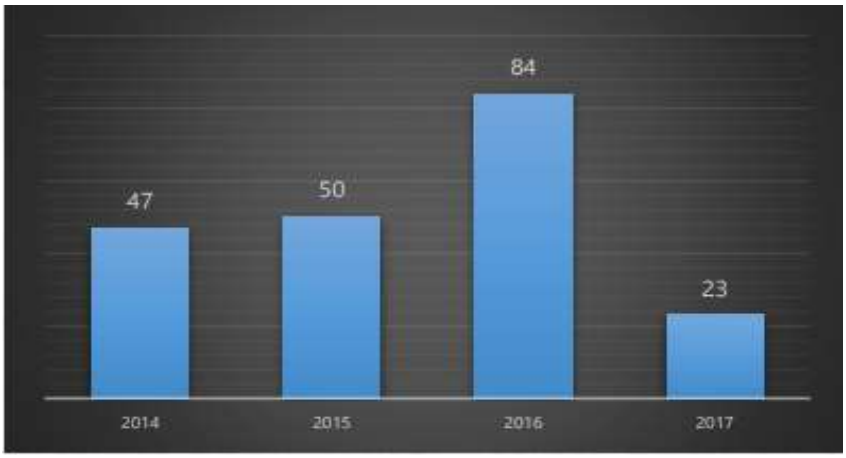
Durante los últimos años se ha notado la presencia de manera frecuente de delincuentes provenientes del extranjero en Colombia que tienen conocimientos sobre técnicas utilizadas en países de Europa del Este: “Según datos que reposan en el CCP, dichos delincuentes traen malware sofisticado y programas maliciosos que en algunos casos llegan incluso a controlar remotamente los computadores de directivos o ejecutivos de áreas financieras, tesorerías y contables de las organizaciones afectadas”[91]

---

[90] CAI VIRTUAL. Informe Amenazas de Cibercrimen en Colombia 2016-2017. [Sitio WEB]. Bogotá D.C. CAI. [6 de mayo de 2021]. Disponible: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

[91] INFOLAFT. Cibercrimen en Colombia. Todo lo que debe saber. [Sitio WEB]. Colombia. Infolaft. [6 de mayo de 2021]. Disponible: https://www.infolaft.com/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia/

Figura 8. Delitos Cibernéticos skimming durante el periodo 2014 – 2017



Fuente: CAI VIRTUAL. Informe Amenazas de Cibercrimen en Colombia 2016-2017. [Sitio WEB]. Bogotá D.C. CAI. [6 de mayo de 2021]. Disponible: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Así mismo, en el Informe de tendencias de cibercrimen en Colombia en el periodo 2019-2020 presentado por la Policía Nacional de Colombia, se puede analizar que los cibercriminales están utilizando inteligencia artificial enviando videos y audios a las organizaciones y haciendo suplantaciones de proveedores, clientes y ejecutivos con el fin de ejecutar transferencias de tipo monetario.

Las plataformas del gobierno también se han visto afectadas por estos cibercrímenes con el envío de correos falsos.

Esto ha afectado a organizaciones estatales como la DIAN, la Fiscalía General de la Nación, el SIMIT (tránsito), etc. Así, los delincuentes han logrado que los ciudadanos descarguen archivos (malware) que les permiten acceder a los equipos para sustraer, secuestrar o destruir información. Por esta tendencia, en 2018 y 2019, altos funcionarios del gobierno de Colombia y de la Organización del Tratado del Atlántico Norte (OTAN) se reunieron para abordar el tema de la Ciberdefensa y la ciberseguridad. [92]

[92] SCIELO. Revista Criminalidad. [En línea]. Bogotá. 2020. [Consultado el 06 de mayo del 2021] Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=es&nrm=iso&tlng=es#B75

Las organizaciones del Estado no se encuentran en buenas condiciones en relación a la seguridad digital, teniendo en cuenta los diferentes sectores donde se encuentran, pues sus calificaciones promedios durante los años 2018 y 2019 fueron de 74,2% y 77.8%, aunque algunos de los sectores del gobierno si han registrado calificaciones que son mayores a 80 esto según el Reporte de Resultados Sectoriales de Desempeño Institucional Nación sobre seguridad digital en el Formulario Único Reporte de Avances de la Gestión -FURAG-, en el marco de Modelo Integrado de Planeación y Gestión –MIPG, estos resultados se pueden apreciar en la tabla.

Tabla 3. Resultados desempeño en seguridad digital (2018-2019) en entidades estatales por sector

Sectores Gobierno Colombia	Puntaje promedio por sector 2018	Entidades consultadas	Puntaje promedio por sector 2019	Entidades consultadas
Relaciones Exteriores	87	2	89,4	2
Comercio, Industria y Turismo	82	9	82,7	9
Tecnologías de la Información y las Comunicaciones	81	6	76,1	7
Presidencia de la Republica	81	5	79,9	5
Ciencia, Tecnología e Innovación	79	1	82,6	1
Planeación	79	4	83,9	4
Hacienda y Crédito Público	79	18	84	18
Educación	78	10	86,4	10
Inclusión Social y Reconciliación	75	4	83	4
Función Pública	74	2	70,6	2
Defensa	74	16	79,7	17
Justicia y Derecho	74	5	77,1	5
Ambiente y Desarrollo Sostenible	74	4	79,2	4
Minas y Energía	74	6	77,1	6
Vivienda, Ciudad y Territorio	73	3	81,1	3
Salud y Protección Social	73	9	77,5	10
Trabajo	72	6	78,2	6
Estadísticas	70	2	67,7	2
Agropecuario, Pesquero y de Desarrollo Rural	69	13	72,6	13
Cultural	67	4	71,5	4
Del Deporte, la Recreación y el Aprovechamiento del Tiempo	65	1	57,4	1
Transporte	65	7	79,4	6
Interior	61	6	71,5	6
Total	**74,2**	**143**	**77,8**	**145**

Fuente: SCIELO. Revista Criminalidad. [En línea]. Bogotá. 2020. [Consultado el 06 de mayo del 2021] Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=es&nrm=iso&tlng=es#B75

En la tabla anterior se puede observar que el Comercio, Industria y Turismo tuvo un puntaje promedio en el año 2018 de 82 y durante el año 2019 aumento a 82.7 lo que significa que se ha mejorado en la seguridad digital en estos sectores del Estado, este fenómeno puede ser debido a que han ido aumentando las normas y la preocupación del gobierno por contrarrestar los cibercrímenes y utilizando estrategias como el Programa Agenda Estratégica de Innovación mostrando que la ciberseguridad se ha convertido en un elemento prioritario para proteger los activos y recursos de la nación.

En este sentido, también se incluye la información publicada en un artículo titulado "Ciberseguridad en Colombia" en el año 2018 en el que se puede evidenciar que dentro de los delitos informáticos y de comercio electrónico que se presentan en el sector turístico se encuentran las estafas por internet:

Según la policía el 55.3% de incidentes atendidos por el @caivirtual fueron estafas en internet, siendo el de mayor afectación a los colombianos, entre las modalidades que más se impactó generaron se destacan compra y venta de productos en internet, estafas a través de llamadas telefónicas, smishing (estafas a través de mensajes de texto SMS o chats de WhatsApp), cartas nigerianas (promesas de herencias o recompensas a través de correos electrónicos y paquetes turísticos (engaños en el alquiler de sitios de esparcimiento, generalmente en temporada de vacaciones).[93]

Los valores que se han recolectado con estas estafas se encuentran entre 500.000 y 20.000.000 de pesos, actualmente estas cifras ascienden a 15 mil millones de pesos con un reporte de fraudes de 6372 como se puede observar en la Figura 9.

[93] UNIPILOTO. Ciberseguridad en Colombia. [En línea]. Articulo. Universidad Piloto de Colombia. Bogotá. 2018. P.12.Consultado el 23 de septiembre del 2021. Disponible en internet: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

Figura 9. Porcentaje de Estafas

Fuente: UNIPILOTO. Ciberseguridad en Colombia. [En línea]. Articulo. Universidad Piloto de Colombia. Bogotá. 2018. P.12.Consultado el 23 de septiembre del 2021. Disponible en internet: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

En definitiva, los accidentes de ciberseguridad en el sector turístico colombiano han ido creciendo en los últimos cinco años, afectando empresas públicas y privadas, destacándose las formas cibercriminales como skimming, fraudes en cajeros automáticos, copias de chips o bandas magnéticas de tarjetas debido o crédito y correos falsos.

5.1.2. Amenazas de Ciberseguridad del Comercio Electrónico en Empresas de Turismo Nacionales e Internacionales

Dentro de las vulnerabilidades se encuentra las filtraciones o pérdidas de información lo que trae consecuencias muy graves para estas empresas que les generan problemáticas en la parte económica y legal, también les ocasiona sanciones y multas por los incumplimientos de las leyes y normas relacionadas con la protección de los datos, además que se desmejora considerablemente la imagen y reputación disminuyendo la demanda de clientes.

Las pérdidas de información se producen debido a que no se crean copias de seguridad por lo que no se pueden obtener respuestas rápidas en casos de contingencias graves.

Otra amenaza es no contar con un cifrado de la información lo que también trae como consecuencia que los ciber atacantes logren una difusión no autorizada de la información, manipulándola a su antojo.

Aun así, muchas veces el cifrado de información es insuficiente, es una realidad que no es muy útil cuando el acceso a los sistemas se obtiene por otros medios, pues este cifrado se logra resolver cuando se presenten los siguientes inconvenientes:

"El acceso físico no autorizado, pérdida o robo de los dispositivos móviles incluyendo computadoras portátiles, unidades USB y otros medios de comunicación. Este es un caso de uso excelente para el cifrado, puesto que la relación costo/beneficio es sesgada hacia el beneficio"[94]

También el realizar manejo de la información y copias de seguridad que están en movimiento constante. Este es un caso conveniente para aplicar el cifrado, pues los backups hacen desplazamientos geográficos desde un emplazamiento a otros lo que significa que ante menores descuidos pueden caer en cualquier momento en manos criminales.

En cuanto a la gestión de contraseñas normalmente en estas empresas se crean de una forma rápida y no se percatan que deben ser contraseñas fuertes y que se debe crear una diferente para cada servicio o requerimiento que los usuarios soliciten, tampoco disponen de una doble autenticación para los servicios como los perfiles de usuarios y aplicaciones.

Figura 10. Contraseñas que no se deben utilizar

[94] WELIVESECURITY. Cuando el Cifrado de Datos no es Suficiente. [Sitio WEB]. Welivesecurity. [16 de mayo de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2014/06/30/cuando-cifrado-de-datos-no-es-suficiente/

Fuente: OSI. Aprende a Gestionar Contraseñas. [Sitio WEB]. Unión Europea. [16 de mayo de 2021]. Disponible en: https://www.osi.es/es/contrasenas

El problema de utilizar contraseñas débiles es que existen infinidad de programas que se diseñaron para hacer pruebas de millones de contraseñas por minuto, en la tabla 4 se puede observar el tiempo que se demoran estos programas en averiguar las contraseñas todo teniendo en cuenta las longitudes y números de caracteres con las que cuentan.

Un caso particular de vulneración de las contraseñas se presentó en una campaña de malware que: “Infecto a más de 20 cadenas hoteleras de Brasil, poniendo en riesgo los datos de las tarjetas de crédito de numerosos clientes, afectando a hoteles en Estados Unidos, Portugal, México, Argentina, Bolivia, Chile, Costa Rica y Colombia”[95]

En este caso los datos de las tarjetas de crédito de los viajeros que se encuentran en las administraciones de los hoteles y en las agencias de viajes corrieron el riesgo de ser vendidos y robados por los delincuentes. Otra de las campañas destacables en este sentido es la RevengeHotels: “Es un tipo de campaña que se encuentra activa desde el año 2015 e incluye distintos grupos de troyanos que efectúan accesos remotos tradicionales para poder infectar a las empresas del sector hotelero”[96]

[95] ITECHSAS. Ciberataque a la industria hotelera. [Sitio WEB]. Itechsas. [02 de agosto de 2022]. Disponible en: http://www.itechsas.com/blog/malware/ciberataque-a-industria-hotelera-en-varios-paises/

[96] Ibid. 88.p.1

Este ataque se centró en actuar sobre los correos electrónicos de los usuarios con documentos maliciosos en formatos pdf, Word y Excel, ejecutando RATs y malwares en los computadores de las víctimas y así poder acceder a todos sus archivos desde la distancia.

Por este motivo surge la necesidad de fortalecer las políticas de contraseñas en este país pues los ciber atacantes con el paso del tiempo se vuelven más sofisticados y utilizan métodos eficaces para ingresar sin permiso a los correos electrónicos de los usuarios de las empresas turísticas.

Las recomendaciones que se pueden sugerir para obtener más seguridad y contraseñas seguras los usuarios de los hoteles y agencias de viajes deben utilizar tarjetas de pagos virtuales para efectuar sus reservaciones realizadas a través de OTA, pues este tipo de tarjetas tienen una caducidad de un solo cobro.

También cuando realicen pagos por una reservación o al hacer el checkout en la recepción del hotel, es conveniente que usen una billetera virtual, como Apple Pay o Google Pay, o tarjetas de crédito secundarias que contengan solo el monto de dinero que se necesita para realizar la transacción.

De igual manera los gerentes y propietarios de los hoteles también deben seguir estos pasos para poder proteger los datos de sus clientes.

