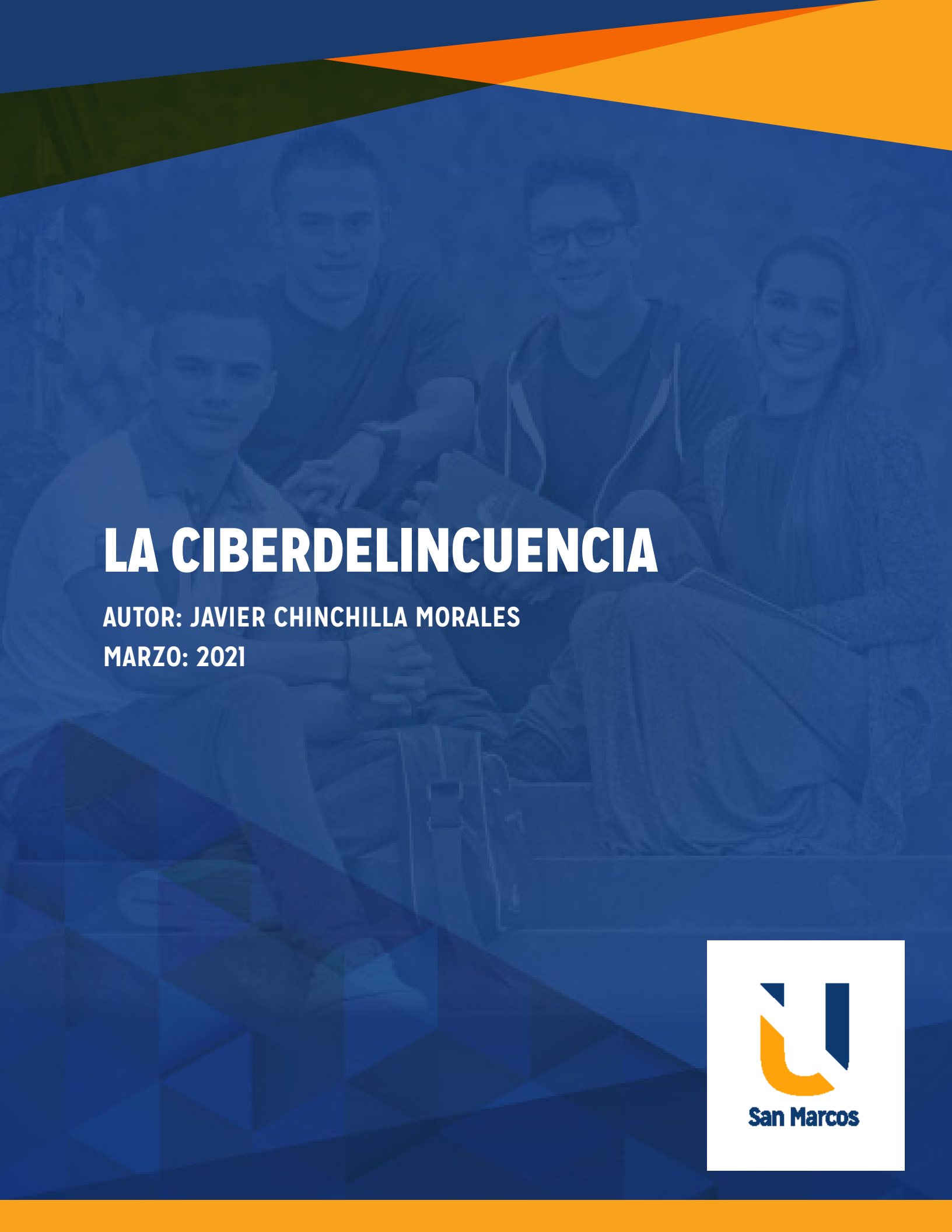

LA CIBERDELINCUENCIA

AUTOR: JAVIER CHINCHILLA MORALES

MARZO: 2021

San Marcos

Tabla de contenido

Introducción 2
La ciberdelincuencia 3
Concepto de delito informático y de ciberdelito 3
Las 4 amenazas más comunes asociadas a ciberdelincuencia 3
Factores que favorecen la expresión de la delincuencia 4
La delincuencia tradicional frente a la ciberdelincuencia 4
Ciberdelincuencia, delincuencia económica y blanqueo 5
Ciberdelincuencia y terrorismo 5
Los ciberdelincuentes 5
Programas indeseables o maliciosos 6
Principios delitos favorecidos por Internet 6
Conclusiones y recomendaciones 8
Referencias bibliográficas 9

