Universidad Tecnológica ECOTEC

Nombre de la Facultad: *DERECHO Y GOBERNABILIDAD*

Título del trabajo: *DELITOS ELECTRÓNICOS: TIPIFICACIÓN JURÍDICA SOBRE EL CARDING Y CRACKING*

Línea de Investigación*: PROYECTO DE INVESTIGACIÓN*

Modalidad de titulación: *ONLINE*

Colocar el nombre de la carrera con su énfasis: *CIENCIAS PENALES Y CRIMINALISTICA*

Título a obtener*: ABOGADO*

Autor (a): *DAVID LENIN PROAÑO MERCHAN*

Tutor (a): *MARÍA SOLEDAD MURILLO*

SAMBORONDON – ECUADOR

2023

Índice

DEDICATORIA

Mi dedicatoria va dirigida a mi valiente padre Omar Proaño y mi sabia madre Yadira Merchan por ser un ejemplo invaluable para mi perseverancia, constancia y de nunca desistir por lo que uno sueña y anhela de corazón; A mi abuelito Goyo, abuelita Nereida y mi hermanito Moisés, que me observan desde el cielo que seguro estarán felices por este logro y paso muy importante en mi vida.

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento a la Universidad Ecotec, por ser la institución que me ha formado y a mi tutora la Abogada María Soledad Murillo, quien me guio de principio a fin en mi elaboración de tesis, por ser una excelente docente y consejera; También una mención especial para mi mejor amigo Jonathan, amiga Roxanna y tía Roció Córdova, quienes siempre me impulsaron hasta el final de esta carrera.

ANEXO N°15

CERTIFICADO DEL PORCENTAJE DE

COINCIDENCIAS

Habiendo sido nombrado MARIA SOLEDAD MURILLO, tutor del trabajo de titulación" (DELITOS ELECTRÓNICOS: TIPIFICACIÓN JURÍDICA SOBRE EL CARDING Y

CRACKING)" elaborado por DAVID PROAÑO MERCHAN, con mi respectiva supervisión como requerimiento parcial para la obtención del título de ABOGADO.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias (9%)
mismo que se puede verificar en el siguiente link: (https://app.compilatio.net/v5/report/8b69c0e1af97f582bd7fbf9365788e35b25e3420/sources).

Adicional se adjunta print de pantalla de dicho resultado.

MARÍA SOLEDAD MURILLO ORTIZ, MGTR

ANEXO N°16

CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN DELTRABAJO DE TITULACIÓN CON INCORPORACIÓN DE LAS OBSERVACIONES DE LOS MIEMBROS DEL TRIBUNAL

Samborondón, 11 de agosto del 2023

Magíster

Andrés Vicente Madero Poveda

Decano(a) de la Facultad Derecho Y Gobernabilidad

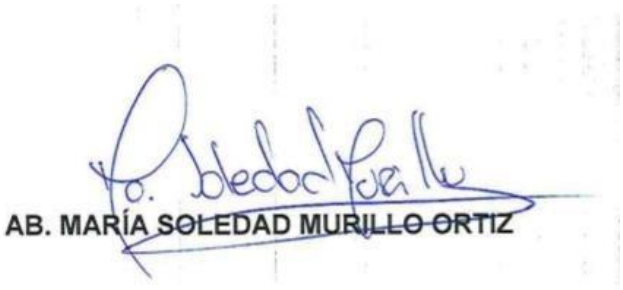
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO:

DELITOS ELECTRÓNICOS: TIPIFICACIÓN JURÍDICA SOBRE EL CARDING Y CRACKING según su modalidad PROYECTO DE INVESTIGACIÓN; fue revisado y se deja constancia que el estudiante acogió e incorporó todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a: ***Proaño Merchan David Lenin,*** *para que proceda a la presentación del trabajo de titulación para la revisión de los miembros del tribunal de sustentación y posterior sustentación.*

ATENTAMENTE



AB. MARÍA SOLEDAD MURILLO ORTIZ

Resumen

En la presente tesis se realizará el análisis sobre el tratamiento jurídico que se le da cabida en legislación penal sobe el carding y el cracking correspondiente entre los años 2020-2022, que, a lo largo de su historia, se relata su evolución y como este afecta a las instituciones jurídicas, patrimonio y datos de los cibernautas. Esta investigación destaca dos delitos en particular que es: el carding, refiriéndose a la utilización fraudulenta de tarjetas de crédito o débito, entre otros datos financieros para realizar transacciones no autorizadas; Y el cracking describe el proceso de eludir o destruir las medidas de seguridad de un software o sistema para obtener acceso no autorizado con fines ilegales. Según los parámetros establecidos, dentro de esta investigación se ha utilizado el Método de Análisis histórico, en la cual permite analizar las instituciones del derecho, se puede verificar los hechos pasados, basándose en los relatos del pasado que han realizado diferentes autores; El Método Jurídico comparado que permite establecer la semejanza y las diferencias existentes entre las reglamentaciones nacionales y extranjeras. Mediante este procedimiento, se busca las igualdades que ostentan los diferentes ordenamientos jurídicos, teniendo en cuenta los otros sistemas jurídicos contemporáneos. El cual esto ha permitido identificar los hitos normativos del carding y el cracking, caracterizar esto delitos con su respectiva aplicabilidad y establecerlo mediante legislación comparada en relación al código penal tanto local como extranjero. Así mismo, se ejemplifico dos casos prácticos que ponen a prueba los derechos de las personas que participan mediante los dispositivos electrónicos, dejando en evidencia que se debería determinar y tipificar de manera precisa los conceptos de estos delitos informáticos en el Ecuador.

Palabras claves: Delito, carding, cracking, fraude, internet, ciberdelitos.

Abstract

In this thesis, the analysis will be carried out on the legal treatment that is accommodated in criminal legislation on carding and the corresponding cracking between the years 2020-2022, which, throughout its history, its evolution and how it is related. affects legal institutions, assets and data of netizens. This investigation highlights two crimes in particular: carding, referring to the fraudulent use of credit or debit cards, among other financial data to carry out unauthorized transactions; And cracking describes the process of bypassing or destroying the security measures of a software or system to gain unauthorized access for illegal purposes. According to the established parameters, within this investigation the Historical Analysis Method has been used, in which it allows analyzing the institutions of law, past events can be verified, based on the stories of the past that different authors have made; The comparative Legal Method that allows determining the similarity and differences between national and foreign legislation. Through this method, the similarities that the different legal systems have are sought, taking into account the different contemporary legal systems.

Which this has allowed to identify the normative milestones of carding and cracking, to characterize these crimes with their respective applicability and to establish it through comparative legislation in relation to the penal code, both local and foreign. Likewise, two practical cases were exemplified that evidence the violation of the rights of the people who intervene through electronic devices, leaving in evidence that the concepts of these computer crimes in Ecuador should be determined and classified in a precise way.

Keywords: Crime, carding, cracking, fraud, internet, cybercrime.

Objetivo general

ANALIZAR el tratamiento jurídico que da la legislación penal al carding y cracking **en los años 2020-2022**

Objetivos específicos

1. **CARACTERIZAR** el delito de Carding y Cracking y su aplicabilidad
2. **ESTABLECER** legislación comparada del delito de carding y cracking, dentro de los países Colombia, México, España.
3. **IDENTIFICAR** hitos normativos del delito de carding y cracking

INTRODUCCIÓN

Los delitos informáticos, también conocidos como ciberdelitos o delitos electrónicos, son acciones ilícitas que se llevan a cabo a través de medios electrónicos o digitales. Con el progreso tecnológico y la gradual conectividad digital, estos delitos se han convertido en una inquietud global, ya que afectan a individuos, empresas y gobiernos en todo el mundo. Los delitos electrónicos comprenden una extensa gama de actividades ilegales, como el hacking, el robo de información personal, los fraudes financieros, la distribución de malware, la suplantación de identidad, el ciberacoso y las violaciones de derechos de autor, cracking y clonación de tarjetas. Estos delitos pueden tener derivaciones graves, como tales pueden ser: pérdidas financieras, daño a la reputación, invasión de la privacidad y angustia emocional para las víctimas. La particularidad de la mayoría de estos ciberdelitos es su accionar transnacional y su capacidad para traspasar fronteras sin restricciones físicas algunas. Los delincuentes cibernéticos pueden maniobrar desde cualquier lugar del mundo, a través de cualquier dispositivo electrónico, y así dirigirse a víctimas en cualquier ubicación territorial. Esto nos hace plantear varios retos significativos en términos de jurisdicción y cooperación internacional para investigar y procesar a los responsables de estos delitos.

Dentro de esta investigación se destacará sobre dos delitos en particular, que son el Carding, que es el uso engañoso de tarjetas de crédito o débito, así como otros datos financieros, para realizar transacciones no autorizadas o también conocida como duplicación de las tarjetas; Y el Cracking que se describe al proceso de evadir o romper las medidas de seguridad de un software o sistema para obtener acceso no autorizado, con fines ilegales.

ANTECENDENTE

La formación de nuevas tecnologías que interceden en las conexiones, entre las personas trae capacitado nuevas posibilidades para su aprovechamiento indebido y arbitrario. Este ha sido el caso desde la invención del telégrafo y la posterior adopción del teléfono en la vida cotidiana. Así ha sido desde el desarrollo del telégrafo y la posterior adopción del teléfono en la vida cotidiana. Con la invención de la computadora personal y el consiguiente crecimiento de Internet y la World Wide Web, se han hecho posibles las capacidades de procesamiento de datos e información, así como la capacidad de llegar a millones de personas a través de medios interactivos de naturaleza global. Estas capacidades se basan en un entorno digital "amigable" que es fácil de usar y conveniente, con aplicaciones sencillas. Los delitos informáticos tienen sus orígenes en la década de 1960, cuando la literatura planteó preocupaciones sobre la recopilación y el almacenamiento de datos personales en las computadoras. La novela alude a 1984 de George Orwell, en la que el omnipresente Gran Hermano utiliza la tecnología para gobernar y observar la vida de las personas. Después de que se publicaran artículos periodísticos sobre casos específicos, apareció por primera vez el término "delito informático" o "delitos relacionados con la informática". Más tarde, la literatura fantástica de la época adoptó el término para publicar obras afines, que luego se definió como un "género". **"Ciberpunk".** Varios programadores o expertos informáticos intentaron protestar contra la financiación gubernamental de la guerra de Vietnam en la década de 1960 mientras muchas flores florecían en América del Norte mediante el uso de un servicio telefónico gratuito.

Los terminales de computadora conocidos como "cajas azules" fueron utilizados por "freak", un neologismo poco común derivado de la palabra inglesa "freak", en el activismo político hippie de esa época. A través de la simulación, se creó la "caja azul" o comunicación libre.

Bell y ATT utilizan principalmente el timbre para comunicaciones de larga distancia. Con el tiempo, estos métodos de piratería han avanzado y también se han utilizado para manipular transacciones financieras realizadas a través de redes telefónicas vulnerables.