Realizar evaluaciones de riesgos y vulnerabilidades a la red de equipos, servidores y comunicaciones existentes. Evaluar e implementar regulaciones relacionadas sobre protección de datos personales y cómo se manejan los datos de los clientes por parte de funcionarios. Utilizar una solución de seguridad confiable con protección web y funcionalidad de control de aplicaciones. La protección web ayuda a bloquear el acceso a sitios web maliciosos y de suplantación de identidad (phishing), mientras que el control de aplicaciones (en modo de lista blanca) permite asegurarse de que ninguna aplicación, excepto las de la lista blanca, pueda ejecutarse en las computadoras de la recepción de los hoteles.[97]

Tabla 4. Tiempo en que Programas demoran en descifrar contraseñas

[97] Ibid. 88. p1

Longitud	Todos los caracteres	Sólo minúsculas
3 caracteres	0,86 segundos	0,02 segundos
4 caracteres	1,36 minutos	0,46 segundos
5 caracteres	2,15 horas	11,9 segundos
6 caracteres	8,51 días	5,15 minutos
7 caracteres	2,21 años	2,23 horas
8 caracteres	2,10 siglos	2,42 días
9 caracteres	20 milenios	2,07 meses
10 caracteres	1.899 milenios	4,48 años
11 caracteres	180.365 milenios	1,16 siglos
12 caracteres	17.184.705 milenios	3,03 milenios
13 caracteres	1.627.797.068 milenios	78,7 milenios
14 caracteres	154.640.721.434 milenios	2.046 milenios

Fuente: OSI. Aprende a Gestionar Contraseñas. [Sitio WEB]. Unión Europea. [16 de mayo de 2021]. Disponible en: https://www.osi.es/es/contrasenas

Así mismo: “Una vulnerabilidad que es recurrente en el sector turístico es no actualizar las aplicaciones y el software lo que les hace blanco fácil de los ciberataques pues se pierde fácilmente la privacidad de la información y datos personales que se manejan de los clientes convirtiéndose en un problema grave de seguridad” [98]

Esta vulnerabilidad se convierte en una amenaza grave para las empresas pues los ciber atacantes se provechan de los posibles fallos que pueden surgir de seguridad y de sistemas operativos que no se encuentran actualizados o programas que manejen las agencias de viajes que cuentan con las últimas versiones, es un hecho que este problema es muy recurrente y no se le da la importancia que debe tener.

Cualquier tipo de sistemas operativos que son obsoletos y se encuentran desactualizados y sin soporte de los fabricantes, de igual manera las herramientas de ofimática, aplicaciones que se utilizan en informática y los softwares de la web o

[98] OSI. Aprende a Gestionar Contraseñas. [Sitio WEB]. Unión Europea. [16 de mayo de 2021]. Disponible en: https://www.osi.es/es/contrasenas

las apps que se bajan al celular para obtener información sobre planes turísticos son un blanco y amenazas para los fallos se seguridad.

Los ciberdelincuentes aprovechan estos agujeros para intentar introducirse en nuestros sistemas y así:

Obtener información sensible y confidencial de nuestra empresa, como cuentas de acceso a otros servicios o bases de datos de clientes o de facturación, cifrar la información del servidor y solicitar un «rescate» por ella, el tan mencionado ransomware, desconfigurar los sistemas de seguridad de la compañía para espiarnos, robar información o atacarnos más adelante y usar nuestros sistemas como plataforma de ataque hacia otros sistemas[99]

Dentro de las vulnerabilidades y amenazas en el sector turístico también se encuentran la carencia en la realización de segmentaciones y monitorizaciones de la red de una forma continua, teniendo en cuenta de antemano en que consiste un monitoreo de red pues este procedimiento permite la aplicación de un sistema de monitorización continua de la red y sus ordenadores buscando componentes que los hacen más lentos y que efectúen su trabajo de forma defectuosa, finalmente genera informes a los administradores de las redes que utilizan comercio electrónico[100]

Si las empresas de Turismo colombianas no cuentan con un software de monitoreo de red se someten a no contar con:

- Comunicación de las alertas.
- Integraciones con servidores externos.
- Usabilidad y presentación de los datos en el panel.

---

[99] INCIBE. Consecuencias de no actualizar tus sistemas. [Sitio WEB]. INCIBE. [16 de mayo de 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/consecuencias-no-actualizar-tus-sistemas-conficker

[100] TOKIO SCHOOL. Características principales del monitoreo de red. [Sitio WEB]. Tokio School. [22 de mayo de 2021]. Disponible en: https://www.tokioschool.com/noticias/caracteristicas-principales-monitoreo-red/

- Flexibilidad a la hora de adaptarse a herramientas o software particulares.
- API de acceso desde sistemas externos.
- Detección de dispositivos de forma automática.
- Integraciones con Bases de Datos.
- Multidispositivo.
- Escalado.
- Soporte del mayor número de protocolos de adquisición de datos posible.
- Seguridad.
- Integración con máquinas virtuales.
- Integraciones hardware.
- Control remoto.
- Inventario de Hardware y Software.
- Geolocalización.
- Monitorización de la nube.

Otra debilidad es la no secularización de accesos remotos de empleados y clientes, los viajeros de negocios son muy vulnerables a un ataque cibernético esto debido a que están utilizando sus dispositivos personales para manejar información de las empresas y acceden a conexión de internet wifi-públicas. Así las cosas, los ciber atacantes están al acecho sobre todo cuando se encuentran trabajando directamente en el aeropuerto, se puede caer en una red malintencionada lo que produciría el robo de información confidencial de las empresas turísticas.[101]

5.1.3. *Peligros de Utilizar Redes Públicas Wifi*

Cuando se realiza el acceso a una red pública wifi existe la posibilidad en gran porcentaje de ser víctimas de un ataque cibernético, riesgos de seguridad y amenazas en la privacidad de los datos personales. Entre los ataques más comunes en este tipo de amenaza se encuentran:

Figura 11. Peligros de Utilizar Redes Públicas Wifi

[101] Ibid 93 p1

Fuente: PASTOR Javier. Porque es Peligroso Conectarse a Wifi Publicas y que debes hacer para protegerte. [Sitio WEB]. Xataca México. [22 de mayo de 2021]. Disponible en: https://www.xataka.com/seguridad/por-que-es-peligroso-conectarse-a-wifis-publicas-y-que-debes-hacer-para-protegerte

1. **Ataques Man in the Middle (MitM)**: “El ciberatacante puede lograr "colarse" en nuestras comunicaciones entre nuestro ordenador o móvil y el otro extremo de esas transferencias de datos, lo que básicamente hará que pueda "leer" todos los datos transmitidos entre ambos extremos”[102]

2. **Redes no cifradas**: Es de aclarar que, algunas veces, los puntos de acceso pueden haber sido configurados con el objetivo de cifrar las transferencias que se hacen de los datos de las personas que se conectan, normalmente los routers no cuenta con esa opción y que se encuentre activa, esto pone en peligro las comunicaciones que hagan los usuarios pues pueden ser objeto de cotilleos de los ciber atacantes.[103]

---

[102] PASTOR Javier. Porque es Peligroso Conectarse a Wifi Publicas y que debes hacer para protegerte. [Sitio WEB]. Xataca México. [22 de mayo de 2021]. Disponible en: https://www.xataka.com/seguridad/por-que-es-peligroso-conectarse-a-wifis-publicas-y-que-debes-hacer-para-protegerte

[103] Ibid 93.p1

3. **Distribución de malware**: A las redes públicas puede acceder cualquier persona, por eso los ciberdelincuentes se pueden infiltrar en estas utilizándolas como herramienta para llenar los dispositivos de los usuarios de malware contagiosos.

4. **Shopping y sniffers**: “Este tipo de técnicas permiten también infiltrarse en las transmisiones de datos que estamos realizando para capturar toda esa información y registrarla. Este tipo de herramientas hacen posible que un atacante pueda descubrir nuestras contraseñas y claves para entrar en redes sociales o realizar operaciones bancarias”[104]

5. **Redes WiFi públicas falsas**: Los viajeros y turistas que se instalan en un hotel o restaurante suelen conectarse a redes wifi de estos sitios, pero en realidad son redes falsas que los ciberatacantes aprovechan para lograr infiltraciones en las comunicaciones y acceder a todos los datos que se encuentran en los portátiles o teléfonos móviles de estas personas.

Otra de las debilidades que deben afrontar las empresas de turismo colombianas es el percatarse de que sus proveedores también tengan implementado un plan en este sentido, pues en caso de no contar con protocolos para proteger los activos digitales de estas empresas se puede tener un acceso fácil para los ciber atacantes.

Si las empresas de turismo dentro de sus planes de ciberseguridad no incluyen a los proveedores, transportistas y agentes externos a la organización se pueden presentar casos de ciberataques que utilicen estos agentes accediendo a la información confidencial de los clientes, turistas y personal involucrado. Esto produce inseguridad en los procesos llevados a cabo tanto interna como externamente de las organizaciones, incluyendo a clientes y su fidelización.

Por otra parte, es importante incluir como se encuentra la situación de riesgos cibernéticos a nivel internacional por este motivo se incluye la información publicada por la Hosteltur de España sobre los ciberataques que se han presentado en las empresas turísticas, según el centro de seguridad industrial presenta estadísticas

[104] Ibid. 41.p 1.

que establecen que más del 50% de los ataques cibernéticos pueden ocasionar interrupciones prolongadas hasta de cuatro horas, tiempo en el cual los delincuentes pueden generar daños importantes en las bases de datos y archivos de las empresas.[105]

Cabe apuntar que un 22% de los ciberdelitos puede durar entre 4 a 24 horas mientras que en un 18% de los casos puede quedar parada una entidad durante más de un día, esto lo explicó José Valiente, responsable de coordinación de la citada institución.

Dentro de los delitos informáticos que pueden presentarse con más recurrencia en las empresas turísticas se encuentran las denegaciones de servicio, los cifrados de información y sabotajes que utilizan los correos electrónicos: “A través de correos electrónicos y de internet pueden introducirse virus informáticos que, tras permanecer latentes un tiempo, atacan al cabo de semanas o meses, llegando a infiltrarse en los sistemas industriales de una empresa, tal como explicó Valiente, que expuso casos reales sucedidos en España”[106]

Según Font (2000): “Es indudable que la vulnerabilidad de los datos en los medios informáticos es una de las principales preocupaciones al realizar transacciones de servicios de Internet por la vulneración de los sistemas de seguridad, por el acceso indebido a información y la introducción de virus informáticos”[107]

Algunas de las vulnerabilidades que se presenta frecuentemente en el uso del internet están asociadas con hechos relacionados con la protección de la información que sufre desapariciones o alteraciones de los datos, los accesos a textos escritos, plagio de imágenes o sonidos y los derechos de la propiedad intelectual.

---

[105] Ibid 97 p1

[106] Ibid. 40. p 1

[107] VARGAS RAMIREZ, Claudia Marcela. El comercio electrónico: estrategia para la incursión de las empresas colombianas en el mercado internacional. [En Línea]. Ensayo. Universidad de la Salle, Bogotá: 2011. [Consultado del 21 de julio de 2022]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/3623/VargasRamirezClaudiaMarcela2011.pdf?sequence=2&isAllowed=y

Los conocidos sabotajes informáticos tienen el objetivo de: “Paralizar las actividades laborales o suspenderlas a través de su desaparición o destrucción de la respectiva información que se tiene en los soportes, bases de datos o equipos”[108]

En lo que respecta a los delitos contra la propiedad intelectual incluye a los actos que son de carácter lucrativo o no, como los que tienen que ver con el plagio, distribución y la reproducción de ataques informáticos que violan los derechos de los autores y que se encuentran relacionados con obras expedidas por estas sin sus autorizaciones.

Otra de las vulnerabilidades que presentan los usuarios de las empresas de turismo es el plagio que se hace de sus imágenes, las cámaras que se utilizan en las agencias de publicidad o las que poseen las personas en sus celulares pueden ser víctimas de espionaje: “De nada sirven luces LED que indican si la webcam está encendida o apagada. Si se es víctima de un hacker este puede utilizar un código malicioso que desactive la luz LED y así espiar sin ser detectados”[109]

5.1.4. Estafas por WhatsApp y Chats

Según un artículo publicado en el año 2018 por Hosteltur indica que se han realizado estafas masivas en el turismo utilizando vías como el WhatsApp y el internet, un caso particular es el presentado en España por un grupo que se dedica a la comisión de estafas masivas que efectúan en el internet, lo que ha generado 348 víctimas en toda la geografía nacional: “Dentro de los servicios que ofrecían se encuentran entradas para conciertos musicales, de ocio y encuentros de fútbol de primera

[108] GNZO. Tipos de delitos informáticos. [Sitio WEB]. La Rioja. [2021]. Disponible en: https://ginzo.tech/blog/tipos-delitos-informaticos/

[109] ARATECNIA. Seguridad Informática en el internet de las cosas. [Sitio WEB]. Zaragoza. Cedase. [29, marzo, 2015]. Disponible en: https://aratecnia.es/webcams-vulnerables/

división, así como el alquiler de inmuebles en zonas de playa y residenciales para vacaciones”[110]

Su operación de engaño iniciaba con el jefe del grupo quien realizaba publicaciones en las correspondientes páginas web de supuestos productos y ofertas, brindando a los posibles clientes teléfonos móviles donde podían comunicarse o por WhatsApp, así tenían contacto con las posibles víctimas generando una mayor confianza, establecían también la fianza y los términos en que se debía hacer la venta que era ingresada en las cuentas corrientes por medio de giros bancarios. Una vez que confirmaban los ingresos, retiraban los dineros de las cuentas y cancelaban las respectivas cuentas.[111]

Otra estafa que se presentó en Colombia estuvo vinculada con una estafa que se efectúa de manera virtual cuyo modo de engaño lo hacen por medio de: “La clonación de los perfiles del chat de Facebook y de Messenger de las víctimas, luego les escriben a los posibles contactos pidiendo una falsa ayuda para poder enviar unos pedidos a Colombia, también suplantaban el proceso con los bancos, autoridades de la aduana y aerolíneas”[112]

Este tipo de fraudes se hicieron a nombre de Avianca por medio de comunicaciones vía chat de los estafadores conversaban con las posibles víctimas por medio de perfiles falsos haciéndoles creer que son familiares lejanos o amigos, el hecho es que compartían guías aéreas falsas de esta empresa en las cuales aparecía un número de teléfono donde los usuarios se podían contactar y en el cual contestaba otro estafador que se hace pasar por funcionario de esta aerolínea convenciendo a los usuarios de girar una cantidad de dinero a una persona natural, las victimas hacen los pagos y al tratar de retirar el giro se percataban que tanto la guía como la carga a su nombre son falsas, al tratar de comunicarse de nuevo con el número del recibo, se encuentra cancelado y el giro fue reclamado por otra persona.