Introducción

- La ciberdelincuencia es uno de los delitos transnacionales de más rápido crecimiento a los que se enfrentan los países miembros de INTERPOL. Aunque la rápida evolución de Internet y la tecnología informática han permitido el crecimiento económico y social, una mayor dependencia de Internet ha generado más riesgos y vulnerabilidades, y ha abierto nuevas posibilidades para las actividades delictivas.

La ciberdelincuencia

La ciberdelincuencia es toda aquella actividad que a través de un sistema informático o por medio de una red de comunicaciones "tenga como objetivo atentar a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, las redes y los datos, así como el uso fraudulento de tales sistemas, redes y datos".

Concepto de delito informático y de ciberdelito

Se define como delito informático, delito cibernético o ciberdelito a toda aquellas acciones antijurídicas que se realizan en un entorno digital como lo es el internet, el mismo ha tenido un crecimiento dado al extendido uso y utilización de las nuevas tecnologías en la economía, cultura, industria, ciencia, educación, información, comunicación, y el creciente número de usuarios como consecuencia de la globalización digital de la sociedad, la delincuencia también se ha expandido a esa dimensión. Gracias al anonimato y a la información personal que se guarda en el entorno digital, los delincuentes han ampliado su campo de acción y los delitos y amenazas a la seguridad que se han incrementado exponencialmente. (Ver)

Además de los ataques que tienen como objetivo destruír y dañar activos, sistemas de información y otros sistemas de computadoras, utilizando medios electrónicos y/o redes de internet, se producen nuevos delitos contra la identidad, la propiedad y la seguridad de las personas, empresas e instituciones, muchos de ellos como consecuencia del valor que han adquirido los activos digitales para la big data empresarial y sus propietarios bien sean entes jurídicos o individuos, también existen otras conductas criminales que aunque no pueden considerarse como delito se definen como ciberataques o abusos informáticos y forman para de la criminalidad informática.

Las 4 amenazas más comunes asociadas a ciberdelincuencia

Ciberdelito tipo 1. Las estafas informáticas: cuya conducta consiste en realizar una actividad engañosa produciendo un desplazamiento patrimonial en perjuicio de la víctima y obteniendo así un ánimo de lucro. La estafa informática se diferencia de la estafa normal en que los actos de engaño se dirigen a sistemas informáticos que asimismo producen el consiguiente engaño en la víctima.

Este delito informático podría considerarse como uno de los más cometidos en Europa, y se puede realizar por una multitud de conductas, entre las más habituales están la estafa Nigeriana, donde su autor remite a la víctima un correo electrónico prometiéndole una gran cantidad de dinero a cambio de un ingreso de una determinada cantidad por adelantado.

Dentro de este tipo de ciberdelito se encuentran:

– *El* **phising***:* que consiste en la obtención fraudulenta de contraseñas bancarias con el fin de transferir dinero a otra cuenta bancaria. En estos casos la jurisprudencia ha admitido que la responsabilidad sería del proveedor de servicios de pago (el banco), salvo que se aprecie fraude o negligencia grave en la víctima.

– *El* **carding***:* que consiste en un copiado de las tarjetas de crédito de la victima para realizar posteriormente una adquisición de bienes con estas.

Ciberdelito tipo 2. Los delitos informáticos de daños: Es el caso de los virus informáticos comunes y en particular el *Wanna Cry* entraría en este tipo delictivo. Son delitos informáticos que consiste en borrar, dañar, deteriorar, hacer inaccesibles, alterar o suprimir datos informáticos sin autorización y con un resultado gravoso para el perjudicado. Lo relevante en este delito es que no se exige una cuantía mínima para que se entienda cometido y recaiga condena.

