UNIVERSIDAD PERUANA DE CIENCIAS E INFORMATICAS

FACULTAD DE DERECHO Y CIENCIAS POLITICAS

CARRERA PROFESIONAL DE DERECHO

TRABAJO DE SUFICIENCIA PROFESIONAL

"EL TRATAMIENTO DE LA EVIDENCIA DIGITAL COMO MEDIO PROBATORIO EN LA INVESTIGACIÓN DEL DELITO INFORMÁTICO EN LA MODALIDAD DE VULNERACIÓN DE CAJEROS AUTOMÁTICOS, LIMA 2019"

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

AUTORES:

Bach.: HUAMAN RAMOS, ZÓSIMO

Bach.: OLIVERA BARRIENTOS, CARLOS FRANZ

ASESOR:

Dr. ARMAS ZÁRATE, FERNANDO

ID ORCID: https://orcid.org/0000-0002-4390-438X

DNI Nº 07973958

LIMA-PERÚ

2022

DEDICATORIA

A nuestros seres queridos y a la Policía Nacional del Perú que son la razón y el motivo de superación y perfeccionamiento continuo.

AGRADECIMIENTO

Nuestro sincero agradecimiento a nuestros seres queridos que, de diferentes maneras han aportado para que esta meta se haga realidad. A nuestros compañeros de aula, quienes con el corazón álgido nos motivaron a seguir adelante. Finalmente, a nuestros catedráticos por compartir con nosotros sus conocimientos y orientarnos con sus palabras y ejemplo a perseverar en un proyecto de vida en beneficio de cada uno.

DECLARACIÓN DE AUTORÍA

Yo, **Huamán Ramos, Zósimo**, identificado con Documento Nacional de Identidad N° **28243039** y **Olivera Barrientos, Carlos Franz** identificado con Documento Nacional de Identidad N° **20074006**, estudiantes de la carrera profesional de Derecho de la Universidad Peruana de Ciencias e Informáticas en la Investigación de Suficiencia Profesional titulado "**El tratamiento de la evidencia digital como medio probatorio en la investigación del delito informático en la modalidad de vulneración de cajeros automáticos, Lima 2019**" con la finalidad de dar cumplimiento a las disposiciones vigentes en el Reglamento de Grados y Títulos de la Universidad Peruana de Ciencias e informáticas:

Dejar en claro que la información vertida en esta investigación es verás y auténtica, recabada con minuciosidad y analizada según los lineamientos establecidos por esta Casada de Estudios.

En tal sentido, asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual nos sometemos a lo dispuesto en las normas académicas de la Universidad Peruana de Ciencias e Informáticas.

Lima, 20 de junio de 2022

Huamán Ramos, Zósimo

Olivera Barrientos, Carlos Franz

ÍNDICE

INTRODUCCIÓN

El presente trabajo de investigación de suficiencia profesional lleva por título “El tratamiento de la evidencia digital como medio probatorio en la investigación del delito informático en la modalidad de vulneración de cajeros automáticos, Lima 2019”. El mismo fue desarrollado teniendo en consideración la aparición de nuevas formas delictivas que son utilizadas por organizaciones criminales para cometer fraude Informático, quienes emplean herramientas informáticas de última generación capaces de vulnerar cualquier medida de seguridad que son implementadas en los cajeros automáticos que se encuentran instalados en las instituciones financieras.

En los últimos años las entidades financieras se han visto perjudicadas con pérdidas millonarias a través de ataques realizados a los cajeros automáticos - ATM. Una investigación conjunta entre Motherboard y la emisora alemana Bayerischer Rundfunk (BR) han descubierto nuevos detalles sobre los ataques realizados a los cajeros automáticos denominado «jackpotting», técnica utilizada el año 2017 en cajeros automáticos del país de Alemania donde organizaciones criminales han sustraído un millón de euros.

En ese sentido, Jackpotting es una técnica ilícita donde los cyber delincuentes usan un malware para engañar a un cajero automático y lograr la expulsión de todo su efectivo, sin la necesidad de utilizar una tarjeta bancaria. Los cyber delincuentes suelen instalar el malware en un cajero automático abriendo físicamente un panel en la máquina para revelar un puerto USB y mediante este soporte captar la información contenida en un ATM.

A finales del año 2018 en nuestro país, organizaciones criminales utilizando la técnica jackpotting han sustraído más de 4 millones de soles de los cajeros automáticos pertenecientes a diferentes entidades bancarias.

En nuestra Legislación Peruana, el Fraude Informático se encuentra tipificado en el Articulo Nº 8 de la Ley 30096 y su Modificatoria Ley Nº 30171- Ley de Delitos Informáticos, en el que se señala: “El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social."

CAPÍTULO I: PLANIFICACIÓN DEL TRABAJO DE SUFICIENCIA PROFESIONAL

El avance de la tecnología de la información y comunicaciones han permitido que organizaciones criminales perfeccionen su modus operandi, siendo importante resaltar que desde el momento que el hombre realizaba las investigaciones empíricas en acciones que constituyen delitos, se encamina a la investigación criminal.

El avance científico y tecnológico tiene dos vertientes claramente delimitados y diametralmente opuestos. En la primera se entiende que la ciencia y la tecnología están al servicio de la humanidad, gracias a este avance se han podido prever muchas situaciones problemáticas para la humanidad; despejar las dudas relacionadas al universo donde el ser humano ocupa un papel preponderante; gracias a ella se pudo dar el giro copernicano, el cambio del geocentrismo al heliocentrismo; el paso de la fuerza bruta en el trabajo a un trabajo tecnificado y una producción a gran escala toda vez que la propalación de la humanidad en la tierra es más acelerada y requiere satisfacer sus necesidades elementales en menor tiempo posible.

Ahora bien, así como la ciencia *per se* resulta beneficiosa, también puede ser tremendamente perjudicial para el mismo ser humano y la sociedad cuando mentes criminales utilizan la misma para cometer actos contrarios a la ley. En ese sentido, en la actualidad se evidencia con mayor frecuencia actos criminales a gran escala cometidos con el apoyo de la ciencia y la tecnología. Justamente en ello radica la gran problemática que queremos presentar en esta investigación, pues, resulta de necesidad imperiosa no solamente el descubrimiento del problema en torno fraude a los delitos informáticos en contra del patrimonio en la modalidad de fraude informático en la vulneración de cajeros automáticos, sino también plantear

alternativas de solución a fin de prever y cierta forma revertir los alcances negativos de este delito.

En ese orden de ideas, en los últimos años los cajeros automáticos de las entidades financieras de nuestro país se han visto afectados con ataques informáticos capaces de vulnerar cualquier medida de seguridad; según los reportes de denuncias que obran en la División de Investigación de Delitos de Alta Tecnología de la DIRINCRI PNP, a finales del año 2018 diferentes entidades financieras se han afectado con pérdidas que superan los 4 millones de soles; sin embargo, debido a las técnicas sofisticadas de ataques informáticos dificultaba el accionar inmediato del Personal Policial, toda vez que existe un reducido número de efectivos con conocimiento de un escenario delictivo de tan compleja estructura.

El 31 de octubre de 2018 el Banco GNB del Perú fue víctima de fraude informático a través de la infección de dos de sus cajeros automáticos, con un malware (Programa malicioso o maligno utilizado para acceder ilícitamente a un dispositivo) a través de la modalidad «jackpotting» ha originado la sustracción de S/.357,530.00 soles y US$34,960.00 Dólares; precisándose que el primer ataque informático fue realizado entre las 20:00 a 22:00 horas al cajero automático Nº 406 instalado en la calle Monterrey N° 227-233 Urb. Chacarilla del distrito de Santiago de Surco, desde donde sustrajeron la cantidad de S/. 234,390.00 soles y USD 27,060.00 dólares; el segundo ataque informático fue realizado entre las 23:00 a 23:59 horas al cajero automático Nº 429, instalado en la Av. 27 de julio 1160 del distrito de Miraflores, desde donde sustrajeron la cantidad de S/.123,140.00 soles y US$ 6,900.00 dólares, significándose que en la sustracción de dinero de ambos cajeros automáticos, participaron los mismos integrantes de la organización criminal, quienes han utilizado como medio de coordinación sus equipos telefónicos.

De igual forma, en los meses de noviembre y diciembre del 2018, seis (06) cajeros automáticos del BBVA - Banco Continental, fueron vulnerados con un malware bajo la modalidad de «jackpotting», organizaciones criminales sustrajeron del cajero automático 1497 ubicado en la Av. Universitaria con el Ovalo José Granda del San Martin de Porras, la suma de S/2,893,200 y US$ 14,400 Dólares americanos; del cajero automático número 1473, ubicado en la Av. Túpac Amaru cdra. 16 (tienda metro de la UNI) del distrito de Independencia, sustrajeron la cantidad de S/.387,000.00 soles; del cajero automático número 293, ubicado en la esquina de la Av. La Marina con parque las Leyendas en la tienda metro distrito de San Miguel, sustrajeron S/.846,000.00 y

$49,800.00 dólares; del cajero automático número 1497 ubicado en la Av. Universitaria N° 313 del distrito de San Martin de Porras, sustrajeron la cantidad de S/ 1,002,000.00 soles y $14,400.00 dólares; del cajero automático número 1317 ubicado en la Av. Oscar R Benavides N° 1608 Bella Vista – Callao, sustrajeron la suma de S/. 255,000.00 soles; del cajero automático número 1474 ubicado en la Av. Túpac Amaru N° 3900 Urb. La Pascana del distrito de Comas, sustrajeron la suma de S/.123.000.00 soles; y del cajero automático número 1424 Ubicado en la Villa María del Triunfo 210 en el interior de la estación del servicio grifo Copetrol del distrito de Villa María del Triunfo, sustrajeron la suma S/. 280,200.00 soles y $3,000.00 dólares.

En consecuencia, en base a los puntos referidos en párrafos precedentes es de considerar que la problemática frente a los delitos informáticas es más que evidente y amerita un tratamiento jurídico más eficiente y eficaz.

En este sentido, este trabajo consta de cuatro capítulos: la primera parte abarca la introducción, luego el marco teórico con los respectivos antecedentes y los subtemas

debidamente estructurados. El tercer capítulo abarca el desarrollo de las actividades programadas para obtener los resultados, conclusiones y recomendaciones.

CAPÍTULO II: MARCO TEÓRICO

Estudios sobre la ciberdelincuencia en el contexto internacional.

En Colombia, Ramírez y Castro (2018), realizaron una investigación titulada "Análisis de la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia". Dicho trabajo de investigación se llevó a cabo en la Universidad Nacional Abierta y a Distancia "UNAD" con el objetivo de identificar las falencias en el tratamiento de pruebas digitales que puedan ocasionar pérdidas, daños o destrucción de las mismas en procesos judiciales por medio del estudio del proceso de cadena de custodia en la investigación de delitos informáticos en Colombia. Esta investigación fue desarrollada de manera exploratoria debido que a las leyes en relación a los delitos informáticos en Colombia aún no están debidamente implementados; el enfoque fue cualitativo toda vez que está basado en la descripción de los hechos según los procedimientos propios de un estudio forense. De lo cual se obtuvo como conclusión que

> La tecnología como herramienta fundamental para el crecimiento y desarrollo personal, social, económico y académico de las personas dentro de una sociedad de consumo, nos ha llevado a ser dependientes en gran escala de los equipos electrónicos ya sean celulares, tablets, computadores, sistemas de cámaras de video vigilancia, software a la medida, equipos de automatización y control de acceso, redes LAN, WAN y MAN como medio masivo de interacción de información más las redes sociales, han logrado que todo este sistema nos facilite las cosas y lograr mantener un control sobre lo que hacemos, pensamos y realizamos ya sea en el ámbito personal o laboral, pero también se volvió en uno de los medios más atacados de forma inapropiada con intereses oscuros por personas que reciben el nombre de ciberdelincuentes los cuales en los últimos años han incrementado sus ataques y también las personas que no tiene un alto grado de conocimiento de las tecnologías se han comprometido con algún acto inapropiado y vandálico por medio de alguna herramienta tecnológica. Por tal efecto Colombia mediante el

> Ministerio de Telecomunicaciones adopto una ley llamada "de la protección de la información y de los datos" Ley 1273 de 2009. (p.111)

En Guatemala, Escobar (2017), realizó una tesis de grado titulada "Manejo de la cadena de custodia en la recolección de evidencia digital". Esta investigación fue realizada en la Universidad Rafael Landívar de Guatemala con la finalidad de Determinar el debido manejo de la cadena de custodia utilizando distintos softwares, para lo cual se utilizó un método estrictamente descriptivo, enfoque cualitativo para llegar a la conclusión que "el debido manejo de la cadena de custodia en la recolección de evidencia digital desde su inicio resulta muy importante en la investigación criminal, esto implica que se desarrollen metodologías locales que observen las propias necesidades y obstáculos que se presentan, como parte de la progresividad en la metodología de la investigación que desarrolla el Ministerio Público de Guatemala".

En Argentina, Sergi (2018), realizó una investigación titulada "Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina", en la Asociación por los Derechos Civiles, con el objetivo de analizar los alcances generales de la evidencia digital en Argentina en consonancia directa con el proceso penal. El método empleado fue netamente descriptivo desde las bases conceptuales a nivel nacional e internacional, en la doctrina y la jurisprudencia. En ese sentido, la conclusión del trabajo fue que:

> La evidencia digital en el proceso penal enfrenta al sistema jurídico penal a uno de los desafíos más importantes de la historia. El problema lo afecta de manera transversal pues se vincula con la recolección de elementos probatorios en todo tipo de casos". La afectación de la tecnología en la intimidad de los ciudadanos obliga a una regulación (cuando ello es necesario) muy rigurosa. En este sentido, resulta interesante el concepto de la Corte Federal Constitucional Alemana que reconoce un nuevo derecho fundamental constituido por la garantía a la confidencialidad e integridad de la información en sistemas informáticos como una derivación

> del derecho a la personalidad y la dignidad. Resulta relevante advertir el grado de amplitud (en virtud de algunos medios tecnológicos o en algunos casos en particular) de la injerencia a la intimidad. (p.98)

En Ecuador, Jiménez (2018), realizó una tesis titulada "Desarrollo de una aplicación de uso didáctico para comunicación segura de datos a través de la red", en la Escuela Politécnica Nacional de Quito con el objetivo de determinar la importancia del uso didáctico para la comunicación segura de datos a través de la red; el método aplicado fue cualitativo, diseño no experimental, para llegar a la conclusión que

> Un algoritmo Hash es una función que toma una cadena o mensaje de longitud variable y produce un valor hash de longitud fija, también llamado resumen de mensaje, que se emplea para verificar la integridad de los datos y mensaje, que se emplea para verificar la integridad de los datos y mensajes, se representa como una cadena corta de letras aleatorias y números, es como una huella digital de un mensajes, es un proceso unidireccional, pues no es posible crear el texto original utilizando cualquier función del hash inverso, si los datos originales cambian incluso por un carácter, la función hash producirá un valor hash diferente, por lo tanto, el receptor sabrá que la información original ha cambiado. (p.33)

En Argentina, Justo (2017), Miembro integrante de la Asociación por los Derechos Civiles de la Policía Federal de Argentina, elaboró un trabajo de investigación titulado "Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal". Un trabajo realizado desde un enfoque analítico a fin de determinar la importancia y los alcances del Cibercrimen a nivel internacional, por afirma en sus conclusiones que:

> El uso de las nuevas tecnologías trae aparejados fenómenos novedosos entre ellos, modalidades delictivas que enfrentan las capacidades de los distintos miembros que conducen una investigación judicial. La escasa interacción entre los operadores judiciales, los investigadores y los peritos dificultan la tarea de investigación, que además se ve comprometida por la falta de recursos para el investigador.

En Colombia, Lasso (2017), presentó una investigación monográfica titulada “Estado del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia”, en la Universidad Nacional abierta y a distancia, UNAD Escuela de Ciencias Básicas Tecnología e Ingeniería Especialización en Seguridad Informática Palmira, con el objetivo de determinar la relación que existe entre la evidencia digital y la administración de justicia que en estos últimos años ha ido en decadencia. Este trabajo se realizó desde un enfoque cualitativo puesto que interpreta los hechos delictivos relacionados a la ciberdelincuencia y su repercusión social; con diseño no experimental, de corte transversal, con instrumentos de recolección de datos debidamente estructurados. La conclusión del trabajo fue que:

> El peritaje informático es una actividad de investigación que ha tomado fuerza a nivel internacional debido a la relevancia que tiene dentro de los procesos judiciales donde interviene la evidencia digital, a raíz del aumento de lo 89ciberdelitos, pues permite esclarecer los hechos ocurridos en un caso específico, brindando las herramientas para dirimir y lograr la impartición de la justicia de manera adecuada. (p.88-89)

Estudios de la ciberdelincuencia en el contexto nacional.

Osco (2019), presentó una tesis para optar el grado de maestro titulada “La admisibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano 2018”, en la Universidad César Vallejo, Lima, con el objetivo de describir alternativas de procedimientos legales e informáticos para el tratamiento de la evidencia digital, para que sean admisibles y tengan el valor probatorio en un proceso penal en el Sistema Jurídico Peruano. Esta investigación fue desarrollada desde un enfoque cualitativo, con diseño de estudio no experimental con casos de estudio, en la cual participaron diversos agentes responsables de la administración de justicia, jueces, fiscales, policías especializados en la investigación criminal. La conclusión a la cual se llegó en esta investigación fue que:

> Los delitos informáticos se desarrollan en el ciberespacio en conexión con internet, la ciberdelincuencia ha dado lugar a los delitos transnacionales donde las leyes no tiene alcance y jurisdicción al involucrar a varios países en un solo hecho, quedando impunes y sin sanción penal, ello también viene generando grandes pérdidas a personas e instituciones públicas y privadas tanto económicas, así como de credibilidad en los servicios a sus clientes. Los ciberdelincuentes en el desarrollo de su actividad ilícita dejan las evidencias digitales, que son los rastros o huellas del delito, siendo el origen de la investigación con participación de la Policía y los operadores de justicia. (p.211)

Nessi (2017) presento el Proyecto de apoyo al sector Justicia *American Bar Association Rule of law Initiative aba roli* Perú, Ministerio Publico y Policía Nacional del Perú, titulada "Manual de Evidencia Digital", que establece que los que participen en el conocimiento, conducción y análisis de la evidencia digital deben realiza en estricto cumplimiento de lo dispuesto en el artículo 67 del Nuevo Código Procesal Penal que la letra establece: "La Policía Nacional en su función de investigación debe, inclusive por propia iniciativa, tomar conocimiento de los delitos y dar cuenta inmediata al Fiscal, sin perjuicio de realizar las diligencias de urgencia e imprescindibles para impedir sus consecuencias, individualizar a sus autores y partícipes, reunir y asegurar los elementos de prueba que puedan servir para la aplicación de la Ley penal. Similar función desarrollará tratándose de delitos dependientes de instancia privada o sujetas a ejercicio privado de la acción penal". Dicho manual contiene los lineamientos especiales sobre las formas y los mecanismos de preservación, control y posterior análisis de la información recabada en la fase inicial de la investigación, de lo contrario estarían propensos a estropearse y no favorecer a la investigación posterior.

Por eso, el Manual de Evidencia Digital antes referido, establece los principios básicos que se deben cumplir y son los siguientes:

> 1. Es fundamental la capacitación y el entrenamiento de los investigadores, técnicos y fiscales para un correcto procedimiento, exento de falencias u objeciones procesales.
> 2. El personal policial no debe adoptar ninguna decisión en la escena del delito que pueda alterar o modificar los datos contenidos en los dispositivos de almacenamiento a utilizar sin previa consulta con el fiscal.
> 3. Del mismo modo, las herramientas y metodologías a utilizar en la escena del delito, deben ser previamente acordadas con el director de la investigación. (p.13)

Sequeiros (2016) presentó un trabajo de investigación en la modalidad de tesis de pregrado titulado "Vacío legales que imposibilitan la sanción de los delitos informáticos en el nuevo Código Penal Peruano", en la Universidad de Huánuco, con el objetivo de determinar los vacíos legales con respecto a la sanción de los delitos informáticos en el Ordenamiento Jurídico Penal peruano. El trabajo fue realizado desde un enfoque cualitativo, interpretativo, con diseño no experimental, a fin de arribar a la conclusión que:

> Es una situación de vacío en la ley que ha sufrido omisión en su texto la regulación concreta de una determinada situación, que no encuentra respuesta legal específica; con ello se obliga a quienes aplican dicha ley (jueces, abogados, fiscales, y otros) al empleo de técnicas sustitutivas del vacío, con las cuales puedan obtener respuesta eficaz a tal ausencia. Ante esta situación, se hace necesario suplir la laguna jurídica a través de distintas herramientas tales como el Derecho Supletorio donde el juez acude a la regulación de una rama del derecho supletoria. La Interpretación extensiva el juez hace una interpretación lo más extensiva posible de una norma cercana. La Analogía el juez aplica normas que están dictadas para situaciones esencialmente parecidas. Acudir a otras fuentes del derecho como la costumbre o los principios generales del Derecho y la Norma Cruzada entre normas principales y otras supletorias, de modo que se sabe cuál debe aplicarse con preeminencia y al mismo tiempo, entre del derecho principal y el derecho supletorio.

Vilca (2018), presentó una tesis para optar el título de abogado titulado "Los Hackers: Delito informático frente al Código Penal Peruano", trabajo realizado en la Universidad Santiago Antúnez de Mayolo. El objetivo del trabajo de investigación fue conocer los vacíos legales que imposibilitan la sanción de los Hackers en el Nuevo Código Penal peruano. El método del trabajo fue netamente descriptivo, de enfoque cualitativo para llegar a la conclusión de que "La falta de una información adecuada sobre los límites de la tecnología informática es

un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones" (p.90).

Nociones generales sobre la ciberdelincuencia

Esta es una modalidad delictiva en la que, utilizando el internet, el delincuente destruye equipos de cómputo o equipos similares, atentando de ese modo contra la veracidad y la certeza de los sistemas informáticos a fin de suplantar la identidad de personas naturales o jurídicas y cometer fraudes a gran escala. En pocas palabras, es la forma de cometer delitos utilizando sistemas informáticos que atraviesan todo tipo de seguridad y quebrantan la identidad de personas vulnerando sus derechos y son de diferentes clases según se evidencia en la siguiente imagen:

Fuente: Agencia Española de Protección de Datos (2018)

La identificación de los cibercriminales

Según Osco (2019), el denominado Hacker viene a ser una persona altamente especializada en los sistemas informáticos, en el manejo de las telecomunicaciones a un nivel superior a lo común cuyo interés es comunicar al resto que pudo vulnerar la seguridad informática de una empresa o institución, aunque no siempre alteran el contenido de la información que

pudo evidenciar; dejan el sistema vulnerado sin alteraciones. Ahora bien, si esta persona utiliza sus conocimientos informáticos y las aprovecha para cometer actos ilícitos, pues, estamos frente un ciberdelincuente.

Según Galindo (2016), director de Negocios y Alianzas Estratégicas de Digiware explica cuál es el perfil de los ciberdelincuentes que operan como grandes organizaciones criminales y atacan alrededor de 600,000 veces por día, información vertida en el Diario Gestión. Según el autor mencionado, el 50% de las bandas dedicadas al cibercrimen se componen de 6 o más personas. De ellos, el 76% son hombres cuyas edades van desde los 14 años (8%) hasta los 50 (11%). Aunque la edad promedio de este tipo de delincuentes es 35 años (43%). El 50% de los grupos de ciberdelincuentes han operado por más de seis meses, mientras que el 25% ha operado 6 meses o menos. La mayor parte de su actividad, se registra Norteamérica y Sudamérica con un 19% del total de ataques generados a nivel mundial".

Las características especiales de los ciberdelincuentes son:

1. Es una persona que tiene un mediano o alto conocimiento de computadores y redes en general.
2. Sujetos con conocimientos en cómputo por encima del promedio. (Cambio de IP, uso de programas Keyloggers, uso de navegadores inusuales entre otros).
3. Personas que aprovechan espacios sociales para preguntar por datos de clientes y demás información de uso restringido.
4. Personal que instala programas espías sin autorización.
5. Sujetos que desactiva el software antivirus en su equipo de trabajo.
6. Personas que hacen uso sin autorización de computadoras o dispositivos de los demás miembros de la organización.
7. Empleados que se quedan a trabajar en horario extra oficina sin dar justificación.

Pues, frente a ello las empresas o las entidades públicas deben tener bastante cuidado a fin de proteger la privacidad de la información y, sobre todo, hacer un seguimiento de los actos que podrían ir cometiendo algunos servidores sin dejar evidencia de aquello.

Fuente: Diario Gestión, delincuente que actúa bajo la sombra (2018).

Ciberdelitos en el mundo

En estos últimos años se ha podido evidenciar en los diferentes medios de comunicación tanto a nivel nacional como internacional ataques contra el sistema de seguridad de entidades bancarias, sobre todo los ataques de hackers en Perú y Chile, los llamados ataques *ransomware*. En caso de Perú tres bancos fueron víctimas de ataques cibernéticos, de igual manera alguna semanas posteriores ocurrió el robo de 10 millones de dólares en el Banco de Chile.

De acuerdo al diario peruano La República, Maurice Fraisinet, jefe de Seguridad Informática de la SEGDI de la Presidencia del Concejo de Ministros, informó que es un ataque de *ransomware* y los afectados son Scotiabank e Interbank han recomendado a los trabajadores

de diversas compañías no abrir joins externos recibidos a través de email y servicios de mensajería. Así también, trabajadores de Scotiabank reportaron haberse quedado sin sistema durante horas de la mañana.

Fuente: Publicación del Diario la Republica el 18/08/2018

En la primera escala de ataque por los delincuentes son las entidades financieras según se ha manifestado en líneas precedentes, luego sigue la industria que se dedica a la administración de energía.

Por eso Osco (2018), afirma que “El “BlackEnergy” es un malware que desconectó a varias estaciones de la red eléctrica en Ucrania, generando un apagón de seis horas que afectó a miles de usuarios. El sector más afligido por el cibercrimen es el energético en el Perú, los ataques han generado un costo de pérdidas de US$ 17.20 millones al año aproximadamente.

También indico que a medida que la renovación virtual ha aumentado, también creció el ilícito". (p.26)

GESTIÓN Tecnología • Portada • Economía • Tendencias • Tu Dinero • Gestión TV • Blogs

Ciberataques al sector energético en Perú cuestan US$ 17.20 millones al año

La industria que se dedica a la generación, transporte y distribución de energía está registrando un elevado índice de incidentes y se ubica en segundo lugar después del sector financiero.

Compartir Compartir Compartir

El "BlackEnergy" es un malware que desconectó a varias estaciones de la red eléctrica en Ucrania y provocó un apagón de seis horas que afectó a 80,000 usuarios. (Foto: Internet)

REDACCIÓN GESTIÓN / 31.07.2018 - 04:47 PM

ÚLTIMAS NOTICIAS

Fuente: Publicación del diario Gestión el 31/07/2018

Se ha podido graficar someramente algunos casos de delincuencias ocurridos en el Perú, son en mayor número según se ha detallado en la descripción de la realidad problemática que cada día resulta alarmante y amerita énfasis en la regulación; pues, de lo contrario, sobre todo las grandes compañías barias y entidades relevantes están destinados al naufragio.

Evidencia digital

Según Nessi (2017), "La evidencia digital es todo registro informático almacenado en un dispositivo informático o que se transmite a través de una red informática y que pudiera

tener valor probatorio para una investigación. Se considera evidencia digital a cualquier información que, sujeta a una intervención humana, electrónica, y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático –computadoras, etc. Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas técnicas especiales". (p.15)

El accionar delictivo sería compatible con los siguientes delitos:

a. DELITO INFORMÁTICO CONTRA EL PATRIMONIO – FRAUDE INFORMÁTICO AGRAVADO (Art.8 - Ley 30171 Ley de Delitos Informáticos) por el uso deliberado e ilegítimo de la TICs para procurar un provecho económico en perjuicio de la entidad financiera, mediante la introducción del malware (support.exe, operator.dat y Request.dat) para la manipulación del sistema informático de los cajeros automáticos.

b. ATENTADO A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS AGRAVADO (Art.4 - Ley 30171 Ley de Delitos Informáticos) por el uso deliberado e ilegítimo del malware (support.exe, operator.dat y Request.dat) que ha generado la inutilización del sistema informático de los cajeros automáticos.

c. ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMÁTICOS AGRAVADO (Art.10 - Ley 30171 Ley de Delitos Informáticos), por el diseño del malware (support.exe, operator.dat y request.dat), para ser utilizado en la presunta comisión del Delito de Fraude Informático y Atentado a la Integridad de Sistemas Informáticos.

Fuentes de la evidencia digital

La evidencia digital puede encontrarse almacenada en dispositivos informáticos (discos rígidos, por ejemplo); en la memoria RAM de procesamiento de un sistema informático; o bien, cuando se transmite a través de una red de dispositivos cuya recolección se realizará en tiempo real (tráfico de datos). En este sentido, las fuentes de evidencia digital pueden ser clasificadas en los siguientes grupos:

a. Sistema de computación abiertos: Son los que están compuestos de las computadoras personales y de sus periféricos; las computadoras portátiles, y los servidores.

b. Sistemas de comunicación: Compuestos por las redes de telecomunicaciones, la comunicación inalámbrica e Internet.

c. Sistemas convergentes de computación: Sólo los que están formados por los teléfonos celulares inteligentes (Smartphones), los asistentes personales digitales PDAs, las tarjetas inteligentes.

Normativa internacional sobre delitos informáticos

Legislación sobre los Delitos Informáticos en Europa

La Carta Magna española establece en su Artículo 18, numeral 4 lo siguiente: "La norma restringirá el empleo de la tecnología buscando asegurar la dignidad y la confianza personal y familiar y el completo conocimiento de sus derechos, como se aprecia en la acotada norma incide directamente en la regulación de los delitos realizados a través de la tecnología, apreciándose que el bien jurídico es el de la intimidad. Así mismo existe varias normas que regulan los actos en conductas en delitos informáticos como: Ley de Servicios de la Sociedad de la información y Comercio Electrónico. Ley General en Telecomunicaciones. Ley Orgánica en Protección de Datos. Ley sobre la Firma

Electrónica. Reglamento sobre medidas en seguridad de archivos automatizados con información personal".

El Código Penal Español consigna conductas ilícitas en relación con los ilícitos informáticos, indica que esta tipificación se aproxima a la regulada por el Convenio de Budapest en la lucha contra la Ciberdelincuencia: Delitos contra la privacidad, la entereza y la disponibilidad de los datos y sistemas informáticos: Artículos 197, 278.1 y 264.2. Delitos informáticos: Artículos 248, 248.2, 249, 255 y 256. Delitos en relación con el contenido: Artículos 186 y 189.

Caso similar a la legislación española encontramos en otros países europeos sobre los delitos informáticos, tales como Austria, Holanda y Portugal.

Austria (1987). **-** El Código Penal Austriaco contempla la figura de Delitos Informáticos de la siguiente forma: Destrucción de datos: Art. 126. Estafa informática: Art. 148. Adherido al convenio de ciberdelincuencia.

Holanda (1993). **-** Cuenta con la Ley de Delitos Informáticos, penalizando las figuras de hacking, el phreaking (evasión de pago de servicios de telecomunicaciones), ingeniería social y la propalación de virus. Cabe resaltar que los virus son tratados de manera especial en la Ley. Adherido al convenio de ciberdelincuencia.

Portugal (1991). **-** Este país europeo cuenta con la una norma que protege datos personales Informatizados y se aplica de manera supletoria del Código Penal: Delito de falsedad informática: Artículo 4. Delito relativo a datos: Artículo 5. Sabotaje en con empleo de la informática: Artículo 6. Acceso ilegitimo: Artículo 7. Interceptación ilegitima: Artículo 8. Reproducción ilegitima de programas protegidos: Artículo 9.

Legislación sobre los Delitos Informáticos en América

México. **-** En América Latina, fue una de las primeras en conectarse a Internet en 1989.

El Código Penal mexicano sanciona los delitos informáticos en lo siguiente: Ingreso

no autorizado a sistemas de información y equipos tecnológicos. Sabotaje informático. Acceso ilegitimo a información. Adherido al convenio de ciberdelincuencia.

Venezuela (2001). **-** Promulgó una ley especial que reprime los ilícitos informáticos tipificando los siguientes delitos: Atentar contra los sistemas que emplean TIC. Los que atentan con la propiedad. Atentar contra las actividades privadas de las personas y las comunicaciones. Los que atentan contra los niños y adolescentes.

Argentina (2008). **-** En su legislación cuenta con una norma que reprime los delitos informáticos la misma que incorpora y rectifica el Código Penal Argentino. Incorpora los términos "documento", "firma" y "suscripción" en lo que se refiere a firma digital y los términos "instrumento privado" y "certificado" que vendrían hacer los documentos digitales. Adherido al convenio de ciberdelincuencia.

Chile (1993). **-** País en Latinoamérica pionero en sancionar los delitos informáticos a través de una Ley. Cuenta con la Ley 19223 que sanciona lo relativo a los delitos informáticos. También cuenta con la Ley 20.009 que sanciona el robo y extravió de tarjetas bancarias y la Ley 18.168 que regula las telecomunicaciones.

Brasil (2012). **-** Mediante la Ley 12.737 tipifica los delitos informáticos que combaten la elaboración, venta y reparación de pornografía infantil y pedofilia en internet. Sanciona también la invasión de los dispositivos informáticos, la interrupción o perturbar el servicio de telégrafo, radiotelegráfico o telefónico, impedir o dificultar su recuperación. La falsificación en su totalidad o parte de un documento o cambiar un documento concreto real.

Estados Unidos (1994). **-** Cuenta con el Acta Federal de abuso computacional que busca eliminar los argumentos de los virus informáticos; mediante un programa, dañar

información, códigos o el interior de un ordenador, así como sistemas informáticos, redes, información de datos y otros. Así mismo cuenta con legislación que sanciona las estafas electrónicas. Cuenta con el Acta de firmas electrónicas en el comercio global y nacional, ley sobre la firma digital.

Admisión de la prueba en el proceso penal

En la etapa del juicio es donde se practica la prueba respetando los principios de inmediación, publicidad, contradicción y oralidad. En ese sentido, según Lluch y González (2013) "con respecto al principio de contradicción, cabe señalar que, para dar cumplimiento al mismo, la evidencia contenida en soportes magnéticos se reproducirá en el juicio oral".

Requisitos de acceso: conducencia, necesidad, pertinencia y utilidad

Resulta interesante traer a colación lo que establece la Ley de Enjuiciamiento Civil en España que, en cierta forma ha aspirado nuestro ordenamiento penal peruano en muchos aspectos, sobre todo en el punto de la valoración de los medios probatorios en el juicio. En ese sentido, la LEC en su artículo 299, numeral 2 establece que las pruebas se "admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso". Estos elementos serán valorados por el juez al momento de actuar los medios probatorios; pues, de no cumplirse con los estándares mínimos requeridos simplemente no podrán ser materia de debate en el juicio oral. Pues, el artículo 283, numeral 1, establece que "No deberá admitirse ninguna prueba que, por no guardar relación con lo que sea objeto del proceso, haya de considerarse impertinente".

En modo estricto, cuando se trata de delitos informáticos, según refiere Castillo (2015), deberán valorarse una serie de características antes de admitir la prueba, tales como:

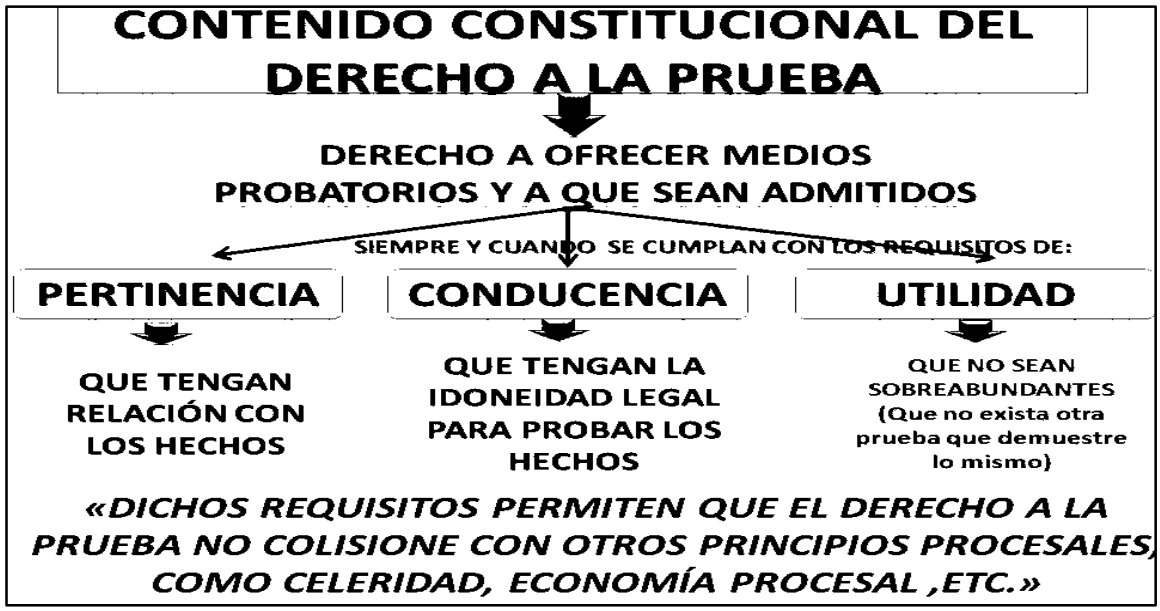
> a) Identificar el ordenador del que procede el documento electrónico, b) verificar que el funcionamiento del ordenador sea el correcto, c) demostrar que como consecuencia de los datos introducidos en el equipo se ha producido el resultado, d) explicar la fiabilidad del proceso de registro y salida de los datos obrantes en el equipo y e) acreditar quienes participaron en el procedimiento de elaboración del documento. El cumplimiento de lo señalado en los puntos expuestos, debido a su complejidad técnica, evidencia la necesidad en muchas ocasiones de aportar prueba pericial informática. (p.48)

Al respecto, Parra (2017) al referirse de la prueba nos da mayores alcances que a continuación detallamos:

La Conducencia: Se trata de que la prueba sea idónea en el aspecto legal y sirva para demostrar un hecho real. Esto significa que no exista una ley que prohíba la aplicación de tal prueba, sino todo lo contrario, está amparada por la norma.

La pertinencia: viene a ser la adecuación entre los hechos que se quieren demostrar en el proceso y el tema propiamente tratado en el debate. En otros términos, la prueba tiene que servir para demostrar un hecho dentro del juicio sin salir del contexto, sino únicamente sobre aquello que se está tratando. Pues, de lo contrario se da el rechazo *in limine* de la misma.

La utilidad: según diversos autores modernos, el móvil de la prueba tiene que ser estimular la actividad probatoria a fin de generar certeza y convicción en el juez; de lo contrario, debe ser rechazado de manera automática.



Fuente: Pavón (2018, Recuperado de Google.com

Procedimientos Tecnológicos de la Evidencia Digital

Normas estandarizadas sobre peritaje informático de la evidencia digital

La norma UNE 71505-2013 (Normalización Española), presenta algunos conceptos relacionados a las evidencias informáticas; establece los elementos claves que debe tener, confiabilidad, originalidad, reservas y cumplimientos. Además, establece los mecanismos de recolección, traslado y comunicación de las evidencias digitales. También establece los mecanismos de registro, ubicación de las evidencias de manera completa a fin de que sean presentados en un juicio posterior.

La normativa acotada tiene por objetivo asegurar las evidencias de manera integral a fin de garantizar la legitimidad y sobre todo la plenitud conservando la legalidad de los mismos para la valoración ante el tribunal, de tal modo que el perito informático pueda analizar y

verificar la realidad de los hechos de manera integral e intacta. En síntesis, esta normativa lo que busca es establecer el procedimiento para el tratamiento de la evidencia digital a fin de preservar, adquirir, documentar, analizar y presentar las evidencias digitales.

Estándares a nivel internacional

Por su parte, la ISO/IEC 27037-2012, establece los patrones de identificación, adquisición, selección y preservación de la evidencia. Por su parte, la ISO/IEC 27042-2015 establece los lineamientos orientadores respecto a la interpretación de la evidencia digital teniendo en consideración de los principios de continuidad, valoración, repetitividad y reproducción.

Además, es muy importante la consideración del documento RFC 3227 toda vez que desarrolla la directiva a fin de recolectar la información y los mecanismos de almacenamiento en un sistema digital; de tal forma que esta debe obtenerse lo más idéntico posible al original, que debe contener fechas, hora, local UTC, análisis de volatilidad de las memorias cachés y de la memoria RAM, finalmente el informe de los dispositivos de almacenamiento.

Recolección y preservación de la evidencia digital.

En el lugar de los hechos pueden darse diversas circunstancias, frente a ello lo que se tiene que hacer es recopilar los datos en su versión original, sin ningún tipo de contaminación, preservando la calidad y cantidad de las evidencias para su posterior admisión en el proceso judicial.

Es de necesidad imperiosa el responsable de la recolección de la información perennice lo ocurrido a través de la documentación correspondiente; pues, tratándose de hechos vinculados con delitos informáticos se dan a través del manejo de una computadora, por ello, a esta se debe tratar con muchas cautela, considerando las estructuras internas y externas de

manera conjunta, toda vez que una computadora contienen elementos que fácilmente se puede dañar si no se toma en cuenta las diligencias correspondientes. Se recomienda perennizar la información a través de galería de imágenes, toma fotográfica, captura de pantallas u otros mecanismos que se tenga al alcance para asegurar una información fidedigna y tenga su valor probatorio para la determinación de hechos delictivos.

Definiciones básicas sobre los cajeros automáticos

Cajero Automático - ATM (Automatic Teller Machine)

El cajero automático es una máquina expendedora que sirve para retirar dinero utilizando una tarjeta de material plástico que tiene banda magnética y un chip; los tipos de tarjeta tienen muchas variedades, pero las más usadas son de débito o crédito. Cabe precisar que estos cajeros automáticos no solamente sirven para retirar dinero, sino también para hacer depósitos, transferencias, apertura de cuentas mediante sus plataformas digitales. En la actualidad existen tres marcas grandes que ocupan el mercado, así tenemos a Wincor Nixdorf, Diebold y National Cash Register (NCR).

La mayoría de los ATMs, del mundo funcionan con sistema operativo Windows, sólo menos del 1% del mundo funciona en Linux (SUSE).

Partes de un cajero automático

El cajero automático tiene diferentes partes tanto a nivel externo como interno que a continuación vamos a detallar de manera gráfica:

Fuente: https://www.emaze.com/@AIZZZIOQ (2019)

PARTES EXTERNAS:

1	Pantalla
2	Teclado
3	Lector de tarjetas
4	Parlante
5	Botones de pantalla
6	Impresora de comprobantes

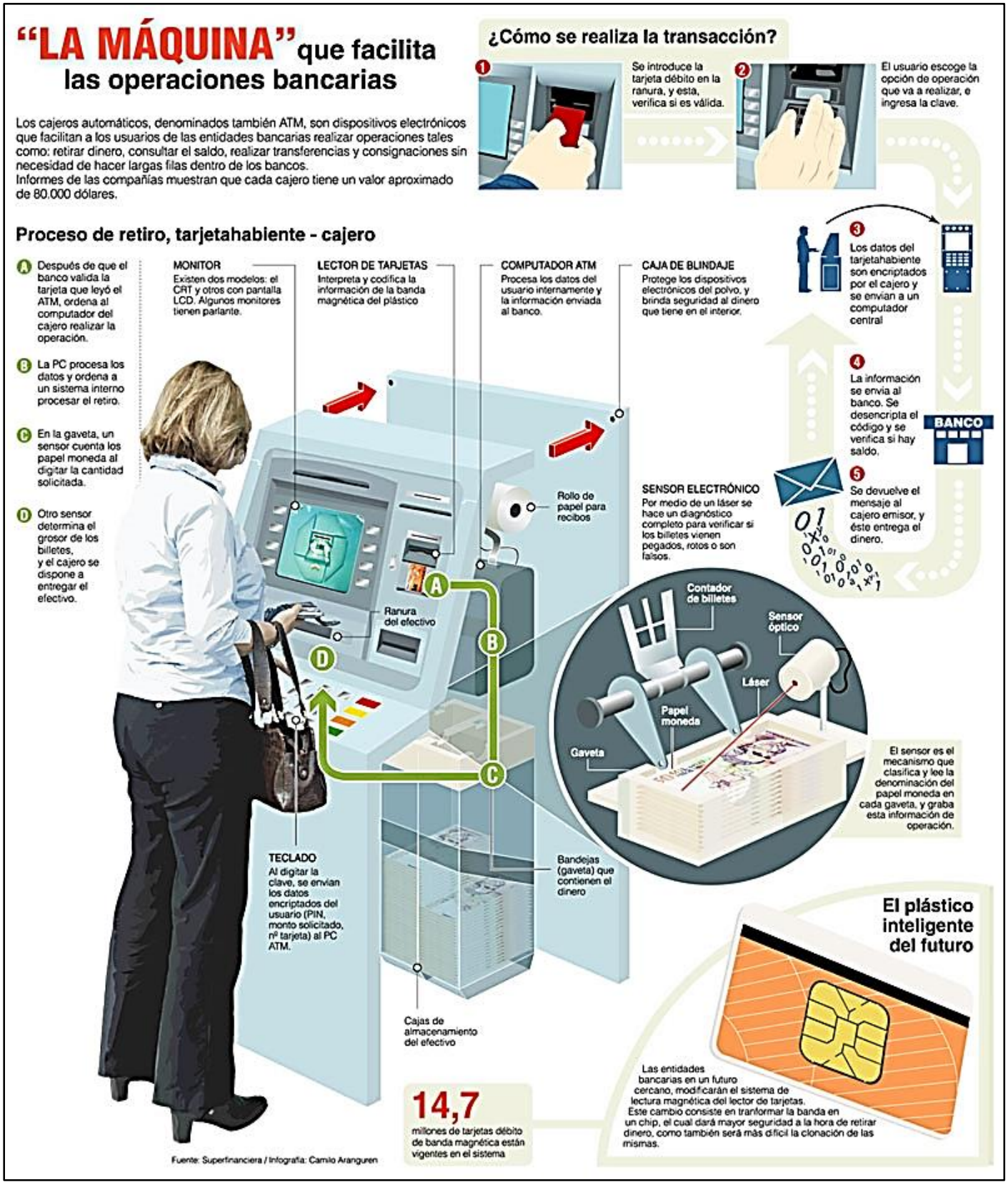
Fuente: elaboración propia (2019)

PARTES INTERNAS:

1	Cajas de almacenamiento
2	Bandejas(gavetas)
3	Rollo de papel
4	Sensor electrónico
5	Contador de billetes
6	Caja de blindaje
7	Purga

Fuente: elaboración propia (2019)

ESTRUCTURA INTERNA:



Fuente: https://www.emaze.com/@AIZZZIOQ **(2019)**

Gestión de red de los cajeros automáticos

Para el cumplimiento del protocolo de comunicación, los cajeros automáticos utilizan el código TCP/IP. Cabe indicar que este protocolo es muy importante a fin de administrar todas las operaciones de manera correcta, integrada y segura, permitiendo a su vez las facilidades de resolución y comunicación en la red.

Protocolo de comunicación

El Core Network es el sistema de comunicación utilizado por todos los cajeros automáticos para realizar las transacciones; es decir, se utiliza para aprobar, denegar, emitir errores y enviar mensajes específicos.

Por temas de facilidad y adaptación, el mercado financiero utiliza el Windows como sistema operativo en la cual se utiliza una comunicación TCP/IP, a fin de garantizar una comunicación fiable con el Core Network. Cabe precisar el protocolo de comunicación se basa en la Norma ISO 8583 (ISO 8583 Financial transaction card originated messages).

Firewall

Llamado también cortafuego que viene a ser un mecanismo de filtro avanzado cuya función es proteger la integridad y la confidencialidad de la información; en ese sentido protege la información de una red en la que se tiene confianza de otra que no la tiene. A nivel funcional viene a ser un dispositivo que sirve para separar, limitar y analizar el flujo de información que circula entre las puertas de acceso.

En cuanto a la variedad existen los firewalls que trabajan a nivel de red, conocidos también como paquetes; los firewall a nivel de aplicativos o proxy, y los firewall activos que son un mezcla de las dos anteriores.

Servidor Switch

A fin de orientar la investigación, este servidor tiene la finalidad de almacenar información relevante sobre las transacciones realizadas, los datos del usuario que le permiten identificar la fecha de operación, la hora, el nombre del servidor dodnde se realizó la transacción, la dirección IP e incluso el nombre del ordenador juntamente con demás datos que se registran en el sistema.

Jackpotting

Viene a ser una de las variantes de Ploutus, que fue diseñado para el el jackpotting en ATMs (técnica utilizada para sustraer grandes cantidades de dinero de un cajero sin tener que usar ninguna clase de tarjeta de crédito o débito)

El sistema Ploutus, en los últimos años ha sido ampliamente utilizado, orientado a cajeros NCR, tada vez que pudo incorporar el software “oficial” y gracias a ello el malware poder tener el control de los dispositivos hardware de los cajeros tales como el dispensador de dinero, el lector de tarjetas y otros sistemas operativos.

Malware

El malware, conocido también como badware, código maligno, software malicioso o software malintencionado, viene a ser un tipo de software cuya finalidad es dañar una computadora y la información que esta contiene sin la autorización del propietario. Es lo que en el lenguaje corriente se denomina virus, de manera incorrecta obviamente, para referirse a todos los tipos de malware, incluido los virus verdades; pues, hay que tener en cuenta que no todos los virus son malos.

En ese sentido se puede decir que la palabra malware es mucho más amplia que virus; pues, abarca los troyanos, virus, gusanos, los rootkits, scareware, spyware, adware intrusivo, crimeware y otros softwares maliciosos e indeseables

Según la información vertida por Symantec publicado en el 2008 sugieren que «el ritmo al que se ponen en circulación códigos maliciosos y otros programas no deseados podría haber superado al de las aplicaciones legítimas». De igual forma, Según un reporte de F-Secure, «Se produjo tanto malware en 2007 como en los 20 años anteriores juntos».

Según Panda Security, durante los 12 meses del 2011 se han creado 73.000 nuevos ejemplares de amenazas informáticas por día, 10.000 más de la media registrada en todo el año 2010. De éstas, el 73 por ciento son troyanos y crecen de forma exponencial los del subtipo downloaders.

Luego de haber descrito los antecedentes nacionales e internacionales, los aspectos teóricos con respecto a la ciberdelincuencia, los mecanismos de alteración de los dispensadores de dinero que ocurren en ATM, es preciso analizar la situación problemática en torno a los hechos ocurridos en el Perú. Pues, como se ha referido anteriormente, nuestro país ha sido víctima de este tipo de ataques cibernéticos concretizados en algunas entidades financieras. Razón por la cual, es pertinente hacer un bosquejo analítico a fin de concordar con los problemas planteados, objetivos de la investigación y los supuestos del trabajo que vienen a ser respuesta tentativa de lo que se pretende.

Fraude en los cajeros automáticos

Según, Domínguez (2013), el fraude en los cajeros automáticos se ha incrementado en número en estos últimos años. Por eso dice: “Generalmente, los delincuentes tratan de realizar estas prácticas en cajeros con gran afluencia de personas, en lugares cercanos donde

se celebran eventos o festivales o bien en cualquier cajero sobre fechas concretas de cobro. Por último, se encuentra otro tipo de fraude no tan sofisticado conocido como “trampa del efectivo” que se distingue por la utilización de mecanismos rudimentarios que se colocan en la boquilla dispensadora de billetes del cajero en cuestión con la finalidad de ocultar e impedir que salga el dinero de la víctima. Usualmente los delincuentes que llevan estos delitos a la práctica no son delincuentes cualesquiera, sino que son conocedores y expertos de la práctica, además suele llevarse a cabo entre grupos de delincuentes organizados.

Análisis de la investigación

Descripción del hecho

El 31 de octubre de 2018 el Banco GNB del Perú fue víctima de fraude informático a través de la infección de dos de sus cajeros automáticos, con un malware (Programa malicioso o maligno utilizado para acceder ilícitamente a un dispositivo) utilizando la modalidad de «jackpotting» accionar delictivo que ha originado la sustracción de S/. 591,920.00 Soles y US$.62,020.00 dólares. De igual forma en noviembre del 2018 el BBVA – Banco Continental, fue víctima de sustracción de S/. 4,000,000.00 millones de soles y S/.70, 000.00 soles.

Análisis secuencial del ataque a los cajeros automáticos

a. Primer paso: descarga del malware

Utilizando una Laptop, registrada como NB - SOP, tuvieron acceso al sitio web www.sendspace.com, desde donde fue descargado el directorio comprimido como: PERU.rar archivo que contenía los malwares denominados: OPERATOR.TXT y REQUEST.TXT. El acceso a internet para la descarga fue realizado a través de Wifi de dos teléfonos celulares registrados a nombre de dos trabajadores.

b. Segundo paso: envío de malware

Utilizando el usuario SSIS, enviaron el malware (support.exe, operator.dat y Request.dat) empaquetado (para evitar la detección del antivirus) al servidor SWITCH, los accesos fueron realizados desde la PC con dirección IP número 170.x.x.x. y con dirección IP N.º 170.x.x.x. **(Ver Imagen N.º 01)**

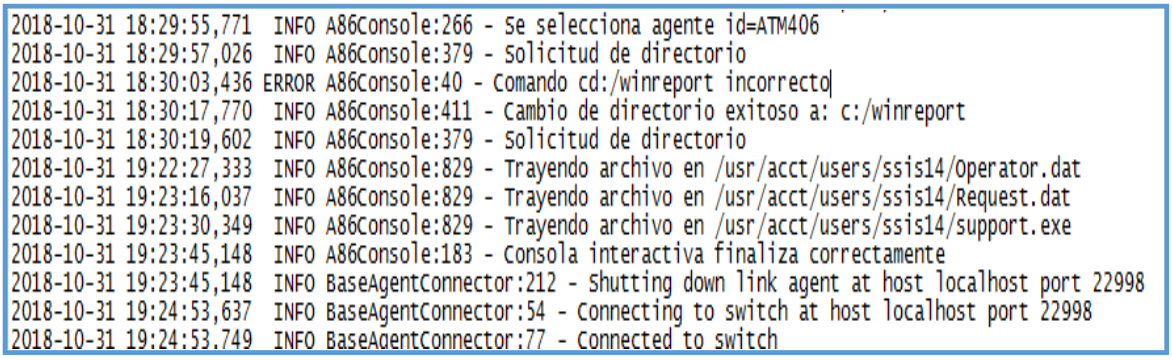


Imagen N.ª 01

c. Tercer paso: desempaquetado de malware

Luego de subir los archivos de malware (support.exe, operator.dat y Request.dat), al servidor SWITCH dichos archivos fueron desempaquetados y cambiados de nombre de support.txt a support.exe, acción que fue realizado a través del programa A86Console **(Ver Imagen Nº 02)**

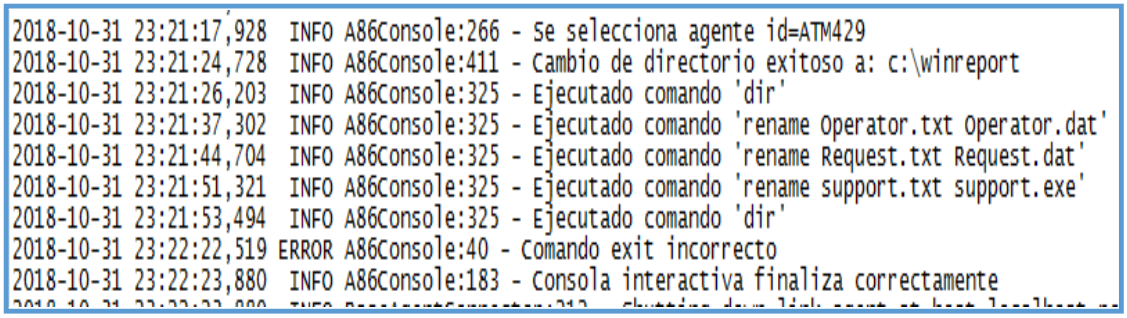


Imagen Nº 02

d. Cuarto paso: envió de ticket

El ticket generado fue subido al servidor SWITCH con la finalidad de forzar el reinicio del cajero automático y lograr el acceso con súper usuario **(Ver Imagen Nº 03)**

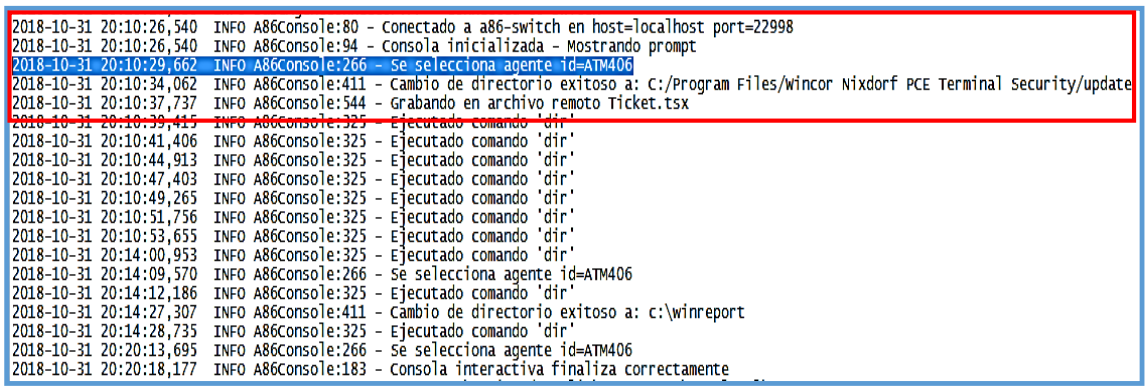
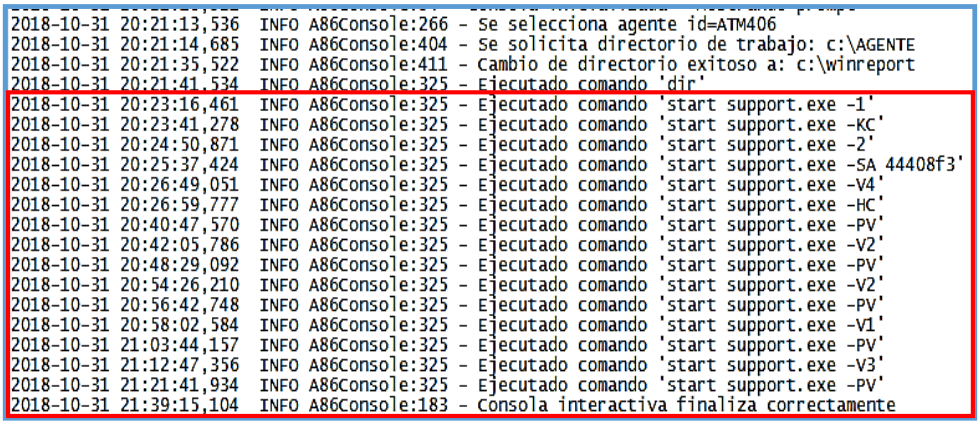


Imagen Nº 03

e. Quinto paso: ejecución del malware

Se ejecuta el malware (support.exe, operator.dat y Request.dat) dando la orden de dispensar el dinero de los cajeros automáticos. **(Ver Imagen Nº 04)**



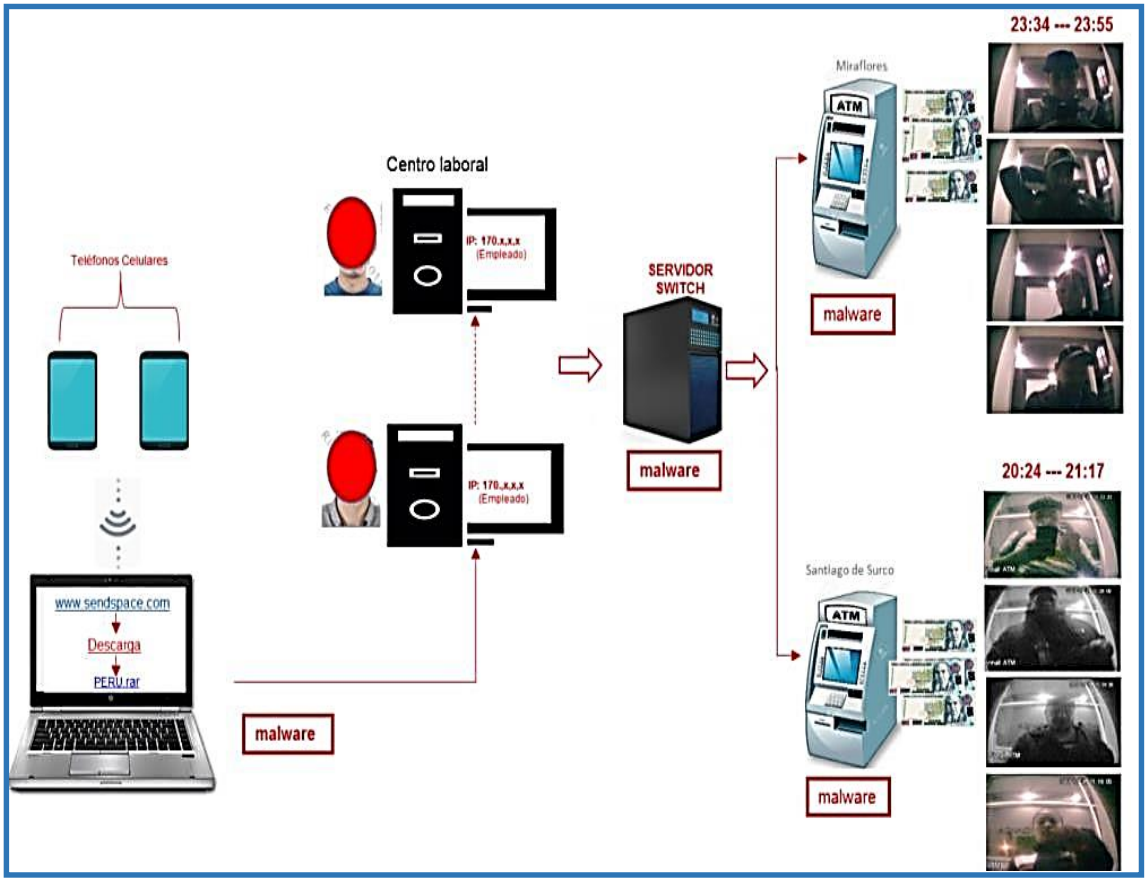
f. Sexto paso: eliminación del malware

Se da la orden de eliminar el malware (support.exe, operator.dat y Request.dat). **(Ver Imagen Nº 05)**

```
2018-10-31 21:39:15,104  INFO A86Console:183 - Consola interactiva finaliza correctamente
2018-10-31 21:39:15,105  INFO BaseAgentConnector:212 - Shutting down link agent at host localhost port 22998
2018-10-31 21:43:36,725  INFO BaseAgentConnector:54 - Connecting to switch at host localhost port 22998
2018-10-31 21:43:36,737  INFO BaseAgentConnector:77 - Connected to switch
2018-10-31 21:43:36,739  INFO A86Console:80 - Conectado a a86-switch en host=localhost port=22998
2018-10-31 21:43:36,739  INFO A86Console:94 - Consola inicializada - Mostrando prompt
2018-10-31 21:43:38,827  INFO A86Console:266 - Se selecciona agente id=ATM406
2018-10-31 21:43:40,788  INFO A86Console:404 - Se solicita directorio de trabajo: c:\winreport
2018-10-31 21:43:56,656  INFO A86Console:325 - Ejecutado comando 'del c:\winreport'
2018-10-31 21:43:59,878 ERROR A86Console:40 - Comando y incorrecto
2018-10-31 21:44:08,936  INFO A86Console:325 - Ejecutado comando 'del c:\winreport -y'
2018-10-31 21:44:14,393  INFO A86Console:404 - Se solicita directorio de trabajo: c:\winreport
2018-10-31 21:44:29,440  INFO A86Console:325 - Ejecutado comando 'dir'
2018-10-31 21:44:35,943  INFO A86Console:325 - Ejecutado comando 'del Request.dat'
2018-10-31 21:44:42,018  INFO A86Console:325 - Ejecutado comando 'del support.exe'
2018-10-31 21:44:43,560  INFO A86Console:325 - Ejecutado comando 'dir'
2018-10-31 21:44:50,938  INFO A86Console:325 - Ejecutado comando 'del support.exe'
2018-10-31 21:44:54,250  INFO A86Console:325 - Ejecutado comando 'dir'
2018-10-31 21:45:02,070  INFO A86Console:325 - Ejecutado comando 'delete support.exe'
2018-10-31 21:45:04,851  INFO A86Console:325 - Ejecutado comando 'dir'
2018-10-31 21:45:39,283  INFO A86Console:325 - Ejecutado comando 'taskkill \f \im support.exe'
2018-10-31 21:45:48,150  INFO A86Console:325 - Ejecutado comando 'delA support.exe'
2018-10-31 21:45:49,859  INFO A86Console:325 - Ejecutado comando 'dir'
2018-10-31 21:45:57,358  INFO A86Console:325 - Ejecutado comando 'stop support.exe'
2018-10-31 21:46:03,282  INFO A86Console:325 - Ejecutado comando 'del support.exe'
2018-10-31 21:46:05,454  INFO A86Console:325 - Ejecutado comando 'dir'
2018-10-31 21:46:27,744  INFO A86Console:325 - Ejecutado comando 'start support.exe -KC'
2018-10-31 21:46:35,468  INFO A86Console:325 - Ejecutado comando 'del support.exe'
2018-10-31 21:46:37,193  INFO A86Console:325 - Ejecutado comando 'dir'
2018-10-31 21:46:40,171  INFO A86Console:183 - Consola interactiva finaliza correctamente
```

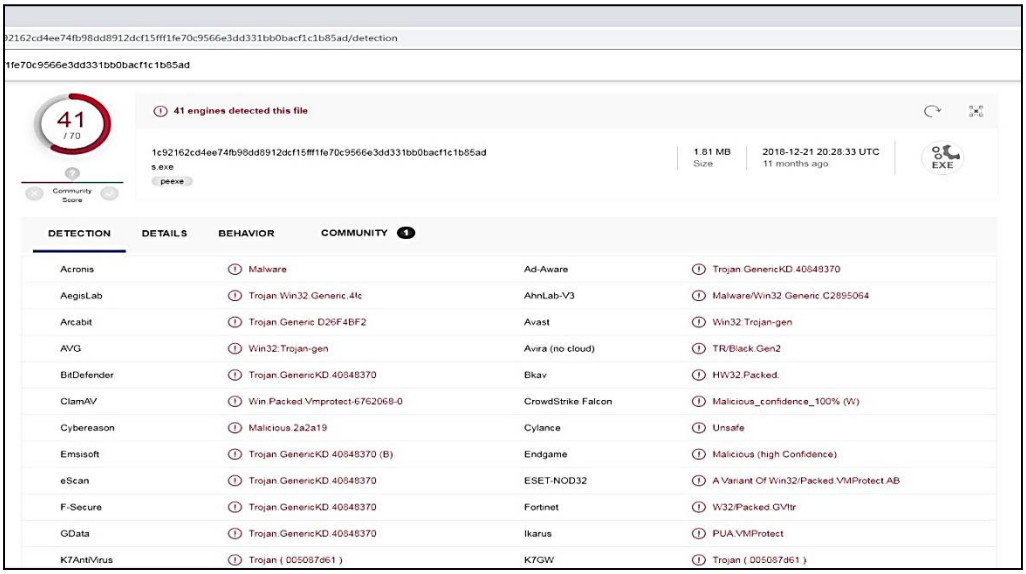
Imagen N°05

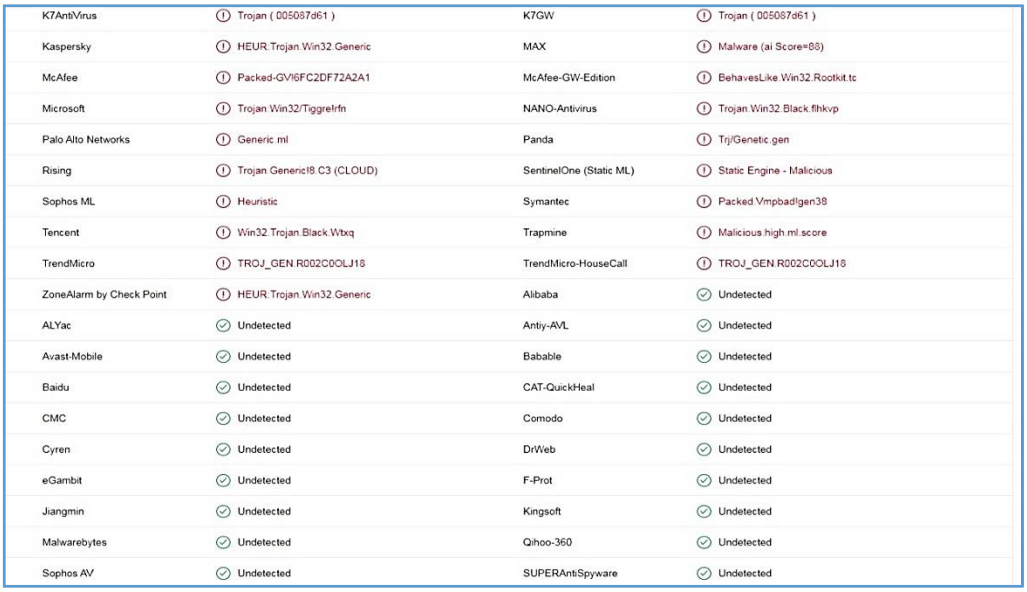
g. Diagrama

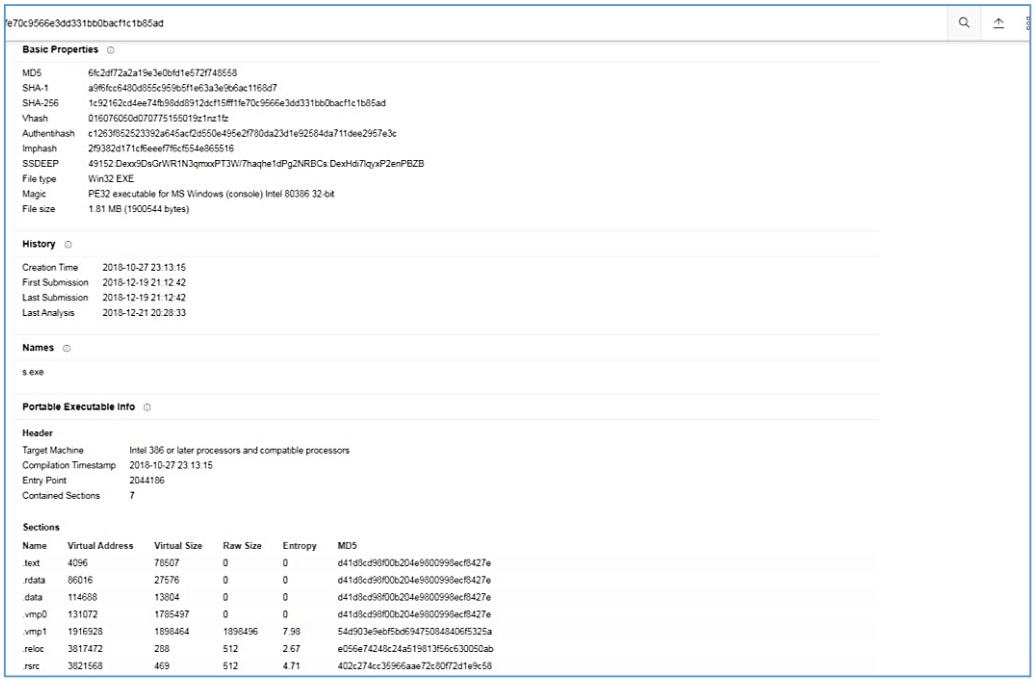


Análisis del malware

El Malware, fue creado el 27 de octubre del 2018; 41 de 70 antivirus lo identifican, información obtenida utilizando la herramienta informática denominada virus total.







fe70c9566e3dd331bb0bacf1c1b85ad

Basic Properties

MD5	6fc2df72a2a19e3e0bfd1e572f748558
SHA-1	a9f6fcc6480d855c969b5f1e63a3e9b6ac1168d7
SHA-256	1c92162cd4ee74fb98dd8912dcf15fff1fe70c9566e3dd331bb0bacf1c1b85ad
Vhash	016076050d07077515501 9z1nz1fz
Authentihash	c1263f652523392a645acf2d550e495e2f780da23d1e92584da711dee2957e3c
Imphash	2f9382d171cf6eeef7f6cf554a865516
SSDEEP	49152:Dexx9DsGrWR1N3qmxxPT3W/7haqhe1dPg2NRBCs:DexHdi7lqyxP2enPBZB
File type	Win32 EXE
Magic	PE32 executable for MS Windows (console) Intel 80386 32-bit
File size	1.81 MB (1900544 bytes)

History

Creation Time	2018-10-27 23:13:15
First Submission	2018-12-19 21:12:42
Last Submission	2018-12-19 21:12:42
Last Analysis	2018-12-21 20:28:33

Names

s.exe

Portable Executable Info

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2018-10-27 23:13:15
Entry Point	2044186
Contained Sections	7

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	78507	0	0	d41d8cd98f00b204e9800998ecf8427e
.rdata	86016	27576	0	0	d41d8cd98f00b204e9800998ecf8427e
.data	114688	13804	0	0	d41d8cd98f00b204e9800998ecf8427e
.vmp0	131072	1785497	0	0	d41d8cd98f00b204e9800998ecf8427e
.vmp1	1916928	1898464	1898496	7.98	54d903e9ebf5bd6947508484061f5325a
.reloc	3817472	288	512	2.67	e056e74248c24a519613f56c630050ab
.rsrc	3821568	469	512	4.71	402c274cc35966aae72c80f72d1e9c58

Comportamiento y cambios realizados en el sistema

Al respecto cabe indicar que para concretar su cometido los dilencuentes utilizaron un iter correlacionado, cerrando el circulo para no ser detectados. De ello existe todo un registro recabado a través de uso de intrumentos sistemáticos y antivirus detectores. (Ver Anexo 5)

CAPÍTULO III: DESARROLLO DE ACTIVIDADES PROGRAMADAS

Es pertinente poner en conocimiento que esta investigación se ha realizado en estricto cumplimiento de las disposiciones establecidas por la Universidad Peruana de Ciencias e Informática, este trabajo de suficiencia se ha realizado en un orden cronológico y metódico. En ese sentido cabe indicar los siguientes aspectos:

PRIMERO: Al estar matriculado en el curso de tesis, por la premura del tiempo y las exigencias propias de UPCI, bajo la dirección y supervisión del docente del curso, se procedió a buscar el tema de investigación; esta fue la etapa inicial del trabajo que no fue nada sencillo, hasta que llegado el momento de tomar una decisión sobre el tema a investigar se optó por estudiar el tema del tratamiento jurídico de la evidencia digital como medio probatorio en la investigación del delito informático en la modalidad de vulneración de cajeros automáticos en Lima.

SEGUNDO: Como siguiente paso de la investigación consistió en buscar información documental y jurisprudencial sobre el tema elegido, a nivel nacional e internacional; además de ello, tratándose de un tema sumamente complejo que amerita la intervención de peritos en la materia, previamente se tuvo que recabar la información ocurrido *in situ*, es decir, bajo la constitución al lugar de los hechos, ello evidentemente implica no solamente un costo monetario sino también un desgaste físico e intelectual.

TERCERO: El siguiente paso consistió en revisar el tema de fondo de la investigación con respecto al tema elegido. Para ello fue necesario recurrir a la revisión normativa vigente en relación con los delitos informáticos, ciberdelitos, los mecanismos de control adoptados por países europeos y latinoamericanos. Además de ello fue necesario conocer los mecanismos a través de los cuales los delincuentes cibernéticos llegan a concretizar su cometido, los

mecanismos de seguridad que tienen los cajeros automáticos, pero también vulnerables, pues, de lo contrario no se cometerían los delitos descritos en el contenido de este trabajo, toda vez que los ilícitos penales relacionados a este tipo de hechos en los últimos años se han incrementado exponencialmente no solo en el Perú sino también en otras partes del mundo. Ello amerita un estudio más profundo, creación de nuevos mecanismos de control y la creación de aparatos sofisticados que puedan ser capaces de bloquear cualquier tipo de ataque cibernético.

CAPÍTULO IV: RESULTADOS OBTENIDOS

A modo de síntesis y de aporte es necesario exponer los resultados alcanzados con esta investigación tanto a nivel teórico como práctico en los términos que se exponen a continuación.

PRIMERO: En relación al objetivo general de la investigación "Conocer la menara en que el **tratamiento de la evidencia digital** como medio probatorio se relaciona con la investigación del delito informático en la modalidad de vulneración de Cajeros Automáticos, Lima 2019", se obtuvo que existe una relación superficial toda vez que su consideración en el proceso penal no es tomado en cuenta en su cabalidad. Ello responde a diversos factores tales como, por un lado, el desconocimiento normativo de los operadores de Derecho en el ámbito de los delitos informáticos y, por otro, poca especialización en la materia por los responsabilidad de la persecución del delito como son los integrantes del Ministerio Público, Policía Nacional del Perú que no cuenta con los instrumentos científicos y tecnológicos de última generación como sí existe en otros países europeos a fin de contrarrestar la delincuencia cibernética. Ello está sustentado por lo manifestado por Lasso (2017), cuando afirma que el peritaje informático es una actividad de investigación que ha tomado fuerza a nivel internacional debido a la relevancia que tiene dentro de los procesos judiciales donde interviene la evidencia digital, a raíz del aumento de los 89 ciberdelitos, pues permite esclarecer los hechos ocurridos en un caso específico, brindando las herramientas para dirimir y lograr la impartición de la justicia de manera adecuada. (p.88-89). En ese sentido, se confirma el supuesto de que el tratamiento de la evidencia digital como medio probatorio se relaciona de manera superficial con la investigación del delito informático en la modalidad de vulneración de Cajeros Automáticos, Lima 2019.

SEGUNDO: Que, en relación al primer objetivo específico que dice "describir la manera en que la **identificación de la evidencia digital** como medio probatorio incide en la determinación del delito informático en la modalidad de vulneración de Cajeros Automáticos, se obtuvo que existen falencias en la identificación de la evidencia digital toda vez que existe la contaminación de dichas evidencias que posteriormente no favorecen una investigación acertada; pues, si el inicio de un proceso está contaminado, por ende, el resultado no será tan favorable. Aunado a ello, se obtuvo que la identificación de la evidencia se hace aún más compleja toda vez que existe la participación de algún agente o colaborador de una entidad financiera; pues, como se ha podido determinar en la descripción del *iter criminis*, hay datos que solamente puede proporcionar alguien que tiene la información de primera mano. En consecuencia, lo establecido en el supuesto de esta investigación se confirma toda vez que la evidencia digital como medio probatorio incide de manera negativa en la determinación del delito informático en la modalidad de vulneración de Cajeros Automáticos.

TERCERO: Que, en relación al segundo objetivo específico de la investigación que consiste en determinar la manera en que la **preservación de la evidencia digital** como medio probatorio repercute en la determinación del delito informático en la modalidad de vulneración de Cajeros Automáticos, se obtuvo que existen falencias al respecto toda vez que en el proceso de análisis de los hechos intervienen elementos externos que alteran la originalidad de las evidencias; pues, como se ha visto, los delitos informáticos son altamente procesados y con un pequeño trastoque de la información se podría alterar todo. Por ello, luego de identificar la evidencia, es muy necesaria la conservación de la misma en su sentido original a fin de que en una eventual incorporación en el juicio pueda ser valorado y sirva como medio para generar convicción en el juez que tiene la responsabilidad de administrar justicia de acuerdo a los hechos. En ese sentido, se confirma el supuesto planteado de que la

preservación de la evidencia digital como medio probatorio repercute superficialmente en la determinación del delito informático en la modalidad de vulneración de Cajeros Automáticos, en ese sentido se debe tener mayor cuidado y diligencia en la conservación de la fuente original de información.

CUARTO: En relación al tercer objetivo del trabajo de investigación que establece conocer la forma en que la **inmediación de la evidencia digital** como medio probatorio se relaciona en la determinación del delito informático en la modalidad de vulneración de Cajeros Automáticos, se obtuvo que existe una relación superficial. Pues, como se ha podido determinar, la inmediación es uno de los principios en los que se asienta el Nuevo Código Procesal Penal de 2004; es la etapa en la cual se da la actuación de los medios probatorios en presencia del juez que dirige la audiencia de juicio oral. Pues, en esta esta fase del proceso sucede que muchas veces resulta sumamente complicada demostrar tecnológica y científicamente los hechos ocurridos de manera fehaciente. Por esa razón, les resulta complicada a los actores del Ministerio Público y la Policía Nacional del Perú formular una acusación a los ciberdelincuentes porque casi no hay forma de determinar la autoría de dichos ilícitos por más que se pueda determinar el *iter criminis*; muestra de ello es que las entidades que sufrieron ese tipo de ataques prácticamente son conscientes que han sufrido pérdidas millonarias y no les queda otra cosa que tomar las precauciones del caso para el futuro. En ese sentido, lo establecido en el supuesto de la investigación se confirma, toda vez que la inmediación de la evidencia digital como medio probatorio se relaciona de manera superficial en la determinación del delito informático en la modalidad de vulneración de Cajeros Automáticos.

CONCLUSIONES

1. Luego del proceso de investigación, en relación con el primer objetivo, se ha podido determinar que el tratamiento de la evidencia digital en el Perú como medio probatorio en los delitos informáticos es muy superficial. Muestra de ello es que se ve un incremento cuantitativo de la contravención normativa en referencia de la protección de los datos de personas jurídicas como son las entidades financieras. Además, se ha podido determinar que los delitos cibernéticos no tienen fronteras y es grandemente perjudicial no solamente para las entidades financieras, sino incluso para los Estados, razón por la cual es de necesidad imperiosa la creación de mecanismos de control frente a un eventual ataque que se pueda suscitar.

2. Se ha podido determinar que es sumamente complejo la identificación de la evidencia digital toda vez que los cometen este tipo de ilícitos son altamente especializados que hacen las operación a larga distancia, toda vez que los registros de dichos ataques informáticos a los cajeros automáticos ATM se encuentran almacenados en el Servidor SWITCH, siendo ello materia principal de análisis en esta modalidad delictiva.

3. Además, se ha podido determinar que la conservación de la evidencia digital resulta sumamente complicada toda vez que no existen instrumentos especializados para dicho fin. Si bien existe un Manual de recojo de evidencia de digital, muy poco se aplica según se ha podido determinar en el transcurso de la investigación.

RECOMENDACIONES

1. Se recomienda mayor capacitación al personal policial que investiga los delitos informáticos en todas sus dimensiones, toda vez que el avance de la tecnología genera también nuevas modalidades delictivas. Ello implica el incremento de presupuesto teniendo en consideración que los delitos cibernéticos se cometen con el auxilio de instrumentos tecnológicos muy sofisticados.

2. Se recomienda a las instituciones encargadas de la investigación y persecución del delito que trabajen de manera conjunta, concatenada, a fin de realizar un trabajo más eficiente y eficaz; pues, una investigación que se prolonga por más allá de los plazos permitidos por ley únicamente aleja la impartición de justicia evidenciándose la impunidad para los que cometen el ilícito penal en relación a la vulneración de cajeros automáticos.

3. Finalmente, se recomienda que el personal policial a cargo de la identificación, preservación y la inmediación de la evidencia digital debe gozar de mayor preparación científica, con cursos de especialización a nivel nacional e internacional; de tal manera que puedan determinar con mayor facilidad la autoría de los ilícitos cometidos, en los que necesariamente existe la participación de los colaboradores de la entidad financiera para quienes deben considerarse diversas pruebas a nivel intrínseco y extrínseco.

REFERENCIAS BIBLIOGRÁFICAS

Escobar, L. (2017). *Manejo de la cadena de custodia en la recolección de evidencia digital* (Tesis de grado), Universidad Rafael Landívar, Guatemala. Recuperado de http://recursosbiblio.url.edu.gt/tesisjcem/2017/07/03/Escobar-Luis.pdf

Carrasco, S. (2013). *Metodología de la investigación científica. Pautas metodológicas para diseñar y elaborar el proyecto de investigación*. Lima: San Marcos.

Domínguez, I. (2013). *Fraude en cajeros automáticos, consejos de seguridad* (blog). Recuperado de https://delitosinformaticos.com/06/2013/fraudes/fraude-en-cajeros-automaticos-consejos-de-seguridad

Hernández Sampieri, R., Fernández, C. y Baptista, P. (2010). *Metodología de la Investigación* (5ª ed.). México: McGraw-Hill.

Jiménez, J. (2018). *Desarrollo de una aplicación de uso didáctico para comunicación segura de datos a través de la red* (Tesis de grado), Escuela Politécnica Nacional de Quito, Ecuador. Recuperado de https://bibdigital.epn.edu.ec/handle/15000/19319

Justo, M. (2017). *Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal.* (Proyecto financiado por Ford Foundation). Recuperado de https://bit.ly/2RumV9F.

Lasso, V. (2017). *Estado del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia.* (Trabajo monográfico). https://repository.unad.edu.co/handle/10596/17473

Mc Cabe, J. D. (2003). *Network Analysis, Architecture and Design USA*: Morgan Kaufmann Series in Networking

Nessi, A. (2017). *Manuel de Evidencia Digital.* Recuperado de https://www.mpfn.gob.pe/Docs/0/files/manual_evidencia_digital.pdf

Ramírez, D. y Castro, E. (2018). *Análisis de la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia* (Investigación de grado), Universidad Nacional Abierta y a Distancia "UNAD", Villavicencio, Colombia. Recuperado de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17370/1/86078250.pdf

Ramos, C. (2011). *Cómo hacer una tesis de derecho y no envejecer en el intento*. Lima: Grijley & Iustitia S.A.C.

Rodríguez, F. (2000). *La investigación jurídica básica y la investigación jurídica aplicada*. Revista Justicia de la Universidad Simón Bolívar, Barranquilla, Colombia, 56.

Sequeiros, I. (2015). *Vacíos legales que imposibilitan la sanción de los delitos informáticos en el Nuevo Código Penal Peruano-2015.* (Tesis para optar el Título profesional de Abogado (Universidad de Huánuco). Recuperado de https://bit.ly/2Fa4Kjy.

Sergi, N. (2018). *Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina*. Recuperado de https://adcdigital.org.ar/portfolio/analisis-juridico-de-la-situacion-de-la-evidencia-digital-en-el-proceso-penal-en-argentina/

Valderrama, S. (2007). *Pasos para elaborar proyectos y tesis de Investigación Científica*. Lima: San Marcos.

Vilca, G. (2018). *Los hackers: delito informático frente al Código Penal Peruano* (Tesis de pregrado), Universidad Nacional Santiago Antúnez de Mayolo, Huaraz. Recuperado de http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2496/T033_47272593_T.pdf?sequence=1&isAllowed=y

Yuni, J. y Urbano, C. (2006). *Técnicas para investigar: recursos metodológicos para la* ***preparación de proyectos de investigación*** **(2ª ed.). Córdova, Argentina: Brujas.**

ANEXOS

Anexo 1. Evidencia de similitud digital

TSP EL TRATAMIENTO DE LA EVIDENCIA DIGITAL COMO MEDIO PROBATORIO EN LA INVESTIGACIÓN DEL DELITO INFORMÁTICO EN LA MODALIDAD DE VULNERACIÓN DE CAJEROS AUTOMÁTICOS, LIMA 2019.

Fecha de entrega: 09-nov-2021 0 8:34 a.m (U.T.C-0500)

Por : ZOSIMO HUAMAN RAMOS - OLIVERA BARRIENTOS CARLOS FRANZ .

Identificador de la entrega: 1697732814

Nombre del archivo:
MODALIDAD_DE_VULNERACI_N_DE_CAJEROS_AUTOM_TICOS,_LIMA_2019.docx (3.06M)

Total de palabras: 10546

Total de caracteres: 60933

TSP EL TRATAMIENTO DE LA EVIDENCIA DIGITAL COMO MEDIO PROBATORIO EN LA INVESTIGACIÓN DEL DELITO INFORMÁTICO EN LA MODALIDAD DE VULNERACIÓN DE CAJEROS AUTOMÁTICOS, LIMA 2019

INFORME DE ORIGINALIDAD

20%	20%	0%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

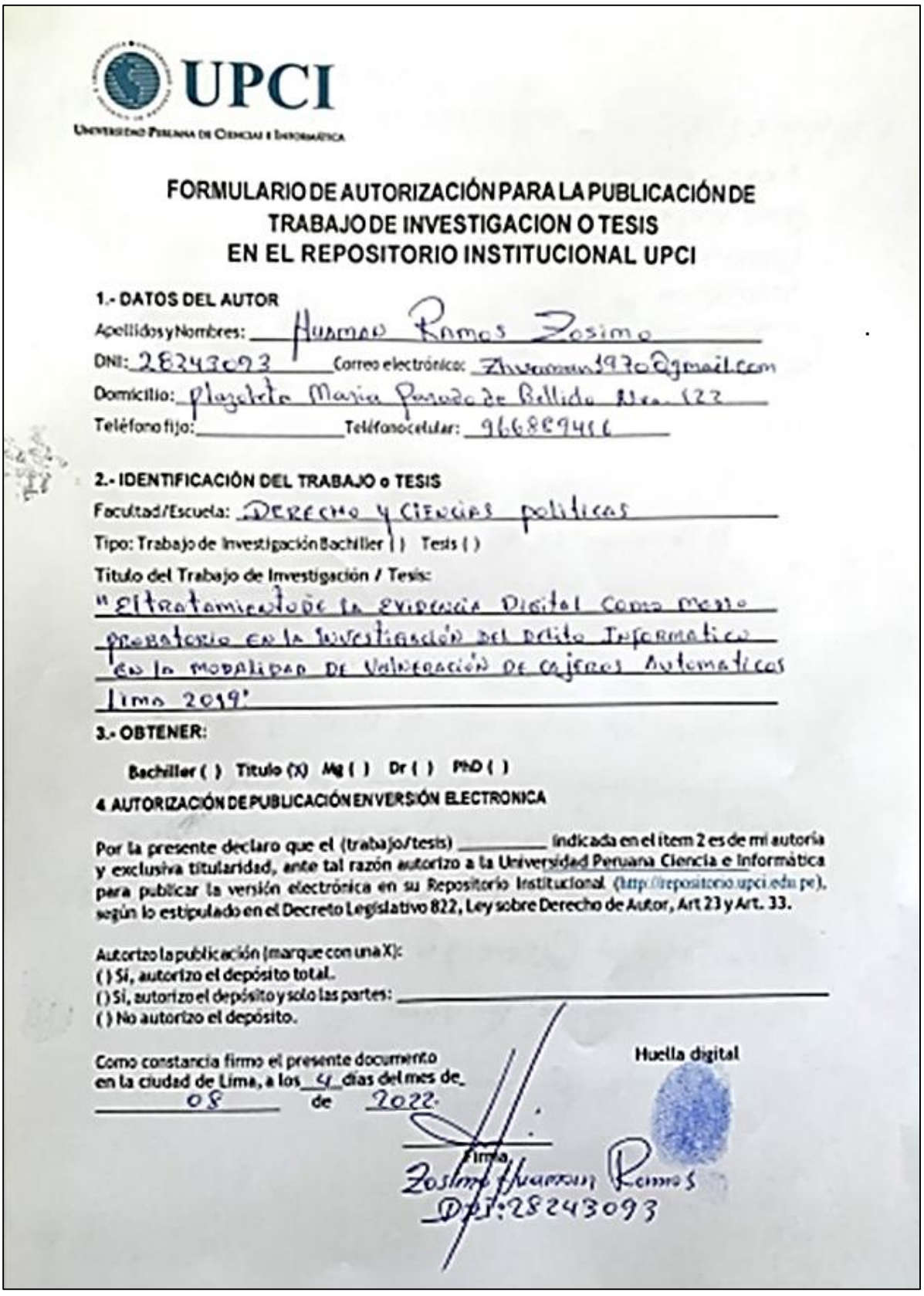
FUENTES PRIMARIAS

1	repositorio.ucv.edu.pe Fuente de Internet	10%
2	gestion.pe Fuente de Internet	1%
3	delitosinformaticos.com Fuente de Internet	1%
4	www.mpfn.gob.pe Fuente de Internet	1%
5	cualquiervaina.com Fuente de Internet	1%
6	jhonmelendezmelendez.blogspot.com Fuente de Internet	1%
7	repositorio.upci.edu.pe Fuente de Internet	1%
8	www.ictea.com Fuente de Internet	1%

9	repository.unad.edu.co Fuente de Internet	1 %
10	www.securitybydefault.com Fuente de Internet	1 %
11	adc.org.ar Fuente de Internet	<1 %
12	moam.info Fuente de Internet	<1 %
13	qdoc.tips Fuente de Internet	<1 %
14	www.coursehero.com Fuente de Internet	<1 %
15	recursosbiblio.url.edu.gt Fuente de Internet	<1 %
16	www.seguridadidl.org.pe Fuente de Internet	<1 %

Excluir citas	Activo	Excluir coincidencias	< 20 words
Excluir bibliografía	Activo		

Anexo 2. Autorización de publicación en repositorio



UPCI

Universidad Peruana de Ciencias e Informática

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACION O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: Huaman Ramos Zosimo

DNI: 28243093 Correo electrónico: Zhuaman1970@gmail.com

Domicilio: Elizabeth María Penado de Bellido Mza. 122

Teléfono fijo: _____ Teléfono celular: 966889416

2.- IDENTIFICACIÓN DEL TRABAJO o TESIS

Facultad/Escuela: Derecho y Ciencias políticas

Tipo: Trabajo de Investigación Bachiller ( ) Tesis ( )

Titulo del Trabajo de Investigación / Tesis:

"El tratamiento de la evidencia Digital como medio probatorio en la investigación del delito Informatico en la modalidad de Valoración de Cajeros Automaticos Lima 2019"

3.- OBTENER:

Bachiller ( ) Titulo (X) Mg ( ) Dr ( ) PhD ( )

4 AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRONICA

Por la presente declaro que el (trabajo/tesis) _____ indicada en el item 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencia e Informática para publicar la versión electrónica en su Repositorio Institucional (http://repositorio.upci.edu.pe), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art 23 y Art. 33.

Autorizo la publicación (marque con una X):
( ) Si, autorizo el depósito total.
( ) Si, autorizo el depósito y solo las partes: _____
( ) No autorizo el depósito.

Como constancia firmo el presente documento en la ciudad de Lima, a los 4 días del mes de 08 de 2022.

Huella digital

Firma
Zosimo Huaman Ramos
DNI: 28243093

UPCI

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACION O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: Olivera Barrientos Carlos Franz

DNI: 20074006 Correo electrónico: carfra-o@yahoo.com

Domicilio: Psj. Encinas 350 Siglo XX - El Tambo - Hyo

Teléfono fijo: 064-204576 Teléfono celular: 954956423

2.- IDENTIFICACIÓN DEL TRABAJO o TESIS

Facultad/Escuela: Derecho y Ciencias Políticas

Tipo: Trabajo de Investigación Bachiller ( ) Tesis ( )

Título del Trabajo de Investigación / Tesis:

"El Tratamiento de la Evidencia Digital como medio probatorio en la investigación del delito informático en la modalidad de Vulneración de cajeros automáticos Lima 2019"

3.- OBTENER:

Bachiller ( ) Título (X) Mg ( ) Dr ( ) PhD ( )

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRONICA

Por la presente declaro que el (trabajo/tesis) _____ indicada en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencia e Informática para publicar la versión electrónica en su Repositorio Institucional (http://repositorio.upci.edu.pe), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art 23 y Art. 33.

Autorizo la publicación (marque con una X):

(X) Sí, autorizo el depósito total.

( ) Sí, autorizo el depósito y solo las partes: _____

( ) No autorizo el depósito.

Como constancia firmo el presente documento en la ciudad de Lima, a los 04 días del mes de agosto de 2022

Huella digital

Firma

CARLOS OLIVERA BARRIENTOS

DNI 20074006

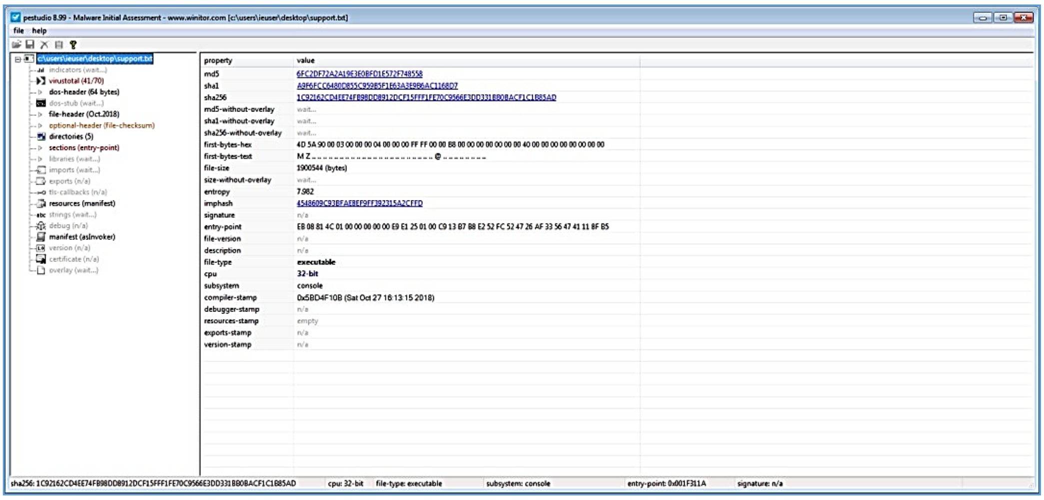
Anexo 3: Otras evidencias

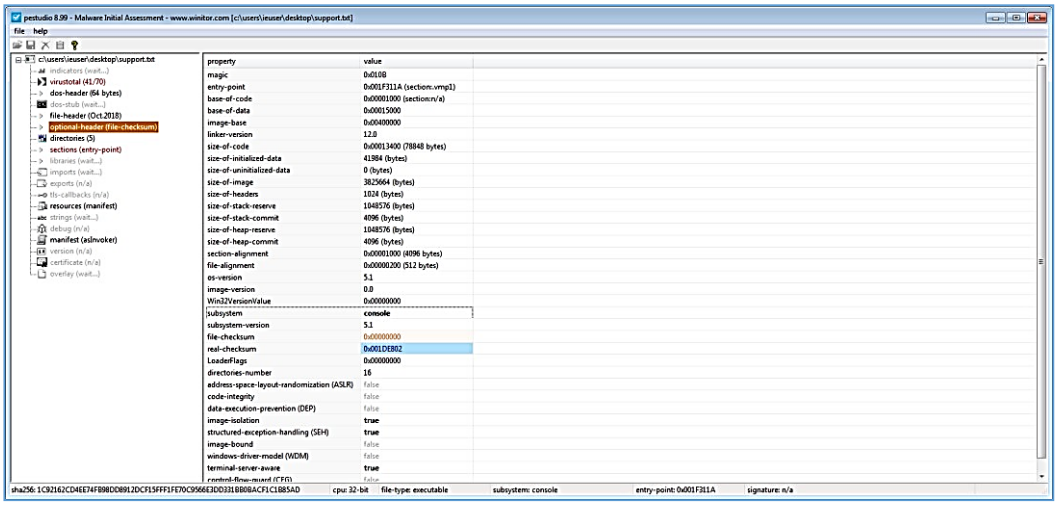
COMPORTAMIENTO Y CAMBIOS REALIZADOS EN EL SISTEMA

```
----------------------------------
Keys added: 12
----------------------------------
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hiv
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hiv
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hiv\OpenWithList
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.hiv
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\23\ComDlg
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\23\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\23\ComDlg
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\23\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}

----------------------------------
Values added: 53
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\PerfTrack\ScenarioOccurrences\86\OccurrencesLessThanOrEqualTo100ScaledTPI: 0x00000001
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\PerfTrack\ScenarioOccurrences\87\OccurrencesLessThanOrEqualTo50ScaledTPI: 0x00000001
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\CIDSizeMRU\3:  52 00 65 00 67 00 73 00 68 00 6F 00 74 00 2D 00 78 00 38 00 36 00 2D 00 4
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU\3:  52 00 65 00 67 00 73 00 68 00 6F 00 74 00 2D 00 78 00 38 00 36 00
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\*\4:  4A 00 31 00 00 00 00 00 7B 4F 82 86 10 00 73 73 73 73 00 00 36 00
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hiv\0:  4A 00 31 00 00 00 00 00 7B 4F 82 86 10 00 73 73 73 73 00 00 36 0
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hiv\MRUListEx:  00 00 00 00 FF FF FF FF
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\12:  68 00 6F 00 73 00 74 00 62 00 75 00 65 00 6E 00 6F 00 2E 00 68 00 69 00 76 00 00
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\13:  73 00 73 00 73 00 73 00 00 00 56 00 32 00 00 00 00 00 00 00 00 00 00 00 73 73 73
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder\5:  73 00 73 00 73 00 73 00 00 00 56 00 32 00 00 00 00 00 00 00 00 00 00 00 73
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.hiv\0:  68 00 6F 00 73 00 74 00 62 00 75 00 65 00 6E 00 6F 00 2E 00 68 00 69 00 76 00
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.hiv\MRUListEx:  00 00 00 00 FF FF FF FF
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\VRHfre\Qrfxgbc\fhccbeg.rkr:  00
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Mode: 0x00000004
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\LogicalViewMode: 0x00000001
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\FFlags: 0x00000001
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\IconSize: 0x00000010
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\ColInfo:  00 00 00 00 00 00 0
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Sort:  00 00 00 00 00 00 00 0
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupView: 0x00000000
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByKey:FMTID: "{00000000-
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByKey:PID: 0x00000000
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\13\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByDirection: 0x00000001
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\23\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Mode: 0x00000004
HKU\S-1-5-21-3583694148-1414552638-2922671848-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\23\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\LogicalViewMode: 0x00000001
```

```
----------------------------------
Values modified: 17
----------------------------------
HKLM\SOFTWARE\Microsoft\.NETFramework\v2.0.50727\NGENService\State\AccumulatedWaitIdleTime: 0x001339E0
HKLM\SOFTWARE\Microsoft\.NETFramework\v2.0.50727\NGENService\State\AccumulatedWaitIdleTime: 0x00258960
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\PerfTrack\ScenarioOccurrences\86\TotalOccurrences: 0x00000001
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\PerfTrack\ScenarioOccurrences\86\TotalOccurrences: 0x00000002
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\PerfTrack\ScenarioOccurrences\86\AverageScaledTpi: 0x000000AF
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\PerfTrack\ScenarioOccurrences\86\AverageScaledTpi: 0x00000071
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\PerfTrack\ScenarioOccurrences\87\TotalOccurrences: 0x00000001
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\PerfTrack\ScenarioOccurrences\87\TotalOccurrences: 0x00000002
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\PerfTrack\ScenarioOccurrences\87\AverageScaledTpi: 0x0000006D
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\PerfTrack\ScenarioOccurrences\87\AverageScaledTpi: 0x0000004C
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009\Counter:  31 00 31 38 34 37 00 32 00 53 79 73 74 65 6D 00 34 00 4D 65 6D 6F 72 79 00 36 00 25 20 50 72 6F 63 65 73 73 6F 72 20 54 69 6D 65 00 31 30 00 46 69


----------------------------------
Total changes: 82
----------------------------------
```

REGISTRO SEGÚN ESTUDIO





LÓGICA DE PROGRAMACIÓN EMPLEADA

{

"scan_result_history_length": 154,

"file_id": "ZTE3MDgyMkh5UmZGTl94cV9a",

"data_id": "ZTE3MDgyMkh5UmZGTl94cV9aUzFsSWU3aGtVNA",

"process_info": {

"result": "Blocked",

"profile": "Sanitize",

"post_processing": {

"copy_move_destination": "",

"converted_to": "",

"converted_destination": "",

"actions_ran": "",
"actions_failed": ""
},
"file_type_skipped_scan": **false**,
"blocked_reason": "Infected"
},
"scan_results": {
"scan_details": {
"Zillya!": {
"threat_found": "Adware.GenericKD.Win32.5471",
"scan_time": 26,
"scan_result_i": 1,
"def_time": "2019-02-26T17:27:00.000Z"
},
...
"Vir.IT ML": {
"threat_found": "",
"scan_time": 2275,
"scan_result_i": 0,
"def_time": "2019-02-22T14:46:00.000Z"
}
},
"rescan_available": **true**,
"scan_all_result_i": 1,
"start_time": "2019-02-26T21:53:32.770Z",
"total_time": 11206,
"total_avs": 37,
"total_detected_avs": 15,
"progress_percentage": 100,
"scan_all_result_a": "Infected"
},
"file_info": {
"file_size": 765024,
"upload_timestamp": "2017-09-05T18:30:04.000Z",

"md5": "6A5C19D9FFE8804586E8F4C0DFCC66DE",
"sha1": "016CD548A5BA78015F85E2591BF6189658ACA066",
"sha256":
"BE41E36233DD8DB2B28A109E7FC7C409E1353BF2D1710158BBE267280E
163353",
"file_type_category": "E",
"file_type_description": "Executable File",
"file_type_extension": "exe",
"display_name": "CleanupConsole.exe"
},
"share_file": 1,
"rest_version": "4",
"additional_info": [],
"votes": {
"up": 0,
"down": 0
}
}

EXAMPLE OF A SUCCESSFUL REQUEST FOR AN ARCHIVE:

{
"scan_result_history_length": 5,
"file_id": "YTE3MDgwMlNKd1pQcmRmSlBX",
"data_id": "YTE3MDgwMlNKd1pQcmRmSlBXcmtrZDdlTlVfNlE",
"process_info": {
"result": "Blocked",
"profile": "File scan",
"post_processing": {
"copy_move_destination": "",
"converted_to": "",
"converted_destination": "",
"actions_ran": "",

```
"actions_failed": ""
},
"file_type_skipped_scan": false,
"blocked_reason": "Infected"
},
"extracted_files": {
"data_id": "YTE3MDgwMlNKd1pQcmRmSlBXcmtrZDdlTlVfNlE",
"files_in_archive": [
{
"scan_result_i": 15,
"progress_percentage": 100,
"file_type": "application/encrypted",
"file_size": 14336,
"display_name": "test_protected.xlsx",
"detected_by": 0,
"data_id":
"WVRFM01EZ3dNbE5LZDFwUWNtUm1TbEJYcnlYdWxWVXVUbQ"
},
{
"scan_result_i": 15,
"progress_percentage": 100,
"file_type": "application/msword",
"file_size": 22528,
"display_name": "test_protected.doc",
"detected_by": 0,
"data_id":
"WVRFM01EZ3dNbE5LZDFwUWNtUm1TbEJYckpIX3hWVU82bQ"
}
]
},
"scan_results": {
"scan_details": {
"TrendMicro House Call": {
"threat_found": "",
```

"scan_time": 975,
"scan_result_i": 0,
"def_time": "2018-11-11T02:00:00.000Z"
},
...
"Vir.IT ML": {
"threat_found": "",
"scan_time": 5,
"scan_result_i": 0,
"def_time": "2018-11-09T14:46:00.000Z"
}
},
"rescan_available": **true**,
"scan_all_result_i": 1,
"start_time": "2018-11-13T13:38:52.680Z",
"total_time": 7001,
"total_avs": 35,
"total_detected_avs": 0,
"progress_percentage": 100,
"scan_all_result_a": "Infected"
},
"file_info": {
"file_size": 1286700,
"upload_timestamp": "2018-03-21T16:47:30.000Z",
"md5": "EF4A5B9ECC9D2E3380D035F71C00AFA1",
"sha1": "972695E77E75307EC38B2F089EDBE129C29FF870",
"sha256":
"0C4161B19D8CE5B2721AA0AF2CDDE5F121DDAB81004DB3B7FF243D74
CFFD3EA4",
"file_type_category": "",
"file_type_description": "ZIP Archive",
"display_name": "archive.zip"
},
"share_file": 1,

"rest_version":
"4",
"additional_inf
o": [], "votes":
{
"up": 0,
"down": 0
}
}

EJECUCIÓNDEL MALWAR