---

[110] HOSTELTUR. Así funcionan las estafas masivas en turismo: por internet y WhatsApp. [Sitio WEB]. Madrid. INCIBE. [03, agosto, 2022]. Disponible en: https://www.hosteltur.com/128292_asi-funcionan-estafas-masivas-turismo-internet-whatsapp.html

[111] Ibid. 99. P1

[112] INFOBAE. El método de estafa virtual que amenaza a los colombianos en el exterior. [Sitio WEB]. Colombia. Infobae. [03, agosto, 2022]. Disponible en: https://www.infobae.com/america/colombia/2020/01/26/el-metodo-de-estafa-virtual-que-amenaza-a-los-colombianos-en-el-exterior/

En síntesis, se puede resumir que las amenazas y riesgos cibernéticos a las que se enfrentan las empresas turísticas colombianas e internacionales en cuanto a la ciberseguridad están determinadas por el mal manejo de la información, contraseñas débiles, falta de actualización de software y aplicaciones, perdidas de información, ausencia de monitorizar la red, no secularizar accesos remotos de clientes y empleados.

5.2 HERRAMIENTAS, TÉCNICAS Y ESTRATEGIAS COMO MECANISMOS DE SEGURIDAD DE LA INFORMACIÓN

Se hizo la división de las herramientas, técnicas y estrategias de seguridad de la información que se utilizan en las organizaciones y los usuarios por aparte.

5.2.1. Organizaciones

En el sector turístico cada vez más se están utilizando los medios electrónicos para poder realizar sus transacciones y dar a conocer sus paquetes turísticos por este motivo deben contar con estrategias que fueron publicadas por INCIBE que les permiten proteger sus datos personales ante posibles ciberataques, entre las cuales se pueden destacar:

1. Control de acceso a la información: “Es necesario establecer políticas de seguridad en la que se defina y clasifique la información que se maneja en la empresa, y se delimite claramente quien y en qué condiciones accederá a la información para evitar filtraciones o perdidas accidentales”[113]

Una práctica que se suele hacer en este sentido es establecer los permisos que son necesarios para cada grupo de usuarios o por cada usuario determinando claramente quien tiene el permiso de acceso y a que información. Este tipo de actividades se deben realizar con regularidad.

[113] INCIBE. 9 claves de Ciberseguridad para el sector del turismo. [Sitio WEB]. Madrid. INCIBE. [28, noviembre, 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/9-claves-ciberseguridad-el-sector-del-turismo

2. Copias de Seguridad: Esta se considera una de las medidas más importantes para evitar la pérdida de información pues se obtiene una respuesta rápida, es prioritario que se realicen continuamente copias de seguridad de los programas y la información importante.

3. Cifrado de información. Para obtener resultados óptimos de seguridad se debe cifrar los soportes donde se realiza almacenamiento como la información confidencial con esta estrategia se evita manipulaciones y fugas de información disminuyendo considerablemente su difusión que no es autorizada.

4. Gestión de contraseñas. El acceso a toda la información debe ser protegido por contraseñas estableciendo una política de las contraseñas para su utilización de una forma correcta. Deben incluir:

   - ✓ Obligación de la utilización de contraseñas que sean fuertes;
   - ✓ Utilización de una contraseña que sea diferente para cada aplicación o servicio;
   - ✓ Cambios de contraseñas cada periodo de tiempo;
   - ✓ Utilizar un doble factor de autenticación para servicios críticos como aplicaciones y perfiles de usuario de administración.

5. Actualización de las aplicaciones. Cualquier tipo de programa puede presentar fallos de la seguridad en su programación, por este motivo, es importante es actualizar correctamente todo el software que se utiliza en los ordenadores de trabajo. Como recomendación se debe evitar usar aplicaciones que sean antiguas que no tenga actualizaciones de seguridad.

6. Eliminación segura de la información. Se debe evitar las difusiones accidentales o no de la información a través de soportes de almacenamiento antiguos u obsoletos, como discos duros, CD, DVD o incluso papel. “Para ello realizaremos un borrado seguro de los soportes digitales antes de proceder a su destrucción. El papel debe ser destruido utilizando trituradoras de papel”[94]

7. Limitar la utilización de herramientas que no son Corporativas: A veces se utiliza herramientas o programas no personales sin control lo que puede ocasionar que se presente perdida de información que es confidencial de las empresas Se debe limitar la trasferencia de información de la Empresa hacia el exterior. Para evitar la fuga de información se debe utilizar correctamente el correo electrónico y los perfiles de tipo personal.

8. Confidencialidad en las contrataciones de los servicios. En caso de tener subcontratado con terceros los soportes informáticos, servicios tecnológicos que necesiten un intercambio de la información que es confidencial de la empresa se deben hacer exigencias sobre los niveles de los servicios y garanticas de protección sobre la información confidencial que se maneja de los clientes y de la comunicación entre los proveedores y la empresa.

9. Cumplimientos legales. Para poder tener una buena reputación de la empresa es fundamental promulgar la protección de la información confidencial de los clientes, en este sentido se deben tener presentes dos leyes que tratan esta temática que es la Ley Orgánica de la Protección de los datos y la Ley de servicios de la Información y de Comercio Electrónico.

En general para evitar una vulnerabilidad muy frecuente que se trata sobre alteración de los datos empresariales se deben realizar acciones como el limitar el acceso a las bases de datos, identificar claramente cuáles son los datos críticos y los datos sensibles, se debe cifrar la información, también se debe anonimizar las bases de datos de que no son productivas y realizar monitoreos en las actividades de las bases de datos.

En este sentido se complementa la información en el contenido propuesto en el Anexo A que se titula: “Líneas de acción de la estrategia nacional de ciberseguridad” escrito por Javier Candau Romero, documento que divide en 10 líneas de acción en las que se abordan temáticas como el Desarrollo del Esquema Nacional de Seguridad, Gestión homogénea de las redes de las AAPP, Desarrollo del PPIC ante ciberamenazas, Programa de formación y concienciación, Coordinación de recursos en la respuesta ante incidentes de seguridad, coordinación de esfuerzos de investigación y desarrollo, potenciar la colaboración internacional y el empleo de productos de seguridad certificados.

Figura 12. Herramientas de Ciberseguridad Sector Turismo

Fuente: Autoría propia

5.2.2. Derechos de Propiedad Intelectual

Los derechos de propiedad intelectual son: “Aquellos que se ofrecen a las personas sobre las creaciones de su mente. Suelen dar al creador derechos exclusivos sobre la utilización de su obra por un plazo determinado”[114]

[114] ORGANIZACIÓN MUNDIAL DEL COMERCIO. ¿Qué se entiende por Derechos de Propiedad Intelectual? [Sitio WEB]. Suiza [2022]. Disponible en: https://www.wto.org/spanish/tratop_s/trips_s/intel1_s.htm

Los derechos de autor protegen a los autores de escritos, obras artísticas y literarias, pinturas, composiciones de tipo musical por un plazo que es mínimo de 50 años después de la respectiva muerte del autor. También se entiende que los derechos de autor incluyen a los que se encuentran vinculados de una manera conexa como, por ejemplo, productores de los fonogramas, artistas e intérpretes que son ejecutantes.

A nivel empresarial existe la propiedad industrial que protege por un lado los signos distintivos, las marcas de comercio o fabrica y las indicaciones geográficas: “La protección de esos signos distintivos tiene por finalidad estimular y garantizar una competencia leal y proteger a los consumidores, haciendo que puedan elegir con conocimiento de causa entre diversos productos o servicios”[115]

Otras clases de propiedad industrial tiene que ver con los que protegen las creaciones, innovaciones e invenciones tecnológicas como los modelos y dibujos industriales y los secretos comerciales.

- Programas Informáticos para optimizar la Ciberseguridad

5.2.3. Herramientas Técnicas De protección de la Seguridad de los Usuarios

Dentro de las herramientas técnicas que se utilizan para proteger la seguridad de la información de los usuarios en las empresas se destacan algunos softwares que protegen eficazmente ante delitos informáticos.

5.2.3.1. Orca Security

El Software denominado Orca Security hace la respectiva protección de 100 activos tecnológicos cuya ubicación se encuentra en la nube sin omitir ninguno, facilitando el mucho trabajo que tienen las plataformas Service, Amazon Web, Google Cloud Platform y el Microsoft Azure, es de aclarar que todos los datos que están ubicados en la nube se pueden exportar y compartir con otros usuarios.[116]

[115] Ibid. 90 p 1.

[116] Ibid. 106 p 1

Con esta herramienta se puede reconocer vulnerabilidades, malware, permite realizar evaluaciones de las contraseñas que son débiles, recibir alertas sobre los recursos que son útiles, organizar los tipos de riesgos según las características que presenten, y tener accesos a los datos por medio de interfaces de usuarios que son amigables.

5.2.4. Netacea Bot Management

El Netacea Bot Management es una de las soluciones con las que cuenta la nube para poder proteger de una forma clara los sitios de páginas web, interfases API y aplicaciones de los celulares que pueden presentar ciertas amenazas cuando se navega por internet, es una buena opción pues cuenta con sistemas que hacen seguimientos en tiempos reales utilizando la herramienta machine learning[117]

Sus características más relevantes es que prohíbe accesos a perfiles que son maliciosos, desga losa los datos, facilita los accesos a los afiliados y a las personas por medio de los motores de búsquedas. También realiza análisis de las aplicaciones web y la reputación que tiene el sitio informando oportunamente sobre Ciberataques y amenazas.

5.2.5.Netwrix Auditor

Es un software de auditoría especializado y centrado en lograr identificar las posibles vulnerabilidades de ciberseguridad incluyendo alertas de posibles amenazas, evalúa con frecuencia los riesgos y automatizaciones de los procesos de la clasificación de los datos: “Las empresas que realizan auditorías externas e internas utilizan software como esta ya que mejora la seguridad, minimiza considerablemente los riesgos de TI, permite el logro de los cumplimientos normativos y hace la recopilación de toda la información en un solo sitio”[118].

---

[117] GAMELEARN TEAM. 5 programas Informáticos para mejorar tu Ciberseguridad. [Sitio WEB]. Gamelearn. [12, octubre, 2021]. Disponible en: https://www.game-learn.com/es/recursos/blog/5-programas-informaticos-para-mejorar-tu-ciberseguridad/

[118] Ibid. 102.p

5.2.6. Bitdefender Total Security

Es un antivirus que ofrece protección multiplataforma y se adapta a diferentes usuarios, desde profesionales hasta pequeñas y grandes empresas. “Cada año apuestan por seguir innovando y actualizan la última versión del producto disponible en el mercado para así evitar fraudes, malware, spam, phishing y otros tipos de ciberataques”[119]

Dentro de sus funcionalidades más destacadas se encuentra que realiza actualizaciones de una forma automática, protege los datos en tiempos reales, controla la banda online y los parentales, gestiona las contraseñas, realiza protección en las redes sociales contra ciberdelitos, contiene un sistema que permite recuperar la información ante ciberataques y hace el cifrado de los archivos.

5.2.7. Viper

Es un buscador que permite detectar plagios en masa de documentos y textos, realizando búsquedas locales y por el internet: “es una utilidad que te ayuda a detectar plagios en los documentos almacenados en tu ordenador o red local, así como en Internet. En el primer paso toca elegir los ficheros, que pueden ser DOC, RTF, HTM y TXT”[120]

5.2.8. Plagium

Este es un programa que utiliza un tipo de técnica que es patentada y que desglosa inteligentemente los textos que se ingresan en pequeños fragmentos que a su vez se comparan con los contenidos de la web, marcando las posibles coincidencias para poder determinar cuáles documentos coinciden con los textos originales: “El resultado es una visión mucho más limpia de posibles documentos coincidentes -

---

[119] Ibid.44. p 1

[120] SOFTONIC. Viper. [Sitio WEB]. Softonic International. [16, Junio, 2015]. Disponible en: https://viper.softonic.com/

una visión con mucho menos ruido que los resultados ofrecidos por los principales motores de búsqueda”[121]

5.3.3. Base MITRE ATT&CK

Es una base de conocimientos que es accesible en todo el mundo y contiene técnicas y tácticas que utiliza el adversario basadas en las observaciones del mundo real: “La base de conocimientos de ATT&CK es útil como base para desarrollar modelos y metodologías de amenazas que son específicos del gobierno y el sector privado, incluyendo la comunidad de servicios y productos de ciberseguridad”[122].