Ciberdelito tipo 3. Las defraudaciones de telecomunicaciones: Todos hemos conocido a algún particular que se creía muy astuto al aprovecharse ilícitamente de la Wifi del vecino sin consentimiento para ello. Este tipo delictivo requiere que se le cause un perjuicio económico a la víctima, y será sancionado con la pena de multa de tres a doce meses si el perjuicio supera los 400 euros .

Ciberdelito tipo 4. Los ciberdelitos contra la intimidad: Son sonados también los casos en que una persona instala en un software en un determinado dispositivo accediendo así a información personal del mismo sin la autorización de su propietario. Podría ser acusado en este caso de un delito de descubrimiento y revelación de secretos con unas penas que no son menores.

Factores que favorecen la expresión de la delincuencia

Hollywood suele hacer mucho daño a la hora de construir estereotipos. Por eso, cuando pensamos en un hacker, nos solemos imaginar a un treintañero con problemas graves de adaptación social, que vive todavía con sus padres y pasa los días y las noches en un sótano lleno de ordenadores y pósters de temáticas comunistas. Nada más lejos de la realidad.

Convertirse en un hacker durante la adolescencia es algo, por desgracia, mucho más habitual y fácil de lo que suele pensar la mayoría de la sociedad. De hecho, para ser un cibercriminal no hace falta ser un programador especializado ni un cerebro privilegiado para el crimen organizado. "*Uno se adentra en este mundo, casi sin darse cuenta, cuando se pone un día a intentar descubrir la contraseña de las redes sociales de un amigo y, poco a poco, se va introduciendo en el lado oscuro*".

La delincuencia tradicional frente a la ciberdelincuencia

Entre los distintos cambios que han sufrido generación tras generación tenemos la evolución tecnológica, lo cual ha cambiado el sistema de comunicaciones entre personas, pero sobre todo ha influído en las transacciones económicas, de la mano con ello los grupos delictivos han visualizado nuevas oportunidades delictivas que les ofrece la interconexión entre culturas con una compleja red de comunicaciones, lo que les permite el desplazamiento de personas mercancías a cualquier lugar del mundo en poco tiempo al igual que la información viaja en tiempo real. Todo éste progreso tecnológico indudablemente ha favorecido a los grupos delincuentes tradicionales a reinventarse. Los avances en las telecomunicaciones (fundamentalmente a través del ciberespacio), ha proporcionado un ilimitado escenario sobre el que operar a los grupos de delincuencia organizada. La extensión del comercio electrónico (identidades virtuales) facilita la ocultación tanto de la actividad delictiva como de los propios delincuentes, por lo que la circulación del dinero (incluyendo las ganancias procedentes de la comisión de delitos) puede hacerse rápidamente y desde un extremo a otro del mundo.

De la misma forma las organizaciones delictivas no se privan de la utilización de cualquier otro tipo de sistema tecnológico (electrónicos, digitales infraestructuras y diversas formas de ocultación) directamente orientado a facilitar la ocultación de la acción investigadora policial y de la justicia.
Una de las grandes ventajas con las que cuentan los delincuentes es su capacidad para adquirir los elementos tecnológicos que precisen sin verse obstaculizados por tener que velar por los costes de aquellos.

Ciberdelincuencia, delincuencia económica y blanqueo

Todos estos términos van de la mano y encadenados uno al otro respectivamente para concluir con el blanqueo de capitales que consiste en ocultar o encubrir la identidad de beneficios obtenidos ilícitamente, de forma que parezcan provenir de fuentes legítimas. Normalmente, es un componente de otros delitos mucho más graves como el tráfico de drogas, robos con violencia o extorsión.
El blanqueo de capitales está presente en todas partes y se encuentra en áreas inesperadas, como en los delitos medioambientales. La llegada de las criptomonedas, como bitcóin, ha exacerbado este fenómeno. Los grupos delictivos transfieren fondos obtenidos ilícitamente por todo el mundo a través de los bancos, sociedades ficticias, intermediarios y empresas de envío de dinero, intentando integrar los fondos ilícitos en negocios y economías legales. Actualmente, las “mulas” desempeñan un papel clave en este contexto. Se trata de personas que actúan como intermediarios para los grupos delictivos, incluso sin ser conscientes de estar blanqueando fondos ilícitos.