La gestión de la información para el almacenamiento y procesamiento de datos personales es la principal preocupación cuando se utilizan computadoras. Varios casos

comenzaron a surgir ya en la década de 1970 del siglo XX, lo que resultó en pérdidas significativas para el sector privado. Se desarrolla a partir de delitos económicos como la extorsión, el robo de software, el espionaje informático y el sabotaje. En el caso del espionaje, estas acciones incluyen la copia directa de equipos de cómputo, el robo directo de equipos de cómputo (como discos duros y disquetes) y la absorción de radiación electromagnética para la recolección de datos. Los delincuentes persiguieron programas informáticos, datos de investigación de defensa, datos de contabilidad comercial y combinaciones de direcciones de clientes. Los gobiernos y las empresas están más preocupados por la extorsión y el sabotaje informático debido a la alta concentración de información almacenada electrónicamente en estos delitos. La forma de hacer las cosas tiene que ver con cómo se manejan las facturas de pago de salarios individuales y los saldos bancarios. Desde principios de la década de 1980, los delitos informáticos han ganado una notoriedad considerable debido al aumento exponencial del fraude y los esfuerzos de las organizaciones internacionales para abordar el problema. Los casos típicos de fraude involucraron la manipulación del uso de la tarjeta de débito en los cajeros automáticos, principalmente al comprometer la banda magnética. Esto motivó a las empresas emisoras de chips a utilizar chips de plástico como medida d e seguridad. En ese momento, comenzaron las protecciones regulatorias para los activos intangibles como el dinero electrónico en los países europeos, un proceso iniciado por l os Estados Unidos en 1978. Se requería el respaldo legal, de las bases de información y datos de las instituciones y empresas bancarias para realizar negocio, en principio contra el robo de información comercial. A fines de esa década, comenzaron a aparecer en las redes contenidos ilegales y dañinos, como amenazas a las personas, discursos de odio y el intercambio de pornografía infantil, así como sucesos de violencia y segregación racial por parte de tropas extremistas**.** Nuevos métodos de hacking manipulaban sistemas destacados, ya sistemas hospitalarios y de salud, específicos como "ataques contra la vida". Esta historia aumentó significativamente al gemelo del aumento de usuarios de la cerca, haciéndose asequible a altura gubernamental en 1989, cuando la neutralidad alemana determino quienes eran los hackers, que manipulaban las redes de antecedentes internacionales para el ataque a declaración privilegiada de Estados Unidos y Gran Bretaña para distribuir la declaración a la KGB. Con la iniciación total de Internet a mediados de los 90s por bocado de la empresa norteamericana y

posteriormente incursiono hacia las empresas y bancos a la cerca para el crecimiento del establecimiento electrónico, la dificultad decisiva pasaba por el crecimiento de estándares de encriptación seguros para el crecimiento de operaciones financieras y la licitación de existencias en fila. Asimismo, la ingenio discográfica y cinematográfica comenzó un borrón versus la diversidad de casos de violaciones a los tributos de ejecutor a quebrar de la fuego e intercambio en fila de canción y películas ruin jurisprudencia de copyright, lo que generó una discusión acerca de cómo armonizar acciones de protección internacional para eludir fugas del negocio.

Las autoridades de varias naciones advierten sobre una ola de pedofilia en casos de abuso sexual o acoso sexual de menores en línea a medida que circulan en línea imágenes y/u ofertas de servicios sexuales a menores. Presente el tema de la protección de la privacidad y los problemas que la rodean en la era de las nuevas tecnologías. *(Sain, 2015)*

Se requiere la regulación de estos delitos cibernéticos, se debe evaluar la gravedad del delito y el daño que causó. Debido a que afectan las bases de datos y la información que comparten múltiples usuarios, estos delitos con frecuencia conducen a referencias significativas que tienen un impacto en varias personas y luego se comparte con usuarios de un nivel superior, y así sucesivamente, hasta llegar al usuario final, que es el último en romper la cadena, perder la información o alterarla.

Debido a que el concepto y el primer paso tienen diferentes significados en México, todo lo relacionado con el delito informático debe ser homogeneizado para detenerlo antes de que las propias instituciones lleguen al punto en que sean incontrolables.

Será necesario que una parte importante de la sociedad de la información trabaje con las autoridades legislativas para normalizar los hechos.

Hay varias leyes vigentes en este momento que, de alguna manera indefinida, protegen a los fabricantes de sistemas de información y, más ampliamente, a los autores intelectuales de programas de computadora.

Estos estatutos son similares a la Ley Federal del Derecho de Autor, al Código Penal en materia de jurisdicción general del distrito federal y al Código Penal de toda la República en materia de jurisdicción federal, pero en sentido estricto sólo contemplan sanciones relativas a la propiedad intelectual y no abordar los delitos informáticos propios**.** No se da a entender que se trata de un programa de computadora, y dado que no tienen ninguna relación fundamental en todos los sentidos, es imposible tratarlos de manera similar.

Como resultado del comercio electrónico, ahora hay minoristas en línea, profesores conectados que ofrecen educación en línea y médicos que asignan pacientes a oficinas en línea. Es cuestión de tiempo y percatarse a simple vista que, existen ciberdelincuentes que cometen ciberdelitos.

Internet es un vasto conglomerado de empresas, individuos, gobiernos, instituciones educativas y organizaciones de todo tipo que generalmente han acordado un conjunto estandarizado de protocolos de comunicación, lo que hace de este servicio un canal de comunicación abierto para todos. En la Super autopista de la Información 424 no hay policías, ni patrullas que trabajen con radar o detengan a los sospechosos para registrarlos, ni para traer armas. En este ambiente hay una gran diferencia con las reglas y normas que se aplican en cada calle, en cada ciudad, en cada país del mundo, y lamentablemente en el ciberesp acio hay personas sin rostro y sin nombre, todo es virtual

CAPITULO 1

Marco teórico

La Teoría Del Delito

La teoría del delito es un proceso categórico y secuencial en el que se deriva paso a paso de concepciones primitivas del comportamiento (diversos elementos básicos comunes a todos los tipos de delitos). *(Machicado, 2010)*

Delito

La palabra "delito" proviene de la palabra "delinquere" que significa "apartarse del camino". *(Solís, 2015)*

El delito se lo conoce por ser una valoración de la dirección humana establecida por el criterio ético de la clase que sujeta la sociedad.

Los conceptos de delito se extienden en los siglos XVIII, XIX y XX. Y se dan a conocer de la siguiente forma:

Concepciones formales o nominales.

Se establece en que la contravención es una acción humana que se afronta a lo que la ley manda o prohíbe bajo el ultimato de una pena. Es la ley la que crea que hechos son delitos, es la ley la que menciona que hecho va ser estimado como delito, es la ley la escoge y fija caracteres delictuales a un hecho, si en algún instante aquella ley es revocada el delito desaparece. El delito es artificial. Se asume: la "concepción judicial" y "filosófica" del delito

Concepciones substanciales o materiales.

Establecen manuales del delito como presupuestos para que un hecho voluntario humano sea considerado como delito, el delito es un acto humano típicamente antijurídico culpable y castigada con una penalidad de representación criminal. Sigue el método analítico. Se asume: la "concepción del dogmatismo" y la "concepción sociológica" del delito. *(Machicado, 2010)*

Clasificación del delito

Por su Gravedad:

El método tripartito divide en delitos, faltas y contravenciones. Permite la individualización, la sociedad responde mejor al delito y tiene beneficios: determina juri sdicción de los tribunales, los jurados conocen los delitos, corrigen los delitos y la policía, los delitos. Crítica. No hay diferencia cualitativa entre un crimen y una felonía; un trauma puede ser ambos, dependiendo de la mínima o maxima amenaza de sus resultados. Método bilateral se fracciona en delitos y faltas.

Se Fundamenta en la penalidad y la jurisdicción. Las discrepancias entre un delito y una infracción penal coexistirían las siguientes: en un delito el daño es real, en un delito hay mero peligro; el delito tiene una intención clara, el delito no tiene intención maliciosa. *(Idocpub, 2019)*

Por la Forma de la Acción: Acción, inacción, inacción. Violaciones criminales de leyes prohibidas, como robo, difamación, aborto. La negligencia viola los términos obligatorios, como la denegación de servicio. *(Cortez & Chang, 2012)*

Por la Forma de Ejecución: momentáneo, intacto, extendido, flagrante, conexo o combinado. *(Cortez & Chang, 2012)*

Delito instantáneo. Esta caduca también aquel en que se cometió el delito en el momento de su comisión. La acc ión coincide con la consumación del hecho; El agente no tiene ningún dominio para prolongarlo ni para hacerlo cesar.

Delito Permanente. La ofensa continuará ininterrumpidamente después de que haya terminado. ej. secuestro, abandono.

Delito Continuado. La acción rodea una cadena de infracciones jurídicas que extienden a un único resultado. *(Idocpub, 2019)*

La ley no da relevancia a estos actos (sí fuera así, serían varios delitos) Ej.: cajero que saca centavo a centavo incluso reunir una suma formidable. *(Cortez & Chang, 2012)*

Delito Flagrante. Es el que se ha considerado públicamente y cuyo causante fue visualizado por muchos informadores en el lapso en que lo cometía. *(Idocpub, 2019)*

Delito Conexo. Las acciones están afines de tal modo que unos resultados dependen de unas acciones y otros resultados de otras acciones. *(Idocpub, 2019)*

Ej., Los delincuentes se ponen de acuerdo antes, luego realizan delitos en diferentes tiempos y lugares. *(Cortez & Chang, 2012)*

Por las Consecuencias de la Acción: formal, material. *(Cortez & Chang, 2012)*

Delito formal (o de simple actividad), es aquel en que la ley no requiere, Considéralo cumplido, es decir, los resultados por los que se esforzó el oficial; también es suficiente el hecho que conduce a estos resultados y el reconocimiento del riesgo de su ocurrencia o simplemente la expresión de la voluntad. *(Cortez & Chang, 2012)*

En los delitos sensatos jamás se da la Tentativa, este sólo se da en los delitos materiales. *(Idocpub, 2019)*

Delito material (o de resultado): es el que se consuma mediante la creación de un daño efectivo que el delincuente se plantea. El acto causa un resultado. *(Idocpub, 2019)*

Ej., el delito, es el resultado de la acción es la muerte de una persona. En el robo, el efecto es la aprehensión del objeto. *(Cortez & Chang, 2012)*

Por la Calidad del Sujeto: Los delitos ilegales, auto ilegales son delitos cometidos por cualquier persona. Un delito personal es un delito cometido por una

persona que cumple ciertas condiciones relacionadas con un cargo público, cargo o profesión. *(Cortez & Chang, 2012)*

Por la Forma Procesal: de acción privada, de acción pública a petición de parte, de labor pública. *(Idocpub, 2019)*

Delito de conducta privada.

En los casos de sobregiro, robo y delitos contra la reputación (como difamación y calumnia), solo se procesa a la parte que ha sido agraviada. violación de la ley a petición de parte.

La única parte necesaria en los casos que los fiscales pueden adelantar es la parte lesionada u ofendida. Por ejemplo, dejar a la familia, dejar a la mujer embarazada, proxeneta. Violación de la conducta pública. Cualquier persona, incluida la oficina del fiscal, tiene derecho a iniciar un caso. por ejemplo, para asesinar.

Por las Formas de Culpabilidad: doloso, culposo. *(Cortez & Chang, 2012)*

Delito doloso. Cometer un acto ilegal típico con el conocimiento y la voluntad de hacer el resultado. No se requiere conocimiento de la ley, es suficiente que sepa que lo que está haciendo es contra la ley, y peor aún, la intención criminal es suficiente. *(Cortez & Chang, 2012)*

Delito culposo.

"Un delito es culposo cuando una persona, desatendiendo la cautela que le dictan sus circunstancias y sus circunstancias personales, y por lo tanto sin darse cuenta de que está cometiendo un delito, está seguro de que lo evitará". resultado, inclus o si era previsible; No fue un agente buscado, sucede por negligencia, o incumplimiento de leyes, reglas, órdenes, etc. Por ejemplo, fumar en una estación de servicio o exceso de velocidad que resultó en un accidente.

En caso de delito doloso, hay dolo; La conducta criminal es negligencia. Delito doloso el delincuente debe tener la intención de causar daño al cometer el delito, en los casos penales es suficiente siempre que las consecuencias sean previsibles o al menos previsibles. *(Library, 2020)*

Por el Trato Psíquica entre Sujeto y su Acto: accionar o ultra intencional.

Delito intencional. Este crimen fue cometido con finalidad (o con extrema intención), pero el resultado fue más severo. Por ejemplo, si quieres hacerle daño en lugar de matarlo. Esta pena se adhiere a la teoría de la responsabilidad.

Hablando objetivamente, se juzgan en función de los resultados, o lo que realmente ocurrió, que no es lo que pretendía el agente; Por El Dígito De Personas: individual, colectivo. *(Cortez & Chang, 2012)*

Delitos Propios. Son los ejecutados por una desierta persona, ej., La infracción, el prevaricato.

Delitos Colectivos. Son los perpetrados por 2 o más personas ej., Insurrección, conspiración. *(Cortez & Chang, 2012)*

Por el Bien Vulnerado: simple, complejo, conexo.

Delito Simple. Transgreden un solo bien o utilidad jurídicamente protegida, ej., El atentado viola el derecho a la vida. *(Cortez & Chang, 2012)*

Delito Complejo. Contravención de varios bienes o intereses protegidos. Ej., Rapto continuo de violación. *(Cortez & Chang, 2012)*

Delito Conexo: Estas actividades están relacionadas de tal manera que algunos resultados dependen de algunas actividades y otros resultados dependen de otras actividades. Por ejemplo, los delincuentes acuerdan de antemano y luego cometen delitos en diferentes momentos y lugares. *(Cortez & Chang, 2012)*

Por La Unidad del Acto y Pluralidad del Resultado: Competencia ideal, competencia real. Tipo ideal de delito (delito compuesto) Un solo hecho viola varios bienes jurídicos. Por ejemplo, acciones como patear pueden dar lugar a dos delitos: herir y agredir. Golpear a una mujer embarazada conduce a delitos como lesiones y aborto. Las infracciones más graves están sujetas a una pena que puede ser aumentada hasta la cuarta parte de la infracción más grave. Crimen Real. Dos o más actos u omisiones dan lugar a dos o más delitos. Por ejemplo, la explosión de un coche bomba en un centro comercial. Las acciones que toman pueden ser: detener autos, colocar bombas. Los delitos son: robo de vehículos y terrorismo. *(Cortez & Chang, 2012)*

Por la Naturaleza Intrínseca: usual, político, social, contra la humanidad Delito común. Lástima los intereses tutelados de los particulares.

Delito político. Criterios El objetivo. Los delitos políticos son aquellos que socavan las estructuras sociales y políticas de la nación. criterio subjetivo.

Es un acto que subvierte la organización política y social con una voluntad altruista y sacrificial.

Estándares mixtos.

Un delito político es aquel que pone en peligro la seguridad interna y externa de la nación, intenta mantener el orden existente o transformarlo para el bien de los demás. actos delictivos contra las personas.

Estas personas transgreden derechos humanos fundamentales.

La vida, la nacionalidad, la religión, las creencias, etc. son algunos ejemplos.

Los crímenes de lesa humanidad se definen como violaciones contra civiles, o incluso contra el propio pueblo en "golpes de estado", y crímenes cometidos por diferencias raciales, nacionales o políticas".

Delito informático o electrónico

Las tecnologías de la indagación y la comunicación están trascendiendo las sociedades en todo el mundo, mejorando los procesos físicos, acelerando los tiempos de respuesta y aumentando la productividad. Sin embargo, estos avances también están dando lugar a nuevos tipos de ciberdelincuencia.

"Es un desafío conceptualizar completa o intuitivamente el delito cibernético.

Si implica el uso de tecnología digital en la comisión de un delito, incluye tecnologías informáticas y de comunicación, u ocasionalmente implica el uso de computadoras para cometer otros delitos, normalmente se considera legalizado y/o prohibido por la jurisprudencia".

La Operación. La estrategia del delincuente es obtener la información del cliente del banco, consultar el saldo de la cuenta y ejecutar una transacción en cuestión de minutos. Luego, el dinero se retira de la cuenta A, se transfiere a la cuenta B, se transfiere a la cuenta C y luego se retira a través de un cajero automático.

Hacen que los clientes del banco cuelguen o bloqueen el sitio web, y si una transacción falla, el cliente cierra la ventana pensando que hubo una falla en la computadora.

Los ciberdelincuentes aprovechan esta oportunidad para transferir dinero y copiar las contraseñas de las cuentas de las víctimas; Los clientes se enteraron del robo en línea cuando volvieron a conectarse al sitio web del banco.

Delincuencia, a Tono con la Tecnología.

En el crecimiento de la tecnología, el quebradero de cabeza permanece en que la disposición humana parece organismo que está sesgada al tropiezo, a retener felicidad a sus deseos a toda costa. Señala que, con el crecimiento de la automatización, aparece asimismo lo que se denomina "tropiezo informático".

De semejante estado que muchas personas se han dedicado a desobstruir sistemas de computación para remediar dificultades de la sociedad, otras tratan de recrearse la tecnología, las computadoras y sistemas, para actividades ilícitas." *(Cortez & Chang, 2012)*

"Delito electrónico en un afligido extenso es cualquier disposición criminógena ya homicida que en su elaboración hace explotación de la tecnología electrónica, ora sea como método, clima ya cesé y que, en un pesaroso estricto, el tropiezo informático es cualquier batalla ilícito penal, en el que las computadoras, sus sistemáticas y funciones redimen un pliego importante como método, clima ya cesé". *(Cortez & Chang, 2012)*

Definiciones de los delitos informáticos

En los últimos cuarenta años, sin duda, ha habido una convergencia entre la definición del concepto de asistencia a los delitos informáticos y los cambios sociales provocados por el desarrollo de las TIC y el comportamiento delictivo (o quizás por las nuevas TIC).

Las innovaciones han hecho posible procesar la información para su verificación utilizando computadoras computarizadas, lo que permite la acumulación de cantidades masivas de información y, al mismo tiempo, la extracción rápida y eficaz de datos.

Los denominados ciberdelincuentes que buscan obtener importantes ganancias extorsionando, difamando o incluso secuestrando la información obtenida, pueden buscar información de cualquier tipo (personal, comercial, financiera, bancaria o corporativa) *(Acosta, Benavides, García, 2020)*.

El fenómeno informático es una situación innegable e irreversible; Ciertamente, la computadora fue implantada entre nosotros para que no pudiera desconectarse fácilmente. Esto es resultado del incesante y progresivo desarrollo del ca mpo de la informática, que ahora se aplica a todos los aspectos de la vida diaria;

por ejemplo, el manejo de computadoras en la industria,
el comercio, la administración pública, los bancos y las instituciones financiera. *(Arroyo, 2016)*.

El delito cibernético, el delito electrónico, el delito informático y el delito informático son otros nombres para el delito informático.

La Organización para la Cooperación y el Desarrollo Económicos la describe como "cualquier práctica ilegal, no ética o no autorizada que involucre el procesamiento y/o la transmisión automatizados de datos". Se incluye un componente de apreciación moral en esta definición que va más allá del ámbito del derecho penal. Agregándose en la categoría de delitos informáticos las conductas delictivas que inicialmente las naciones intentaron catalogar como representaciones típicas de carácter tradicional, como el robo o hurto, el fraude, la falsificación, el daño, el fraude, el sabotaje, etc.

Pero debe enfatizarse que el uso de la tecnología de la información ha abierto nuevas posibilidades para el uso inapropiado de las computadoras, lo que ha resultado en una supervisión legal insuficiente. *(Delgado, 2015)*.

Características principales del delito informático

Son delitos difíciles de intentar ya que, en varios casos, es complejo hallar las pruebas, se conoce la acción criminal pero no a su autor, son actos que conseguir llevarse a cabo de forma rápida y sencilla, en momentos estos delitos alcanzan ejecutarse en materia de segundos, manipulando sólo un aparato informático y sin estar presente justamente en el lugar de los hechos, los delitos electrónicos tienden a extenderse y evolucionar, lo que involucra aún más la individualización y persecución de los mismos. *(Jiménez, 2015)*

Contrastando los delitos informáticos con otro tipo de delitos, existen diferencias en los perpetradores, la reincidencia del delito, la complejidad del delito en el momento en que se comete y los medios disponibles.

Estos son los rasgos principales de estos delitos:

Son conductas penales de cuello blanco. En que proporción solo un número explícito de personas con ciertos tipos de sapiencias logran cometerlos. *(CALDERÓN, 2020)*

Son acciones ocupacionales. Porque varias ocasiones, se elaboran por personas que están específicamente en el trabajo. *(CALDERÓN, 2020)*

Son acciones de oportunidad. Establecido por la doctrina: "Debido a que se vale de una estación creada o altamente intensificada en el mundo de oficios y organizaciones del régimen tecnológico y monetario"; En su mayoría son dolosos**.** Aunque asimismo hay muchos de carácter culposo o imprudenciales. *(CALDERÓN, 2020)*

Incitan serias pérdidas para los afectados. Las familias y las instituciones financieras invierten millones de dólares en seguridad informática para defenderse de ataques informáticos, aunque últimamente con el surgimiento y la utilización firme del comercio electrónico, las conductas delictivas son ejecutadas por personas que a veces no tiene bastos ilustraciones en informática, sino que, con sus conocimientos básicos, averiguan las maneras de vender productos y afectar a sus víctimas. *(CALDERÓN, 2020)*

Muestran dificultades para su comprobación. Las empresas solicitan de programadores para que consigan el rastro al delincuente informático; y, por otra parte, como existe la habilidad de borrar la información a veces las víctimas no cuentan con los elementos que demuestren que fueron estafados. En el siguiente gráfico, se revela la clasificación de los delitos informáticos. *(CALDERÓN, 2020)*.

Tipos de delitos informáticos

Los delitos informáticos se originan cada vez con más frecuencia en la sociedad, y en la mayoría de casos, las víctimas no cuentan con la información bastante para no

caer en ellos o para denunciarlos si se ven afectados. A continuación, estudiamos cuáles son los tipos de ciberdelitos: *(CALDERÓN, 2020)*

Estafas

Las estafas no son un delito desconocido que haya ocupado en la vida de los ciber usuarios con la perspectiva de las tecnologías de la Información y la comunicación; A excepción, las TIC han perfeccionado la tendencia, y quien más quien menos, ha aceptado algún mensaje o e-mail inseguro con este objetivo. *(CALDERÓN, 2020)*

Robo de datos

Existen programas que se alcanzan emplear para acceder a los datos de un puntual individuo, sociedad, o institución. Las administraciones públicas y oficiales son principalmente vulnerables a este tipo de delitos, y por eso requieren de equipos de alta capacidad para combatirlos. *(CALDERÓN, 2020)*

Amenazas

Estas logran ser realizadas por una individua totalmente extraña con el objetivo de conseguir cierto beneficio, o por individuos conocidas al margen de las tecnologías. En este actual caso, las amenazas suelen ser una amplificación de otros delitos originados en la vida real. *(CALDERÓN, 2020)*

Abuso a menores o pornografía infantil

Las tecnologías de la información y la comunicación siempre han sido el modus operandi de las redes mafiosas y de abuso infantil para difundir sus contenidos. La policía cuenta con unidades especializadas encargadas de perseguir este tipo de delitos y retirarlos de la web.

Sabotajes informáticos

En España, el vandalismo informático es muy común porque la administración pública lo tolera más que nunca.

Tales delitos tienen por objeto detener el funcionamiento de una empresa, organización o institución y causar pérdidas productivas o económicas. En la mayoría de los casos, es difícil encontrar al culpable.

Ataques a la intimidad

Los ataques a la privacidad se producen al recuperar información privada de otros dispositivos o al difundir datos privados de una persona que no están destinados a ese fin. Este es un delito muy común en España, especialmente entre los jóvenes que no se dan cuenta del alcance de compartir o difundir algún contenido privado.

Phishing

La finalidad del phishing es obtener de forma fraudulenta la información bancaria de determinadas personas. Esto se suele hacer haciéndose pasar por el propio banco para que la víctima proporcione datos hablando con el dispositivo. Una vez adquirido, el saqueo continúa.

Carding

El carding consiste en copiar u obtener información de la tarjeta de una víctima para obtener su dinero de manera fraudulenta y cometer un robo. Este es el uso ilegal de la tarjeta de crédito de otra persona o su número. Esto tiene relación con el hackeo porque una de las formas de conseguir números de tarjetas de crédito es a través de la ingeniería social, específicamente de nuestra inteligencia (que es lo más importante). Tenemos que tener mucho cuidado al hacer esto porque podemos meternos en muchos problemas. Tenemos que tener cuidado con nuestra tarjeta de crédito porque alguien puede leerla antes que tú y te puede engañar.

Tal vez se pueda recuperar el dinero, pero para ello necesitamos comunicarnos con el administrador del sitio donde se realizó el pago de este artículo, solicitar la IP al momento de la compra, al final necesitamos demostrar que no lo hicimos. hacer la compra

El carding es la práctica de realizar compras utilizando la cuenta bancaria o la tarjeta de crédito de otra persona. Requiere un poco de ingeniería social y mucha persistencia. Cuando alguien usa una tarjeta para comprar un artículo físico, muchas veces usa una orientación falsa y una identificación falsa, es decir, se llena todo el formulario de compra con información falsa. De esta forma, los consumidores pueden esperar a que la mercancía sea entregada en el lugar indicado, como si estuviera en su propia casa.

La filosofía del emisor de la tarjeta es que hay mucha gente con mucho dinero, y administrar algo de dinero para comprar algo para todos no es malo, ya que el titular de la tarjeta puede no darse cuenta. compra. no hice.

Un tipo de fraude en línea se llama carding. De esta forma, los ciber atacantes pueden acceder a nuestra información personal y de tarjetas de crédito a través de plataformas digitales. Este delito es cada vez más común y los ciberdelincuentes pretenden robar la información de nuestra tarjeta de crédito y luego realizar transacciones en línea sin nuestro consentimiento. Su actuación fue por tanto un delito de usurpación de identidad.

Una de las tácticas más comunes que utilizan estos piratas informáticos es realizar transacciones iniciales con montos financieros pequeños para que los tarjetahabientes no los noten hasta que se realice una transacción mayor.

A continuación, se explican las formas más comunes en que los delincuentes obtienen y usan su información. De esta forma, podrás prevenir futuros ataques que afecten tus finanzas.

- a través de Internet:

Esto generalmente se ofrece a través de un mensaje o correo electrónico. Los atacantes cibernéticos usan correos electrónicos falsos con logotipos de bancos e imágenes de empresas para engañar a los titulares de cuentas para que proporcionen información de seguridad importante, como números de tarjetas y números de seguridad.

- uso del teléfono

Estos falsos operadores se hacen pasar por bancos y ofrecen promociones a las que los tarjetahabientes no pueden resistirse, por lo que terminan regalando información personal y de seguridad.

- Suplantación de identidad

En este tipo de delito digital, los delincuentes crean llamativos sitios web falsos para ganarse la confianza de los titulares de tarjetas engañándolos para que realicen transacciones que implican revelar toda su información de seguridad.

- Virus o malware

Usando esta táctica, los delincuentes instalan virus en nuestras computadoras, teléfonos inteligentes u otros dispositivos donde almacenamos información segura. Luego, utilizando estos virus, nuestra información se extrae y se envía a los atacantes cibernéticos. Por lo general, estos virus se instalan en nuestros dispositivos cuando llegan por correo electrónico o SMS.

Cuidado con este tipo de estafas porque en esta era digital, la inclusión financiera es una necesidad para todos los usuarios que realizan transacciones comerciales y bancarias digitalmente a diario. De esta forma, les ayudamos a simplificar su vida y ganar más seguridad.

Al conocer y comprender estos tipos de fraude, podemos prevenirlos y evitar grandes pérdidas financieras que pueden significar grandes problemas o la bancarrota para algunos. Todos los días, los delincuentes continúan interrumpiendo nuestras transacciones a través de la suplantación de identidad y el fraude, por lo que es necesario fortalecer todos los sistemas de seguridad de nuestra red.

Las redes de Internet tampoco son seguras, pero si no tenemos dinero en efectivo en nuestras manos, podemos evitar ataques que afectan nuestra seguridad personal, como robos a mano armada. Solo es cuestión de entender nuestra información personal y adoptar buenas prácticas para una mayor seguridad, tranquilidad y una mejor calidad de vida.

Fraude

En ocasiones, los delincuentes aprovechan las oportunidades que ofrece Internet para sustraer la identidad de las víctimas y realizar trámites en su nombre, por ejemplo, firmar un préstamo en plataformas de crédito online o comprar productos.

Extorsión

Las grandes empresas y las agencias gubernamentales a veces son objeto de extorsión por parte de los ciberdelincuentes. El chantaje implica exigir beneficios a cambio de no piratear equipos de la empresa o divulgar datos críticos.

Cracking

Nos referimos a estas acciones ilegales como "hackeo de delitos digitales" si se realizan con la intención de dañar, deshabilitar o eliminar los sistemas de procesamiento de datos automatizados o los datos que contienen. *(Correa, 2014)*

Tenga en cuenta que, si bien las tarjetas robadas se pueden usar para compras directas, muchas personas las usan para pagar sus gastos mediante la compra de tarjetas prepagas y/o tarjetas de regalo y luego usarlas o venderlas para obtener ganancias inmediatas. De hecho, el término "tarjeta" se usa a veces para describir este tipo particular de "tarjeta de regalo". Los ciberdelincuentes de todos los niveles también pueden tratar de vender (o comprar) grandes cantidades de información de tarjetas de crédito robadas para obtener ganancias.

Según el Consumer Sentinel Fact Book 2020 de la Comisión Federal de Comercio, las tarjetas de crédito son el método de pago más común utilizado para el fraude en los Estados Unidos, con pérdidas por un total de $149 millones. Los consumidores informaron casi 400 000 incidentes de fraude con tarjetas de crédito, un aumento del 44 % con respecto al año anterior, mientras que el fraude con tarjetas de débito aumentó año tras año, un 32 % más que en 2019.

En este contexto, INCIBE y la Oficina para la Seguridad en Internet (OSI) advierten a los usuarios sobre este tipo de estafas, considerándola una de las estafas "más comunes" vistas por los actores malintencionados en la actualidad, tal y como afirman en su comunicado publicado al respecto. Blog.

El objetivo de estos ataques es utilizar las tarjetas bancarias del usuario para otros fines fraudulentos. Entonces, una vez que se recuperan los datos de estas tarjetas, se copian en la tarjeta virtual, que ahora pueden usar. Pero el delincuente primero debe asegurarse de que la información de la tarjeta sea válida e intentar averiguar el saldo disponible.

Además, OSI explica que existen diferentes métodos de atención. En primer lugar, los actores malintencionados pueden utilizar ataques conocidos como "carding" mediante correo electrónico fraudulento, "phishing" mediante mensajes de texto (SMS) o "espionaje desde el hombro" que se basa en "Look Back" para espiar a los usuarios. pantalla para ver información personal, como patrones de desbloqueo.

¿Cómo funciona el Carding?

La estafa del Carding trabaja en dos fases:

En primer lugar, cuando los ciberdelincuentes obtienen información de la tarjeta bancaria (ya sea de crédito o débito), pueden hacerlo a través de métodos como el phishing o simplemente clonando la tarjeta o el número de la propia tarjeta. *(OpenBank, 2021)*

Las tarjetas logran ser clonadas en cajeros automáticos y igualmente en establecimientos comerciales, en virtud que el delincuente en un descuido del cliente puede deslizar la tarjeta en un dispositivo para clonar (skimmer). “Por eso es muy importante estar atento y no perder de vista la tarjeta al momento de hacer el pago”

Una vez logrado los datos, los ciberdelincuentes se consagran a realizar compras, como por ejemplo en compañías de comida rápida, productos de belleza, contratos a canales de streaming y análogos. *(Policia Nacional del Ecuador, 2022)*

La suma de estas compras suele ser online y/o telefónicas, el objetivo de los ciberdelincuentes es que estas anulaciones pasen desapercibidas para el usuario durante el mayor tiempo posible. *(OpenBank, 2021)*

¿Cómo funciona Cracking?

Incluyendo actos de sabotaje o daño extenso a sus métodos, datos, computadoras o programas telemáticos. El objetivo principal de tales acciones es atacar el manual lógico del sistema, es decir. archivos o registros informáticos que indiquen el software en su conjunto, así como la acumulación de datos, información o documentos electrónicos, independientemente de su contenido específico. Como dice la doctrina, el modo exacto de operación (eliminar, formatear, virus) no es importante. Entre las actividades más peligrosas cabe mencionar las actividades de ciberbancos o ciberbancos, que en español se puede traducir como sabotaje electrónico o sabotaje informático, mediante las cuales se dedica el objeto de la actividad a su supresión, supresión o modificación sin el consentimiento de la persona. El propietario de la computadora, funcionalidad o datos que interfieren con su correcto funcionamiento. Las formas a través de las que esta conducta se lleva a cabo son, desde el punto de vista de la lógica del funcionamiento de los sistemas y mecanismos informáticos, muy variadas y normalmente, desde el punto de vista terminológico, todas ellas se reúnen por referencia a la infección de los sistemas por virus informáticos. *(Rodríguez, 2020)*

Tradicionalmente, se ha hecho una distinción teórica entre piratería y piratería. Por lo tanto, un cracker es cualquier persona que viola la seguridad de un sistema informático de manera similar a un hacker, excepto que el cracker lo hace para beneficio personal o para comprometer sus objetivos. Un hacker es en realidad un término que se usa para referirse a aquellos que acceden a los sistemas informáticos con fines específicos (como exponer vulnerabilidades de seguridad cibernética), mientras que el término "cracker" se usa para referirse a aquellos que hacen lo mismo, pero con intenciones maliciosas. Apunta a la desgracia. Sin embargo, es el uso más común hoy en día.

Los piratas informáticos llevan a cabo varios ataques a las computadoras. Como técnica principal para desarrollar otros ataques, por un lado, se debe mencionar la llamada ingeniería social, por otro lado, se debe mencionar la llamada ingeniería social. Esto

incluye persuadir a los usuarios para que hagan algo que normalmente no harían, como revelar contraseñas u otra información personal (por ejemplo, hacerse pasar por un empleado de la empresa para obtener la contraseña de un usuario y decirle que pronto se probará un nuevo sistema). De otro para proteger los métodos; como el anonimato o el cifrado para evitar la detección de la IP que utiliza. *(Quevedo, 2017)*

Cualquiera puede ser un objetivo activo para el cracking. El comportamiento de un principio válido es suficiente para la implementación. Es un delito común que permite diversos tipos de injerencia delictiva. Cualquiera puede ser un sujeto pasivo.

Esta infracción temporal se comete alterando, destruyendo o invalidando datos, archivos, programas o sistemas informáticos. Forman las consecuencias de una acción típica y pueden separarse del comportamiento en el espacio y el tiempo. Tales intentos son aceptables. El daño a la computadora es un agravio basado en el grado de violación del objeto físico de la propiedad estatutaria, ya que requiere un efecto físico en la seguridad material de la propiedad estatutaria. *(Arocena, 2008)*

Término cracker.

Fue definido por la comunidad hacker para referirse a aquellos que utilizan su conocimiento con fines poco éticos. Según The Hacker's Dictionary, un cracker es la "forma de vida más baja", a veces denominada hacker primitivo. Esto se debe a que algunos piratas informáticos pasan por la fase de Cracker, pero a medida que maduran, encuentran objetivos más interesantes. Este es el próximo y primer paso en la familia rebelde. Un cracker es un hacker que está fascinado por su habilidad para dañar sistemas y software y se especializa en hackear sistemas. Pero el problema no está ahí, es que suelen difundir este avance en la web para hacerse con el conocimiento de otras personas, compartiendo así las ideas y filosofía de los hackers. Actualmente, las versiones descifradas de la mayoría del software son comunes y están disponibles gratuitamente en Internet. Por lo tanto, es fácil comprender que un cracker necesita comprender completamente los aspectos tecnológicos, la parte de programación y la parte física de la electrónica. El tema de Cracker también es bastante claro, pero recuerda que es un hacker experto, tanto en términos de conocimiento de programación como de destreza técnica.

Los crackers diseñan y crean programas y hardware de guerra para interrumpir el software y las comunicaciones, como el teléfono, el correo electrónico u otro control remoto de la computadora. Varios Crackers "cuelgan" páginas web por esparcimiento o envían a la red su existente creación de virus polimórfico. También coexisten Crackers que se consagran a crear cracks para softwares importantes y negocia con ellos. Existen cracks para tarjetas shareware, DVD y las consolas PlayStation, X box entre otros. *(Alarcón, 2006)*

Los habitantes del ciberespacio

Hay muchas formas de categorizar a los habitantes del ciberespacio, pero la más común se basa en su conocimiento del medio de comunicación. Entonces, hay usuarios domésticos, personas que tienen una comprensión bastante buena de cómo funcionan las cosas, usuarios habituales, técnicos, programadores y piratas informáticos. Como resultado, la gente está confundida sobre el papel real de los piratas informáticos.

Bucaneros.

Son vendedores de redes, pero no existen en eso, pero son peores que Lammers, porque no entienden la tecnología y no pueden aprender nada. A diferencia de los piratas informáticos, los piratas solo buscan ofertas negras en productos ofrecidos por imitadores. Los piratas solo tienen cabida fuera de la red, porque a los que entregan productos "crackeados" en la red se les llama "hackers". De hecho, los piratas solo son empresarios deshonestos cuando utilizan productos descifrados a gran escala. *(Alarcón, 2006)*

El gran valor de los datos

INCIBE advierte que las tarjetas de crédito son una amenaza progresiva en la actualidad, ya que los datos de las tarjetas de crédito son un objetivo importante para los ciberdelincuentes. La información hurtada puede venderse en foros secretos en la dark web y utilizarse con fines ilegales. Con el auge de las compras en línea y el uso generalizado de tarjetas de crédito para transacciones en línea, los ciberdelincuentes tienen aún más oportunidades de hacer un mal uso de la información de la tarjeta de crédito.

Malware e ingeniería social

Otra técnica de manipulación en el robo de tarjetas es el uso de malware, un software riesgoso diseñado para infiltrarse en el dispositivo de un usuario y robar información confidencial, como la información de la tarjeta de crédito. El malware se puede descargar en el terminal de un usuario a través de un archivo adjunto de descarga de correo electrónico o visitando un sitio web infectado. Una vez instalado en el dispositivo de un usuario, el malware puede recopilar información de las tarjetas de crédito utilizadas en ese dispositivo y enviarla a los ciberdelincuentes.

La ingeniería social es otra técnica de mapeo que implica manipular a las personas para obtener información confidencial. Los ciberdelincuentes pueden usar técnicas de ingeniería social para engañar a los usuarios para que revelen la información de su tarjeta de crédito, como hacerse pasar por una empresa legítima o crear una página web falsa haciéndose pasar por una empresa legítima para obtener información del usuario. *(Rentero, 2023)*

¿Qué son los "bin"?

Estas asociaciones de ciberdelincuentes se instituyen en grupos llamados BIN y sus partidarios son “bineros”.

Este nombre expresa que el BIN (Bank Identificación Number, que son los seis primeros dígitos de la tarjeta bancaria) sirve para asemejar el banco y el tipo de tarjeta, y es lo que los “bineros” usan para generar de forma aleatoria códigos y números.

Estos grupos se consagran a explotar debilidades, hacerse con números de tarjetas e ainclusive venderlos posteriormente a terceros. *(OpenBank, 2021)*

Derecho informático

El concepto de derecho informático fue inventado en la década de 1970 por el Dr. Wilhelm Steinmüller, académico de la Universidad de Regensburg en Alemania, pero no es un término específico, ya que también se han explorado varios términos para su uso en derecho electrónico. Derecho Telemático, Derecho de las Nuevas Tecnologías, Derecho de la Sociedad de la Información, Derecho de la Cibernética, Derecho de las Tecnologías, Derecho del Ciberespacio, Derecho de Internet, etc. Actualmente, el término "derecho de las tecnologías de la información y las comunicaciones" es ampliamente utilizado en América Latina, incluso por delante del uso de "derecho informático". La Legislación Informática es considerada un punto de inflexión en el derecho, Porque todos los ámbitos del derecho se ven afectados por el surgimiento de la llamada sociedad de la información, que modifica los procesos sociales y, por tanto, los procesos políticos y jurídicos. La legislación informática surge como una medida normativa de carácter legal. Para aclarar los conceptos básicos del derecho informático, debemos volver a su piedra angular: la informática. La informática al decir de (Téllez Valdés, 1996, pág. 5) surge en el seno de la cibernética. El respaldo histórico para el surgimiento de la cibernética como género y la informática como especie se puede encontrar en el papel de los factores sociales, a saber, la necesidad social de producción y aumento de capital, es decir, factores tecnocientíficos. Es decir, el progreso de la ciencia y la tecnología en todas las áreas del conocimiento humano y el desarrollo de los factores históricos que actúan como una sola unidad de cantidad durante las convulsiones, porque es necesario unificar el momento histórico. *(Jácome, 2016)*

Análisis Forense Informático.

Se piensa que el Argumento Forense Informático está en el estudio de técnicas científicas y analíticas especialistas a una infraestructura tecnológica que permite asemejar, salvaguardar, analizar y exhibir datos que sean validos dentro de un asunto legal. *(Hidalgo, Yasaca, Lema, & Hidalgo, 2018)*

Cuando se solicita de servicios profesionales para elaborar un análisis forense o peritaje, es prioritario proteger toda la información que inmediatamente será o no judicializada. *(Hidalgo, Yasaca, Lema, & Hidalgo, 2018)*

El discernimiento del informático forense abarca aspectos no solo del software, sino además de hardware, redes, seguridad, hacking, cracking, recuperación de información.

Es muy importante tener clara la diferencia entre informática forense, seguridad informática y auditoría, para impedir confusiones como la que vincula a la primera con la prevención de delitos, cuando la que se encarga de esto es la seguridad informática. *(Hidalgo, Yasaca, Lema, & Hidalgo, 2018)*

Entre las funciones que puede realizar un perito se encuentran *(Cajo, 2018)*:

- Asesoría técnica contra el cibercrimen, considerando que se pueden presentar dificultades por la presencia de un malware que afecte una entidad financiera y, por ende, a sus clientes.
- Situación de evidencias electrónicas, es decir, de los archivos que han sido eliminados y cuyo asiento se solicita determinar.
- Auditorías y seguridad informática forense mediante test de sutileza.
- Evaluación y tasación de dispositivos tecnológicos.
- Certificaciones y homologaciones.
- Recuperación de datos.
- Asesoría informática y formación de profesionales del derecho, la administración pública, de cuerpos y fuerzas de seguridad del estado, y también como detectives privados.
- Contraespionaje informático.
- Vigilancia de actividad laboral informática.
- Localización y asesoría en casos de infidelidad empresarial que se da cuando un trabajador se aparta de una empresa y se carga consigo información que no le

corresponde como, por ejemplo, una base de datos de todos los clientes. *(Hidalgo, Yasaca, Lema, & Hidalgo, 2018)*

¿Cómo prevenir el carding?

Si utiliza con frecuencia su tarjeta bancaria para realizar compras en línea o pagar servicios, debe tomar ciertas medidas de seguridad para evitar en la medida de lo posible las siguientes situaciones, entre ellas:

Utilice una red segura cuando pague o compre en línea.

No comparta información sobre tarjetas, firmas electrónicas o números de seguridad.

Compre en sitios seguros en Internet.

PAÍS	***EVOLUCIÓN DEL DELITO INFORMÁTICO***	***CRACKING***	***CARDING***
Colombia	*La Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la Ley de Delitos Informáticos, tuvo sus propios antecedentes jurídicos. El primero de ellos se expide veinte años atrás, cuando a través del Decreto 1360 de 1989 se reglamenta la inscripción 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.*	*Artículo 269 B y siguientes. De acuerdo con el Código Penal de Colombia, las penas van de 48 a 96 meses de prisión y multa de $100 a $1.000 al salario mínimo aplicable, sin derecho a impedir o evitar interferencias en los sistemas informáticos o que impliquen el funcionamiento o normal acceso a datos o redes de telecomunicaciones. E igualmente le corresponderá igual pena a quien dañe, borre, deteriore, altere o suprima datos informáticos o un sistema de tratamiento de información o sus partes o componentes lógicos.*	*Si bien la conducta de copiar fraudulentamente los datos de alguien produce un clon de la tarjeta original, no se puede decir que ése sea el delito, sino que, al tenor de lo establecido en la Ley 1273 de 2009, sería violación de datos personales (Artículo 269 F del Código Penal). Situaciones como ésta han contribuido de alguna manera, a dificultar no sólo la definición de delito informático, sino su interpretación para un adecuado tratamiento jurídico e institucional.*
México	*El 17 de mayo de 1999 se publicó en el Diario Oficial de la Federación una reforma integral en elemento penal a nivel federal relacionada con delitos informáticos, la cual incluía dentro de su marco jurídico distintas figuras*	*Al artículo 211 se le agrega un capítulo entero dedicado a definir y castigar el acceso ilícito a procedimientos y equipos de informática (también llamado cracking), por el que se instituye una pena de entre tres meses y un*	*Siendo un tipo de delito sin marco legal, además de que es muy difícil de rastrear, el funcionario asegura que, en caso de ser castigado, se incluye el robo de identidad y alcanza penas de uno a seis años de cárcel.*

	delictivas que protegen la información contenida en los sistemas y equipos de cómputo. (Rojas, 2016)	*año de prisión a quien "sin autorización acceda, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática". La pena se incrementa en dos terceras partes, en caso de que la penetración impida el uso o acceso del sistema afectado.*	
España	*Artículos del Código Penal Español relativos a Delitos Informáticos, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.*	*Los daños y sabotaje informático se dan con el uso de software malicioso, también denominado malware. Estas prácticas tienen un gran perjuicio para organizaciones y empresas. La penalización es de 3 meses a 2 años de prisión y de multa de 3 a 18 meses según el artículo 197 del Código Penal.*	*Presentemente, en España el carding se castiga en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal en sus artículos 386 y 387. En el art. 386 se castiga con una condena de ocho a doce años y sanción del tanto al décuplo del valor aparente de la moneda el que altere la moneda o fabrique moneda falsa, el que exporte moneda falsa o alterada o la importe a España o a cualquier otro Estado miembro de la Unión Europea.*

CUADRO COMPARATIVO

Disponen de un precinto de seguridad para proteger tus datos bancarios. Revise su estado de cuenta bancario con frecuencia.

Habilite las alertas de movimiento de tarjetas para que pueda monitorear la actividad y detectar cualquier movimiento inusual temprano.

Si usted es víctima de este tipo de estafa u otro tipo de fraude, debe informar la situación a su banco de inmediato para que puedan ayudarlo en los próximos pasos. Recuerda también que Condusef puede ayudarte en cualquier caso de fraude en internet relacionado con tu tarjeta bancaria.

En Ecuador, el Código Orgánico Integral Penal (COIP) observa leyes que condenan los delitos informáticos.

Temperini 2013, indica que los países latinoamericanos muestran una falla de homogeneización en el ámbito característico del procedimiento penal aplicable a los delitos informáticos, se insiste en la necesidad de perfeccionar los niveles de encuadernación y reforma legislativa. Para el caso de Ecuador este estudió alcanzó como consecuencia la posición número 12 en el ranking exhibido para los países latinoamericanos, con un 63% de representación de la sanción penal en la legislación vigente del país para los delitos informáticos analizados.

Como todos los países, Ecuador también tiene un problema con los delitos informáticos, y en 2013 Crece el número de denuncias ciudadanas online autoridades públicas ecuatorianas. Residentes denuncian casos relacionados Ataques ilegales de escuchas telefónicas a la integridad de la información, Abuso del sistema de la máquina, suplantación de identidad cibernética, fraude informático, pornografía Los niños y los delitos contra la propiedad intelectual. Desde que comenzó a trabajar el 10 de agosto La Ley de Organización Criminal consolidada tiene vigencia hasta el 31 de mayo de 2015.

En Ecuador, la fiscalía general de la República registró 530 casos de delitos informáticos los primeros cinco meses de 2016 en comparación con el mismo período del año pasado 635 Quejas. Los números muestran una caída. Guayas tiene 18 casos; Pichincha, 145; Manabí, 24; oro, 22; todas las provincias restantes tienen una cantidad menor. La mayoría de las denuncias (368) estaban relacionadas con "fraude de fondos públicos" fraude electrónico.

La investigación fue elaborada por la Policía Estatal, INTERPOL, Emergency Response eventos Informáticos del Ecuador (Ecucert) con el apoyo de organizaciones similares un estudio realizado en América Latina muestra que el 85% de todos los ataques a los sistemas informáticos son causados por errores causados por consumidores que no toman precauciones al visitar el sitio redes sociales, uso de correo electrónico y uso de usuarios y contraseñas Se debe concienciar a las personas sobre el uso de los recursos informáticos. Y los riesgos que plantean deben tomarse en serio, no solo a nivel individual o sino también en las expresiones sociales de la propia perspicacia por fallas en los sistemas de seguridad y ataques criminales en el ciberespacio hay una falta de actores para combatir tales crímenes. (Gonzalez, 2018)

La revisión estadística de la unidad de lucha contra el ciberdelito de la policía muestra que desde 2020 hasta el 6 de julio de 2022 se registraron 3183 casos de delitos informáticos. En todo el año 2020 hubo 682 casos; En 2021, este tipo de casos aumentó a 1.851, mientras que, en 2022, en poco más de seis meses, la policía de todo el país ha iniciado 650 investigaciones. Las provincias de Guaya, Pichincha, Manabí, Imbabura, Carchi y Azuaya tienen el mayor número de casos.

Cinco de estas categorías delictivas ocurren con mucha frecuencia en el país. Estos incluyen:

fraude en línea, invasión de la privacidad, acceso no autorizado a los sistemas informáticos, ataques a la integridad de los sistemas informáticos y apropiación indebida fraudulenta por medios electrónicos. Este último es el más común. Esto ocurre cuando una persona utiliza de manera fraudulenta un sistema informático o una red electrónica para defraudar la propiedad de otra persona, transferir

dinero o propiedad sin consentimiento en perjuicio de otra persona. Según el artículo 190 del Código Integral Penal (COIP), la pena es de 1 a 3 años de prisión.

En el 2021 se registró un caso de estafa por internet donde los afectados perdieron alrededor de $100.000,00. Las indagaciones señalaron que tres personas recogían el dinero de las estafas y depositaban en las cuentas de quien dirigía el grupo.

Caso de España

En el 2021 en España desarticulan una red internacional pirateo de tarjetas de créditos, dedicada a la delegación de delitos afines con el fraude informático en todo su espectro, especialmente a través del carding.

A la organización se le imputo más de 2.500 sucesos delictivos con más de 300 empresas, con un daño al patrimonio que se estima llegaría alcanzar un millón de euros, consiguiendo información de 42.000 tarjetas de crédito por parte de los diferentes integrantes de la organización delictiva.

Actualmente, en España el carding se pena en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal en sus artículos 386 y 387.

***En el art. 386 se castiga con una pena de ocho a doce años** y multa del tanto al décuplo del valor aparente de la moneda el que altere la moneda o fabrique moneda falsa, el que exporte moneda falsa o alterada o la importe a España o a cualquier otro Estado miembro de la Unión Europea. (BOE, 2019)*

Caso Estados Unidos

En el 2006, en Estados Unidos se le acuso a Albert González, del delito fraude informático y robo de identidad, el cracker habría robado los datos de más de 130 millones de tarjetas bancarias, tras estos delitos se le condeno a 20 años de prisión.

CAPITULO 2

Metodología del proceso de Investigación

Enfoque de la investigación

El trabajo de investigación está establecido en un enfoque Cualitativo porque explica los fenómenos en profundidad, se lleva fundamentalmente en ambientes naturales, los significados se extraen de los datos, no se fundamenta en la estadística. El proceso es inductivo, recurrente, analiza múltiples realidades subjetivas, no tiene secuencia lineal.

Con un tipo de investigación explicativa para identificar que está causando el carding y el cracking.

La información se analizará a través de entrevistas a un grupo focalizado en la materia sobre delitos electrónicos tipificados en el carding y el cracking

Enfoque de la investigación

Cualitativo: Las investigaciones cualitativas intentan describir metódicamente las particularidades de las variables y fenómenos (con el fin de constituir y corregir categorías conceptuales, formular y validar asociaciones entre fenómenos o comparar los constructos y postulados creados a partir de fenómenos observados en distintos contextos), así como el hallazgo de relaciones causales, pero evita asumir constructos o relaciones a priori. Pretenden descubrir teorías que expliquen los datos. *(Lecanda, 2002)*

Tipo de Investigación

La investigación explicativa: es aquella que tiene relación causal; no sólo persigue representar o acercarse a un problema, sino que pretende encontrar las causas del mismo.

Universo y muestra.

A través de un encuentro con 3 abogados analistas en temas de delitos electrónicos se prevé recopilar información que nos explique como la Ley Ecuatoria trata este tipo de delitos.

Métodos empleados e instrumentos de la investigación.

Entrevista: Es una herramienta técnica de mucha en la investigación cualitativa, para obtener datos e información que nos proporcione información sobre los delitos electrónicos tipificados en el carding y cracking.

Método Jurídico comparado:

- Permite establecer la similitud y las discrepancias existentes entre las legislaciones nacionales y extranjeras.
- Mediante este método, indagamos las semejanzas que poseen los distintos ordenamientos jurídicos, teniendo en cuenta los diferentes sistemas jurídicos contemporáneos.

Método de Análisis histórico:

- Analizar las instauraciones del derecho.
- Se confirman los hechos pasados.
- Parte de las opiniones y de los juicios tomados de los relatos del pasado que han realizado diferentes autores o historiadores.

Método Teórico-jurídico:

- Se utiliza durante toda la investigación.
- Se relaciona con los conceptos y con las interpretaciones de la investigación.
- Permite el análisis del estado del arte del objeto de investigación.

CAPITULO 3

Análisis e Interpretación de los Resultados de la investigación:

ENTREVISTAS

ENTREVISTA # 1

NOMBRE: Ab. David Vergara Solís

1. ¿Desde un contexto histórico cómo definiría el delito informático?

El delito informático es aquella conducta que reúne las características del delito que se comete a través de medios electrónicos o que ataca la integridad de sistemas informáticos; La evaluación de los delitos electrónicos que se cometen en la actualidad, son bastantes y de forma regular, a comparación de los que se cometían han mutado conforme ha pasado el tiempo, por ejemplo, las estafas, apropiaciones fraudulentas, violación a la intimidad o injurias.

2. ¿A su criterio, ¿cómo definiría el delito del carding y el cracking?

El delito de carding se refiere a la estafa informática, se refiere al uso de una tarjeta de crédito o débito que se ha obtenido ilícitamente, según la definición anglosajona; Y el delito de cracking es el delito sabotaje informático así lo considero personalmente, cuando una persona que podría ser un cracker inserta un malware o programa dañino para provocar que un sistema informático deje de funcionar.

3. Considera Ud. que estos delitos deberían ser juzgados con una pena mínima o máxima, ¿por qué?

Debería tener una pena proporcional al cometimiento de la infracción y depende de muchos factores sí que contienen agravante o no, una pena media, no soy partidario de la idea que siempre se debe sustentar con la máxima, dependerá de cada caso en particular.

4. ¿Sabe de las medidas preventivas para no ser víctimas de carding y cracking?

Para prevenir cualquier delito informático, se pudiese sugerir a las víctimas que constantemente cambien sus claves de tarjeta de crédito o débito, de sus dispositivos electrónicos, cambios del pin de la computadora, cambio de claves de correo electrónicos; Evitar de conectarse a redes públicas o que verifique el ingreso a una página determinada cuando esta se encuentra encriptada.

5 ¿Qué caso emblemático conoce sobre este tipo de delitos (carding o cracking) y que conclusión tiene al respecto de ello?

Sobre el delito de carding no se ha escuchado un caso muy llamativo pero es muy común entre los delitos cuando la víctima recibe su estado de cuenta y ahí mira el reflejo de consumos no realizados; Del caso de cracking se ha sabido casos como de muchos ciber atacantes que se han infiltrados en páginas del FBI, Instituciones públicas de los Estados Unidos que han dejado inoperantes a estos sistemas y por su riesgo hay delincuentes informáticos que han recibidos penas privativas de libertad muy importantes, evidenciando la importancia de estos delitos.

6. Alguna medida para regular los delitos carding o cracking o qué tipo de propuesta propondría?

Trataría en que la legislación sea más sencilla la redacción, ya que es muy técnica en ciertos aspectos o siendo un poco más general para entender y cubrir todos esos conceptos del carding y cracking dándole su respectivo encuadramiento penal; Con la redacción clara y especifica de la norma, sumándole a una modificación de la pena.

ENTREVISTA #2

Nombre: Ab. Andrés Jacome.

Entrevistas

1. ¿Desde un contexto histórico cómo definiría el delito informático?

Es toda conducta típica, antijuridica, culpable que es objeto de sanción conforme la ley y que se comente a través del uso de la tecnología y que afecta propiamente a los equipos, sistemas o plataformas informáticas o a la confidencialidad, integridad y disponibilidad de la información. Hay que considerar que hay otras conductas, que emplean para el cometimiento de la infracción la tecnología, sin embargo, considero que dichas conductas no deben ser consideradas propiamente como parte de los delitos informáticos.

2. ¿A su criterio, ¿cómo definiría el delito del carding y el cracking?

El carding se encuentra catalogado dentro de la categoría de "fraude cibernético" y consiste en la falsificación y copia y tráfico parcial de la información incluida en las tarjetas de crédito y débito (número de la tarjeta, claves de seguridad, nombre del titular, etc.) y también tiene relación con la generación ilegitima de la información y datos de dichos instrumentos financieros. Capturada la información por parte del sujeto infractor, este la puede utilizar, entre otras cosas, para acceder a las cuentas bancarias y obtener el dinero que se encuentra depositado en ellas o realizar compras o pagos directamente a través del uso no autorizado de la tarjeta. Se realiza a través de prácticas irregulares como "hacking y cracking".

3. Considera Ud. que estos delitos deberían ser juzgados con una pena mínima o máxima, ¿por qué?

Considero que dicha conducta debe ser sancionado con una pena privativa de la libertad que se encuentre dentro de los parámetros establecidos para las penas aplicadas a la defraudación, es decir, de 3 a 5 años. Sin embargo, en el caso de que el sujeto infractor

no subsanaré los efectos producidos por su conducta sobre el patrimonio de la persona, considero que debería aplicarse esa situación como un agravante y por tanto la pena debería partir de 5 a 7 años, parámetro que actualmente no está establecido en la Ley.

4. ¿Sabe de las medidas preventivas para no ser víctimas de carding y cracking?

Acorde diferentes recomendaciones internacionales y nacionales podríamos señalar las siguientes:

1.- Utilizar las tarjetas de crédito y débito solamente en páginas Web autenticadas y seguras, así como en comercios seguros, para lo cual hay que verificar la legitimidad del sitio y la valides de sus certificaciones.

2.- Instaurar y emplear siempre contraseñas seguras, de por lo menos 8 dígitos entre datos alfanuméricos y numéricos. Mientras más complejas sean las contraseñas se logra reducir el riesgo de que puedan afectar el sistema informático.

3. Cambiar y restablecer periódicamente las contraseñas. No enviar a nadie los datos de las tarjetas de crédito o débito, ni si quiera personas de confianza o de parentesco.

4.- Comprobar al realizar transacciones a través de Atm (Cajeros automáticos), que estos no hayan sido manipulados por terceros no acreditados.

5.- Emplear billeteras "especiales", que puedan aislar la transmisión y captura de datos.

5 ¿Qué caso emblemático conoce sobre este tipo de delitos (carding o cracking) y que conclusión tiene al respecto de ello?

Un caso en concreto no conozco, sim embargo, al haber participado en varias capacitaciones respecto a ciberseguridad pude conocer varios de los mecanismos que se emplean para cometer el ilícito.

6. Alguna medida para regular los delitos carding o cracking o a tipo de propuesta propondría?

Con respecto a esto debo indicar que el término cracking hace referencia a la práctica que consiste en atacar sistemas informáticos y software con intención maliciosa y cuyo resultado es la apropiación ilegitima de información y datos. Esta conducta ya se encuentra tipificada en nuestro código en el artículo 234 del COIP. La clonación de información se encuentra tipificada en el art. 230 # 4 que trata de la interceptación ilegal de datos. Sin embargo, considera que debería aclarar de mejor forma el título del artículo, puesto que el delito de carding, no solamente se puede cometer a través de la interceptación de los datos cuando estos son transmitidos, sino que pueden ser capturados, a través de medios tecnológicos, directamente de sus soportes, sin que haya la intención del titular de transmitir o hacer una transacción.

ENTREVISTA #3

Nombre: Ab. Giovanny Vaca

1. ¿Desde un contexto histórico cómo definiría el delito informático?

El delito informático se refiere a las acciones ilegales o criminales que se cometen utilizando la tecnología de la información y las comunicaciones. A medida que la tecnología ha avanzado, han surgido nuevas formas de delincuencia que aprovechan las vulnerabilidades y las posibilidades que ofrece el entorno digital. En sus inicios, en las décadas de 1960 y 1970, el término "delito informático" estaba más relacionado con el acceso no autorizado a sistemas informáticos y la manipulación de datos. Los primeros

casos implicaban principalmente a hackers y programadores que intentaban acceder a sistemas para los que no tenían autorización, o que alteraban información para obtener ventajas ilegales.

2. ¿A su criterio, ¿cómo definiría el delito del carding y el cracking?

El carding y el cracking son dos formas de delitos informáticos que involucran actividades ilegales relacionadas con sistemas de seguridad y datos personales. El carding se refiere a la práctica de utilizar información de tarjetas de crédito o débito robadas para realizar compras no autorizadas o fraudulentas en línea. Los ciberdelincuentes que practican el carding adquieren la información de las tarjetas a través de técnicas como el phishing, la intromisión en bases de datos vulnerables. Luego, utilizan esta información para realizar compras en sitios web o tiendas online, consiguiendo bienes o servicios sin pagar por ellos, causando pérdidas a los dueños legítimos de las tarjetas y a las instituciones financieras. Por otro lado, el cracking se refiere al acto de esquivar o interrumpir las medidas de seguridad de sistemas informáticos, software con la finalidad de acceder a estos sistemas informáticos.

3. Considera Ud. que estos delitos deberían ser juzgados con una pena mínima o máxima, ¿por qué?

La determinación de las penas para delitos como el cracking y el carding es responsabilidad de los sistemas judiciales y legislativos de cada país, y está basada en una serie de factores legales, sociales y de un programa de política criminal. Estos delitos pueden causar un daño significativo a individuos o empresas, incluso hasta gobiernos. Por lo tanto, en muchos países, las penas para estos delitos son proporcionales al hecho cometido y pueden incluir penas de prisión y multas económicas bastante elevadas. Las penas deben ser agravadas según el patrimonio afectado y según el hecho cometido, haciéndose un cálculo referencial en base a esa perdida

4. ¿Sabe de las medidas preventivas para no ser víctimas de carding y cracking?

Se debería tener un seguro apropiado para los dispositivos utilizados según el usuario, entre una de esas cambiar contraseñas básicas por una clave más ilógica o compleja, la autenticación de los datos por medio de estos dispositivos que puede ser biométricamente o el uso de la huella.

Al momento de navegar en el internet, evitar entrar a sitios maliciosos o que no muestren las credenciales de seguridad prestablecidas, por último, utilizar redes seguras e inhibirse de conectarse a redes públicas.

5 ¿Qué caso emblemático conoce sobre este tipo de delitos (carding o cracking) y que conclusión tiene al respecto de ello?

Uno de los casos representativos relacionados con el delito informático es el caso de "Albert González", que sucedió en Estados Unidos, González fue aprehendido por liderar una organización de hackers que atacó a varias empresas de suma importancia que, incluidas tiendas minoritarias y determinado restaurantes reconocidos. Utilizando técnicas de hacking sofisticadas, su grupo robó datos de millones de tarjetas de crédito y débito. El caso de Albert González fue impresionante porque demostró la habilidad de un grupo de hackers para complicar la seguridad de grandes corporaciones y sustraer enormes cantidades de información secreta. Además, el caso también puso en a puros e incluso en la necesidad de que estas empresas y las instituciones refuercen su seguridad en sus sistemas electrónicos adoptando medidas más preventivas y más seguras para tranquilidad de sus clientes.

6. Alguna medida para regular los delitos carding o cracking o qué tipo de propuesta propondría?

Regular los delitos de carding y cracking es fundamental para proteger la seguridad de los ciber usuarios o datos de las empresas en general, para evitar el robo de datos o código de suma importancia; Sobre una de las medidas que se puede tomar para contrarrestar puede ser como el fortalecimiento leyes y rigurosidad en materia

sancionatoria. 2) Acuerdos o convenios sobre cooperación internacional en seguridad digital, ejemplo uno de ellos el convenio de Budapest. 3) La concientización a los usuarios sobre campañas de protección de datos, ya sean seguros particulares o campañas gratuitas sobre medidas básicas como el cambio de contraseñas, redes encriptadas, renovación de las cuentas. 4) La creación de unidades especializadas en Ciberdelitos, con la cooperación respectiva de Policía Nacional y Organismos Internacionales.

ANALISIS DE ENTREVISTAS:

Los delitos electrónicos, como su nombre lo dicen son actividades ilícitas que en su gran mayoría son realizadas a través de medios electrónicos para su posterior realización, que en la mayoría de los casos terminan afectando patrimonios, datos personales, y también pérdidas económicas. Dentro del delito de carding es uno de los delitos más cotidianos que pueden existir que es el la clonación de la tarjeta o la obtención de los datos de dicha tarjeta en la cual el tarjetahabiente, no se percata hasta visualizar una transacción no consentida, este tipo de acción son las que mediante los conceptos ya establecidos en la investigación y a comparación de otras legislaciones se puede ser más preciso o generalizado a la hora de redactar estos artículos, que para este tipo específicamente de delito(carding), que no siempre es por medio electrónico, siendo que este se pueda puntualizar.

El otro delito analizado que es el cracking, a sabiendas que el alcance de la tecnología está de la mayoría de personas en cuestión de aprendizaje de estas conductas es fácil acceder a través del internet, la enseñanza de estas actividades ilícitas, eso implica el uso adecuado del internet, un control por parte de los entes respectivos e incluso de los mismos familiares al momento de regular el internet a sus hijos en cierto punto de limitar la información; Se debe utilizar mecanismos que se puedan aislar los datos o acceso a los diferente medios electrónicos en la cual se tiene almacenado la información.

Desde tener claves encriptadas o ilógicas, hasta tener billeteras especiales para evitar la captura de datos, a través de la tecnología “Contac”, contratar seguros particulares que tenga estos sistemas de protección de datos; Sumándole a una correcta tipificación de los delitos y la pena que tenga correlación al hecho o caso en específico, siendo esta equivalente al patrimonio afecta.

Capítulo 4

CONCLUSIONES, RECOMENDACIONES Y ANEXOS

Conclusiones:

Las caracterizaciones del carding y el cracking es la explicación detallada de lo que significan cada uno de estos delitos y como afectan en nuestra sociedad para esto se debe de considerar nuevas reformas que ayuden a mitigar este tipo de delitos, que incrementan gracias al avance tecnológico.

Es importante mencionar el accionar de los países como México, España y Colombia ante los delitos electrónicos y como estos países los clasifican para su correcta ejecución, sin embargo Ecuador ha ofrecido sus inicial cambios en relación a las leyes existentes, en las que se observan detalles de la información y la informática, lo que se cree un avance significativo ante el adelanto tecnológico que se ha asumido en los últimos años en el país, pero es cierto que aún falta mucho por legislar, para afirmar que no queden en la impunidad los actos que se comentan concernientes con las tecnologías.

Tomar en cuenta los delitos cometidos en España y Estados Unidos con respecto al carding y cracking es importante para conocer la magnitud del problema como los llamados crackers se pueden aprovechar de sus víctimas y robarse su dinero, hay que añadir también que este tipo de infracciones son difíciles de revelar o perseguir, debido a que los sujetos activos proceden sigilosamente con instrumentales capaces de borrar toda huella de intrusión o de la consumación del delito; se debe ya estimular estos avances tecnológicos que son contextos sociales.

Recomendaciones

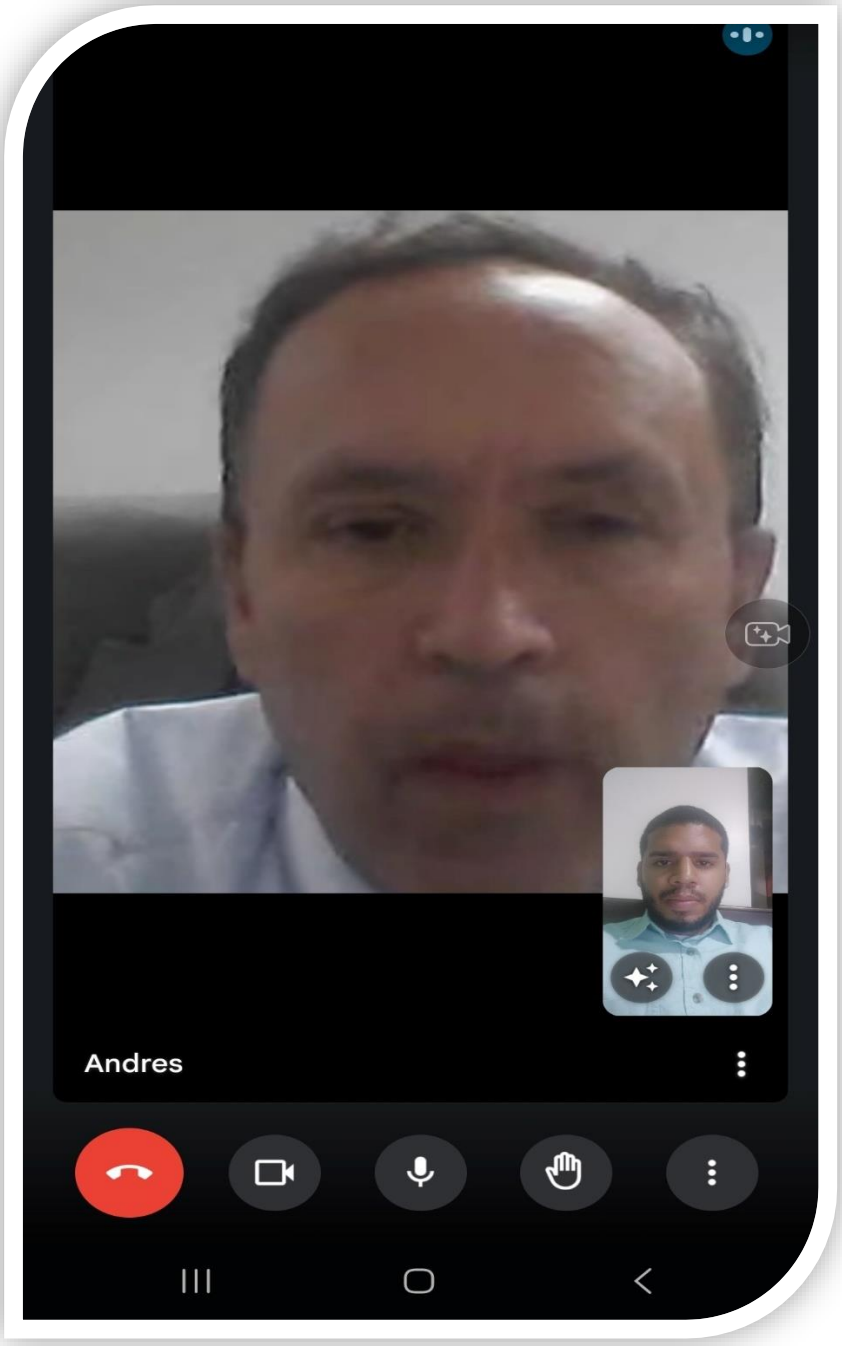
1. En el Ecuador se generaliza el contexto de delitos informáticos, por lo cual, requiere de reformas acorde a cada tipo de delito y estar en constante actualización mediante los cambios en la sociedad y la tecnología para facilitar seguridad a los ecuatorianos.

2. Tomando como reseña los conceptos dados por otros países los cuales tipifican los delitos informáticos, para un mejor análisis jurídico.

ANEXOS:

Se adjunta las fotos, que comprenden a las entrevistas que se realizó en el presente trabajo:

1 Ab. David Vergara



2 Ab. Andrés Jacome

Referencias

Acosta, Benavides, García. (2020). Impunidad organizacional y su complejidad en el mundo de los negocios. Obtenido de https://www.redalyc.org/journal/290/29062641023/29062641023.pdf

Alarcón, B. M. (2006). LA FILOSOFÍA HACKING & CRACKING. *Hidalgo. Obtenido de https://core.ac.uk/download/pdf/71450528.pdf*

Arocena, G. (2008). LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL ARGENTINO. INTRODUCCIÓN A LA LEY NACIONAL NÚM. 26.388*. *Obtenido de https://www.scielo.org.mx/pdf/bmdc/v45n135/v45n135a2.pdf*

Arroyo, R. (2016). Análisis de los delitos informáticos por ataque y acceso no autorizados a sistema electronicos, tipicados en los articulos 232 y 234 del codigo organico integral penal en el Ecuador. Obtenido de http://www.dspace.uce.edu.ec/bitstream/25000/5953/1/T-UCE-0013-Ab-121.pdf

BOE. (21 de febrero de 2019). DISPOSICIONES GENERALES. *ESPAÑA: BOLETÍN OFICIAL DEL ESTADO. Obtenido de Boe: https://boe.es/boe/dias/2019/02/21/pdfs/BOE-A-2019-2363.pdf*

Cajo, I. M. (2018). Análisis Comparativo De Herramientas Forenses Informáticas Para La Realización De Peritajes En Medios Digitales. *Chimborazo. Obtenido de file:///C:/Users/david/Downloads/11578-Article%20Text-33158-1-10-20181230.pdf*

CALDERÓN, V. L. (2020). "LAS NUEVAS PERSPECTIVAS REGULATORIAS DE DELITOS INFORMÁTICOS EN LAS COMPRAS A TRAVÉS DE INTERNET". Obtenido de http://dspace.unach.edu.ec/bitstream/51000/7607/1/8.-TESIS%20VER%C3%93NICA%20LILIANA%20PAGUAY%20CALDER%C3%93N-DER.pdf

Correa, C. P. (2014). Delitos Informáticos y la Ley 19.223. Obtenido de https://derecho.udd.cl/actualidad-juridica/files/2021/01/AJ29_553.pdf

Cortez, A., & Chang, C. (2012). Diseño de un nuevo esquema para el procedimiento de indagacion de los delitos informaticos. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/2812/1/UPS-GT000312.pdf

Delgado, M. d. (2015). DELITOS INFORMÁTICOS DELITOS ELECTRÓNICOS. Obtenido de http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf

Gonzalez, j. (2018). DELITOS INFORMÁTICOS: UNA REVISIÓN EN LATINOAMÉRICA. *Machala. Obtenido de file:///D:/Universidad%20Ecotec/TITLACION/262-Texto%20del%20art%C3%ADculo-401-1-10-20180716%20(1).pdf*

Hidalgo, I., Yasaca, S., Lema, L., & Hidalgo, B. (2018). Informatica Forense. *Chimborazo: La Caracola Editores. Obtenido de http://cimogsys.espoch.edu.ec/direccion-publicaciones/public/docs/books/2019-09-19-133251-70%20Libro%20Informatica%20Forense.pdf*

Idocpub. (diciembre de 2019). idocpub. *Obtenido de idocpub: https://idoc.pub/documents/elementos-constitutivos-del-delito-6klzm5go0gng*

Jácome, R. A. (2016). Análisis de los delitos informáticos por ataque y acceso no autorizado a sistemas electrónicos, tipificados en los artículos 232 y 234 del Código Orgánico Integral Penal en el Ecuador. *Quito. Obtenido de http://www.dspace.uce.edu.ec/bitstream/25000/5953/1/T-UCE-0013-Ab-121.pdf*

Jiménez, J. (Septiembre de 2015). DELITOS INFORMÁTICOS. Obtenido de https://intercoonecta.aecid.es/Gestin%20del%20conocimiento/Jim%C3%A9nez%20Martin%20Jorge%20-%20Delitos%20inform%C3%A1ticos.pdf

Lecanda, R. Q. (2002). Introducción a la metodología de investigación cualitativa. *España. Obtenido de https://www.redalyc.org/pdf/175/17501402.pdf*

Library. (2020). Library. *Obtenido de Library: https://1library.co/es/download/881149333809430530*

Machicado, J. (2010). Conceptos de delitos. *La Paz. Obtenido de https://jorgemachicado.blogspot.com/2009/02/que-es-el-delito.html*

OpenBank. (14 de diciembre de 2021). ¿Qué es el delito de "carding"? Obtenido de https://www.openbank.es/open-news/carding/

Policia Nacional del Ecuador. (agosto de 2022). Policia Nacional del Ecuador. *Obtenido de Policia Nacional del Ecuador: https://www.policia.gob.ec/wp-content/uploads/downloads/2022/08/boletin-que-es-el-carding-y-como_protegernos.pdf*

Quevedo, J. (2017). Investigacion y prueba de ciberdelitos. Obtenido de https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y

Rentero, A. (2023). Carding: Alerta del INCIBE sobre el robo de datos de tarjetas de crédito. *España: Silicon. Obtenido de https://www.silicon.es/carding-alerta-del-incibe-sobre-el-robo-de-datos-de-tarjetas-de-credito-2477403*

Rentero, Antonio. (24 de ABRIL de 2023). Carding: Alerta del INCIBE sobre el robo de datos de tarjetas de crédito. Obtenido de SILICON: https://www.silicon.es/carding-alerta-del-incibe-sobre-el-robo-de-datos-de-tarjetas-de-credito-2477403

Rodríguez, F. G. (2020). NUEVOS DELITOS INFORMÁTICOS: PHISING, PHARMING, HACKING Y CRACKING. Obtenido de https://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf

Rojas, J. R. (4 de febrero de 2016). Revista Seguridad. *Obtenido de Revista Seguridad: https://revista.seguridad.unam.mx/numero26/delitos-inform-ticos-en-m-xico*

Sain, G. (2015). Evolución Historica de los Delitos Informáticos. *REVISTA/ PENSAMIENTO PENAL. Obtenido de https://www.pensamientopenal.com.ar/system/files/2015/04/doctrina40877.pdf*

Sampaoli, J. (2018). Peritaje informático: marco teórico-practico. *Obtenido de https://repositorio.uca.edu.ar/bitstream/123456789/523/11/peritaje-marco-tecnico-practico.pdf*

Solís, G. (2015). ESTRUCTURA JURÍDICA DE MÉXICO. *Ciudad de Mexico. Obtenido de https://www.uaeh.edu.mx/docencia/P_Presentaciones/prepa4/derecho/Delitos.pdf*

Thofehrn, M. B. (2013). Grupo focal: Una técnica de recogida de datos en investigaciones cualitativas. *España. Obtenido de https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1132-12962013000100016*