Las tácticas empresariales representan el "por qué" de las técnicas o subtécnicas de ATT&CK. En resumen, es el objetivo táctico de los adversarios: las razones para realizar cierta acción.

Tabla No 5. Tácticas Empresariales ATT&CK

[121] PLAGIUM. Preguntas frecuentes. [Sitio WEB]. Plagium. [2022]. Disponible en: https://www.plagium.com/es/faq

[122] GREAT PLACE TO WORK. Analizando la postura de seguridad de su organización con ayuda de la matriz Mitre Att&ck. [Sitio WEB]. Soluciones Seguras. [2022]. Disponible en: https://www.solucionesseguras.com/landing/guias-de-interes/38-analizando-la-postura-de-seguridad-de-su-organizacion-con-ayuda-de-la-matriz-mitre-att-ck

IDENTIFICACIÓN	Nombre	Descripción
TA0043	Reconocimiento	El adversario está tratando de recopilar información que pueda usar para planificar operaciones futuras.
TA0042	Desarrollo de recursos	El adversario está tratando de establecer recursos que puedan usar para apoyar las operaciones.
TA0001	Acceso inicial	El adversario está tratando de entrar en su red.
TA0002	Ejecución	El adversario está tratando de ejecutar un código malicioso.
TA0003	Persistencia	El adversario está tratando de mantener su punto de apoyo.
TA0004	Escalada de privilegios	El adversario está tratando de obtener permisos de nivel superior.
TA0005	Evasión de defensa	El adversario está tratando de evitar ser detectado.
TA0006	Acceso a Credenciales	El adversario está tratando de robar nombres de cuenta y contraseñas.
TA0007	Descubrimiento	El adversario está tratando de averiguar su entorno.
TA0008	Movimiento lateral	El adversario está tratando de moverse a través de su entorno.
TA0009	Recopilación	El adversario está tratando de recopilar datos de interés para su objetivo.
TA0011	Comando y control	El adversario está tratando de comunicarse con los sistemas comprometidos para controlarlos.
TA0010	exfiltración	El adversario está tratando de robar datos.
TA0040	Impacto	El adversario está tratando de manipular, interrumpir o destruir sus sistemas y datos.

Fuente: Attack.Mitre. Tácticas Empresariales. [En línea]. 2022. (Recuperado el 10 de mayo del 2022) Disponible en: https://attack.mitre.org/tactics/enterprise/

En lo que respecta a las tácticas móviles representan el "por qué" de las técnicas o subtécnicas de ATT&CK. Es el objetivo táctico y la razón del adversario para efectuar una acción. Por ejemplo, un adversario puede querer obtener acceso mediante credenciales.

Tabla No 6. Tácticas Móviles ATT&CK

IDENTIFICACIÓN	Nombre	Descripción
TA0027	Acceso inicial	El adversario está tratando de ingresar a su dispositivo.
TA0041	Ejecución	El adversario está tratando de ejecutar un código malicioso.
TA0028	Persistencia	El adversario está tratando de mantener su punto de apoyo.
TA0029	Escalada de privilegios	El adversario está tratando de obtener permisos de nivel superior.
TA0030	Evasión de defensa	El adversario está tratando de evitar ser detectado.
TA0031	Acceso a Credenciales	El adversario intenta robar nombres de cuentas, contraseñas u otros secretos que permitan el acceso a los recursos.
TA0032	Descubrimiento	El adversario está tratando de averiguar su entorno.
TA0033	Movimiento lateral	El adversario está tratando de moverse a través de su entorno.
TA0035	Recopilación	El adversario está tratando de recopilar datos de interés para su objetivo.
TA0037	Comando y control	El adversario intenta comunicarse con dispositivos comprometidos para controlarlos.
TA0036	exfiltración	El adversario está tratando de robar datos.
TA0034	Impacto	El adversario está tratando de manipular, interrumpir o destruir sus dispositivos y datos.
TA0038	Efectos de red	El adversario intenta interceptar o manipular el tráfico de red hacia o desde un dispositivo.
TA0039	Efectos de servicio remoto	El adversario está tratando de controlar o monitorear el dispositivo usando servicios remotos.

Fuente: Attack.Mitre. Tácticas Móviles. [En línea]. 2022. (Recuperado el 10 de mayo del 2022) Disponible en: https://attack.mitre.org/tactics/enterprise/

Las tácticas ICS realizan la representación de él "por qué" de una de las técnicas o subtécnicas de ATT&CK. Su objetivo principal táctico del adversario: la verdadera razón para poder realizar una determinada acción. Por ejemplo, uno de los adversarios puede querer obtener ciertos accesos utilizando credenciales. En la tabla 4 se pueden observar las tácticas ICS ATT&CK en cuanto a los dispositivos móviles.

Tabla No 7. Tácticas ICS ATT&CK

IDENTIFICACIÓN	Nombre	Descripción
TA0108	Acceso inicial	El adversario está tratando de ingresar a su entorno ICS.
TA0104	Ejecución	El adversario intenta ejecutar código o manipular funciones, parámetros y datos del sistema de forma no autorizada.
TA0110	Persistencia	El adversario está tratando de mantener su punto de apoyo en su entorno ICS.
TA0111	Escalada de privilegios	El adversario está tratando de obtener permisos de nivel superior. La escalada de privilegios consiste en técnicas que utilizan los adversarios para obtener permisos de nivel superior en un sistema o red. Los adversarios a menudo pueden ingresar y explorar una red con acceso sin privilegios, pero requieren permisos elevados para cumplir con sus objetivos. Los enfoques comunes son aprovechar las debilidades del sistema, las configuraciones incorrectas y las vulnerabilidades.
TA0103	Evasión	El adversario está tratando de evitar las defensas de seguridad.
TA0102	Descubrimiento	El adversario está localizando información para evaluar e identificar sus objetivos en su entorno.
TA0109	Movimiento lateral	El adversario está tratando de moverse a través de su entorno ICS.
TA0100	Recopilación	El adversario está tratando de recopilar datos de interés y conocimiento del dominio en su entorno ICS para informar su objetivo.
TA0101	Comando y control	El adversario intenta comunicarse y controlar sistemas, controladores y plataformas comprometidos con acceso a su entorno ICS.
TA0107	Función de inhibición de respuesta	El adversario está tratando de evitar que sus funciones de seguridad, protección, garantía de calidad e intervención del operador respondan a una falla, peligro o estado inseguro.
TA0106	Deterioro del control de procesos	El adversario está tratando de manipular, deshabilitar o dañar los procesos de control físico.
TA0105	Impacto	El adversario está tratando de manipular, interrumpir o destruir sus sistemas ICS, sus datos y el entorno que los rodea.

Fuente: Attack.Mitre. Tácticas Móviles. [En línea]. 2022. (Recuperado el 10 de mayo del 2022) Disponible en: https://attack.mitre.org/tactics/enterprise/

Las técnicas empresariales de Attack.Mitre representan: “'Cómo' un adversario logra un objetivo táctico al realizar una acción. Por ejemplo, un adversario puede volcar las credenciales para lograr el acceso a las mismas”.[123]

Las técnicas móviles suelen representan el 'cómo' los adversarios logran un tipo de objetivo táctico al poder realizar una determinada acción. Por ejemplo, los adversarios pueden volcar las credenciales para lograr sus accesos.

Cuenta con 66 técnicas y 41 sub- técnicas que abarcan aspectos como mecanismos de Control de Elevación de abuso, permisos de administrador de dispositivos, acceder a notificaciones, eliminación de acceso a la cuenta, protocolos de las capas de aplicación y la web, control de llamadas y datos del portapapeles entre otros.

Las técnicas ICS representan el 'cómo' los adversarios logran sus objetivos tácticos al poder realizar una determinada acción. Por ejemplo, los adversarios pueden volcar las credenciales para poder lograr su acceso. Contiene 78 técnicas que incluyen aspectos como el activar el modo de actualización de firmware, supresión de alarma, cobranza automatizada, mensaje de comando de bloque y mensajes de informes de bloqueo, bloque serie COM, cambiar el modo de funcionamiento.

5.3.4. Formación a los Usuarios

Es una responsabilidad que tienen las empresas el poder realizar correctas capacitaciones y concientizaciones sobre las posibles amenazas de la seguridad de la información que se puedan aplicar en sus entornos, así como también los procedimientos y políticas para poder administrarlas: “Las políticas de seguridad de la información están contempladas en distintas normas y estándares de seguridad de la información y se incluye adicional como control de cumplimiento la correcta divulgación y capacitación sobre las mismas”[124]

---

[123] MITRE ATT&CK. Revista de investigación. [en línea]. Bedford.: 2022. [Consultado 19, julio,2022]. Disponible en: https://attack.mitre.org/tactics/enterprise/

[124] CIBERSEGURITY. Revista de investigación. [en línea]. Guatemala.: 2019. [Consultado 19, julio,2022]. Disponible en: https://csecmagazine.com/2020/04/13/educacion-para-usuarios-sobre-seguridad-de-la-informacion/

Los avances de las tecnologías de la información han permitido obtener herramientas con las que se puede educar y capacitar a los usuarios de forma permanente y remota, por ejemplo, utilizando plataformas como las de E-Learning que contienen diferentes funciones con las que se pueden efectuar cursos y capacitaciones que sean una necesidad en las organizaciones.

5.3.5. Estrategias de Seguridad de la Información de los Usuarios

Para poder conservar la seguridad de la información en los usuarios es importante antes que cualquier cosa se tiene que educar y tomar conciencia sobre estos riesgos, además que: “Los usuarios siempre deben desconfiar de los e-mails no solicitados una de las principales formas de actuación que utilizan los cibercriminales es realizando los ataques de phishing, que pueden contaminar los e-mails que los usuarios reciben en sus correos electrónicos”[125]

Tampoco los usuarios deben descargar archivos sospechosos y bloquear estos vínculos, de igual manera deben verificar a los remitentes de sus correos electrónicos pues los cibercriminales están utilizando inteligencia artificial para lograr sus propósitos, si los correos son correctos y pertenecen a empresas legales.

Los usuarios también deben verificar el dominio de las páginas y mantener sus dispositivos actualizados pues si los usuarios mantienen las versiones anteriores de sus aplicaciones y programas, pueden verse afectados por los cibercriminales que aprovechan estas circunstancias para robar los datos e invadir los dispositivos.

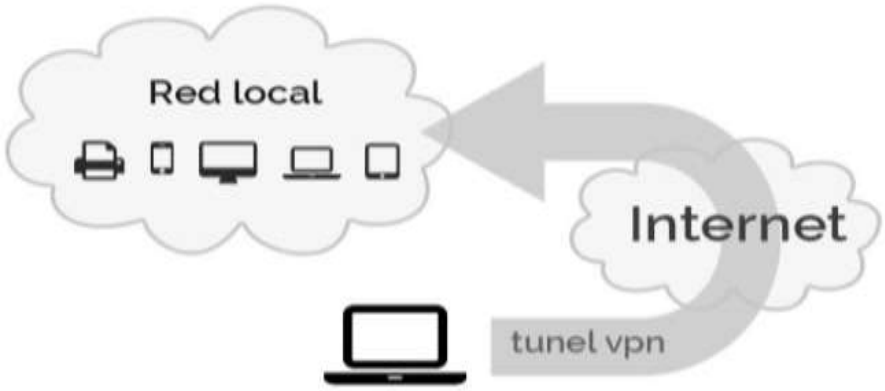
5.3.5.1. Utilización de VPN

Sus siglas significan Virtual Private Network, o perteneciente a una red privada virtual: “Este tipo de redes se utilizan en la creación de redes locales sin que sus

[125] SINNEX WESTCON- COMSTOR. 6 consejos prácticos de seguridad de la información para usuarios. [Sitio WEB]. [2, septiembre, 2019]. Disponible en: https://digital.la.synnex.com/6-consejos-practicos-de-seguridad-de-informacion-para-usuarios

usuarios tengan que estar conectados unos con otros, sino lo pueden hacer a través de internet teniendo una cobertura global” [126]

Figura 14. Red VPN



Fuente: XATACA. [En línea]. ¿Qué es una conexión VPN, para qué sirve y qué ventajas tiene? Bogotá D.C.: 2021. (Recuperado el 11 de mayo del 2021) Disponible en: https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

Otra de las peculiaridades de las conexiones VPN son los llamados túneles de datos. Es un procedimiento que mientras se utiliza el Internet el dispositivo se pone en contacto con el proveedor de Internet, que es el que permite conectar con los distintos servicios web para ofrecerte.

Las conexiones VPN se utilizan en el teletrabajo, para evitar bloqueos de tipo geográfico y censuras, sirve de capa extra de seguridad y en las descargas P2P.

[126] Ibid. 127.p.1

5.4. RECOMENDACIONES DE BUENAS PRÁCTICAS CIBERNÉTICAS

5.4.1. *Usuarios*

Las buenas prácticas cibernéticas que pueden adoptar los usuarios de paquetes turísticos están relacionadas con medidas preventivas que pueden adoptar para evitar ataques cibernéticos en estos procesos, dentro de las recomendaciones que se estipulan en este sentido se encuentran:

- ✓ Contraseñas que sean seguras: “Casi siempre que se accede a una página web de cualquier entidad que ofrece productos o servicios como en este caso paquetes turísticos se debe crear una cuenta que requiere usuario y contraseñas que deben ser robustas que incluyan todo tipo de letras minúsculas, mayúsculas, símbolos y números para que sea más difícil de descifrar por los ciberdelincuentes y no crear la misma contraseña en varias plataformas”[127]

- ✓ Se debe proteger la red personal de intrusos: “Los routers de última generación presentan niveles buenos en cuanto a la seguridad, lastimosamente muchas personas pasan por alto hacer el cambio de sus contraseñas que vienen configuradas de las fábricas, esto lo aprovechan los ciberdelincuentes para poder ingresar a sus cuentas y tomar información personal de forma ilegal”[128]

- ✓ Saber identificar las prácticas que comúnmente utilizan los cibercriminales: el ‘phishing’, es de las más recurrentes pues se realiza la suplantación de entidades y organismos con el fin de solicitar los datos personales que son valorizados en los mercados negros en los cuales se hace la venta de estas bases de datos hasta que finalmente consiguen los datos bancarios de las personas afectadas y realizan los robos: “También se utiliza el software ransomware que es de secuestro, se hace por medio de un correo o sitio web que incluye un enlace, al hacer clic sobre este enlace, se ejecuta una descarga que bloquea los dispositivos hasta que los usuarios paguen por su respectiva liberación”[129]

---

[127] APIC. [sitio web]. Bogotá: Atlantic Pacific SAS. 15 consejos de ciberseguridad para no exponerse en la red. [08-04-2020]. Disponible en: https://www.apintlcorp.com/articulos/atlantic-15-consejos-seguridad-red.html

[128] Ibid. 127 pág. 1

[129] Ibid. 127 pág. 1

- ✓ “Los organismos de tipo oficial nunca hacen solicitudes de datos personales a los usuarios por sus correos electrónicos, tampoco por medio de encuestas y cuestionarios externos, por este motivo no se deben responder este tipo de correos”[130]

- ✓ “No se debe tener confianza total en los bloqueos que se realizan por la opción “spam” de los correos electrónicos, pues lastimosamente sueles ser efectivas, lo mismo suele pasar con los antivirus”[131]

- ✓ Se debe acudir a agencias de viajes seguras y reconocidas: “Al realizar compras y pagos por internet los usuarios deben verificar que son los sitios web oficiales de las entidades de turismo, se debe verificar que las aplicaciones o sitios web ofrezcan garantías, que sean seguras, su dirección oficial, las políticas que tienen en caso de devoluciones, formas de pago etc”[132]

- ✓ Conocer con antelación los métodos de pago que tienen disponibles: “Los pagos que se realizan por internet que son más comunes y fáciles se hacen por medio de tarjetas debido o crédito, pero se debe verificar que exista la debida seguridad en la web de la agencia o si no se pone en peligro el dinero con el que se está realizando los pagos, es más seguro optar por realizar pagos por PSE o PayPal”[133]

- ✓ Se deben tratar con cuidado los datos personales: “Muchas empresas o entidades turísticas suelen aconsejar el uso de chats internos que son exclusivos, o la información y documentos que deben enviar por la web que sean en formato PDF”[134]

- ✓ Tener cuidado con los fake news: “los ciberdelincuentes suelen disfrazar sus actuaciones delictivas por medio de publicidad engañosa o noticias que son falsas de las cuales hacen difusión por los correos electrónicos o las redes

---

[130] Ibid. 127 pág. 1

[131] Ibid. 127 pág. 1

[132] Ibid. 127 pág. 1

[133] Ibid. 127 pág. 1

[134] Ibid. 127 pág. 1

sociales, por eso los usuarios deben verificar que la fuente de estos sitios sea de entera confianza"[135]

- ✓ Poner atención a la página web: "Los usuarios deben verificar que los sitios web que manejan las empresas de turismo inicien con HTTPS pues son sitios protegidos y seguros, se identifican con un candado de color verde que se encuentra al lado izquierdo de la URL y no ingresar a los que empiezan con HTTP"[136]

- ✓ "Se recomienda a los usuarios solo hacer descargas de los archivos que son realmente necesarios evaluando con antelación su procedencia e importancia"[137]

- ✓ Deshabilitar complementos: "Los usuarios de empresas turísticas suelen utilizar navegadores para realizar sus búsquedas en internet, esto propicia que algunos datos queden en la web lo que puede ocasionar la introducción de softwares que son maliciosos y virus de toda clase, por eso es importante habilitar los plugins en los navegadores"[138]

- ✓ "Es importante que los usuarios mantengan actualizados los softwares de sus pc y aplicaciones del celular para evitar tener vulnerabilidades ante los ataques de los delincuentes en la red"[139]

5.4.2. Recomendaciones a los usuarios sobre el uso de las VPN

Las conexiones VPN cuenta con muchas ventajas que pueden favorecer la seguridad de la información de los usuarios, algunas de las más importantes se describen a continuación:

---

[135] Ibid. 127 pág. 1

[136] Ibid. 127 pág. 1

[137] Ibid. 127 pág. 1

[138] Ibid. 127 pág. 1

[139] Ibid. 127 pág. 1

Puede funcionar en todas las aplicaciones: “Pues enruta todo el tráfico de Internet, a diferencia de los servidores proxy, que solo puedes usar en el navegador web y un puñado de aplicaciones más que te dejan configurar las opciones de conexión avanzadas”[140]

Se puede conectar y desconectar de una manera fácil, cuando se logra configurar se puede activar y también desactivar la conexión cuando se desee, es una seguridad que se adiciona a los puntos de los accesos que tiene el Wifi, es de aclarar que la conexión debe estar cifrada.

En los casos de falseo de la ubicación las conexiones VPN son eficaces para evitar censuras o poder acceder a contenidos limitados a ciertas regiones.

5.4.3. Organizaciones

Las recomendaciones de buenas prácticas cibernéticas también le corresponden directamente adoptarlas a las entidades de turismo, por este motivo a continuación se presentará algunas recomendaciones que brinda la Organización Mundial del Turismo sobre la accesibilidad de la información turística.

El suministro que se hace de la información debe ser accesible para los usuarios y turistas que genere en ellos confianza a la hora de revisar esta información, por este motivo se deben tener en cuenta cinco elementos fundamentales:

El primero de ellos es que se debe: “Incluir información sobre la accesibilidad de las infraestructuras y los servicios cuando sea posible o facilitar una referencia a otro lugar en el que puedan encontrar esa información”[141]

---

[140] XATACA. [Sitio WEB]. México. [19, julio, 2022]. Disponible en: https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

[141] UNWTO. [sitio web]. Madrid: Organización Mundial del Turismo. Recomendaciones de la OMT sobre accesibilidad de la información turística. [12-03-2021]. Disponible en: https://www.e-unwto.org/doi/pdf/10.18111/9789284417926

El segundo es que: “Se debe facilitar la información o el material que contiene las promociones, procedimientos y servicios a los usuarios con el fin de indicarles cuales son los puntos de contacto para que los lectores puedan obtener más información”[142].

El tercer elemento es que se debe asegurar que, en todos los canales y medios de comunicación, la información que se suministra debe ser clara y coherente tanto la que se brinda directamente como la que se da a conocer en línea, utilizando los medios de comunicación como el correo electrónico, por teléfono o chat.

El cuarto elemento es una recomendación que se brinda a las organizaciones de brindar la formación necesaria a las personas que están encargadas de gestionar la información en técnicas específicas y en el caso que se haga la contratación de servicios informáticos o de un sitio web se debe solicitar al personal técnico que cuente con la preparación necesaria para que pueda realizar estas funciones.

Finalmente, el quinto elemento sugiere a las empresas que los contenidos de los sitios web y aplicaciones deben estar actualizándose en todo momento para mejorar la calidad que se maneja en la información y así evitar peligros de seguridad a los visitantes de estos sitios digitales.

En lo que respecta a los documentos digitales son una herramienta fundamental para las empresas turísticas pues se trasmite por medio de estos gran cantidad de información: “En todo documento enviado por correo electrónico, folleto o pasaje de viaje, o en documentos descargables en páginas web sobre turismo, es importante asegurarse de que el público sepa qué se está descargando y de que el contenido sea utilizable y accesible”[143]

Las tecnologías web también cumplen un papel importante en las empresas de turismo, pues se brinda el acceso a gran cantidad de servicios y productos turísticos

[142] Ibid. 100. p 5

[143] Ibid. 48. p 11

a nivel mundial que incluyen agencias de viajes virtuales, sitios en los que se pueden realizar las reservas hasta la información detallada de las instalaciones como los hoteles, playas turísticas.

La accesibilidad que se debe hacer a los contenidos web debe cumplir con las normas internacionales y las pautas de accesos a los contenidos web que deberían seguir las orientaciones que se especifican en cuatro principios como se puede analizar a continuación:

- Perceptibles: se pueden utilizar sin tener en cuenta las capacidades que tienen los clientes para tocar, oir y ver como la creación de contenidos que se puedan presentar de formas diferentes utilizando tecnologías que apoyen sin perder su verdadero significado, se podría proporcionar otras alternativas para contenidos que sean multimedia, también se debe hacer que los accesos de los usuarios a las plataformas se hagan de forma fácil.

- Manejables: la utilización de medios de navegación por medio de botones y formas: “Hacer que toda funcionalidad sea accesible a través de un teclado, dar a los usuarios suficiente tiempo para leer y usar el contenido, no utilizar contenidos que puedan causar crisis epilépticas, ayudar a los usuarios a navegar y a encontrar los contenidos”[144]

- Comprensible: Con la utilización de contenidos fáciles de entender con sus respectivas interfaces esto se logra utilizando textos comprensibles y legibles, se deben crear contenidos cuyo funcionamiento y apariencia sean predecibles, también se brindar la ayuda a los usuarios a corregir y evitar errores.

- Robusto: Los contenidos deben tener la facultad de ser utilizados de una manera confiable utilizando una gran cantidad de dispositivos, esto se puede lograr maximizando las compatibilidades con las herramientas actuales y futuras de los usuarios.

Para terminar se incluye algunas de las recomendaciones y principios básicos de Ciberseguridad CCN-CERT BP/01 que es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional de España, su

[144] Ibid. 48. p 16

principal misión es poder: “Contribuir al mejoramiento de la ciberseguridad en España, pues es un centro de respuesta y alerta a nivel nacional que colabora brindando respuestas rápidas responder de forma rápida y eficiente a los ciberataques que se presentan afrontándolos de una forma activa”[145]

5.4.4. Recomendaciones y Principios Básicos de Ciberseguridad CCN-CERT BP/01

En este informe se establece que para poder lograr la implementación de seguridad en las empresas es fundamental la planificación teniendo en cuenta los siguientes aspectos:

- ✓ Los Análisis de Riesgos: “Se deben estudiar los riesgos y realizar la valoración de las consecuencias que han tenido sobre los activos de las empresas, es decir en aspectos como el servicio y la información”[146]
- ✓ La Gobernanza para poder lograr la adaptación operativa que es regular de la entidad a las respectivas medidas de seguridad.
- ✓ Gestión de Riesgos y la vigilancia para poder valorar las diversas medidas de protección y poder decidir cual alternativa de solución se adecua a las entidades o en otras palabras se debe determinar el riesgo que es residual: “En lo que concierne a la vigilancia se debe efectuar una observación de manera continua de todas las medidas de seguridad como también las adecuaciones de estas en las apariciones de nuevas tecnologías”[147]

También se deben tener presentes los planes de contingencia para poder determinar las medidas ante los posibles incidentes de ciberseguridad que se puedan presentar.

De acuerdo con lo indicado en este informe sugiere algunas recomendaciones para poder fortalecer las comunicaciones por internet garantizando de esta manera la privacidad y el anonimato, uno de ellos es la RED TOR cuyas siglas significan The Onion Router que fue un tipo de proyecto diseñado por la Marina de los Estados Unidos cuyo lanzamiento fue en el año 2002 y permite: “A los usuarios a los usuarios navegar por la web de forma anónima. Los datos no viajan de forma directa, sino a través de varios nodos que facilitan el anonimato de las comunicaciones. Existe un

[145] INFORME DE BUENAS PRACTICAS. (marzo, 2021.España). Centro Criptológico Nacional. 2021. 56 p

[146] Ibid. 75 p 5

[147] Ibid. 75 p 5

directorio de nodos intermedios con las claves públicas asociadas para poder establecer la comunicación cifrada”[148]

TOR crea circuitos que son virtuales y se encuentran compuestos por tres tipos de nodos que son escogidos aleatoriamente en la red. “De manera que las comunicaciones entre el origen, e equipo y los destinos, recorren estos nodos utilizando información que se trasmite de una forma cifrada”[149]

Otro ejemplo se puede observar en el uso de aplicaciones que se instalan en los dispositivos móviles y equipos, por este motivo se debe mantener su integridad para ello es fundamental que: “El empleo de software legal ofrece garantía y soporte, con independencia de las implicaciones legales de utilizar software no legítimo”[150]

De igual manera se debe considerar las superficies de exposición que se encuentran relacionadas a los sistemas que son heredados, específicamente aquellos que tienen una década de antigüedad pues son extremadamente vulnerables.

5.4.5. Actualización de Sistemas Operativos

Un sistema operativo es un programa que se encarga de dirigir, coordinar y controlar los conjuntos de los servicios y aplicaciones que utilizan los usuarios, siendo la parte central o el núcleo que necesita un computador para que pueda funcionar eficazmente.

En efectuar una actualización simplemente es “mejorar” los parches de la seguridad que son los encargados de ayudar a mantener el funcionamiento óptimo y de seguridad para los equipos de cómputo.

Es importante que: “Todo programa, aplicación o sistema es propenso a errores y/o fallas de seguridad lo que conlleva a que los desarrolladores o propietarios de los

[148] Ibid. 75 p 11

[149] Ibid. 75 p 11

[150] Ibid. 75 p 13

sistemas lancen nuevas versiones (actualizaciones) para que el sistema operativo contrarreste el error y esté preparado ante cualquier vulnerabilidad posible” [151]

Las actualizaciones de los sistemas operativos pueden incluir desde las aplicaciones que se encuentran instaladas en el ordenador como también los parches que maneja en el núcleo, se debe incluir también la actualización de los antivirus, es de aclarar que de no ser actualizados se pueden ocasionar robos y destrucción de la información de los usuarios y organizaciones.

[151] ASSISTEMAS. Importancia de la actualización de tu sistema operativo. [Sitio WEB]. México. [25, febrero, 2020]. Disponible en: https://assistemas.net/importancia-de-las-actualizaciones-de-tu-sistema-operativo%EF%BB%BF/

6 CONCLUSIONES

Se logró identificar las principales amenazas y riesgos cibernéticos asociados a la adquisición de servicios turísticos a través de medios electrónicos reconociendo que los que más se presentan están relacionados con ransomware, ataques DDos, denegación de servicios, fraudes en las entidades financieras que utilizan cajeros automáticos tipo ATM, skimming, suplantación de proveedores, clientes y ejecutivos y estafas a través de internet, llamadas telefónicas, WhatsApp o mensajes de texto.

Dentro de las herramientas, técnicas y estrategias que proporcionan mecanismos de seguridad de la información a usuarios y organizaciones de servicios turísticos que utilizan medios electrónicos para su consulta y/o adquisición se pueden destacar algunas recomendaciones como el realizar controles de acceso a la información y copias de seguridad de los programas e información importante de las empresas, también es fundamental ejecutar el cifrado de la información confidencial, la respectiva gestión de contraseñas fuertes con doble autenticación y que se cambien de una manera regular, de igual manera es importante que se actualicen las aplicaciones que se haga la eliminación de información de una forma segura y el limitar el uso de herramientas que no son corporativas, todas estas recomendaciones teniendo en cuenta las normas y leyes colombianas vigentes en este sentido.

En cuanto a las herramientas técnicas que permiten optimizar la seguridad de la información existen algunos software que protegen eficazmente contra delitos informáticos entre los cuales se pueden destacar el Orca Security, Netácea, Bot Management, el Netwrix Auditox y el Bitdefender Total Security, en general la mayoría de estos software realizan actualizaciones de una forma automática, protege los datos en tiempos reales, controlan la banda online y los parentales, gestionan contraseñas, protegen en las redes sociales contra ciberdelitos y contienen un sistema que permite recuperar la información ante ciberataques y hace el cifrado de los archivos.

Se propusieron algunas recomendaciones de buenas prácticas cibernéticas para la consulta y/o adquisición de servicios turísticos por medios electrónicos como son la creación de contraseñas seguras, identificar las practicas que utilizan los cibercriminales, no responder correos electrónicos donde se soliciten datos

personales ni spam, los clientes deben ser precavidos y acudir a agencias de viajes que sean seguras y reconocidas, hacer descarga de archivos que son necesarios, tener cuidado con los fake news, deshabilitar complementos y actualizar regularmente los software de sus ordenadores.

7 RECOMENDACIONES

Es recomendable que los clientes y viajeros de las empresas de turismo, agencias de viajes y hoteles que utilizan las páginas web y aplicaciones tengan una actitud preventiva frente a estos ataques informáticos, ser conscientes de los graves problemas que tendrían al perder su dinero en transacciones ilícitas, fraudes y estafas, con lo que perderían la privacidad de sus documentos por este motivo deben actualizarse en todo momento para evitar estos inconvenientes.

Es fundamental que este tipo de información sea multiplicada, es decir, por todos los medios ya sean virtuales o los medios de comunicación como la televisión, radio, para que las personas sean conscientes de las consecuencias graves que trae el utilizar los datos personales y contraseñas de una forma ligera sin ninguna prevención, esto debido a que en Colombia y en general a nivel mundial aumento abruptamente estos ataques durante la pandemia del Covid 19 sin que existan regulaciones que sean eficaces para castigar a los infractores como tampoco se han brindado soluciones claras ante esta problemática que afecta a gran parte de la población, es una tarea del gobierno nacional que aplique políticas y sanciones severas en este sentido.

Es recomendable que todas las empresas en este caso las que centran sus actividades comerciales en base al turismo el mantener y mejorar los sistemas de ciberseguridad, su planificación y el cumplimiento de los objetivos organizacionales todo con el fin de minimizar y evitar los riesgos que se ven reflejados en los costos operativos.

8 DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este; con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de análisis de las amenazas y riesgos cibernéticos que afrontan los usuarios y las organizaciones en la consulta y/o adquisición de servicios turísticos a través de medios electrónicos, puedan acceder al documento.

BIBLIOGRAFÍA

ACIS. Hotelería y Turismo el Tercer Sector más afectado por ataques informáticas. [Sitio WEB]. Bogotá D.C. ACIS. [28, noviembre, 2018]. Disponible en internet: https://acis.org.co/portal/content/hoteler%C3%ADa-y-turismo-tercer-sector-m%C3%A1s-afectado-por-ataques-inform%C3%A1ticos

ASSISTEMAS. Importancia de la actualización de tu sistema operativo. [Sitio WEB]. México. [25, febrero, 2020]. Disponible en: https://assistemas.net/importancia-de-las-actualizaciones-de-tu-sistema-operativo%EF%BB%BF/

ARATECNIA. Seguridad Informática en el internet de las cosas. [Sitio WEB]. Zaragoza. Cedase. [29, marzo, 2015]. Disponible en: https://aratecnia.es/webcams-vulnerables/

ATICO 34. Suplantación de Identidad ¿Qué es? ¿Cómo Evitarlo? [Sitio WEB]. Madrid. Grupo Atico 34. [28 de febrero de 2020]. Disponible en: https://protecciondatos-lopd.com/empresas/suplantacion-de-identidad/

CAMACHO, Reinerio. Ciberseguridad y Ciberdefensa en Colombia. [En línea]. Articulo. Universidad Piloto de Colombia. Bogotá D.C.: 2013. (Recuperado el 04 de mayo del 2021) Disponible en: http://polux.unipiloto.edu.co:8080/00001172.pdf

CAI VIRTUAL. Conoce como funciona el CAI VIRTUAL de la Policía. [Sitio WEB]. Bogotá. 2020. (19 de octubre de 2020). Disponible en: https://bogota.gov.co/mi-ciudad/seguridad/conoce-como-funciona-el-cai-virtual-de-la-policia

CAI VIRTUAL. Informe Amenazas de Cibercrimen en Colombia 2016-2017. [Sitio WEB]. Bogotá D.C. CAI. [6 de mayo de 2021]. Disponible: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

CÁMARA DE COMERCIO DE BOGOTÁ. [sitio web]. Bogotá: CCB. El turismo mueve más de $1 billón en comercio electrónico en el país. [12-03-2021]. Disponible en: https://www.ccb.org.co/Clusters/Cluster-de-Turismo-de-Negocios-y-Eventos/Noticias/2017/Marzo-2017/El-turismo-mueve-mas-de-1-billon-en-comercio-electronico-en-el-pais

CANALIS, Xavier. Ciberataques a empresas turísticas: las amenazas que vienen. En: Hosteltur. España. 28, junio, 2016. Sec 3. P.1.

CCIT. Tendencias Cibercrimen en Colombia 2019-2020 (29 de octubre 2019, Bogotá D.C.) Tendencias Cibercrimen en Colombia. 2019. 36p

CIBERSEGURITY. Revista de investigación. [en línea]. Guatemala.: 2019. [Consultado 19, julio,2022]. Disponible en: https://csecmagazine.com/2020/04/13/educacion-para-usuarios-sobre-seguridad-de-la-informacion/

CNUDMI. Naciones Unidas. (2013). Guía de la CNUDMI. Datos básicos y funciones de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/12-57494-guide-to-uncitral-s.pdf

DATTA. 11 ataques Informáticos que cambiaron para siempre la ciberseguridad [Sitio WEB]. [28, noviembre, 2018]. Disponible en Internet: https://datta.com.ec/articulo/11-ataques-informaticos-que-cambiaron-para-siempre-la-ciberseguridad

Decreto 2364 de 2012. La firma electrónica y se dictan otras disposiciones. (22 de noviembre de 2012). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=50583

Decreto 1377 de 2013. Protección de datos personales. (27 de junio de 2013). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

DEFINICION ABC. Definición de Contraseña. [Sitio WEB]. Definición ABC. [Diciembre de 2015]. Disponible en internet: https://www.definicionabc.com/tecnologia/contrasena.php

DELGADILLO, P. Revista Iberoamericana de Producción Académica y Gestión Educativa. [en línea]. México: 2015. [Consultado 19, julio,2022]. Disponible en: https://www.pag.org.mx

Dirección General de Sistemas y Tecnologías de la Información. (s.f). Redes. Gobierno del Estado de México. https://normas-apa.org/referencias/citar-pagina-web/comment-page-1/

DW Made for minds. Periódico. [en línea]. 2019. [Consultado 28, noviembre,2018]. Disponible en: https://www.dw.com/es/seis-ataques-cibern%C3%A9ticos-que-sacudieron-el-mundo/a-46967214

El Santuario de la Electrónica. Sistemas electrónicos. [Sitio WEB]. El Santuario de la Electrónica. [2011]. Disponible en: https://elsanturariodelaelectronica.webnode.es/sistemas-electronicos/

ESERP. ¿Qué es e-commerce o comercio electrónico? [Sitio WEB]. España. Eserp Business & Law School. [28, noviembre, 2020]. Disponible en: https://es.eserp.com/articulos/e-commerce-o-comercio-electronico/?_adin=02021864894

FANDIÑO, Jesús Rafael. Marketing digital en las empresas de Turismo de Naturaleza del Departamento de Magdalena. [En Línea]. Articulo. Universidad Nacional Abierta y a Distancia. Santa Marta. (Consultado el 6 de mayo de 2021). Disponible en internet: https://www.researchgate.net/publication/330295536_Marketing_digital_en_las_empresas_de_Turismo_de_Naturaleza_del_Departamento_de_Magdalena

FERNANDEZ, Anibal. La ciberseguridad en España 2011–2015 una propuesta de modelo de organización. [En línea]. Tesis Doctoral. Universidad Nacional de Educación a Distancia España. . 2015. p. 20. Consultado el 6 de julio de 2022. Disponible en: http://e-spacio.uned.es/fez/eserv/tesisuned:CiencPolSoc-Avillalba/VILLALBA_FERNANDEZ_Anibal_Tesis.pdf

GAMBOA, José Luis. Importancia de la seguridad Informática y ciberseguridad en el Mundo actual. [En línea]. Articulo. Universidad Piloto de Colombia. Bogotá D.C. (Consultado el 03 de Mayo del 2021) Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8668/IMPORTANCIA%20DE%20LA%20SEGURIDAD%20INFORM%C3%81TICA%20Y%20CIBERSEGURIDAD%20EN%20EL%20MUNDO%20ACTUAL.pdf?sequence=1&isAllowed=y

GAMELEARN TEAM. 5 programas Informáticos para mejorar tu Ciberseguridad. [Sitio WEB]. Gamelearn. [12, octubre, 2021]. Disponible en: https://www.game-learn.com/es/recursos/blog/5-programas-informaticos-para-mejorar-tu-ciberseguridad/

GNZO. Tipos de delitos informáticos. [Sitio WEB]. La Rioja. [2021]. Disponible en: https://ginzo.tech/blog/tipos-delitos-informaticos/

GREAT PLACE TO WORK. Analizando la postura de seguridad de su organización con ayuda de la matriz Mitre Att&ck. [Sitio WEB]. Soluciones Seguras. [2022]. Disponible en: https://www.solucionesseguras.com/landing/guias-de-interes/38-analizando-la-postura-de-seguridad-de-su-organizacion-con-ayuda-de-la-matriz-mitre-att-ck

HOSTELTUR. Así funcionan las estafas masivas en turismo: por internet y WhatsApp. [Sitio WEB]. Madrid. INCIBE. [03, agosto, 2022]. Disponible en: https://www.hosteltur.com/128292_asi-funcionan-estafas-masivas-turismo-internet-whatsapp.html

INCIBE. 9 claves de Ciberseguridad para el sector del turismo. [Sitio WEB]. Madrid. INCIBE. [28, noviembre, 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/9-claves-ciberseguridad-el-sector-del-turismo

INDEC. Turismo, concepto y definiciones. Consultado el 18 de Julio de 2022. Disponible en: https://www.indec.gob.ar/ftp/cuadros/economia/turismo_cyd.pdf

INFOBAE. El método de estafa virtual que amenaza a los colombianos en el exterior. [Sitio WEB]. Colombia. Infobae. [03, agosto, 2022]. Disponible en: https://www.infobae.com/america/colombia/2020/01/26/el-metodo-de-estafa-virtual-que-amenaza-a-los-colombianos-en-el-exterior/

INFOLAFT. Cibercrimen en Colombia. Todo lo que debe saber. [Sitio WEB]. Colombia. Infolaft. [6 de mayo de 2021]. Disponible: https://www.infolaft.com/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia/

INFORME TENDENCIAS DE CIBERCRIMEN PRIMER TRIMESTRE DE 2020. (abril del 2020, Bogotá D.C.). Informe Tendencias del Cibercrimen en Colombia. Bogotá. Policía Nacional. 2021. 14p.

INFORME DE BUENAS PRACTICAS. (marzo, 2021.España). Centro Criptológico Nacional. 2021. 56 p

INFOSECURITY. Ciberseguridad. Una guía completa del concepto, tipos, amenazas y estrategias, [Sitio WEB]. México. Infosecurity México. [6 de octubre de 2022]. Disponible en Internet: https://www.infosecuritymexico.com/es/ciberseguridad.html

ITECHSAS. Ciberataque a la industria hotelera. [Sitio WEB]. Itechsas. [02 de agosto de 2022]. Disponible en: http://www.itechsas.com/blog/malware/ciberataque-a-industria-hotelera-en-varios-paises/

IZAGUIRRE OLMEDO, Jorge. Análisis de los Ciberataques Realizados en América Latina [En línea]. Articulo. Universidad Internacional del Ecuador. Ecuador D.C.: 2018. (Consultado el 11 de octubre del 2021) Disponible en: https://repositorio.uide.edu.ec/bitstream/37000/3782/13/An%C3%A1lisis%20de%20los%20Ciberataques%20Realizados%20en%20Am%C3%A9rica%20Latina.pdf

KASPERSKY. (2004). Historia de Ciberataques. [Sitio WEB]. AO Kaspersky Lab. [07 de octubre 2022]. Disponible en: https://encyclopedia.kaspersky.es/knowledge/year-2004/

KASPERSKY. ¿Qué es la Ciberseguridad? [Sitio WEB]. AO Kaspersky Lab. [2022]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

KASPERSKY. (2021). Una breve historia de los virus informáticos y lo que nos depara el futuro. [Sitio WEB]. Kaspersky. [11 de mayo de 2021]. Disponible en: https://latam.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds

KUESKI STAFF. ¿Qué es el Carding y los Bineros?. [Sitio WEB]. Bogotá. 2020. (18 de mayo de 2020). Disponible en: https://kueski.com/blog/finanzas-personales/diccionario-finanzas/que-es-carding/

LEGADOO. El Delito Cibernético: [Sitio WEB]. Legadoo. [28 Diciembre de 2016].. . Disponible en: http://legadoo.com/legal/index.php/delitos/delitos-ciberneticos/delito-cibernetico-concepto-clasificaciones/

Ley 527 de 1999. or medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. (18 de agosto de 1999). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

Ley 599 de 2000. Por la cual se expide el Código Penal. (24 de Julio de 2000). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

Ley 1266 de 2008. Habeas data e información contenida en bases de datos personales. (31 de diciembre de 2008). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Ley 1273 de 2009. Por medio del cual se modifica el Código Penal. (5 de enero de 2009). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 1480 de 2011. Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones. (12 de octubre de 2011). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=44306#:~:text=Esta%20ley%20tiene%20como%20objetivos,para%20su%20salud%20y%20seguridad.

Ley Estatutaria 1581 de 2012. Protección de datos personales. (17 de octubre de 2012). https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf

MARIN, Ana Milena. Estudio monográfico sobre casos más comunes de cibercrimen en las pymes colombianas. [En línea]. Monografía. Universidad Nacional Abierta y a Distancia UNAD. Bogotá. 2018. p. 19. Consultado el 6 de mayo de 2021. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/30322/1098663077.pdf?sequence=1&isAllowed=y

MESA, Sara. Impacto del Riesgo Cibernético en el Bienestar del Segmento Mipyme. [En línea]. Trabajo de Grado. Universidad EAFIT. Medellín. 2018. p. 6. Consultado el 6 de mayo de 2022. Disponible en: https://repository.eafit.edu.co/bitstream/handle/10784/12890/Sara_VillaMesa_2018.pdf?sequence=2&isAllowed=y

MITRE ATT&CK. Revista de investigación. [en línea]. Bedford.: 2022. [Consultado 19, julio,2022]. Disponible en: https://attack.mitre.org/tactics/enterprise/

ORGANIZACIÓN MUNDIAL DEL COMERCIO. ¿Qué se entiende por Derechos de Propiedad Intelectual? [Sitio WEB]. Suiza [2022]. Disponible en: https://www.wto.org/spanish/tratop_s/trips_s/intel1_s.htm

PANOSSO, Alexandre. Teorías, Sistemas y Modelos. En; Teoría del Turismo. México. Editorial Trillas.2012.9-38

PAESSLER. ¿Qué es un servidor? [Sitio WEB]. Paessler AG. [2022]. Disponible en: https://www.paessler.com/es/it-explained/server

PÉREZ, Yuly. Importancia de la Ciberseguridad en Colombia. [En línea]. Articulo. Universidad Piloto de Colombia. Bogotá D.C. (Consultado el 03 de mayo del 2021) Disponible en: http://polux.unipiloto.edu.co:8080/00003620.pdf

OJEDA PEREZ, Jorge Eliecer. Delitos informáticos y entorno jurídico vigente en Colombia. [en línea]. Articulo. Universidad Santo Tomas, Bogotá D.C.: 2010. [Consultado 28, noviembre,2018]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

OSI. Aprende a Gestionar Contraseñas. [Sitio WEB]. Unión Europea. [16 de mayo de 2021]. Disponible en: https://www.osi.es/es/contrasenas

PASTOR Javier. Porque es Peligroso Conectarse a Wifi Publicas y que debes hacer para protegerte. [Sitio WEB]. Xataca México. [22 de mayo de 2021]. Disponible en: https://www.xataka.com/seguridad/por-que-es-peligroso-conectarse-a-wifis-publicas-y-que-debes-hacer-para-protegerte

PLAGIUM. Preguntas frecuentes. [Sitio WEB]. Plagium. [2022]. Disponible en: https://www.plagium.com/es/faq

RAMOS, Camino. La Ciberseguridad de los datos en mi Hotel. 2021. En: Entorno Turístico. 21 de enero de 2021. Sec.3. p.3. Disponible en internet: https://www.entornoturistico.com/la-ciberseguridad-de-los-datos-en-mi-hotel/

RIVEROS, Fredy. Administración del Riesgo Cibernético un enfoque desde la alta gerencia empresarial en Colombia. [en línea]. Articulo. Universidad Militar Nueva Granada, Bogotá D.C.: 2016. [Consultado 28, noviembre,2018]. Disponible en internet: https://repository.unimilitar.edu.co/bitstream/handle/10654/15837/RiverosCardenasFredyOrlando2017.pdf?sequence=1&isAllowed=y

ROUSE, M. Copia de Seguridad o Respaldo. [Sitio WEB]. ComputerWeekly. [2018]. Disponible en internet: https://www.computerweekly.com/es/definicion/Copia-de-seguridad-o-respaldo

SAAVEDRA, Jorge Emilio. Diseño de un plan de gestión de riesgos y vulnerabilidades del caso de estudio de la empresa QWERTY S.A., basados en los estándar NTC-ISO/IEC 27001 Y NTC-ISO/IEC 27032. [En línea]. Proyecto de Especialización. Universidad Nacional Abierta y a Distancia UNAD. Boyacá. 2020. p. 21. Consultado el 6 de julio de 2022. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/36866/jsaavedraag.pdf?sequence=3&isAllowed=y

SCIELO. Revista Criminalidad. [En línea]. Bogotá. 2020. [Consultado el 06 de mayo del 2021] Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=es&nrm=iso&tlng=es#B75

SISTEMIUS. Ciberdelincuencia: Los 4 delitos informáticos más comunes. [Sitio WEB]. Santiago de Compostela (24 de abril de 2020). Disponible en Internet: https://www.sistemius.com/ciberdelincuencia-4-tipos-de-delitos-informaticos/

SOFTONIC. Viper. [Sitio WEB]. Softonic International. [16, junio, 2015]. Disponible en: https://viper.softonic.com/

SOLICIT. Seguridad Informática. [Sitio WEB]. Solicit S.R.L. [2022]. Disponible en: http://www.solicit.com.bo/en-us/Productos/Infraestructura-TI/Software/Seguridad-informatica

SINNEX WESTCON- COMSTOR. 6 consejos prácticos de seguridad de la información para usuarios. [Sitio WEB]. [2, septiembre, 2019]. Disponible en: https://digital.la.synnex.com/6-consejos-practicos-de-seguridad-de-informacion-para-usuarios

TicTac. Tendencias del Cibercrimen en Colombia 2019-2020. [en línea]. Articulo. CCIT Bogotá D.C.: 2019. [Consultado 4, octubre,2022]. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

TOKIO SCHOOL. Características principales del monitoreo de red. [Sitio WEB]. Tokio School. [22 de mayo de 2021]. Disponible en: https://www.tokioschool.com/noticias/caracteristicas-principales-monitoreo-red/

UNIPILOTO. Ciberseguridad en Colombia. [En línea]. Articulo. Universidad Piloto de Colombia. Bogotá. 2018. P.12.Consultado el 23 de septiembre del 2021. Disponible en internet: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

UNWTO. [sitio web]. Madrid: Organización Mundial del Turismo. Recomendaciones de la OMT sobre accesibilidad de la información turística. [12-03-2021]. Disponible en: https://www.e-unwto.org/doi/pdf/10.18111/9789284417926

URCUQUI, Cristian Camilo. Ciberseguridad un enfoque desde la ciencia de datos.1 ed. Cali. Editorial Universidad ICESI.2018.90p. ISBN: 978-958-8936-55-0

VALOYES MOSQUERA, Avancio. Ciberseguridad en Colombia. [En línea]. Articulo. Universidad Piloto de Colombia. Colombia. (Consultado el 25 de abril de 2021. Disponible: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

VARGAS RAMIREZ, Claudia Marcela. El comercio electrónico: estrategia para la incursión de las empresas colombianas en el mercado internacional. [En Línea]. Ensayo. Universidad de la Salle, Bogotá: 2011. [Consultado del 21 de julio de 2022]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/3623/VargasRamirezClaudiaMarcela2011.pdf?sequence=2&isAllowed=y

VENDES FACIL. La historia del ecommerce en Colombia. [Sitio WEB]. Medellín. Vendes fácil. [03, octubre, 2022]. Disponible en internet: https://www.vendesfacil.com/ecommerce/la-historia-del-ecommerce-en-colombia/

WELIVESECURITY. Cuando el Cifrado de Datos no es Suficiente. [Sitio WEB]. Welivesecurity. [16 de mayo de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2014/06/30/cuando-cifrado-de-datos-no-es-suficiente/

WELIVESECURITY. Crece el ecommerce y aumentan las estafas y los incidentes de seguridad. [Sitio WEB]. Welivesecurity. [25, noviembre, 2020]. Disponible en: https://www.welivesecurity.com/la-es/2020/11/25/crece-ecommerce-aumentan-estafas-incidentes-seguridad/

WELIVESECURITY (2016). Martes de Retrospectiva: el gusano Morris. [Sitio WEB]. Welivesecurity. [1 de agosto de 2022]. Disponible en: https://www.welivesecurity.com/la-es/2016/11/08/retrospectiva-gusano-morris

XATACA. [Sitio WEB]. México. [19, julio, 2022]. Disponible en: https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

YEPES, H. Las Teorías de la Seguridad. Revista de Ciencias de Seguridad y Defensa. [en línea]. Articulo. Academia de Guerra del Ejercito, Ecuador.: 2018. [Consultado 28, noviembre,2020] Disponible en: https://www.researchgate.net/publication/325023212_LAS_TEORIAS_DE_LA_SEGURIDAD

ZAMBRANO MACIAS, María. Ciberseguridad, riesgo y amenazas de los jóvenes en las redes sociales caso: Colegio Fiscal Mixto Camilo Ponce. [en línea]. Proyecto de Investigación. Universidad Laica “Eloy Alfaro”, Ecuador: 2018. [Consultado 28, noviembre,2020]. Disponible en: https://repositorio.uleam.edu.ec/bitstream/123456789/1756/1/ULEAM-PER-0031.pdf

ANEXOS

Anexo A. Líneas de acción de la estrategia nacional de ciberseguridad

Javier Candau Romero

Línea de acción 1: Desarrollo del Esquema Nacional de Seguridad

Como se ha descrito anteriormente el ENS acaba de nacer. Los organismos tienen un plazo de 12 meses, en principio hasta enero de 2011 para su completa implementación.

Se considera que para los sistemas categorizados en nivel ALTO las medidas de seguridad a implementar podrían necesitar a un tiempo de implantación mayor por lo que tras la presentación del correspondiente plan de adecuación, el RD permite una prórroga de hasta 48 meses (enero del 2014).

Este tiempo de aplicación es una muestra del nivel de exigencia que conlleva el cumplimiento del esquema. Además, para cumplir eficazmente muchas de las medidas de seguridad es necesario formar personal especialista, realizar los análisis de riesgos pertinentes, supervisar la implantación de las medidas mediante auditorias, adquirir tecnología o contratar servicios especializados. Por ello su aplicación requerirá una inversión extraordinaria continuada en el tiempo que no está contemplada en la publicación del Real Decreto y que queda bajo responsabilidad de los diferentes organismos.

Sería necesario, por tanto, dentro de la estrategia nacional de ciberseguridad, impulsar mediante las dotaciones presupuestarias que se estimen convenientes proyectos que faciliten esta implantación. Además, se deben impulsar programas de investigación dirigidos a la mejor implantación de las medidas de seguridad contempladas.

Línea de acción 2: Gestión homogénea de las redes de las AAPP

Para poder gestionar la amenaza de una manera adecuada se debería realizar una gestión única desde el punto de vista de seguridad de las redes de las AAPP. Las interconexiones con INTERNET deben ser las mínimas posibles y deben cumplir los mismos requisitos de seguridad (este aspecto se trata parcialmente en el ENS).

Actualmente la gestión y la seguridad de las redes corporativas es responsabilidad de cada uno de los Ministerios, CCAA, organismos autónomos y Ayuntamientos. Siendo responsabilidad de cada organismo la seguridad tanto de su red corporativa como de las interconexiones. Para ello y a través del Consejo Superior de Administración Electrónica, la conferencia sectorial de las AAPP y la conferencia nacional de la Administración local se deben alcanzar unos requisitos mínimos de interconexión que aseguren una defensa homogénea.

Línea de acción 3: Sistemas de protección de las redes de las AAPP

Para garantizar el nivel de seguridad adecuado en los sistemas de las administraciones públicas es necesario actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance.

Se debe impulsar la entrada en servicio de sistemas de Alerta Temprana para la detección rápida de incidentes y anomalías dentro de las redes de la Administración. Estos sistemas, basado en el análisis y correlación de registros (logs) generados por las herramientas de seguridad instaladas en las citadas redes, permite detectar de manera proactiva cualquier anomalía y ataque analizando el tráfico que circula en y entre los diferentes Ministerios y Organismos.

Por otro lado, es del máximo interés la potenciación de los sistemas similares que permitan monitorizar en tiempo real el tráfico entrante y saliente de las salidas de Internet de los diferentes organismos, recolectando información de seguridad relevante y proporcionando información de los ataques recibidos. Se debe

considerar, además, la inclusión de los sistemas de las empresas que manejan infraestructuras críticas en estos programas.

Entre otros beneficios, los sistemas de alerta temprana permiten:

– Ofrecer una visión en tiempo real del estado de la seguridad de las redes monitorizadas, relacionando la información proporcionada por los diferentes sensores y disponiendo de estadísticas que permitan medir la eficacia de las medidas de seguridad

.

– Disponer de información técnica que permita la implantación de medidas de seguridad adicionales que impidan que ataques similares se vuelvan a reproducir.

– Detección de patrones de ataque comunes a diversas organizaciones que permitan aplicar de forma eficaz medidas de contención y eliminación de estos. La implantación de esta línea de acción será muy costosa en recursos humanos y económicos y su aplicación es muy prolongada en el tiempo, por ello se debe considerar como un servicio horizontal al mayor número de organizaciones posible.

Línea de acción 4: Desarrollo del PPIC ante ciberamenazas

Esta línea de acción se encuentra en su fase inicial pues el borrador de normativa solo lo contempla marginalmente. Sería necesario, por tanto, impulsar la colaboración entre el CNPIC y los organismos especializados en la ciberamenaza en los siguientes campos:

– Gestión de incidentes de seguridad para un tratamiento adecuado de los ciberataques sobre infraestructuras críticas.

– Actualización de información sobre vulnerabilidades tanto de sistemas SCADA como de otros sistemas que soporten estas infraestructuras.

– Cumplimiento por parte de los operadores de los estándares de seguridad que se definan como mínimos.

– Realización de análisis de riesgos y auditorias de seguridad que establezcan los niveles de riesgos a los que están sometidos estos sistemas.

La coordinación debe llevarse a cabo a través de las estructuras que se establezcan al efecto. Sería del máximo interés que estos operadores que manejan infraestructuras críticas se acojan a servicios de alerta temprana similares a los descritos en la línea de acción nº 3.

Línea de acción 5: Programa de formación y concienciación

Según establece la disposición adicional primera del ENS, el personal de las AAPP recibirá la formación necesaria para garantizar el con Líneas de acción de la estrategia nacional de ciberseguridad conocimiento de las medidas de seguridad a implementar.

Es necesario por tanto un esfuerzo continuado en acciones de formación del personal encargado de su aplicación. Además, serán necesarias acciones de concienciación a todos los usuarios para que conozcan y en la medida de lo posible reduzcan las nuevas amenazas a las que nos enfrentamos y que por su naturaleza cambiante se deben plantear a largo plazo.

Por tanto se deben implicar diversos organismos y se deben desarrollar actividades de formación en seguridad horizontales en los diferentes cursos de acceso a las Administraciones Públicas, programas de sensibilización dirigidos a personal que maneje información sensible o clasificada en sistemas, a usuarios de todas las AAPP que estén implicados en servicios de administración electrónica, a empresas que gestionen infraestructuras críticas con sistemas informáticos que los soporten y especialmente a la alta dirección de los diferentes organismos para que proporcione el apoyo necesario a las actividades de seguridad.

También se debe potenciar el desarrollo de cátedras y jornadas en Universidades y otros centros de formación que traten la seguridad en los sistemas de información y comunicaciones. Con estas acciones, a largo plazo, se debería construir una cultura de seguridad en el manejo de los sistemas de información que actualmente es prácticamente inexistente en ciudadanos, empresas y administraciones.

Línea de acción 6: Coordinación de recursos en la respuesta ante incidentes de seguridad

El intercambio fluido de información es fundamental para mitigar los daños causados por los ataques desde el ciberespacio al permitir una pronta identificación de éste y la ejecución temprana de una respuesta rápida y adecuada.

Con esta línea de acción se pretende aumentar las capacidades de inteligencia y defensa por ello, se deben mejorar los procedimientos de intercambio de información entre los centros de operación y los centros de respuesta ante incidentes. Es del máximo interés la realización de ejercicios que demuestren la efectividad de estos canales de coordinación.

Esta coordinación se podrá mejorar si se crean estructuras de Ciberdefensa similares a las de otras naciones en las que se integren las capacidades de respuesta ante incidentes de seguridad existentes actualmente.

Línea de acción 7: Coordinación de esfuerzos de investigación y desarrollo

Observando la rapidez con la que evolucionan los sistemas, la continua aparición de vulnerabilidades que suponen una amenaza para la integridad de éstos, y la creciente dependencia de la sociedad respecto a las tecnologías de la información, se hace necesario el desarrollo de programas, estrategias y tecnologías que proporcionen unos niveles de seguridad superiores a las que ofrecen los actuales sistemas.

En España, además, una de las deficiencias más importantes que se detectan es la escasez de empresas que desarrollen tecnologías de seguridad. Este vacío, empieza a ser crítico cuando se trata del desarrollo de productos de cifra.

Para poder disponer de autonomía en el empleo de las estas tecnologías es necesario potenciar la coordinación en la promoción, el desarrollo, la obtención, la

adquisición y puesta en explotación de productos de seguridad, especialmente si incluyen cifra.

Esta iniciativa se considera crítica para evitar redundancias y para identificar huecos o deficiencias en estos esfuerzos, así como para intentar evitar el empleo de tecnologías de terceros países en aspectos tan críticos como la protección de la información.

Es necesario por tanto impulsar el desarrollo de sistemas más seguros, involucrando para ello al sector privado por su papel en muchas de las infraestructuras críticas nacionales.

Línea de acción 8: Potenciar la colaboración internacional

Por la naturaleza transnacional de la amenaza y del ciberespacio hace necesario una cooperación internacional para hacerle frente. Se deben impulsar la firma de acuerdos en materia de ciberdelitos y crear unas normas de comportamiento en el ciberespacio consensuadas por todas las naciones que pueda facilitar la atribución de los ataques.

Línea de acción 9: Potenciar el empleo de productos de seguridad certificados

Aunque el ENS contempla que las AAPP valoraran positivamente el empleo de productos que tengan sus funciones de seguridad certificadas, este aspecto no es de obligado cumplimiento para poner cualquier sistema en servicio. Es necesario que las tecnologías y productos hayan sido revisadas desde el punto de vista de seguridad. Estos procesos son costosos y difíciles de abordar especialmente para pequeñas y medianas empresas.

Por tanto, se deben impulsar programas que faciliten esta actividad que indudablemente elevará la calidad de los mismos y mejorará la calidad de los productos que consigan esta certificación.

Esta acción permitiría que los productos desarrollados nacionalmente puedan competir en el ámbito internacional pues normalmente poseer una certificación según un estándar internacional (Common Criteria (1) por ejemplo) es requisito para poder acceder a cualquier concurso internacional.

Línea de acción 10: Mejoras de seguridad en los sistemas clasificados

Estas redes manejan la información clasificada y sensible de la Administración para conducir Operaciones de Mantenimiento de Paz, Operaciones Militares, actividades diplomáticas, actividades contraterroristas, actividades de las FCSE o de inteligencia, así como las actividades de seguridad interior. La integridad de estas redes es crítica y cualquier incidente declarado en las mismas puede dañar de forma grave la soberanía nacional.

Se deben reforzar por tanto las medidas de seguridad de estos adaptando las salvaguardas y procedimientos existentes a la evolución de los ciberataques. Para ello a través de las estructuras que es establezcan se debería diseñar un plan de mejora de las mismas y potenciar las capacidades de los organismos que deben auditar y monitorizar la actividad de estas

Anexo B. Normativa internacional relacionada con asuntos de seguridad digital

Instrumento	Materia
Convenio sobre Ciberdelincuencia del Consejo de Europa – CCC (conocido como el convenio sobre Cibercriminalidad de Budapest) Adoptado en noviembre de 2001 y entrada en vigor desde el 1° de julio de 2004	El objetivo principal del convenio es la adopción de una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas.
Resolución AG /RES 2004 (XXXIV-O/04) de la Asamblea General de la Organización de los Estados Americanos	Se establece una estrategia Integral para combatir las amenazas a la seguridad cibernética con un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética. Se estipulan tres vías de acción: i) Creación de una Red Hemisférica de CSIRT, cometido asignado al CICTE de la OEA; ii) Identificación y adopción de normas técnicas para una arquitectura segura de Internet, labor desarrollada por la Comisión Interamericana de Telecomunicaciones; y iii) Adopción o adecuación de los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información de los delincuentes y los grupos delictivos organizados que utilizan estos medios, a cargo de las Reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas - REMJA.
Decisión 587 de la Comunidad Andina, adoptada el 10 de julio de 2004	Por la cual se establecen los lineamientos de la Política de Seguridad Externa Común Andina. Dentro de los objetivos de dicha política se encuentra el prevenir, combatir y erradicar las nuevas amenazas a la seguridad y cuando corresponda sus interrelaciones, a través de la cooperación y coordinación de acciones orientadas a enfrentar los desafíos que representan dichas amenazas para la Comunidad Andina.
Consenso en materia de ciberseguridad de la Unión Internacional de Telecomunicaciones - UIT, en el seno de Naciones Unidas, en desarrollo del programa de acciones de Túnez para la sociedad de la información de 2005	Busca la promoción del examen de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones. Las Resoluciones que emita la UIT son vinculantes para Colombia, puesto que a través de las Leyes 252 de 1995 y 873 de 2004, se aprobó la constitución de la UIT y el Convenio de la UIT, así como las enmiendas posteriores que se han realizado.
Resolución 64/25 "Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional". Asamblea General de las Naciones Unidas (UNGA). (2009)	La Asamblea General exhorta a los Estados miembros a seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en ese ámbito, de manera compatible con la necesidad de preservar la libre circulación de información.

Instrumento	Materia
Directiva 2006/24 de la Unión Europea	Se establece la conservación de datos en la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y fue el referente aplicado por los países miembros hasta el año 2014.
Pronunciamientos de Principios	Resoluciones UNGA: 55/63 y 56/121 sobre la lucha contra el uso delictivo de tecnologías de información; 57/239, 58/199 y 64/211 sobre la creación de una cultura mundial de seguridad cibernética y la protección de infraestructuras críticas de información; Cumbre Mundial sobre la Sociedad de la Información (CMSI), Declaración de Principios y Orden del Día de la Fase de Túnez (en particular la línea de acción C5). Estas son normas o principios generales, que no constituyen reglas y no son vinculantes, sin embargo estos actos o instrumentos jurídicos sin carácter obligatorio, son incardinados de una forma u otra, en el sistema de fuentes del Derecho Internacional (Soft Law).
Marco de trabajo de estrategias nacionales de ciberseguridad. Manual de la OTAN	LA OTAN publica en el año 2012 en colaboración con la NATO Cooperative Cyber Defence Centre of Excellence el manual para la formulación de estrategias nacional de ciberseguridad para sus países miembros.
Declaración de la Cumbre de Gales de la OTAN en 2014	Documento oficial de los resultados de la Cumbre de la OTAN celebrada en Cardiff (Gales) los días 4 y 5 de septiembre de 2014, en donde se resaltan acuerdos para abordar la ciberseguridad en los países de dicha alianza.
Declaración sobre la protección de infraestructura crítica ante las amenazas emergentes (Aprobado durante la quinta sesión plenaria, celebrada el 20 de marzo de 2015)	Declaración en donde, entre otros, la Secretaría Ejecutiva del CICTE de la OEA desarrolla un proyecto de asistencia técnica que, permita a estos la elaboración de un listado de su infraestructura crítica y su clasificación, basados en sus respectivos activos, sistemas, redes y funciones esenciales, para hacer posible la mejor evaluación de vulnerabilidades, brechas, amenazas, riesgos e interdependencia.
Declaración sobre Seguridad en las Américas de la OEA (México, 2003)	Identifica como relevantes, entre otras nuevas amenazas, el terrorismo y los ataques a la seguridad cibernética, y comprometió a los Estados miembros a desarrollar una cultura de seguridad cibernética en las Américas con la adopción de medidas de prevención eficaces para prever, enfrentar y responder a los ataques cibernéticos, cualquiera fuera su origen, luchando contra las amenazas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas.

Fuente: Adaptado de CRC, 2015