Ciberdelincuencia y terrorismo

El Consejo de Europa define el ciberterrorismo como al “terrorismo que utiliza las tecnologías de la información para poder intimidar, coaccionar o causar daños a grupos sociales con fines políticos-religiosos”. La ciberdelincuencia y el ciberterrorismo buscan desestabilizar las estructuras sociales establecidas. España fue el tercer país, tras Estados Unidos y Reino Unido, que mayor número de ataques cibernéticos sufrió en 2014. Según declaraciones del ministro de Asuntos Exteriores, existieron más de 70.000 ciberincidentes de los que no detalló la gravedad. Los crímenes del ciberterrorismo, cuando tienen intención de causar pánico colectivo, una alarma social generalizada, responden a una motivación ideológica determinada, conllevan implicaciones más graves que los delitos comunes para la seguridad nacional y la política de defensa. Determinando que el origen del ciberterrorismo radica intrínsecamente en su misma raíz como espacio cibernético, escenario dónde se desarrollan las amenazas cibernéticas. Si tomamos como base la conceptualización emanada del Departamento de Defensa de los Estados Unidos en el año 2016, el ciberespacio sería “un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores”. Estas nuevas ventajas son usadas por las organizaciones terroristas para el cumplimiento de sus objetivos estratégicos, el funcionamiento de cuidadosas estrategias de marketing, una adecuada utilización de redes sociales virtuales, y así conseguir recursos económicos y otros, con el fin de realizar su cruzada armamentista.

Los ciberdelincuentes

Con el uso de las nuevas tecnologías para cometer ataques cibernéticos contra gobiernos, negocios e individuos, palabras y frases que hace una década apenas existían, forman ahora parte de nuestro vocabulario diario. Estos delitos no conocen fronteras, ni físicas ni virtuales, causan importantes daños y suponen un peligro muy real para las víctimas de todo el mundo.
La ciberdelincuencia crece a un ritmo muy acelerado, con nuevas tendencias emergiendo continuamente. Los ciberdelincuentes se están volviendo más ágiles, explotan las nuevas tecnologías a una velocidad de vértigo, adaptan sus ataques utilizando nuevos métodos y cooperan entre sí de manera nunca vista hasta ahora. Las redes delictivas operan a escala planetaria, coordinando ataques complejos contra sus objetivos en cuestión de minutos.
La policía debe por tanto mantenerse al día en las nuevas tecnologías, con el fin de comprender las posibilidades que crean para los delincuentes y su uso como herramientas para luchar contra la ciberdelincuencia.

Programas indeseables o maliciosos

El malware es el nombre que agrupa a distinto software malicioso como virus, gusanos o caballos de Troya, que crecen rápidamente y afectan a los contenidos de los sistemas informáticos al que accedes. En relación con los ataques basados en el uso de la web, hay que indicar que existe gran variedad, como, por ejemplo, las web que visita el usuario y compromete a su equipo, abren puertas traseras y vulneran su navegador. También se usan ataques a través de una aplicación web, quedando expuestos o vulnerables sectores importantes como la administración pública.
Los ataques por denegación de servicio (DDoS, Denial of service) hacen que sea imposible el acceso a los propios recursos y servicios de una organización o empresa y posteriormente solicitan un rescate para detener los ataques. El “bot” es otro programa malicioso utilizado para tomar el control de un equipo informático, sin que sea detectado fácilmente. El phishing es el término informático que se utiliza cuando el atacante intenta suplantar la identidad de cualquier víctima para adquirir su información confidencial. El conocido de forma universal como spam o correo basura, centra su acción en el envío de correos a un gran número de usuarios perjudicando al receptor.
El ransomware es otro software malicioso que infecta y le da al atacante la posibilidad de bloquear su equipo informático y controlar sus datos. En relación con la amenaza interna hay que indicar que se trata de una persona o agente, normalmente empleado o funcionario de una institución que tiene acceso a los programas informáticos de la organización para causar un incidente grave de seguridad. El robo o pérdida de material sensible, también se considera como una amenaza que afecta a la fuga de datos y robos de identidad. Si se tiene un conocimiento y habilidades especiales, se puede desarrollar un kit de explotación de vulnerabilidades de seguridad para tener una posición dominante sobre los competidores tanto económicos como institucionales, esas habilidades pueden proporcionar una brecha o violación de datos de carácter confidencial, robar la identidad, violar los datos correspondientes a registros personales, o realizar operaciones de espionaje cibernético a gran escala.

Principios delitos favorecidos por Internet

El desarrollo de la tecnología y la interacción social a la que venimos asistiendo, ha propiciado el acceso ilimitado a mucha información y ha facilitado la difusión de contenidos de forma masiva.
La nueva forma de vivir con la tecnología también ha favorecido la aparición de delitos asociados a este

ámbito y cada vez existe mayor preocupación en relación a la legislación en este nuevo entorno.
En este sentido, tenemos recientemente claros ejemplos, de cómo esta nueva configuración social-tecnológica ha influido, por ejemplo, en la difusión de contenidos que nunca debieran haber salido de la vida privada.
Nuestra legislación es clara en este aspecto y la vigente normativa de protección de datos tipifica como delito contra la intimidad la difusión de datos correspondientes a la esfera de la vida privada sin consentimiento de la persona implicada.
En cualquier caso, en este tipo de situaciones, la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico otorga competencias al poder judicial para ordenar la retirada o bloqueo del contenido ilícito incluso a través de los proveedores de servicios de datos alojados en servidores extranjeros.

Conclusiones y recomendaciones

Con la aparición del ciberespacio, el hábitat delictivo ha crecido exponencialmente, pues la era de la información multiplica las oportunidades de los delincuentes. El ciberterrorismo se aprovecha de la existencia del ciberespacio para magnificar sus ataques y se ha convertido en la mayor pesadilla para la seguridad de las naciones occidentales. Tiene unas características tan amplias y destructivas que exige una respuesta inmediata, contundente, unida, continuada e incansable de las naciones. Nacen tantas amenazas desde cualquier lugar del mundo, la mano es tan larga y puede ser tan destructiva, que los Estados deben responder a tanto y tan rápido, que de no hacerlo, se podrían causar daños humanos, sociales y económicos irreparables.

Una vez determinados los nuevos delitos y sus penas, podemos decir que las leyes deben estar atentas a los cambios constantes de las amenazas, porque de no hacerlo los delincuentes sacarían un gran partido de ello. Así la Unión Europea y sus miembros, siguen la línea de estandarizar todo lo posible los delitos y sus legislaciones propias antiterroristas, para en consecuencia poder combatir de forma compacta y unida este germen llamado ciberterrorismo. De forma seguida, al análisis legislativo y hablando ya de las directrices defensivas, tras nuestro análisis, intuimos que para el éxito en la lucha contra el ciberterrorismo, no sirve un sistema de defensa nacional simple y convencional, además de la tecnología más moderna, se necesita un conjunto de sistemas de defensa que a su vez se unen a otros, creciendo según aumentamos fronteras, esto nos hace concluir que la ciberdefensa es un gran entramado mundial de sistemas defensivos. La Unión Europea y la OTAN tratan de marcar las directrices de esta lucha en Europa.

Referencias bibliográficas

- Corletti, A. (2017). *Ciberseguridad (una estrategia informático (militar).* www.darFe.es. Recuperado de https://www.slideshare.net/acorletti/libro-ciberseguridad-una-estrategia-informtico-militar?from_action=save
- Salas, A. (2015). *Los hombres que susurran a las máquinas*. Espasa Libros, S. L. U. Recuperado de https://www.planetadelibros.com/libros_contenido_extra/32/31258_1_PREFACIO_Los_hombres_que_susurran_a_las_maquinas.pdf

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica