UNIVERSIDAD NACIONAL SANTIAGO ANTUNEZ DE MAYOLO

ESCUELA DE POSTGRADO

"APLICACIÓN DE METODOLOGÍAS Y HERRAMIENTAS DE LA INFORMÁTICA FORENSE PARA REDUCIR EL RIESGO DE LA SEGURIDAD INFORMÁTICA EN LA DIRECCIÓN NACIONAL DE COMUNICACIÓN Y CRIMINALÍSTICA DE LA POLICÍA NACIONAL DEL PERÚ – HUARAZ - 2015"

Tesis para optar el grado de Maestro
en Ciencias e Ingeniería
Mención en auditoría y seguridad informática

FRANS RENZO DE LA CRUZ JO

ASESOR: Dr. Eddy Jesús Montañez Muñoz

HUARAZ – PERÚ

2017

N° Registro: T0531

MIEMBROS DEL JURADO

Doctor Maximiliano Epifanio Asís López Presidente

_____

Magister Erick Giovanni Flores Chacón Secretario

_____

Doctor Eddy Jesús Montañez Muñoz Vocal

_____

ASESOR

Doctor **Eddy Jesús Montañez Muñoz**

AGRADECIMIENTO

Agradecemos a todos aquellos amigos que en forma desinteresada me proporcionaron información para la tesis en los temas de Metodologías y Herramientas de la Informática, Informática Forense, Reducir El Riesgo de la Seguridad Informática.

A mis amigos, familiares, docentes amigos profesionales de otras carreras profesionales que también aportaron información de acuerdo a sus conocimientos. por el aporte con la guía para la elaboración de informes de investigación, por su ayuda incondicional y su apoyo con la estructura de la tesis así mismo por su constante apoyo en las asesorías y consultas que encaminaron esta tesis

A Quienes fueron guías para la culminación de esta tesis, a la Universidad Nacional Santiago Antúnez de Mayolo por brindarnos la educación, apostando por nuestra región Ancash y sin olvidarnos de Dios por darnos la vida, salud y bienestar, para poder realizarnos como seres humanos que contribuyan a la sociedad, construyendo un país mejor.

La presente Tesis de Maestría está dedicada a mi esposa Marita a quien amo con todo mi corazón, a mi principal motivación mi hijita Marie, a mis padres Lorenzo y Ninfa en agradecimiento a su dedicación a su gran esfuerzo por llevarnos por el buen camino hacia la excelencia, a mis ahora también padres Marco y Cris hoy puedo dar fé que la Tía, Profesora Lilian Jo, quien incentiva a seguir estudiando y recomendaba con una frase muy real "quien a los 20 años no busca a los 30 no encuentra a los 40 no es rico a los 50 arrea borricos" a todos nuestros docentes de la escuela de postgrado por los consejos brindados durante las horas de clase.

A todas aquellas personas que colaboraron con un granito de arena para que esta tesis se haga realidad a todos aquellos amigos que aportaron con información y la paciencia prestada.

Índice

Índice figuras

Índice de tablas

Resumen

El propósito fundamental del presente trabajo de investigaciones estuvo referido a la aplicación de metodologías y herramientas la informática forense para lograr reducir la inseguridad informática tomando como lugar de aplicación la Dirección Nacional de Comunicación y Criminalística de la Policía Nacional del Perú – Huaraz.

Investigación aplicada, descriptivo, de diseño no experimental transversal , la población de estudio para el trabajo de investigación estuvo comprendida por los trabajadores de la Dirección Nacional de Comunicaciones y Criminalística de la Policía Nacional del Perú, con una muestra de 45 trabajadores , el instrumento que se utilizó para la recolección de la información fue el cuestionario, la información se procesó mediante el programa SPSS V19, para el análisis de datos se utilizó el análisis estadístico, a través de la estadística descriptiva.

El resultado de la investigación forense está relacionado con la seguridad informática en la Dirección Nacional de Comunicación y Criminalística de la PNP, los conocimientos de metodologías y herramientas de la informática forense tienen una relación directa con la seguridad informática en un 89%.

Se concluyó: Que el nivel de preparación para la informática forense y sus capacidades en el departamento de Dirección Nacional de Comunicación y Criminalística de la Policía Nacional del Perú en Huaraz es bajo tan solo representa un 20% que el personal no está capacitado para afrontar temas forenses.

Palabras Claves: Computación forense, Crimen cibernético, Practica de asalto

Abstract

The fundamental purpose of this research work was to apply the methodologies and tools forensic computer to reduce computer insecurity taking as a place of application the National Directorate of Communication and Criminalistics of the National Police of Peru - Huaraz.

Applied research, descriptive, non-experimental cross-sectional design, the study population for the research was comprised of workers from the National Communications and Criminalistics Directorate of the National Police of Peru, with a sample of 45 workers, the instrument that Was used for the collection of the information was the questionnaire, the information was processed using the program SPSS V19, for the analysis of data was used statistical analysis, through descriptive statistics.

The result of the forensic investigation is related to computer security in the National Directorate of Communication and Criminalistics of the PNP, the knowledge of methodologies and tools of computer forensics have a direct relationship with computer security in 89%. It was concluded: That the level of preparation for computer forensics and its capacities in the National Directorate of Communication and Criminalistics of the National Police of Peru in Huaraz is low only represents 20% that the staff is not qualified to address issues Forensics.

Key Words: Computer Forensics, Cyber Crime, Assault Practice

I INTRODUCCION

En la actualidad se cuenta con un área de ingeniería forense muy precaria y no especializada, así mismo se encuentra centralizado en la ciudad de lima, en el departamento de Ingeniería Forense.

La falta de un área especializada de ingeniería forense en la PNP en la Ciudad de Huaraz no posibilita identificar el crimen cibernético al desconocer las metodologías y herramientas de la informática forense.

Con esta investigación elabore y explicare la metodología y herramientas que serán aplicadas a la informática forense de acuerdo a las leyes vigentes en el Perú y disminuir el crimen cibernético, por ende, el riesgo de ataques en Seguridad Informática.

Los pasos que hoy en día se dan en el campo de la tecnología son vertiginosas, computadoras, celulares, Internet, automatización de tareas mediante la implementación de programas, telecomunicaciones, etc., han llegado a ser parte de la vida del ser humano, no solo en el ámbito laboral sino también personal debido a la información sobre la identidad de cada persona, almacenada en las diversas Bases de Datos, de igual manera la formalización las técnicas y los procedimientos para darle valor probatorio a esas evidencias digitales. De un delito informático muchas veces las computadoras portátiles, de escritorio, medios físicos de almacenamiento como CD’s, DVD’s, memorias usbs, teléfonos celulares, dispositivos de almacenamiento masivo son evidencias que requiere de

mecanismos para recuperar, interpretar y usarlas para que puedan servir como pruebas.

Analizare la metodología y herramientas para que la Policía Nacional del Perú PNP pueda ser orientado y ayuden a manejar una escena del delito donde se vean involucrados sistemas de información o redes de telecomunicaciones y posterior recuperación de las evidencias digitales. Transacciones de compra, venta, pagos, depósitos, etc., se realiza a través de Internet.

Lo que engloba esta era tecnológica trae interrogantes como, ¿Qué tan protegida está la información?, ¿Cómo se puede reaccionar a ataques contra la integridad del individuo o de las empresas?, ¿De qué, si las leyes y medios existentes en nuestro país pueden descubrir cómo, ¿quién cometió el delito y que sentencia recibirá?

En el Perú se han manifestado casos de delitos informáticos que no son divulgados o denunciados por los individuos o empresas afectadas por evitar un caos, por resguardar su imagen o, muchas veces por desconocimiento de la ley que incrimina ciertos delitos informáticos.

La Policía Nacional tiene como finalidad resguardar y proteger a la ciudadanía, por ello se considera que el crecimiento de la institución debe ser permanente y en constante actualización, ya que cada vez más la tecnología informática se ha convertido en un instrumento para cometer crímenes. La Policía es consciente de que los delitos tan tradicionales como el crimen cibernético que se suscitan en nuestro país, demandan grandes desafíos en sus investigaciones ya que se han obtenido evidencias como computadoras, teléfonos celulares, dispositivos de almacenamiento, programas o cualquier tipo de hardware que requieren de

conocimiento, técnicas y herramientas de Informática Forense para que se pueda realizar una reconstrucción, análisis y reconocimiento del delito de una manera adecuada y llegar así hasta el atacante. En la misma institución se han dado casos de extorsión mediante la tecnología, en donde no se ha podido aplicar una metodología de investigación de análisis forense para poder obtener evidencias contundentes y de esta manera detectar a tiempo al individuo y que sea enjuiciado.

1.1 Objetivos

Objetivo general

Determinar la relación entre la informática forense y seguridad informática de la Dirección nacional de Comunicaciones y Criminalística de la PNP - Huaraz.

Objetivos específicos

1. Conocer las características de la informática forense y la seguridad informática de la Dirección Nacional de Comunicaciones y Criminalística de la PNP – Huaraz.

2. Determinar el nivel de seguridad informática de la Dirección Nacional de Comunicaciones y Criminalística de la PNP – Huaraz.

1.2 Hipótesis

La Informática Forense está relacionada con la Seguridad Informática de la Dirección nacional de Comunicaciones y Criminalística de la PNP de Huaraz.

1.3 Variables

Variable independiente

X = Metodología y herramientas de la **informática forense**

Variable dependiente

Y = Seguridad Informática en la Dirección Nacional de Comunicación y Criminalística de la Policía Nacional del Perú – Huaraz

Tabla 1.01 Operacionalización de variables

Variables	Dimensiones	Indicadores	Tipo de var
Independiente: X (informática forense)	Hardware	-Servidor -Fibra óptica -Terminales	Cualitativo
	Software	-Data center -Licenciamiento -Software especializado	
	Marco Jurídico	-Conocimiento de normas -Asesoramiento	
	Políticas de seguridad de la información	-Conocimiento de seguridad de la información	
Dependiente: Y (Seguridad Informática)	Riesgos del manejo de la información	- Detección de riesgos de información - Registro de incidencias de seguridad por los usuarios	Cualitativo
	Delito, Evidencia	-Detección de delitos informáticos.	
	Reporte de tráfico de información más seguro de los sistemas de información.	- Reporte formalmente comunicado	

Fuente: Elaboración propia

II MARCO TEÓRICO

2.1 Antecedentes

A. Nivel nacional

Pacheco, Hugo; Moreno, Jorge (2012) "Esclarecimiento de hechos delictivos usando informática forense", Universidad Nacional De Trujillo, Trujillo - Perú

En esta tesis se tiene una revisión de las herramientas más adecuadas tanto de hardware como de software disponible en el mercado y que son indispensables para recolectar evidencia digital, ya que dicha evidencia debe ser idéntica a la original y debe permanecer inalterable la escena del crimen.

Para tal fin se hizo un estudio de la metodología CP4DF (código de prácticas digitales forenses) de la informática forense en el estudio de un delito, basado en el análisis forense de un sistema, que involucra primeramente la recolección de información dispersa de todo el sistema y posterior análisis de la misma; mientras más compleja y precisa resulte dicha información, más verídico será el análisis realizado.

La adecuada conservación de la información del sistema original cumple un rol fundamental en la investigación, de modo que el procesamiento de la misma debería llevarse a cabo una copia de los datos del sistema original. Para ello se utilizará software libre (Open Source) para llegar a generar pruebas válidas para esclarecer hechos delictivos

Pineda, German (2015) "Efectos de la auditoria forense en la investigación del delito de lavado de activos en el Perú 2013-2014", Universidad San Martín de Porres, Lima – Perú.

El presente trabajo de investigación titulado "Efectos de la Auditoría Forense en la Investigación del Delito de Lavado de Activos en el Perú 2013 - 2014", es de mucha importancia ya que la aplicación de la Auditoria Forense, permitirá fiscalizar, combatir, prevenir y minimizar el Delito de Lavado de Activos, a través de la investigación que realiza el Ministerio Público, Policía Nacional del Perú y la Contraloría General de la República. Asimismo, el efecto de la Auditoria Forense, va a poner en consideración de la justicia las evidencias encontradas en el proceso de Auditoria y poder culpar a los imputados por los delitos cometidos y en especial el Delito de Lavado de Activos.

Por consiguiente, la Auditoría Forense se vale de profesionales competentes para poder realizar investigaciones en materia de Lavado de Activos y preparar el informe de auditoría que realiza el Auditor Forense y que forma parte del proceso investigatorio. Como sabemos, el Delito de Lavado de Activos es la introducción de dinero ilícito al mercado y hacerlo legal y transparente; es por eso, que la implementación de este sistema de Auditoria Forense en el Estado peruano es de vital importancia para actuar más rápida y eficientemente en los procesos que se están investigando.

La presente tesis llegó a determinar que la Auditoría Forense incide en la investigación del Delito de Lavado de Activos, porque existe la predisposición de

prevenir y luchar de manera frontal este mal que distorsiona los movimientos contables - financieros del dinero adquirido.

B. Nivel internacional

Álvarez, María; Guamán Verónica, (2008): "Metodologías, estrategias y herramientas de la informática forense aplicables para la dirección nacional de comunicación y criminalística de la policía nacional", Universidad Politécnica Salesiana sede Cuenca – Ecuador

La Policía Nacional al tener un Proyecto de Implementación de un Departamento de Investigación de delitos informáticos con una sección de Análisis Forense, es recomendable que se acople con herramientas Open Source ya que después de un análisis comparativo con respecto a las comerciales, tienen algunas ventajas en sus características de rendimiento y la gran diferencia del costo, teniendo en cuenta que tanto herramientas comerciales como libres tienen que ser herramientas avaladas por instituciones autorizadas, para que de esta manera se pueda dar credibilidad a la evidencia y pueda servir como prueba contundente.

A usar la guía de buenas prácticas adjunta en el Capítulo 4, ya que está basada en los lineamientos de la IOCE y la RFC 3227, partiendo de una metodología probada como es la inspección ocular, la guía permite optimizar y agilizar los pasos dependiendo del caso de la investigación.

Forman parte de Redes Internacionales de Informática Forense ya que la cooperación de países con experiencia será de mucha utilidad para el Ecuador, que está empezando en esta área.

Villacís Viviana, (2006) "Auditoria Forense: Metodología, Herramientas y Técnicas Aplicadas en un siniestro informático de una empresa del sector comercial", Escuela Superior Politécnica del Litoral Guayaquil – Ecuador.

La mejor forma de evitar situaciones engorrosas de fraudes, robo y siniestros informáticos es estableciendo controles, pero por, sobre todo, promover una cultura de seguridad en las organizaciones

Se desarrollan prácticas y procedimientos de programación y control que busquen disminuir los problemas de seguridad en los productos de software y hardware.

Prácticas y políticas de seguridad informática, como pruebas pre constituidas para la organización.

Rodríguez Lizeth (2011) "Análisis informático forense para la recopilación confiable de datos y evidencias digitales", Universidad Mayor de San Andrés La Paz – Bolivia

La seguridad es la mayor prioridad para el equipo de seguridad y auditoria fue la disponibilidad de procesos formales y la capacidad en cuanto a la identificación de vulnerabilidades análisis forense y atención a incidentes de seguridad a la que

necesita estar capacitados y contar con los recursos necesarios para cumplir con sus actividades diarias

El método podría utilizar en proyectos en donde se desee determinar las vulnerabilidades y mitigaciones de riesgos a los que están expuestos ciertos recursos.

Arquillo José (2007), "Herramientas de apoyo para el análisis forense de computadoras", Universidad de Jaén, Escuela Politécnica Superior de Jaén Andalucía – España 2007.

Primeramente, se ha llevado a cabo un repaso sobre la historia y los diferentes modelos presentados para el análisis forense de computadoras. Siguiendo el modelo de Case se han visto las diferentes tareas que ocupa y se ha profundizado en la más importante y compleja: el análisis de los datos o extracción de información. Dentro de este hemos visto las distintas partes a revisar dentro de un dispositivo y pasando por las distintas capas de un sistema de ficheros se han revisado las técnicas usadas para recuperar datos.

A continuación, se han recopilado todas las herramientas que se usan o se han usado en los análisis forenses de computadoras, desde la adquisición de datos al examen de los mismos, pasando por herramientas específicas para una parte de un sistema de ficheros (por ejemplo, metadatos), hasta llegar a las herramientas de análisis de discos.

En base a lo visto anteriormente se ha planteado una aplicación asistente que aparte de servir como herramienta proporcionando acceso a las herramientas, sirva de forma didáctica a un usuario que carece de conocimientos sobre esta área. Usando herramientas de libre distribución como Python, The Sleuth Kit, o QEMU, se ha desarrollado una aplicación útil e intuitiva que guía al usuario sobre el proceso de análisis forense y sobre el manejo de la propia aplicación.

Esta aplicación se ha incluido en un Cd-Live auto arrancable de manera que pueda ser probada al arrancar con este Cd. Para la creación de este Cd se han realizado varios scripts que automatizan en cierto modo el proceso.

Posteriormente se ha probado la aplicación sobre varios sistemas de ficheros, LINUX y FAT, realizando pruebas en relación a la naturaleza de la imagen. Aquí se comprueba que la aplicación a pesar de ser bastante completa, está lejos de ser más que una aplicación con una mera función didáctica y en cualquier caso, de recuperación de datos, ya que un análisis forense implica el uso de todas las técnicas y herramientas conocidas por el investigador, así como la realización de largos exámenes, exhaustivos y precisos

2.2 Bases teóricas

2.2.1 Definición informática forense

Es la ciencia forense que se ocupa de la utilización de los métodos científicos aplicables a la investigación de los delitos, no solo informáticos y donde se utiliza

el análisis forense de las evidencias digitales en toda información o datos que se guarda en una computadora o sistema informático. (Acurio del Pino, 2013)

Preservación, identificación, extracción, interpretación y presentación de la información o datos que han sido procesados electrónicamente y guardados en una computadora o sistema informático, que servirá como evidencia digital. La ciencia forense es sistemática y se basa en hechos premeditados para recabar pruebas que luego serán analizadas. Existen múltiples definiciones a la fecha sobre el tema forense en informática:

Computación forense, digital forensics (forense digital), network forensics (forense en redes), entre otros.

Este conjunto de términos puede generar confusión en los diferentes ambientes o escenarios donde se utilice, pues cada uno de ellos trata de manera particular o general temas que son de interés para las ciencias forenses aplicadas en medios informáticos

Computer forensics, Su traducción es computación forense. Se interpreta de dos maneras:

1. Disciplina de las ciencias forenses que, considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos.

2. La disciplina científica y especializada que entendiendo los elementos propios de tecnologías el equipo de computación ofrece un análisis de la información residente en dichos equipos.

Forense digital, Es una nueva especialidad. Semejanza con informática forense, al ser una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes. (Cano, 2013)

2.2.2 Objetivo de la informática forense

La informática forense tiene 3 objetivos.

1. Crear y aplicar políticas para prevenir posibles ataques y de existir antecedentes evitar casos similares.
2. Perseguir y procesar judicialmente a los crímenes.
3. Compensar daños causados por los criminales o intrusos.

La informática forense busca encontrar y reconstruir el ataque que fue realizado con el fin de obtener que datos pudieron ser manipulados durante el mismo y lograr identificar el origen del ataque. Con el fin de poder remediar el daño realizado por el atacante y poder capturarlo para poder realizar un proceso judicial contra él. Para ello es necesario el apoyo de los gobiernos con el fin de que existan regulaciones contra los delitos informáticos y que al momento de identificación no queden impunes.

Los objetivos perseguidos pueden verse divididos en los dos papeles que puede tomar la informática forense según la informática forense preventivos y correctivos o reactivos.

El primer objetivo entra en la parte preventiva de ella, mientras que los objetivos restantes son cubiertos cuando se toman medidas reactivas y correctivas luego de un ataque. (Ramirez Rivera)

2.2.3 Modelo y buenas prácticas

Modelo de referencia del descubrimiento electrónico. (ERDM DUKE LAW, 2014)

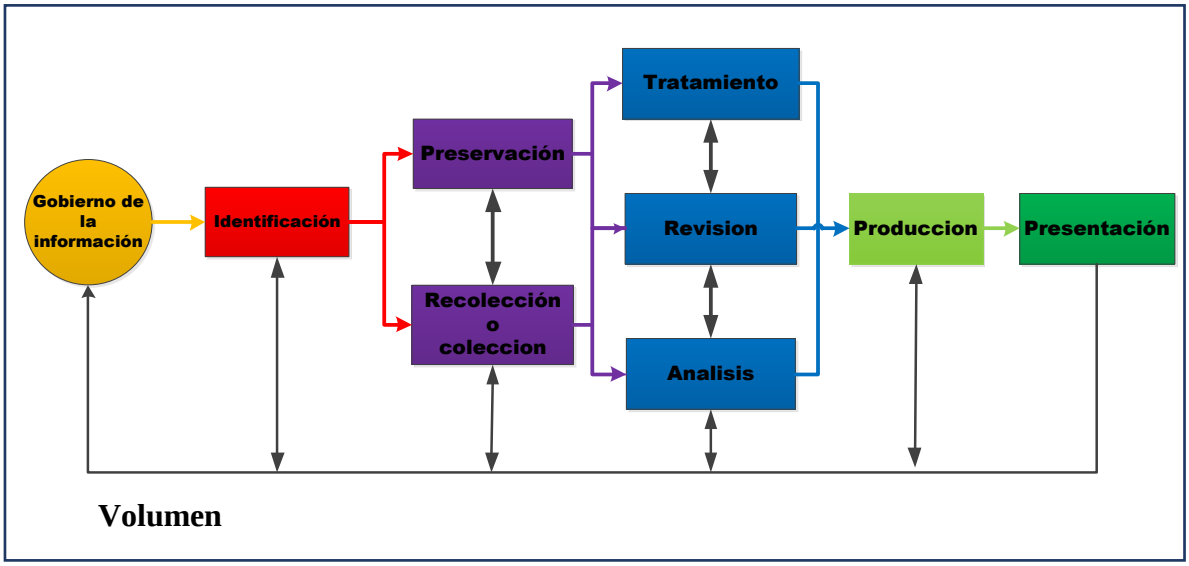
El diagrama representa un EDRM conceptual vista del proceso de e-discovery, no un modelo de cascada literal, lineal o. Uno puede participar en algunos, pero no todos los pasos que se indican en el diagrama, o uno puede elegir para llevar a cabo los pasos en un orden diferente al que se muestra aquí.

El diagrama también retrata un proceso. Uno podría repetir los mismos tiempos de las etapas numerosas, afinando en un conjunto más preciso de los resultados. Uno podría también pasar de nuevo por pasos anteriores, refinando el enfoque de uno como una mejor comprensión de los datos surge o como la naturaleza de los cambios en la materia.

El diagrama pretende ser una base para la discusión y el análisis, no como una receta para el único camino correcto para acercarse e-discovery.

se presentan de la figura 2.01 explicaciones resumidas de cada etapa EDRM. Para las guías para cada etapa del proceso de e-discovery, mueva el cursor sobre las casillas de abajo para enlaces a guías para cada etapa del proceso de e-discovery o seleccione una de las partidas anteriores de las explicaciones sumarias.

Figura 2.01 Modelo de referencia del descubrimiento electrónico



Fuente: http://www.edrm.net/resources/edrm-stages-explained.

a. **Administración de la información.** Para que la administración electrónica con el fin de mitigar el riesgo y los gastos que enviar un descubrimiento convierta en un problema, desde la creación inicial de ESI (información almacenada electrónicamente) a través de su disposición final.

b. **Identificación.** Localización de las fuentes potenciales de ESI y determinar su alcance, amplitud y profundidad.

c. **Preservación.** Asegurar que ESI está protegido contra la alteración o destrucción inapropiada.

d. Colección. Recopilación de ESI para su uso posterior en el proceso de e-discovery (elaboración, revisión, etc.).

e. Tratamiento. Reducir el volumen de ESI y su conversión, si es necesario, a formas más adecuadas para la revisión y análisis.

f. Revisión. La evaluación de ESI para relevancia y privilegio.

g. Análisis. La evaluación de ESI para el contenido y contexto, incluidos los patrones clave, temas, personas y discusión.

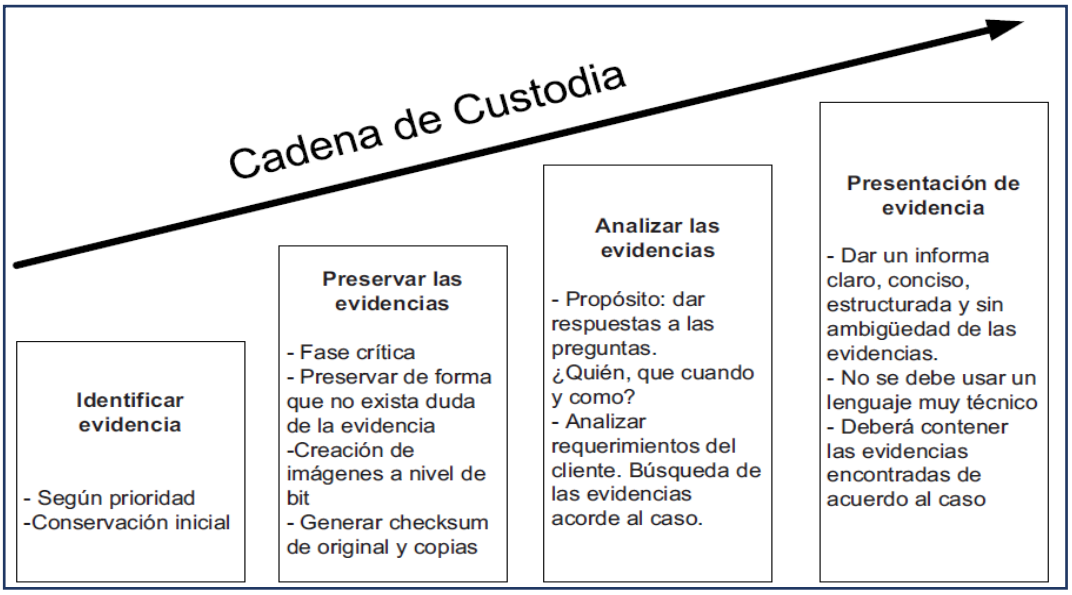
h. Producción. Entrega de ESI a otros en formas adecuadas y utilizando los mecanismos de entrega adecuados.

i. Presentación. Viendo ESI antes de las audiencias (en deposiciones, audiencias, juicios, etc.), especialmente en las formas nativas y cerca de nativos, para obtener más información, validar los hechos o las posiciones existentes, o persuadir a una audiencia. (ERDM DUKE LAW, 2014)

2.2.4 Fases de la informática forense

El manejo de evidencias sobre un crimen o delito informático cometido, deberá actuar como proceso criminal, el primer paso es asegura la escena del delito restringiendo el acceso a la misma para no modificar la evidencia. Los peritos que manejen el caso deberán poseer conocimientos sobre las metodologías del análisis forense informático que se deben aplicar según el caso.

Figura 2.02 Metodología del Análisis Forense



Fuente: Equipo de Investigación de Incidentes y Delitos Informáticos.

Para llevar a cabo una investigación forense es adecuado conocer ciertos aspectos tales como:

A.1 Conocer las condiciones bajo las cuales, la evidencia será considerada como

Tabla 2.01 Condiciones de la evidencia

a. Admisible	b. Autentica	c. Completa	d. Confiable	e. Creíble

Fuente: Equipo de Investigación de Incidentes y Delitos Informáticos.

Conocer el procedimiento para llevar a cabo una investigación, cuando debe llevarse a cabo las cuestiones legales a tener en cuenta, dependiendo del país donde se lleve a cabo.

A.2 Existen modos de análisis para la informática forense

a. Análisis post-mortem: se realiza con un equipo dedicado específicamente para fines forenses para examinar discos duros, datos o cualquier tipo de información recabada de un sistema que ha sufrido un incidente. En este caso, las herramientas de las que se puede disponer son aquellas que existen en el laboratorio destinado al análisis de discos duros, archivos de logs de firewalls, etc.

b. Análisis en caliente: se lleva a cabo cuando un sistema presume que ha sufrido un incidente o está sufriendo un incidente de seguridad. En este caso, se debe emplear un CD con las herramientas de Respuesta ante Incidentes y Análisis Forense compiladas de forma que no realicen modificaciones en el sistema. Una vez hecho este análisis en caliente, y confirmado el incidente, se realiza el análisis post-mortem.

A.3 Cadena de custodia

Es conjunto de pasos o procedimientos seguidos para preservar la prueba digital que permita convertirla y usarla como evidencia digital en un proceso judicial. No existe un estándar reconocido públicamente

Tabla 2.02 Cadena de custodia

La cadena de custodia	La cadena de la evidencia debe seguir el siguiente orden	La cadena de la evidencia muestra
Reducir al máximo la cantidad de agentes implicados en el manejo o tratamiento de evidencias.	Recolección e identificación de evidencia	Quién obtuvo la evidencia
Mantener la identidad de las personas implicadas desde la obtención hasta la presentación de las evidencias.	Análisis	Dónde y cuándo la evidencia fue obtenida
Asegurar la firmeza de las evidencias	Almacenamiento	Quién protegió la evidencia
Registros de tiempos, firmados por los agentes, en los intercambios entre estos de las evidencias. Cada uno de ellos se hará responsable de las evidencias en cada momento.	Preservación	Quién ha tenido acceso a la evidencia
Asegurar la firmeza de las evidencias cuando las evidencias están almacenadas asegurando su protección	Transporte.	
	Presentación en el juzgado	
	Retorno a su dueño	

Fuente: Equipo de Investigación de Incidentes y Delitos Informáticos.

A.4 Identificación de la Evidencia Digital

En esta fase se debe localizar los dispositivos donde podemos encontrar evidencias, ya que muchas veces la información que directa o indirectamente se relaciona con esta conducta criminal queda almacenada de forma digital dentro de estos Sistemas Informáticos.

La evidencia digital Es el conjunto de datos en formato binario, comprende los ficheros, su contenido o referencias a éstos (meta-datos = datos acerca de datos) que se encuentren en los soportes físicos o lógicos del sistema atacado, los mismos pueden ser recolectados y analizados con herramientas y técnicas especiales.

A.4.1 Tipo de evidencia digital

i. Constante: evidencia almacenada en un medio informático y que se mantiene preservada después de que la computadora sea apagada.

ii. Volátil: evidencia que se encuentra almacenada temporalmente, en la memoria RAM, o en el caché, y al interrumpir la alimentación eléctrica la evidencia se pierde. Este tipo de evidencia deber ser recuperada casi de inmediato, guardarlas a ficheros de esta forma se convertirá en evidencias no volátiles.

Es importante considerar la diferencia que hay entre la evidencia digital y evidencia electrónica ya que estas pueden ser usadas como sinónimos, sin embargo, la primera se refiere a los aparatos electrónicos como celulares y PDAS 9 y la segunda a la información digital que estos contengan.

A.4.2 Clasificación de la evidencia digital

A.1. Evidencia física

Tabla 2.03 Evidencia física

Soportes de almacenamiento	Dispositivos electrónicos	Dispositivos de comunicaciones de red
CPU	Discos Externos	Router
CD ROMs, DVD	Tables	Switch
USB	Organizadores electrónicos	Access point
Disco externos		
Cintas magnéticas		

Fuente: Equipo de Investigación de Incidentes y Delitos Informáticos.

A.2 Evidencia lógica

Cualquier dato almacenado o generado en un medio magnético, este tipo de evidencia puede ser clasificada en tres categorías:

A. **Registros generados por computador.** Estos registros son generados como efecto de la programación de un computador, y son inalterables por una persona, los mismos son llamados registros de eventos de seguridad (logs).

B. **Registros no generados sino simplemente almacenados por o en computadores.** Estos registros son generados por una persona, son

almacenados en el computador, por ejemplo, un documento realizado con un procesador de palabras.

C. Registros híbridos. Estos registros incluyen tanto registros generados por computador como almacenados en los mismos. Los registros híbridos son aquellos que combinan afirmaciones humanas y logs.

D. Registros de cada servidor. Son aquellos registros del sistema y de cada programa en ejecución, como pueden ser los de un servidor Web Apache.

E. Registros de tráfico de red. Router: enrutador o encaminador, dispositivo de hardware para interconexión de redes de las computadoras que opera en la capa tres (nivel de red)

F. Registros de aplicación. Son aquellos registros a los que cada aplicación almacena sobre el acceso de los usuarios, errores ocurridos e información sobre las actividades de cada usuario en la aplicación.

A.3. Evidencia digital

Tabla 2.04 Evidencia digital

Sistemas de computación abiertos	Sistemas de Comunicación	Sistemas Convergentes de Computación
Están compuestos por computadoras personales y servidores con sus periféricos (teclado, Mouse, monitor), son una fuente de evidencia digital muy importante ya que almacenan gran cantidad de información en sus discos duros.	Están compuestos por redes de telecomunicaciones, Internet y comunicación inalámbrica.	Formados por teléfonos celulares, llamadas inteligentes, asistentes personales digitales, tarjetas inteligentes y cualquier dispositivo electrónico que posea tendencia digital.

Fuente: Equipo de Investigación de Incidentes y Delitos Informáticos.

A.4. Identificación de la evidencia

Para la identificación de la evidencia dentro del proceso forense se debe:

a. Anticipar qué procedimientos serán empleados en la práctica forense al momento de recopilar la evidencia.

b. Identificar el tipo de información almacenada en un dispositivo y el formato en que se guarda, con la finalidad de usar la tecnología apropiada para extraer la información que se mantienen en el mismo.

c. Los investigadores forenses deben estar en capacidad de reconocer qué formato tiene determinada información, cómo extraerla y qué medio requieren para almacenar y preservar la misma. Con la finalidad de determinar dónde debe ser ubicada y como debe ser usada la evidencia, se definen categorías para distinguir entre un sistema informático o hardware (evidencia electrónica) y la información contenida en este (evidencia digital).

El hardware se refiere a todos los componentes físicos de un sistema informático, la información se refiere a datos, programas almacenados, mensajes de datos trasmitidos usando el sistema informático.

Tabla 2.05 Identificación de la evidencia (I)

Sistema Informático	
Hardware (elementos físicos)	Evidencia electrónica
El hardware es mercancía ilegal o fruto del delito	-El hardware es una mercancía ilegal cuando su posesión no está autorizado por la ley. - El hardware es fruto del delito cuando es obtenido mediante robo, fraude u otra clase de infracción.
El hardware es un instrumento	-Es un instrumento cuando del hardware cumple un papel importante en al cometer del delito, es decir si se lo usa como una arma o herramienta tal como pistola. (ejemplo snifers).
El hardware es evidencia	-Es un delito físico que se constituye como prueba de la comisión de un delito

Fuentes: Álvarez y Guamán "Metodología, Estrategias y Herramientas de la Informática Forense Aplicables Para la Dirección Nacional de Comunicaciones y Criminalística de la Policía Nacional", Cuenca, febrero 2008

Tabla 2.06 Identificación de la evidencia (II)

Sistema Informático	
Información	Evidencia electronica
La información es mercancía ilegal o fruto del delito.	-La información es mercancía ilegal cuando su posesión no está autorizada por la ley. (Ejemplo, pornográfica infantil) -La información es fruto del delito cuando sea el resultado de la comisión de una infracción. (Ejemplo copias piratas de programa, secretos industriales hurtados)
La información es un instrumento	-La información es un instrumento o herramienta, cuando es usado como medio para cometer una infracción penal (Ejemplo programas usados para romper seguridad de un sistema informático, rompiendo contraseñas.)

Fuentes: Álvarez y Guamán "Metodología, Estrategias y Herramientas de la Informática Forense Aplicables Para la Dirección Nacional de Comunicaciones y Criminalística de la Policía Nacional", Cuenca, febrero 2008

A.5 Descubrimiento de las señales del ataque.

Para descubrir algún tipo de anomalía, incidente o ataque se deberá tomar en consideración las siguientes tareas:

a. Interpretar comandos en modo consola (cmd, bash)

b. Enumerar puertos TCP y UDP abiertos y sus aplicaciones asociadas (fport, lsoft)

c. Listar usuarios conectados local y remotamente al sistema

d. Obtener fecha y hora del sistema (date, time)

e. Enumerar procesos activos, recursos que utilizan, usuarios o aplicaciones que los lanzaron (ps, pslist).

f. Enumerar las direcciones IP del sistema y mapear la asignación de direcciones físicas MAC con dichas IP (programas: ipconfig, arp, netstat, net)

A.1 Macmac times

i. Cada entrada del Sistema de Ficheros mantiene tres fechas y horas de todas las entradas que se encuentran en este (ficheros, directorios, links, etc.).

ii. Importantes para el análisis de máquinas comprometidas.

A.2 Los mac times

a. Modificación: Cambios en el fichero o directorio a nivel de su contenido.

b. Acceso (Access): Acciones de lectura, escritura (puede no implica cambio), etc.

c. Cambio: Cambio a nivel de características del fichero (permisos, usuarios, propietarios, etc.)

d. Buscar ficheros ocultos o borrados (programas: hfind, unrm, lazarus)

e. Visualizar registros y logs del sistema (programas: reg, dumpel)

f. Visualizar la configuración de seguridad del sistema (auditpol)

g. Generar funciones hash de ficheros (programas: sah1sum, md5sum)

h. Leer, copiar y escribir a través de la red (programas: netcat, crypcat)

i. Realizar copias bit-a-bit de discos duros y particiones (programas: dd, safeback)

j. Analizar el tráfico de red (programas: tcpdump, windump)

A.3 Opciones de búsqueda

Realizar una verificación de integridad de los ficheros del sistema, utilidades como Tripwire o AIDE (Advance Intrusion Detection Enviroment) ayudarán a ello.

a. Conocer los procesos que se están ejecutando actualmente en el equipo y ver cuál de ellos consume más recursos, con ubicaciones poco frecuentes en el sistema de archivos y los que mantengan conexiones de red en puertos TCP o UDP no habituales.

b. Listar todos los puertos TCP y UDP abierto, se deberá tomar muy en cuenta aquellos procesos que emplean puertos altos por encima del 1024.

c. Editar los archivos de registro del sistema y logs en busca de entradas y avisos sobre fallos de instalación, accesos no autorizados, conexiones erróneas o fallidas.

Al momento de descubrir una evidencia, se deberá

a. Conservar la evidencia, y por ningún motivo modificarla.

b. Utilizar herramientas que no modifiquen el tiempo de ejecución de los archivos.

c. No modificar los archivos ni borrarlos.

2.2.5 Recolección de evidencias

La recopilación de evidencias permite determinar el método de entrada al sistema, la actividad de los intrusos, su identidad y origen, para todo ello se debe poseer

mucha precaución para evitar alterar las evidencias durante el proceso de recolección.

La recolección de evidencia, varía de país en país, y por lo tanto, un análisis exacto y completo está fuera de los límites. Sin embargo, se presentan guías básicas que pueden ayudar a cualquier investigador forense:

La IOCE (Organización Internacional de Evidencias en Computadora) define cinco puntos principales para el manejo y recolección de evidencia digital:

1. Al recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
2. La persona que tenga acceso a evidencia digital original, deberá ser un profesional forense.

3. Toda la actividad referente a la recolección, el acceso, almacenamiento o a la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para la revisión.

4. Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras que ésta esté en su posesión.

5. Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

A.1 Cuidados en la recolección de evidencias

La recolección de evidencia informática es un aspecto frágil de la computación forense, especialmente porque requiere de prácticas y cuidados adicionales que no se tienen en la recolección de evidencia convencional. Es por esto que:

a. Se debe proteger los equipos del daño.

b. Se debe proteger la información contenida dentro de los sistemas de almacenamiento de información (muchas veces, estos pueden ser alterados fácilmente por causas ambientales, o por un simple campo magnético).

c. Algunas veces, será imposible reconstruir la evidencia (o el equipo que la contiene), si no se tiene cuidado de recolectar todas las piezas que se necesiten.

El hardware es uno de los elementos que se deben tener en cuenta a la hora de la recolección de evidencias, es por eso que se deben tener consideraciones especiales.

Lo primero que se debe preguntar el investigador es qué partes se deben buscar o investigar.

A.2 Inicio de la recolección

Para iniciar la recolección de evidencias se debe:

a. Apagar el equipo atacado

b. Anotar la fecha, hora de inicio y fin de cada uno de los pasos que se realicen

c. Anotar las características y números de serie de cada equipo, de sus componentes, de su S.O. (Sistema Operativo), etc.

d. Fotografiar los equipos del entorno.

e. Es recomendable que exista un acompañante durante el proceso de recopilación de evidencias, ésta actuaría como testigo al tomar cualquier acción en la escena, si es un Notario es mucho mejor.

E1. Una vez que ya se realizaron las tareas anteriores se deberá definir el estado del sistema y del atacante:

E2. Elegir el tipo de análisis que se efectuará en el equipo:

E.2.1. Análisis con el equipo apagado = En frío: es válido si se lo realiza bien, pero no se posee toda la información del ataque.

E.2.2. Análisis en caliente = mientras el ataque se está realizando: brinda más información (procesos, conexiones de red, etc.), pero si se lo realiza de forma inadecuada, puede perjudicar el posterior análisis en frío, esto puede conllevar a problemas legales, disminuyendo la contundencia de la evidencia.

E3. Mantenerse precavidos ante el estado del atacante, ya que este puede seguir conectado y provocar borrado, modificado la información mediante una puerta de entrada.

E4. Acechar al atacante evitando que evada la vigilancia en caso de que este se mantenga conectado.

Otro de los tantos problemas que posee un investigador forense, es buscar evidencia volátil, es decir evidencia que se encuentre alojada temporalmente en la memoria RAM o en el CACHE, son evidencias que se pierden cuando se apaga el computador, por ello, este tipo de información debe ser recuperada de forma inmediata.

2.2.6 Preservación de la evidencia.

La preservación se enfoca en resguardar los objetos que tengan valor como evidencia, de manera que estos permanezcan de forma completa, clara y verificable, es importante que cualquier examen que se lleve a cabo no genere cambios, en caso de suscitarse un cambio de manera inevitable, es esencial que se presente la razón por la que se dio tal acontecimiento, explicando el suceso detalladamente, posterior a ello debe ser registrado y justificado.

En esta fase se utiliza técnicas criptográficas como códigos de seguridad (función hash, checksums).

La fase de preservación interviene a lo largo de todo el proceso de investigación forense, la misma interactúa con las demás fases.

Las tareas que se deben seguir para preservar la evidencia digital son:

a. Realizar dos copias de las evidencias obtenidas.

b. Generar una suma de comprobación de la integridad de cada copia empleando función hash (MD5 o SHA1).

c. Incluir las firmas obtenidas en la etiqueta de cada copia de la evidencia en el CD o DVD, incluir fecha, hora de la creación de la copia y el nombre de la misma.

d. Proteger los dispositivos de factores externos como: cambios bruscos, temperatura o campos electromagnéticos, ya que pueden alterar la evidencia.

Si se extraen discos duros se deberá seguir el mismo procedimiento. Y en caso de que se requiera que los discos sean analizados por otras empresas especializadas, se debe solicitar que lo aseguren.

Otro aspecto que se debe tomar en cuenta es la cadena de custodia, donde se establecen las responsabilidades y controles de cada una de las personas que manipulen la evidencia, se deberá registrar los datos personales de todos los implicados en el proceso de manipulación de las copias:

d1. Dónde, cuándo y quién manejo o examinó la evidencia, incluyendo su nombre, su cargo, número de identificación, fechas y horas, etc.

d2. Quién estuvo custodiando la evidencia, durante cuánto tiempo y dónde se almacenó.

d3. Cuando se cambie la custodia de la evidencia también deberá documentarse cuándo y cómo se produjo la transferencia y quién la transportó.

2.2.7 Análisis de la evidencia digital

AFD (Análisis Forense Digital), es un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial.

Este análisis se dará por concluido cuando se conozca cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc.

Antes de realizar un análisis se debe tener en cuenta la siguiente información:

a) Sistema operativo afectado.
b) Inventario de software instalado en el equipo
c) Tipo de hardware del equipo
d) Accesorios y/o periféricos conectados al equipo

e) Si posee firewall

f) Si está en el ámbito del DMZ (Zona desmilitarizada)

g) Conexión a Internet.

h) Configuración.

i) Parches y/o actualizaciones de software

j) Políticas de seguridad implementadas

k) Forma de almacenamiento de la información (cifrada o no)

l) Personas con permisos de acceso al equipo

m) El computador está dentro del DMZ

n) Existe IDS 16

o) Cuantos equipos en red se encuentran conectados.

p) Listar usuarios conectados local y remotamente al sistema.

2.2.8 Preparación para el análisis

A.1 El entorno de trabajo

Es importante establecer estaciones de trabajo para realizar las distintas pruebas y estudios al surgir un caso, dependiendo del ataque o crimen cometido. Para ello se deberá:

a. Clasificar el tipo de incidente

b. Seguir el proceso inter-departamental para el manejo de las evidencias

c. Identificar el tipo de dispositivo (computador, celular, memorias, etc.) y las herramientas necesarias para su análisis.

En las estaciones se deberá operar de la siguiente manera:

a. Montar imágenes de discos duros.

b. Instalar Sistemas Operativos para realizar el estudio de evidencias.

c. Realizar copias exactas del disco duro con la finalidad de realizar pruebas y verificaciones conforme surjan las hipótesis del ataque.

d. En caso de no disponer de recursos se puede usar de software para crear una plataforma de trabajo con varias máquinas virtuales.

e. Se puede crear un entorno de trabajo hipotético con las copias obtenidas para realizar la emulación de los ataques.

A.2 Reconstrucción de la secuencia temporal del ataque

Una vez establecida la estación de trabajo, el primer paso es crear una línea temporal de sucesos o time line, para ello se deberá recopilar la siguiente información sobre los ficheros:

a. Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado).

b. Ruta completa del fichero.

c.Tamaño en bytes y tipo de fichero.

d. Usuarios y grupos a quien pertenece el fichero.

e. Permisos de acceso.

f. Identificar si fue borrado o no.

Esta información es la que más tiempo lleva recopilar, pero es el punto de partida para el análisis. Es importante preparar un script con la finalidad de automatizar el proceso de creación del tiempo en línea (timeline).

Luego de realizar lo antes mencionado se deberá:

a. Ordenar los archivos por sus fechas MAC, esto se debe realizar debido a que los archivos tendrán la fecha de instalación del sistema operativo, por lo que un sistema que se instaló hace meses y que fue comprometido recientemente presentará en los ficheros nuevas fechas MAC muy distintas a las de los ficheros más antiguos.

b. Buscar ficheros y directorios que han sido creados, modificados o borrados recientemente.

c. Buscar instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes.

d. Buscar en lugares donde no se suele mirar, por ejemplo, en los directorios temporales.

e. Buscar los archivos de sistema modificados tras la instalación del sistema operativo, averiguar archivos ocultos donde se encuentran y que tipo son.

f. Buscar archivos borrados, ya que pueden ser restos de logs y registros borrados por sus atacantes.

g. En las imágenes realizadas a los discos duros se puede acceder al espacio residual que hay detrás de cada archivo ya que los mismos suelen almacenarse por bloques, de tal manera que se pueda leer zonas que el sistema operativo no ve.

h. Recuperar archivos borrados, al momento de hacerlo, se deberá intentar recuperar su contenido y fecha de borrado.

i. Examinar y las horas de manera más detallada de los ficheros logs y registros que ya se revisaron con la finalidad de encontrar una correlación entre eventos.

j. Revisar el archivo de contraseñas, buscar la creación de usuarios y cuentas extrañas relacionar la hora de la creación de estas cuentas en caso de que existan con la hora en la que se inició el ataque al sistema.

A.3 Determinación de cómo se realizó el ataque

Una vez que se disponga de la cadena de acontecimientos que se han producido, se deberá determinar cuál fue la vía de entrada al sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse de tal brecha. Para ello se deberá:

a. Combinar consultas a archivos logs, registro, claves cuentas de usuarios etc.

b. Prestar atención a los servicios y procesos abiertos, puertos abiertos TCP/UDP y conexiones que ya se tomaron como evidencia volátil cuando el sistema estaba aún vivo.

c. Examinar las circunstancias sospechosas encontradas al indicio del ataque, y buscar con ellas si son o no vulnerabilidades a través del Internet, ejemplo: www.google.com, www.cert.com, www.securityfocus.com.

d. Si ya está claro cuál fue la vulnerabilidad del sistema, se deberá buscar en Internet algún exploit 18 anterior a la fecha del ataque, que utilice esa vulnerabilidad.

e. Reforzar cada una de las hipótesis mediante la fórmula causa-efecto.

f. Utilizar la máquina "conejillo de Indias" con la finalidad de realizar las pruebas y exploits encontrados.

g. Comprobar si la ejecución del exploit sobre una máquina igual a la atacada, genera los mismos eventos que se han encontrado entre las evidencias.

A.4 Identificación del autor o autores del incidente

Una vez que se determinó como se infiltraron al sistema, ahora se tiene que saber quién o quienes lo hicieron, para ello se deberá consultar nuevamente algunas evidencias volátiles que fueron recopiladas en la primera fase:

a. Revisar las conexiones que se encontraban abiertas, que puertos y que direcciones IP las solicitaron, a más de ello se deberá buscar entre las entradas a los logs de conexiones.

b. Indagar entre los archivos borrados que se han recuperado. Para Identificar a los atacantes se debe realizar algunas averiguaciones como parte del proceso de identificación:

c. Averiguar la dirección IP del atacante, para ello se deberá revisar detenidamente los registros de conexiones de red, los procesos y servicios que se encontraban a la escucha. Esta información se podría encontrar en fragmentos de las evidencias volátiles, la memoria virtual o archivos temporales y borrados, como restos de e-mail, conexiones fallidas, etc.

d. Al adquirir la dirección IP sospechosa, se deberá comprobar en el registro RIPE NCC (www.ripe.net) a quien pertenece, es importante considerar que no se puede sacar conclusiones prematuras, debido a que muchos atacantes falsifican la dirección IP con técnicas de spoofing. Los atacantes también pueden utilizar ordenadores zombis, éstos son comprometidos en primera instancia por el atacante y posteriormente son utilizados como instrumentos del ataque final sin que sus propietarios sepan que están siendo cómplices de tal hecho. Por ello, para identificar a su atacante tendrá que verificar y validar la dirección IP obtenida.

e. Se puede emplear técnicas hacker para identificar al atacante ya que el equipo del mismo debe tener inevitablemente un puerto que se encuentre esperando noticias o buscando víctimas. Nmap

f. Averiguar el perfil del atacante, se puede encontrar con los siguientes tipos:
Hackers: personas con conocimientos en técnicas de programación, redes, Internet y sistemas operativos, sus ataques son en sentido ideológico y pacifista.

ScriptKiddies: son personas nuevas que han saltado a la escena de la delincuencia informática recientemente. Se trata de jóvenes que con unos conocimientos aceptables en Internet y programación emplean herramientas ya fabricadas por otros para realizar ataques y "ver qué pasa".

Profesionales: son personas con muchísimos conocimientos en lenguajes de programación, redes y su equipamiento (routers, firewall, etc.), Internet y sistemas operativos tipo Unix.

A.5 Evaluación del impacto causado al sistema

El análisis forense ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron al sistema. Esto permitirá evaluar el ataque cometido a los equipos y realizar una estimación del impacto causado. Generalmente se pueden dar dos tipos de ataques:

a. Ataques pasivos: en los que no se altera la información ni la operación normal de los sistemas, limitándose el atacante solo a fisgonear.

b. Ataques activos: en los que se altera la información, y en ocasiones seriamente, la capacidad de operación del sistema.

Se deberá tener en cuenta los efectos y el impacto que cause el ataque a sistemas, servidores de Bases de Datos, servidores WEB, cortafuegos, router con la finalidad de ser un aporte, presentando los daños encontrados, al personal de seguridad informática de la institución atacada o en último de los casos a la compañía de seguros de la misma.

2.2.9. Presentación de evidencia digital

Esta es la fase final de la investigación forense informática ya que se presentan los resultados y hallazgos del investigador. Tan pronto como el incidente haya sido detectado es importante tomar nota sobre las actividades que se llevan a cabo, cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta finalizar la presentación, la misma debe ser entendible, creíble, confiable y convincente, es decir se deberá especificar claramente los procedimientos y las técnicas utilizadas para recolectar, preservar y filtrar la evidencia de tal manera que sea legalmente aceptable para ser presentadas a las entidades investigadoras y judiciales.

A.1 Utilización de formularios de registro del incidente

La aplicación de formularios ayudará a presentar una resolución del incidente mediante la presentación de informes uno Técnico y otro Ejecutivo. estos formularios deben ser llenados por departamentos o entidades afectadas o por el equipo que gestiona el incidente, los formularios que se deben preparar son:

i. Documento de custodia de la evidencia.
ii. Formulario de identificación de equipos y componentes.
iii. Formulario de incidencias.
iv. Formulario de publicación del incidente.
v. Formulario de recogida de evidencias.
vi. Formulario de discos duros.

A.2 Informe técnico

Este informe consiste en una exposición detallada del análisis efectuado. Deberá describir en profundidad la metodología, técnicas y hallazgos del equipo forense. Deberá contener, al menos, los siguientes puntos: (Delgado, 2007)

Tabla 2.07 Informe técnico

Antecedentes del incidente	Información del sistema analizado	Descripción de los hallazgos
Recolección de los datos	Características del SO	Huellas de la intrusión
Descripción de la evidencia	Aplicaciones	Herramientas usadas por el atacante
Entorno del análisis	Servicios	Alcance que ha tenido el delito
Descripción de las herramientas	Vulnerabilidades	El origen del ataque
Análisis de la evidencia	Metodología	Cronología del delito
		Conclusiones
		Recomendaciones específicas
		Referencias

Fuente: Análisis forense digital, (Delgado, 2007)

A.3 Informe ejecutivo

Este informe es un resumen del análisis efectuado a las evidencias digitales, el mismo deberá:

a. Ser redactado en un lenguaje común que sea legible para cualquier persona.

b. No ser escrito de manera técnica.

c. Exponer los hechos más destacables de lo ocurrido en el sistema analizado.

d. Constará de pocas páginas, entre tres y cinco,

e. Deberá ser de interés para exponer lo sucedido a personal no especializado en sistemas informáticos, como el departamento de Recursos Humanos, Administración e incluso algunos directivos.

Tabla 2.08 Informe ejecutivo se debe describir

Motivos de la intrusión.	Desarrollo de la intrusión.	Resultados del análisis.	Recomendaciones.

Fuente: http://velezconde.wordpress.com/844-2/

A.3.1 Características

a. Interrumpe el proceso de recolección de evidencias

b. Incrementa los tiempos necesarios de dedicación a un caso

c. Genera dudas sobre un proceso forense o testimonio

d. Afecta la ejecución y utilización de las herramientas forenses

e. Evita la detección de alguna clase de evento ocurrido

La informática forense posee aspectos positivos y negativos tales como:

A.3.2 Positivos

a. Replantean y validan: procesos forenses, herramientas forenses y habilidades.

A.3.3 Negativos

a. Pueden exonerar a un culpable.

b. Pueden inculpar a un inocente.

c. Afectar al proceso forense.

A.3.4 Nivel físico y lógico

Física: a través de campos magnéticos (Deggauser), Guardian Dog (dispositivo magnético).

Lógica: cambio de la composición de los datos, sobrescribir datos (Metada, Data), a más de eliminar las referencias de los datos.

Wipe (Liberar): sobrescribir los datos mediante la utilización de algoritmos, a continuación, se listan los métodos utilizados para esto algoritmos y su nivel de segurida.

Tabla 2.09 Nivel de seguridad de métodos anti-forenses

Método	Nivel de seguridad
Borrado rápido	Bajo
RCMP TSSIT OPS-11	Medio
DoD Simple	Medio
DoD 5220 M	Medio
Gutman	Alto
PRNG Stream	Medio - Alto

Fuentes: Álvarez y Guamán "Metodología, Estrategias y Herramientas de la Informática Forense Aplicables Para la Dirección Nacional de Comunicaciones y Criminalística de la Policía Nacional", Cuenca, Febrero 2008

El nivel de complejidad al usar estas herramientas es sencillo, y la recuperación de estos datos es casi imposible, una de las posibles soluciones ante este tipo de ciencia Anti – Forense es Análisis Magnético.

2.2.10 Sintaxis de un ataque informático o vector de ataque

A.1 Seguridad

Es una práctica orientada a la eliminación de las vulnerabilidades para evitar o reducir la posibilidad que las potenciales amenazas se concreten se presenta el flujo de los atacantes en la Figura 2.03 (Esteban Vélez, 2014)

Figura 2.03 Flujo de ataque

Fuente: http://velezconde.wordpress.com/844-2/

A.2 Amenazas

Entrada: información sobre las amenazas obtenida de los propietarios de los activos, de los usuarios, de la revisión de incidentes, y de otras fuentes, incluidos los catálogos de amenazas externas.

Acción: se deberían identificar las amenazas y sus orígenes (se relaciona con la norma ISO/IEC 27001, numeral 4.2.1 d) 2)).

A.2.1 Guía para la implementación

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Es recomendable identificar tanto los orígenes de las amenazas accidentales como de las deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización. Las amenazas se deberían identificar genéricamente y por tipo (por ejemplo, acciones no autorizadas, daño físico, fallas técnicas) y, cuando sea adecuado, las amenazas individuales dentro de la clase genérica identificada. Esto significa que ninguna amenaza se pasa por alto, incluidas las inesperadas, pero teniendo en cuenta que el volumen de trabajo requerido es limitado.

Algunas amenazas pueden afectar a más de un activo. En tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

La entrada para la identificación de las amenazas y la estimación de la probabilidad de ocurrencia se puede obtener de los propietarios o los usuarios del activo, del personal de recursos humanos, del administrador de las instalaciones y de especialistas en seguridad de la información, expertos en seguridad física, área jurídica y otras organizaciones que incluyen organismos legales, bien sea autoridades, compañías de seguros y autoridades del gobierno nacional. Los

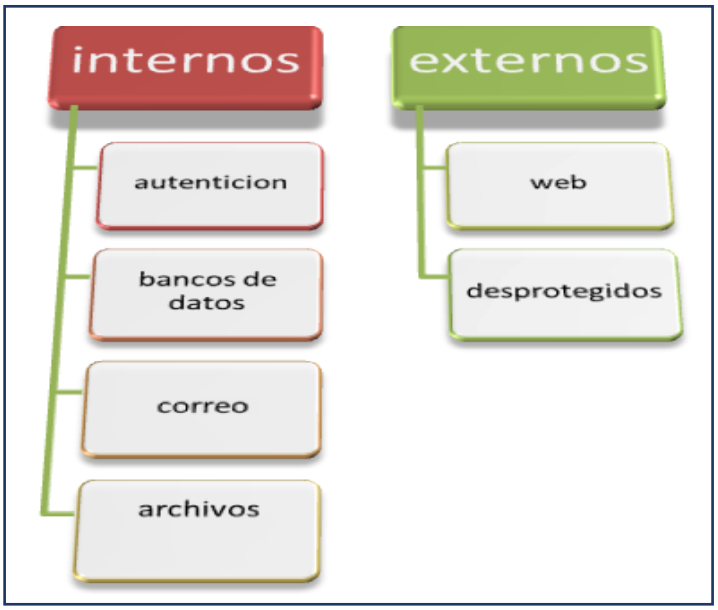
aspectos ambientales y culturales se deberán tener en cuenta cuando se consideran las amenazas.

La experiencia interna obtenida de los incidentes y las valoraciones anteriores de las amenazas, se deberían tomar en consideración en la valoración actual. Podría ser valioso consultar otros catálogos de amenazas (pueden ser específicas para una organización o un negocio) para completar la lista de amenazas genéricas, cuando sea pertinente. Los catálogos y las estadísticas sobre las amenazas están disponibles en organismos industriales, del gobierno nacional, organizaciones legales, compañías de seguros, etc.

Cuando se utilizan catálogos de amenazas o los resultados de valoraciones anteriores delas amenazas, es conveniente ser consciente de que existe un cambio continuo de las amenazas importantes, en especial si cambia el ambiente del negocio o los sistemas de información.

Salida: una lista de las amenazas con la identificación del tipo y el origen de la amenaza. (SS-ISO / IEC 27005: 2013, 2011)Se muestra en la figura 2.04

Figura 2.04 Amenaza



Fuente: http://velezconde.wordpress.com/844-2/

A.3 Vulnerabilidades

Entrada: lista de las amenazas conocidas, lista de los activos y los controles existentes.

Acción: se deberían identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o la organización (se relaciona con ISO/IEC27001, numeral 4.2.1 d) 3)).

A3.1 Guía para la implementación

Se pueden identificar vulnerabilidades en las siguientes áreas

a. organización;

b. procesos y procedimientos;

c. rutinas de gestión;

d. personal;

e. ambiente físico;

f. configuración del sistema de información;

g. hardware, software o equipo de comunicaciones;

h. dependencia de partes externas.

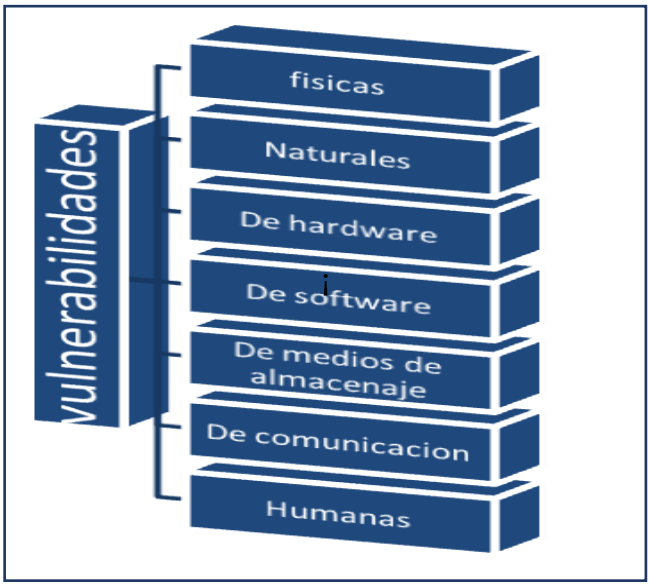
La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios. Conviene anotar que un control implementado de manera incorrecta o que funciona mal, o un control que se utiliza de modo incorrecto podrían por sí solo constituir una vulnerabilidad. Un control puede ser eficaz o ineficaz dependiendo del ambiente en el cual funciona. Por el contrario, una amenaza que no tiene una vulnerabilidad correspondiente puede no resultar en un riesgo.

Las vulnerabilidades pueden estar relacionadas con las propiedades de los activos que se pueden usar de una manera, o para un propósito, diferente del previsto cuando se adquirió o se elaboró el activo. Las vulnerabilidades que se originan desde fuentes diferentes se deben considerar, por ejemplo, aquellas intrínsecas o extrínsecas al activo. Ejemplos de vulnerabilidades y métodos para la valoración de la vulnerabilidad.

Salida: una lista de las vulnerabilidades con relación a los activos, las amenazas y los controles; una lista de las vulnerabilidades que no se relacionen con ninguna

amenaza identificada para revisión. (SS-ISO / IEC 27005: 2013, 2011) Se muestra en la figura 2.05

Figura 2.05 Vulnerabilidades

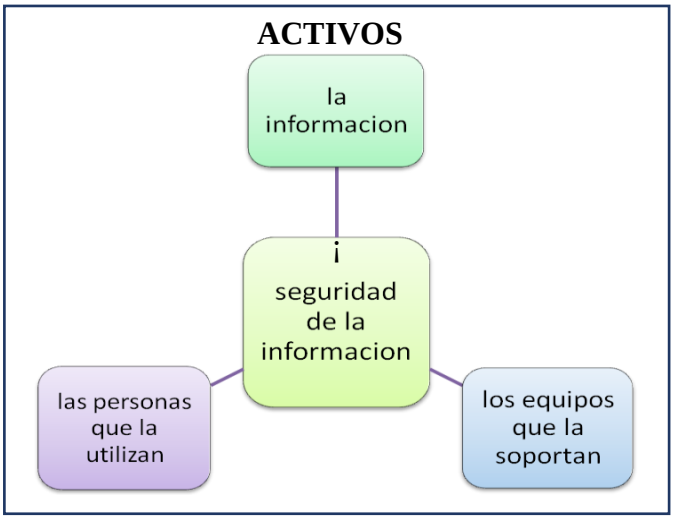


Fuente: http://velezconde.wordpress.com/844-2/

A.3.1 Disponibilidad

La información llega en el momento oportuno. Se muestra en la figura 2.06

Figura 2.06 Activos



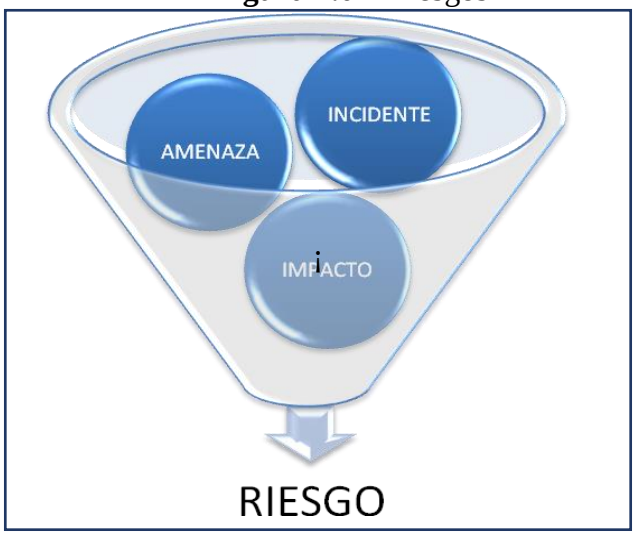
Fuente: http://velezconde.wordpress.com/844-2/

a. Información

b. Equipo que la soportan, Software, Hardware, Organización

c. Personas que los utilizan o usuarios:

Figura 2.07 Riesgos



Fuente: http://velezconde.wordpress.com/844-2/

A.4 Riesgo

Es la probabilidad que las amenazas exploten los puntos débiles, causando pérdidas a daños en los activos e impactos afectando la confidencialidad, la integridad y la disponibilidad de la información. Se muestra en la figura 2.07, figura 2.08

Figura 2.08 Ataque

Fuente: http://velezconde.wordpress.com/844-2/

Figura 2.09 Planteamiento de la situación

Fuente: http://velezconde.wordpress.com/844-2/

A.5 Reconocimiento

Fase preliminar con la información, busca un vector de ataque. Se muestra en la figura 2.10

Figura 2.10 Reconocimiento

Fuente: http://velezconde.wordpress.com/844-2/

Recursos para obtener esta información

Ingeniería social:

Localizar conversación con personas que están en interacción con el objetivo recursos que se pueden utilizar:

Tabla:2.10 Objetivo recursos

teléfono	correo	electrónico	físicamente	internet

Fuente: http://velezconde.wordpress.com/844-2/

Obtener

1. Números de teléfono secretos
2. Contraseñas

3. Cuentas de usuarios
4. Encargados de recursos humanos.

Dumpster drive: revisar en la basura del objetivo en busca de información sensible, que de una u otra forma se descartó de manera incorrecta localizar.

1. Información sobre un objetivo
2. Listas de empleados y sus correos electrónicos.
3. Tecnología que emplean, software, hardware.
4. Rangos de direcciones IP
5. Servicios disponibles
6. Nombre de dominio

Las técnicas de reconocimiento de forma general se clasifican:

Pasivas: En esta forma no se interacciona de forma directa con el sistema.

Tabla: 2.11 Las técnicas de reconocimiento

Activas	Seguridad
Mapa de la red	Políticas para proteger los activos
Equipo accesible	Guía para conocer el uso de las políticas
Sistemas operativos	Responsabilidades a cada usuario
Puertos abiertos	

Fuente http://velezconde.wordpress.com/844-2/

A.6 Exploración

Fase donde se va utiliza la información recogida en la fase de reconocimiento Se muestra en la figura 2.11

Figura 2.11 Exploración

Fase pasiva——————————fase activa

Fuente: http://velezconde.wordpress.com/844-2/

1. Escáner de red, trazado de rutas
2. Escáner de host
3. Escáner de puertos y servicios (ejecución, escucha)
4. Escaneo de manera sigilosa
5. Comandos del sistema operativo
6. Vulnerabilidades
7. Base de datos (whois ripe)

Obtener

1. Software utilizado
2. Versiones del sistema
3. Infraestructura en la red
4. Routers y cortafuegos

Ping, Fping, Hping, Xprobe, P0f, Nmap, análisis metadatos, OSINT, traceroute, descubrimiento con DNS, dig

Seguridad

1. Ejecutar los servicios y aplicaciones necesarias.
2. IDS, si el escaneo se realiza muy rápido puede ser detectado
3. Aplicar las actualizaciones a todos los paquetes que tenga disponibles

A.7 Enumeración

Obtener más información sobre el objetivo ya identificado y escoger las más apropiadas para el acceso, en esta fase es donde el atacante ya está en el objetivo. Se muestra en la figura 2.12

Figura 2.12 Enumeración

Fuente: http://velezconde.wordpress.com/844-2/

Obtener

1. Conexiones activas al sistema
2. Peticiones directas (sistemas de seguridad) enumeración

Recursos de red, Recursos compartidos. Usuarios, Nombres de grupos acceso.

El medio de ataque:

Tabla: 2.12 Recursos de red

Red inalámbrica	Internet	Lan

Fuente: http://velezconde.wordpress.com/844-2/

Obtener el acceso en el objetivo. Recursos

Tabla: 2.13 Recursos vulnerabilidad

Vulnerabilidad	Exploit	Acceso	Secuestro de sesión

Fuente: http://velezconde.wordpress.com/844-2/

A.8 Escalamiento

Figura 2.13 Escalamiento

Fuente: http://velezconde.wordpress.com/844-2/

Lo que el atacante realizará después de obtener acceso a un sistema:

- privilegios y derechos en caso de que no sea administrador

En esta fase el intruso intentara obtener otras formas de acceso.

Obtener

1. agregar usuarios con altos privilegios
2. robar contraseñas de otros usuarios

Recursos

Tabla: 2.14 Fase del intruso

Sniffers	Keyloggers	Rootkits	Troyanos

Fuente: http://velezconde.wordpress.com/844-2/

Un rootkit es un conjunto de herramientas que le permite al atacante ocultar procesos, sesiones y conexiones.

A.9 Eliminación del rastro

Fase a todas las acciones que realizará el atacante para cubrir su rastro y poder incrementar el mal uso del sistema sin ser detectado. Eliminación de evidencia del ataque

Una fase opcional en la que puede incurrir el atacante es colocar puertas traseras. Se muestra en la figura 2.14

Figura 2.14 Puerta Trasera

Fuente: http://velezconde.wordpress.com/844-2/

Las puertas traseras son un método utilizado para regresar al sistema sin volverlo a explotar.

1. Estenografía
2. Túneles en TCP. (Esteban Vélez, 2014)

A.10 Vector de ataque web con social-engineer toolkit (SET)

Social-Engineer Toolkit (SET) es un conjunto de colección de scripts en Python especialmente diseñadas para realizar ataques de ingeniería social en procesos de auditorías de seguridad. Esta herramienta fue creada por David Kennedy (ReL1K), el mismo creador de otra herramienta muy popular llamada Fast-Track, que también es una herramienta que automatiza algunos ataques más comunes y más usados en las pruebas de penetración (penetration test) mediante algunos scripts hechos en Python.

Social-Engineer Toolkit (SET) nos permite crear archivos PDF, sitios web falsos y enviar correos electrónicos con código malicioso incrustado, por cierto, también se integra con el Metasploit Framework.

Como bien sabrán y se han dado cuenta, la ingeniería social no es nada nuevo, los ataques de ingeniería social están ahora en su punto más alto, es decir en pleno auge y siempre han sido un gran riesgo para muchas organizaciones. Una persona que está tratando de convencer a otras personas para que realicen actos que normalmente no harían es muy antigua como la misma historia de la tierra:

Muchos creen que la ingeniería social es uno de los mayores riesgos que enfrentan

las organizaciones actualmente, ya que es muy difícil proteger a las organizaciones de estos ataques. Por ejemplo, puede que se acuerden del ataque a Google, del llamado “Operación Aurora” (también conocida como Comele o Hydraq) en el que la técnica de ingeniería social fue utilizada para atacar a Gmail y otras fuentes de Google.

Un vector de ataque es la vía que se utiliza para obtener información o acceso a un determinado sistema y la herramienta Social-Engineer Toolkit (SET) clasifica a los ataques por vectores de ataques web, correo, electrónico y también los ataques basados en USB. Utiliza correo electrónico, sitios web falso y otros vectores que típicamente lo que hacen es engañar a los usuarios a comprometer la información sensible. Cada vector puede tener éxito o, todo lo contrario, dependiendo del objetivo a atacar y también el tipo de comunicación utilizada. SET también viene con correos electrónicos y plantillas de páginas web ya predefinidas que pueden ser utilizadas para los ataques de ingeniería social, también utiliza la herramienta Metasploit Framework. Así que en este post se mostrara un ejemplo de vector de ataque basado en web, manos a la obra y listos para la primera prueba.

2.2.11 Aspectos tecnológicos

2.2.11.1 Herramientas de adquisición de datos

Dentro de la informática forense existe una actividad primordial la investigación de los soportes de datos, la cual sigue siendo clave en las evidencias que se presentan ante la justicia, ya que en ella se pueden hallar datos los cuales fueron

alterados o removidos. Al ver la funcionalidad de esta actividad se piensa solo que el soporte va dirigido a los discos duros, pero en la actualidad y con la evolución de los dispositivos, ya se pueden realizar estas adquisiciones a discos externos, tabletas, teléfonos móviles, dispositivos USB y en general todo dispositivo que permita el almacenamiento de información. 4.11 procedimiento de adquisición. El investigador encargado trabaja con una imagen a bajo nivel la cual ya se encuentra guardada y sellada en un depósito de pruebas, esto para tener un mejor control de quien las utiliza, ante todo se debe tener la información de quien la utiliza para evitar posibles alteraciones de información.

2.2.11.2 Adquisición por hardware

Existe elementos hardware que permiten realizar estos procesos de forma cómoda, precisa y con altas garantías. Aunque no es la solución más económica si es la que ofrece mayor profesionalidad y seguridad para un analista forense. Hay que tener presente no obstante que la diversidad de tipos de discos existentes en el mercado y su evolución, podría llegar a suponer que un determinado hardware pudiera no ser válido en un proceso de copiado al no disponer de los accesorios adecuado para copiar un tipo de disco específico.

Para realizar esta adquisición, se debe realizar la extracción del disco duro del equipo investigado, observar si el disco presenta fallas de arranque o está en mal estado, viendo esto se puede utilizar un equipo alterno en el cual están instaladas las herramientas forenses para realizar la copia del disco duro, el disco clonado debe ser colocado como disco esclavo. Se debe tener mucho cuidado con esta esta

implementación para que no se vaya a realizar escritura en el disco esclavo, porque puede afectar la investigación.

Existen dispositivos Firewire para la lectura de discos IDE y/o SATA **Figura 2.15, Figura 2.16**. Estos permiten utilizar el disco duro en modo lectura para evitar que se afecte la información del disco. (Muñoz, 2015)

Figura 2.15. Disco duro sata de laptop conectado a Equipo Firewir

Fuente: Elaboración propia

Figura 2.16. Disco duro sata de pc conectado a Equipo Firewir

Fuente: Elaboración propia

Pero existen equipos especializados sin necesidad de utilizar los ordenadores, son como mini ordenadores los cuales son capaces de realizar copia de los datos a gran velocidad y permite la extracción de los hashes, realizan registros de actividades y permiten la compresión, SUPERIMAGER ™ 12″ Unidad con pantalla táctil protegida e interfaces USB 3.0, SAS/SATA-3. Figura 10. Una computadora forense completa de investigación informática de campo y plataforma de unidad de análisis, es un sistema de análisis portable de campo de alta velocidad, siendo a su vez un equipo forense de adquisición de datos en la misma plataforma y, con cuatro puertos de interfaz de 6Gb / s SAS / SATA y cuatro puertos USB 3.0. La unidad es compatible con múltiples fuentes para el funcionamiento simultáneo de objetivos múltiples. (Muñoz, 2015)

Figura 2.17. Superimager™ 12″

Fuente: Estudio de metodología de análisis forense ante incidentes de ciberseguridad

2.2.11.3 Adquisición por software

Este soporte también se puede realizar en el ordenador afectado sin necesidad de retirar el disco duro, se utiliza Live CD Linux los cuales incluyen herramientas de copiado a bajo nivel, distribuciones como Kali Linux Figura 3. Son de ayuda para realizar esta obtención de datos ya que tiene herramientas forenses y un modo boot forense que pueden ser de ayuda.

Al realizar esta opción se debe tomar muchas precauciones para evitar que se escriba dentro del disco. (Muñoz, 2015)

i. Social-Engineer Toolkit (SET) versión 2.5 (incluida en BackTack 5, Kali Linux)

ii. Metasploit Framework versión 4.2.0 (incluida en BackTack 5, Kali Linux)

iii. VMware Workstation versión 10

iv. Windows XP SP3 (La víctima o el objetivo a atacar)

v. Backtrack 5 R1 (Equipo atacante o penetration testers machine)

2.2.12 Delitos informáticos

Los delitos informáticos, son aquellos actos delictivos que en su realización hacen uso de las tecnologías electrónicas ya sea como método, medio o fin y los delitos en que se daña estos equipos, redes informáticas, o la información contenida en ellos, vulnerando bienes jurídicos protegidos. Los tipos de Delitos son:

Tabla: 2.15 Delitos informáticos

Manipulación de computadoras	**Falsificaciones informáticas**	**Fraudes en Internet**	**Seguridad Lógica**	**Propiedad Intelectual**	**Accesos no autorizados**	**Otros delitos**
Manipulación de datos de entrada	Cuando se alteran datos de los documentos almacenados en forma computarizada	Carding: uso de tarjetas de crédito ajenas o fraudulentas	Sabotaje informático mediante: virus, gusanos, ataques de denegación de servicio, sustracción de datos, hacking, descubrimiento y revelación de secretos, suplantación de personalidades, sustracción de cuentas de correo electrónico.	Piratería de programas de ordenador, de música y de productos cinematográficos	Acceso no autorizado a servicios y sistemas informáticos	A través de Internet se pueden comprar drogas ilícitas, armas, productos
Manipulación de programas	Cuando se usan las computadoras para efectuar falsificaciones de documentos de uso comercial.	Ventas de productos que nunca llegan a entregarse	Delitos de injurias, calumnias y amenazas a través del e-mail, news, foros, chats o SMS.	Robos de código.	Piratas informáticos o hackers	farmacéuticos no regulados, documentos falsos.
Manipulación de los datos de salida		Estafas, subastas ficticias			Reproducción no autorizada de programas informáticos de protección legal.	Pornografía infantil (producción, distribución y posesión).
Daños o modificaciones de programas o datos computarizados		Phising: redirección mediante correo electrónico a falsas páginas simuladas trucadas.				

Fuente: http://www.tuabogadodefensor.com/delitos-informaticos/#delitos

2.2.13 Reglas de la informática forense

Las reglas generales para aplicar a cualquier proceso en la informática forense, su cumplimiento es fundamental para asegurar la aceptación, recepción de cualquier evidencia en un juzgado. Dado que la metodología que se emplee será determinada por el especialista forense, el proceso escogido debe aplicarse de forma que no se vulneren las reglas básicas de la informática forense.

Esencialmente, las reglas de la informática forense son:

A.1 Regla 1: Minimizar el manejo del original

La aplicación del proceso de la informática forense durante el examen de los datos originales se deberá reducir al mínimo posible. Esto se puede considerarse como la regla más importante en la informática forense. Cualquier análisis debe dirigirse de manera tal que minimice la probabilidad de alteración, esto se logra copiando el original y examinando luego los datos duplicados.

La duplicación de evidencia tiene varias ventajas:

a. Asegurar que el original no será alterado en caso de un uso incorrecto o inapropiado del proceso que se aplique.

b. Permitir al examinador aplicar diferentes técnicas en casos dónde el mejor resultado no está claro. Si durante tales ensayos los datos se alteran o se destruyen, simplemente se recurre a otra copia.

c. Permite a varios especialistas de informática forense trabajar en los mismos datos, o en partes de los datos, al mismo tiempo.

d. Asegurar que el original se ha preservado en el mejor estado posible para la presentación en un juzgado.

Aunque hay ventajas al duplicar la evidencia, hay también desventajas.

a. La duplicación de evidencia debe realizarse de la mejor manera y con herramientas, que aseguren que el duplicado es una copia perfecta del original. El fracaso para autenticar el duplicado apropiadamente, producirá un cuestionamiento sobre su integridad, lo que lleva inevitablemente a preguntar por la exactitud y fiabilidad del proceso del examen y los resultados logrados.

b. Duplicando el original, se está agregando un paso adicional en el proceso forense, a más de que la recreación de este ambiente se torna una tanto difícil.

Esto implica que se requieren más recursos y tiempo extra para facilitar el proceso de duplicación, y la metodología empleada debe extenderse para incluir el proceso de la duplicación.

A.2 Regla 2: Documentar los cambios. Cuando ocurren cambios ya sea en la evidencia original o duplicados durante un examen forense, la naturaleza, magnitud y razón para ellos debe documentarse apropiadamente, esto se aplica tanto a nivel físico como lógico. Adicionalmente, el perito debe ser capaz de

identificar correctamente la magnitud de cualquier cambio y dar una explicación detallada de por qué era necesario el mismo, este proceso depende directamente de las habilidades y conocimiento del investigador forense.

Durante el examen forense este punto puede parecer insignificante, pero se vuelve un problema crítico cuando el examinador está presentando sus resultados en un juicio.

Aunque la evidencia puede ser legítima, las preguntas acerca de las habilidades del examinador y conocimiento pueden afectar su credibilidad, así como la confiabilidad del proceso empleado. Con una duda razonable, los resultados del proceso forense, en el peor de los casos, se considerarán inaceptables. Aunque la necesidad de alterar los datos ocurre pocas veces, hay casos dónde al examinador se le exige el cambio para facilitar el proceso del examen forense.

A.3 Regla 3: Cumplir con las reglas de evidencia. Para la aplicación o el desarrollo de herramientas y técnicas forenses se deben tener en cuenta las normas pertinentes de evidencia.

a. Asegurar que el uso de herramientas y técnicas no disminuye la admisibilidad del producto

b. Presentar la información de una manera que sea tan representativa del original como sea posible. Es decir, el método de presentación no debe alterar el significado de la evidencia.

A.4 Regla 4: No exceda su conocimiento El especialista en informática forense no debe emprender un examen más allá de su nivel de conocimiento y habilidad. Es esencial que el perito sea consciente del límite de su conocimiento y habilidad. Llegado a este punto, dispone de las siguientes opciones:

a. Detener cualquier examen y buscar la ayuda de personal más experimentado.

b. Realizar la investigación necesaria para mejorar su propio conocimiento, para que le permita continuar el examen y se alcance a obtener lo que se busca.

Es indispensable que el examinador forense puede describir correctamente los procesos empleados durante un examen y explicar de la mejor manera la metodología seguida para ese proceso. El fracaso para explicar competentemente y con precisión, la aplicación de un proceso puede producir cuestionamientos sobre el conocimiento y credibilidad del examinador.

Los análisis complejos deben ser emprendidos por personal calificado y experimentado que posea un apropiado nivel de entrenamiento. Adicionalmente, dado que la tecnología está avanzando continuamente, es importante que el examinador reciba entrenamiento continuo.

2.2.14 Aspectos Normativos

De conformidad con lo establecido en el Artículo Único de la Ley Nº 26633, corresponde al Ministerio de Justicia y Derechos Humanos editar la "Compilación de la Legislación Peruana", lo que comprende a todas las leyes, decretos legislativos y demás normas con rango de ley vigentes, debidamente concordadas, así como sus respectivos reglamentos y las disposiciones derogadas, con indicación del número y fecha de publicación.

En concordancia con lo anterior, el Literal j) del Artículo 7º de la Ley Nº 29809 - Ley de Organización y Funciones del Ministerio de Justicia y Derechos Humanos señala que es una función específica del ministerio sistematizar la legislación e información jurídica de carácter general.

En atención al mandato contenido en dichas normas, la Dirección Nacional de Asuntos Jurídicos del Ministerio de Justicia y Derechos Humanos pone a disposición de la ciudadanía y la comunidad jurídica nacional el Sistema Peruano de Información Jurídica - SPIJ, el cual contiene en formato electrónico y de manera sistematizada la legislación nacional, concordada y actualizada periódicamente, con carácter de edición oficial conforme a lo establecido en el Decreto Supremo Nº 001-2003-JUS publicado el 06 de febrero de 2003.

El SPIJ está diseñado con la finalidad de acceder fácilmente a las disposiciones constitucionales, legales y reglamentarias vigentes. Asimismo, contiene una sección denominada "Compendios de legislación por materias" que permite al lector el estudio de la normativa sobre algún tema jurídico particular que sea de su interés académico o profesional.

De esta manera, el Ministerio de Justicia y Derechos Humanos cumple con su función de promover la difusión y sistematización de la legislación nacional, así como facilita su estudio y accesibilidad (Ministro de Justicia y Derechos Humanos, 2014).

Lima, 2014

Daniel A. Figallo Rivadeneyra,

Ministro de Justicia y Derechos Humanos

Tommy R. Deza Sandoval,

Director General de Desarrollo y Ordenamiento Jurídico

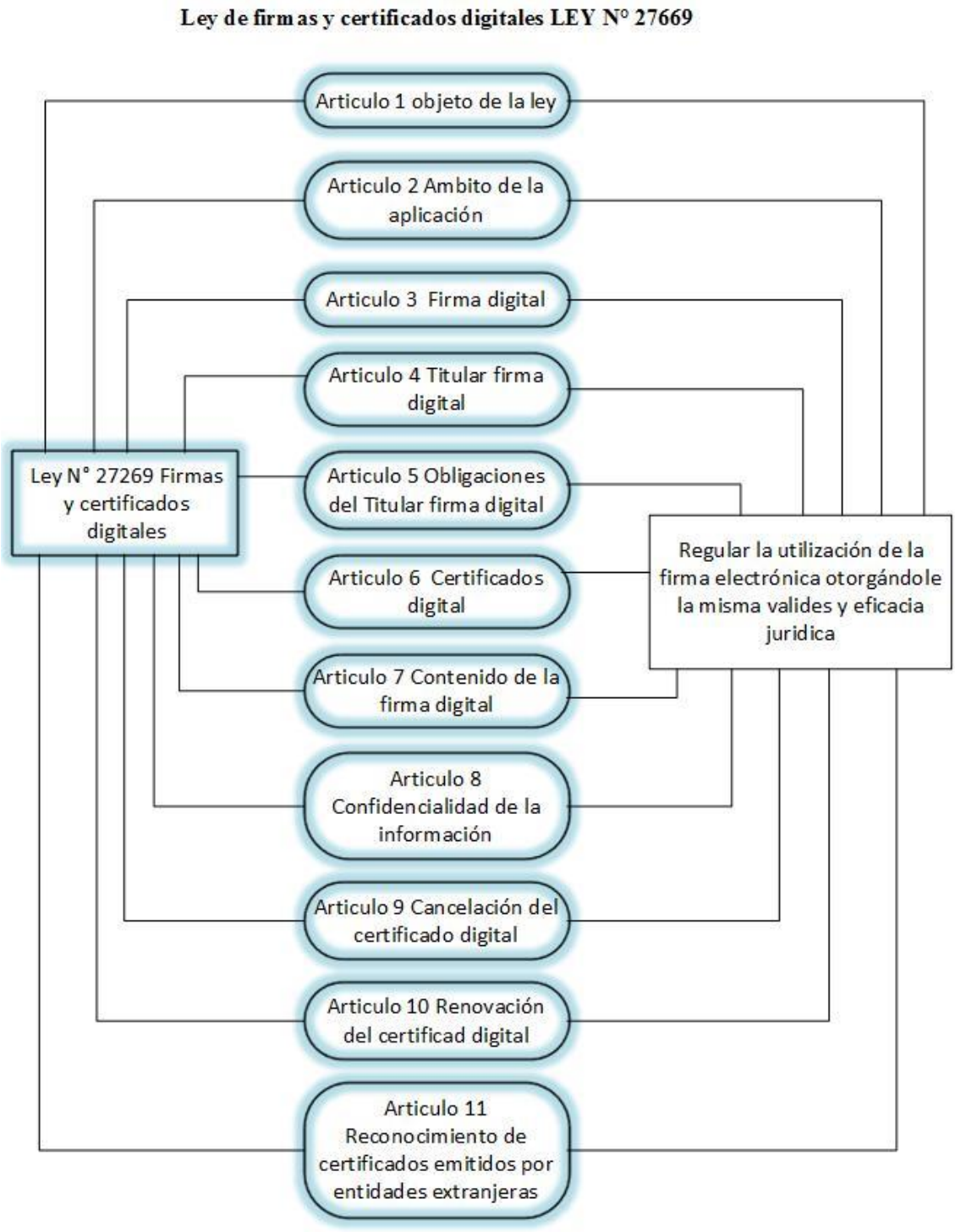
Carlos Enrique Cobeñas Castillo,

Director de Sistematización Jurídica y Difusión

Figura: 2.18 Sistema peruano de información judicial,

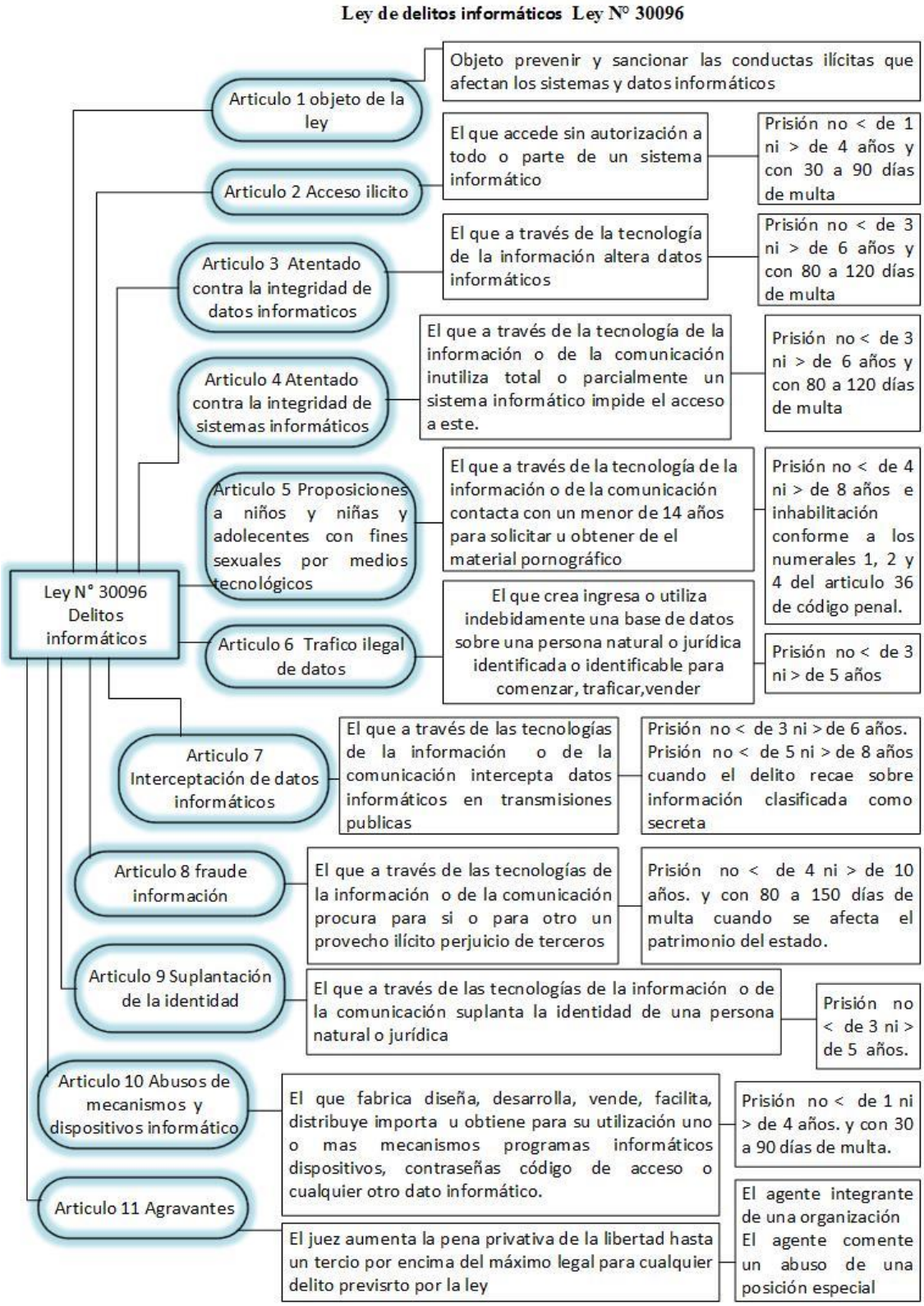
Fuente: Sistema Peruano de Información Judicial (SPIJ) (Ministro de Justicia y Derechos Humanos, 2014)

Figura 2.19 Ley de firmas y certificados digitales Ley N° 27669



Fuente: SPIJ

Figura 2.20 Ley de delitos informáticos Ley N° 30096



Fuente: SPIJ

2.3 Definición de términos

Acústica forense, imagen forense e informática forense: En el siglo de la información y las comunicaciones, no podemos obviar las nuevas formas de delito que surgen al abrigo del progreso. Se hacen un sitio en nuestras vidas con un claro propósito de "Sabotear", en primera instancia el sentido de seguridad que da estar rodeado de "Tecnología inquebrantable" en cada una de nuestras acciones cotidianas. (Ferro Veiga, 2015)

Por tanto, especialización versus especialización debe ser el caballo de batalla frente a nuestro objetivo a batir. (Ferro Veiga, 2015)

NoScrip: que permite controlar todo lo que va ejecutar una página web al acceder a ella, como códigos JavaScript, extensiones y objetos realizados flash. (Ferro Veiga, 2015)

Listas bancas: es decir el usuario añade manualmente aquellos sitio web de confianza donde está permitida la ejecución de estos códigos. (Ferro Veiga, 2015)

Cadena de custodia: Procedimiento mediante el cual se busca garantizar la integridad de la evidencia digital mediante la documentación detallada de las interacciones y procesos a los que es sometida. (Ferro Veiga, 2015)

Ciberdelincuencia: Es una de las desventajas del uso de Internet. De la misma manera que hay diferentes tipos de delincuencia tradicional, la delincuencia

cibernética tiene un gran número de formas. Hay tres grandes categorías: delitos contra las personas, la propiedad y el gobierno. Dentro de estas categorías, hay varios métodos de ataque. (Ferro Veiga, 2015)

Criminología y Criminalísticas: Que introducen a todos sus conocedores en una actualización permanente en temas jurídicos, tecnológicos, humanos y organizacionales. (Cano Martinez, 2015)

DDoS: siglas en inglés para Denegación de Servicio Distribuido. Es un tipo de ataque en el que se utilizan diferentes equipos para hacer muchas peticiones a un recurso con el fin de bloquear las peticiones legítimas. (Ferro Veiga, 2015)

Evidencia digital: Es la materia para los investigadores donde la tecnología informática es parte fundamental de proceso. (Cano Martinez, 2015)

Firma hash: cadena de longitud fija producto resultante de la aplicación de una función matemática irreversible a una cadena de longitud variable

Hactivista: grupo de personas organizadas que realiza protestas a través de Internet, realizando ataques a sitios web de organizaciones con ideales contrarios a los suyos.

Man-in-the-middle: ataque en el que un intruso es capaz de leer, insertar y modificar mensajes en una comunicación entre dos partes sin que estas se den cuenta de la presencia del intruso.

Phishing: Es más que conocida por los usuarios de la red: llega a un e-mail de su banco online solicitando al cliente que por motivos de seguridad o mantenimiento confirme sus datos personales dicha web no pertenece, por supuesto a una verdadera entidad bancaria sino que es una copia del original creada para "Pescar" datos bancarios y despellejar a los confiados dueños (Ferro Veiga, 2015)

Script: script (VBS, JavaScript, Bat, PHP, etc.). Ellos infectan otros script, ej. Archivos de instrucción y servicios de Windows o Linux, o forman parte de virus multi-componentes. Los virus script pueden infectar otros formatos de archivo, tales como HTML, si el formato de archivo permite la ejecución de scripts. (Ferro Veiga, 2015)

SHA1: siglas en inglés para Algoritmo de Hash Seguro. Segunda versión del algoritmo desarrollado por la Agencia de Seguridad Nacional de Estados Unidos y publicado por el Instituto Nacional de Estándares y Tecnología.

Criptografía: Actualmente se encuentra resuelto mediante el uso de diversos procedimientos de uso de claves secretas, tales como los mecanismos de clave pública y privada, así como los mecanismos de confianza, vigencia y revocación de las claves. (Ferro Veiga, 2015)

Deggauser: Sistema de borrado de alta energía, diseñado para eliminar información residente en discos duros o cintas magnéticas.

DMZ: En la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. Un corta fuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección. (Ferro Veiga, 2015)

Exploits y herramientas de hacker: Estas utilidades son diseñadas para penetrar los equipos remotos para usarlos como zombies (usado puerta trasera) o para descargar otros programas maliciosos de los equipo víctima. (Ferro Veiga, 2015)

Freeware: Es un tipo de software de distribución sin costo y por tiempo ilimitado, suele incluir una licencia de uso, que permite su redistribución, pero con algunas restricciones, como no modificar la aplicación en sí, ni venderla. También puede desautorizarse el uso en una compañía con fines comerciales o en una entidad gubernamental.

IDS: Monitorea las actividades a nivel de usuario o procesos y actividades de un sistema (HIDS), o las actividades de una red (NIDS), Cifrado de datos, hace un diagnóstico completo del ataque y en algunos casos puede dar recomendaciones de cómo controlar el ataque. (Cano Martinez, 2015)

Kernel: El hacker instala el rootkit después, obteniendo un acceso similar al del usuario: por lo general, crakeando una contraseña o explotando una vulnerabilidad, lo que permite usar otras credenciales hasta conseguir el acceso de raiz o administrador. (Ferro Veiga, 2015)

Máquinas virtuales: Varios equipos lógicos independientes funcionando sobre un equipo físico. El software que se puede emplear para la creación de plataforma es VMware.

Spoofing: Internet (web spoofing), que imitan grandes webs comerciales. Por su parte, los bancos pueden, asimismo, comprobar la identidad del titular y del comerciante. (Ferro Veiga, 2015)

III METODOLOGIA

3.1 Tipo de investigación

De acuerdo a la orientación o finalidad

Es de carácter **aplicada** en merito a que la investigación depende a priori de la teoría existente en las ciencia ingenieriles y porque además, se tiene interés en su aplicación para desarrollar soluciones a problemas prácticos y porque, analizará las variables identificadas a fin de actuar en la solución del problema mediante la utilización de los conocimientos en la práctica, en la mayoría de los casos, en provecho de la sociedad.

De acuerdo al alcance temporal

Transversal o transeccional, debido a que se mide las variables en un momento especifico, en un punto cronológico.

De acuerdo al nivel o profundidad

Relacional, debido a que revelará las relaciones entre las dos variables, es decir, entre la informática forense y la seguridad informática.

Descriptiva. La investigación responderá a descripciones, pero no de variables individuales sino de sus relaciones midiendo la correlación de variables en un tiempo determinado, sin precisar su sentido de causalidad.

3.2 Diseño de la investigación

La investigación a realizar es de tipo **no experimental y transversal** en razón a que la relación de datos que se llevara a cabo en un momento sin manipular las variables objeto del estudio.

Población

La población está constituida por 45 trabajadores de la Dirección Nacional de Comunicaciones y Criminalística de la PNP, dado que fue proporcionado por la Comandancia

Muestra

En el caso de la muestra, está no requiere ningún cálculo puesto que el número será censal, debido a que los sujetos, todos los trabajadores PNP, constituyen un grupo reducido, asi se trabajó con la totalidad de la población.

La n es 45.

3.3. Instrumentos de recopilación de la información

La técnica a emplear para esta investigación será la **encuesta**. El cuestionario, será el instrumento para la recolección de datos definida como "un conjunto de preguntas respecto a una o más variables a medir", (Sampieri, 2014, pág. 285), utilizando preguntas con escalas tipo Likert, en función a la naturaleza del indicador. La fuente o informante para el caso serán los trabajadores de la citada dirección de la PNP. Se formularán preguntas para la variable independiente y dependiente en función a los indicadores expuestos en el presente.

La fiabilidad del cuestionario se hará a través del estadístico de medida del Alfa de Cronbach. Su validez como instrumento se refiere al grado en que el instrumento mide aquello que pretende medir. Y la fiabilidad de la consistencia interna del instrumento se puede estimar con este recurso estadístico.

3.4. Plan de procesamiento y análisis estadístico de la información

Para el análisis de datos se utilizará el análisis estadístico, a través de la estadística descriptiva para las variables tomadas individualmente y se presentarán en una distribución de frecuencias, específicamente en tablas.

Este análisis se realizará de acuerdo con la codificación que se estableció para la recolección de datos. Se efectuará el registro en una base de datos preparada para las mediciones a través del programa SPSS v23 (*Statistical Package for the Social Sciences*).

Interpretación de datos

Dichos datos luego de ser analizados y procesados mediante los programas anteriormente mencionados, serán presentados en un informe que contendrá tablas descriptivas y cruzadas que proporcionarán una visión más amplia y sencilla sobre los resultados de este trabajo de investigación.

IV RESULTADOS

4.1. Determinación de la relación entre la informática forense y la seguridad informática

4.1.1. Datos Generales

Tabla 4.01 Género

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Masculino	30	66,7	66,7	66,7
	Femenino	15	33,3	33,3	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

De acuerdo a esta tabla, se aprecia que el género masculino es quien lidera el número de trabajadores en la dependencia. Eso se muestra en los dos tercios de la masa labora (66.7%)

Tabla 4.02 Años de labor en la DNCC (agrupado)

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	<= 3	15	33,3	33,3	33,3
	7 - 9	9	20,0	20,0	53,3
	4 - 4	8	17,8	17,8	71,1
	10+	7	15,6	15,6	86,7
	5 - 6	6	13,3	13,3	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

La mayoría de los que laboran están en el rango menor a los 3 años (33%), al tanto que los que tienen de 7 a 9 años también representan un grueso de la masa que laboran (20%)

Tabla 4.03 Grado de instrucción

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Técnica	28	62,2	62,2	62,2
	Univ Titulado	9	20,0	20,0	82,2
	Univ Bachiller	5	11,1	11,1	93,3
	Secundaria	3	6,7	6,7	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

La mayoría del personal que laboran tienen estudios técnicos un 62.2% y los titulados universitarios el porcentaje es 20 %

4.1.2. Resultados sobre las metodologías y herramientas de la informática forense

Tabla 4.04 Se dispone de un servidor o servidores exclusivamente para el tema de la informática forense

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	23	51,1	51,1	51,1
	A veces	11	24,4	24,4	75,6
	Siempre	6	13,3	13,3	88,9
	Casi siempre	3	6,7	6,7	95,6
	Casi nunca	2	4,4	4,4	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

El personal que laboran con todo lo relacionado a informática forense, 51.1% no tienen servidor o servidores y solo un 6.7 % dice que si tiene acceso.

Tabla 4.05 Se cuenta con instalaciones de fibra óptica

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	35	77,8	77,8	77,8
	Quizá no	4	8,9	8,9	86,7
	Sí	3	6,7	6,7	93,3
	Indeciso	2	4,4	4,4	97,8
	Quizá sí	1	2,2	2,2	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

Los trabajadores de la PNP Huaraz no cuenta con servicio de fibra óptica y es un porcentaje de 77,8%.

Tabla 4.06 Esta dirección tiene terminales para el monitoreo del trabajo de informática forense

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	25	55,6	55,6	55,6
	A veces	10	22,2	22,2	77,8
	Casi nunca	6	13,3	13,3	91,1
	Siempre	4	8,9	8,9	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

Los encuestados revelan que a veces se cuenta con un terminal para monitorear el trabajo de informática forense (22.2%), pero nunca en un 55.6%.

Tabla 4.07 A través de un Data Center se logra efectivizar la labor

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	13	28,9	28,9	28,9
	A veces	11	24,4	24,4	53,3
	Siempre	8	17,8	17,8	71,1
	Casi nunca	7	15,6	15,6	86,7
	Casi siempre	6	13,3	13,3	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

A veces intentan efectivizar la labor con un datacenter (24.4%) y nunca hacen uso en un 28.9%

Tabla 4.08 El uso del software se hace gracias al uso de la licencia correspondiente.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nada importante	18	40,0	40,0	40,0
	Muy importante	14	31,1	31,1	71,1
	Importante	6	13,3	13,3	84,4
	Poco importante	5	11,1	11,1	95,6
	Indeciso	2	4,4	4,4	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

Consideran nada importante usar la Licencia respectiva para el uso del software (40.0%), pero hay un 31.1% que si lo toma muy importante usar la respectiva licencia.

Tabla 4.09 Se dispone de software especializado en el tema de la informática forense

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	15	33,3	33,3	33,3
	De acuerdo	9	20,0	20,0	53,3
	Casi de acuerdo	8	17,8	17,8	71,1
	Indeciso	7	15,6	15,6	86,7
	Casi en desacuerdo	6	13,3	13,3	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

El departamento de la PNP de Huaraz no dispone de software especializado un 33.3% y un 13.3% tiene software especializado.

Tabla 4.10 Conozco las normas correspondientes a las prácticas de la informática forense

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	17	37,8	37,8	37,8
	De acuerdo	9	20,0	20,0	57,8
	Indeciso	8	17,8	17,8	75,6
	Casi de acuerdo	8	17,8	17,8	93,3
	Casi en desacuerdo	3	6,7	6,7	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

En cuanto al conocimiento de las normas de la práctica forense se encuentran en desacuerdo un 37.8%, y de acuerdo un 20%.

Tabla 4.11 Cuando se requiere, tenemos el asesoramiento para realizar de manera óptima nuestra labor.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi de acuerdo	14	31,1	31,1	31,1
	En desacuerdo	10	22,2	22,2	53,3
	De acuerdo	10	22,2	22,2	75,6
	Indeciso	7	15,6	15,6	91,1
	Casi en desacuerdo	4	8,9	8,9	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

En cuanto a la asesoría que tienen para desempeñarse mejor, están de acuerdo y en desacuerdo un 22,2% respectivamente, es decir el mismo tamaño muestral revela que tienen asesoría y no tienen asesoría. Los que a veces tienen asesoría es 31.1%.

Tabla 4.12 Constantemente me actualizo en el rubro de la seguridad de información.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi de acuerdo	12	26,7	26,7	26,7
	De acuerdo	12	26,7	26,7	53,3
	En desacuerdo	11	24,4	24,4	77,8
	Casi en desacuerdo	7	15,6	15,6	93,3
	Indeciso	3	6,7	6,7	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

Constantemente se actualizan en el rubro de la seguridad informática un 26.7%, y casi de acuerdo 26.7%, en desacuerdo un 24.4%.

Tabla 4.13 En general la práctica de la informática forense es:

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	18	40,0	40,0	40,0
	Regular	11	24,4	24,4	64,4
	Bueno	11	24,4	24,4	88,9
	Pésimo	5	11,1	11,1	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

Para los encuestados la práctica de la informática forense en la PNP Huaraz, es malo en un 40.0%, a su vez que para algunos es bueno y regular 24.4% respectivamente.

4.1.3. Resultados sobre la seguridad informática

Tabla 4.14 Soy capaz de detectar riesgos de información con mi pericia y los equipos que dispongo.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	16	35,6	35,6	35,6
	A veces	11	24,4	24,4	60,0
	Casi nunca	8	17,8	17,8	77,8
	Casi siempre	8	17,8	17,8	95,6
	Siempre	2	4,4	4,4	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

Este dato es preocupante, un 35.6% revela que nunca es capaz de detectar riesgos de información, un 24.4% a veces.

Tabla 4.15 El sistema que manejo es capaz de registrar las incidencias de seguridad.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	14	31,1	31,1	31,1
	Quizá no	12	26,7	26,7	57,8
	Quizá sí	8	17,8	17,8	75,6
	Indeciso	7	15,6	15,6	91,1
	Sí	4	8,9	8,9	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

Manejan un sistema que no es capaz de registrar incidencias de seguridad en un 31.1%, quizá no en un 26.7%.

Tabla 4.16 Estoy en condiciones de detectar delitos informáticos.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	16	35,6	35,6	35,6
	Indeciso	11	24,4	24,4	60,0
	Casi de acuerdo	10	22,2	22,2	82,2
	Casi en desacuerdo	4	8,9	8,9	91,1
	De acuerdo	4	8,9	8,9	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

El personal en un 35.6% está en desacuerdo para revelar sus condiciones para detectar dichos delitos.

Tabla 4.17 Mi sistema puede reportar formalmente a través de una comunicación algún incidente.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	16	35,6	35,6	35,6
	Casi en desacuerdo	10	22,2	22,2	57,8
	Casi de acuerdo	8	17,8	17,8	75,6
	Indeciso	6	13,3	13,3	88,9
	De acuerdo	5	11,1	11,1	100,0
	Total	45	100,0	100,0	

Fuente: Elaboración propia

Están en 35.6% de desacuerdo en cuanto al reporte de algún incidente a través de una comunicación.

4.1.4. Prueba de Hipótesis General

A continuación, se hará una contrastación de cada indicador de la variable independiente con la variable dependiente.

Tabla 4.18 Se dispone de un servidor o servidores exclusivamente para el tema de la informática forense * Seguridad informática

Tabla cruzada

		En general el nivel de seguridad informática es:					
		Muy bajo	Bajo	Regular	Alto	Muy alto	Total
Se dispone de un servidor o servidores exclusivamente para el tema de la informática forense	Nunca	7	9	4	3	0	23
	Casi nunca	0	1	1	0	0	2
	A veces	1	5	2	3	0	11
	Casi siempre	0	0	0	1	2	3
	Siempre	1	0	2	2	1	6
Total		9	15	9	9	3	45

Fuente: Elaboración propia

Medidas simétricas

		Valor	Error estandarizado asintótico	T aproximada	Significación aproximada
Ordinal por ordinal	Tau-b de Kendall	,385	,116	3,203	,001
N de casos válidos		45			

Fuente: Elaboración propia

Tabla 4.19 Se cuenta con instalaciones de fibra óptica * Seguridad informática

		En general el nivel de seguridad informática es:					
		Muy bajo	Bajo	Regular	Alto	Muy alto	Total
Se cuenta con instalaciones de fibra óptica	No	9	13	7	4	2	35
	Quizá no	0	2	1	1	0	4
	Indeciso	0	0	1	1	0	2
	Quizá sí	0	0	0	1	0	1
	Sí	0	0	0	2	1	3
Total		9	15	9	9	3	45

Fuente: Elaboración propia

Medidas simétricas

		Valor	Error estandarizado asintótico	T aproximada	Significación aproximada
Ordinal por ordinal	Tau-b de Kendall	,394	,102	3,023	,003
N de casos válidos		45			

Fuente: Elaboración propia

Tabla 4.20 Esta dirección tiene terminales para el monitoreo del trabajo de informática forense * Seguridad informática

		En general el nivel de seguridad informática es:					
		Muy bajo	Bajo	Regular	Alto	Muy alto	Total
Esta dirección tiene terminales para el monitoreo del trabajo de informática forense	Nunca	9	9	3	3	1	25
	Casi nunca	0	2	4	0	0	6
	A veces	0	4	1	4	1	10
	Siempre	0	0	1	2	1	4
Total		9	15	9	9	3	45

Fuente: Elaboración propia

Medidas simétricas

		Valor	Error estandarizado asintótico	T aproximada	Significación aproximada
Ordinal por ordinal	Tau-b de Kendall	,455	,105	4,058	,000
N de casos válidos		45			

Fuente: Elaboración propia

Tabla 4.21 A través de un Data Center se logra efectivizar la labor * Seguridad informática

		En general el nivel de seguridad informática es:					
		Muy bajo	Bajo	Regular	Alto	Muy alto	Total
A través de un Data Center se logra efectivizar la labor	Nunca	6	3	1	3	0	13
	Casi nunca	1	4	2	0	0	7
	A veces	1	4	4	2	0	11
	Casi siempre	0	2	1	2	1	6
	Siempre	1	2	1	2	2	8
Total		9	15	9	9	3	45

Fuente: Elaboración propia

Medidas simétricas

		Valor	Error estandarizado asintótico	T aproximada	Significación aproximada
Ordinal por ordinal	Tau-b de Kendall	,341	,128	2,621	,009
N de casos válidos		45			

Fuente: Elaboración propia

Tabla 4.22 El uso del software se hace gracias al uso de la licencia correspondiente. * Seguridad informática

		En general el nivel de seguridad informática es:					
		Muy bajo	Bajo	Regular	Alto	Muy alto	Total
El uso del software se hace gracias al uso de la licencia correspondiente.	Nada importante	6	5	2	4	1	18
	Poco importante	2	3	0	0	0	5
	Indeciso	0	1	1	0	0	2
	Importante	0	1	3	2	0	6
	Muy importante	1	5	3	3	2	14
Total		9	15	9	9	3	45

Fuente: Elaboración propia

Medidas simétricas

		Valor	Error estandarizado asintótico	T aproximada	Significación aproximada
Ordinal por ordinal	Tau-b de Kendall	,232	,129	1,786	,074
N de casos válidos		45			

Fuente: Elaboración propia

Tabla 4.23 Se dispone de software especializado en el tema de la informática forense * Seguridad informática

		En general el nivel de seguridad informática es:					
		Muy bajo	Bajo	Regular	Alto	Muy alto	Total
Se dispone de software especializado en el tema de la informática forense	En desacuerdo	7	4	1	3	0	15
	Casi en desacuerdo	1	4	1	0	0	6
	Indeciso	0	3	2	2	0	7
	Casi de acuerdo	0	3	3	2	0	8
	De acuerdo	1	1	2	2	3	9
Total		9	15	9	9	3	45

Fuente: Elaboración propia

Medidas simétricas

		Valor	Error estandarizado asintótico	T aproximada	Significación aproximada
Ordinal por ordinal	Tau-b de Kendall	,423	,122	3,417	,001
N de casos válidos		45			

Fuente: Elaboración propia

Tabla 4.24 Conozco las normas correspondientes a las prácticas de la informática forense * Seguridad informática

		En general el nivel de seguridad informática es:					
		Muy bajo	Bajo	Regular	Alto	Muy alto	Total
Conozco las normas correspondientes a las prácticas de la informática forense	En desacuerdo	7	6	1	3	0	17
	Casi en desacuerdo	0	3	0	0	0	3
	Indeciso	0	2	3	3	0	8
	Casi de acuerdo	0	3	4	1	0	8
	De acuerdo	2	1	1	2	3	9
Total		9	15	9	9	3	45

Fuente: Elaboración propia

Medidas simétricas

		Valor	Error estandarizado asintótico	T aproximada	Significación aproximada
Ordinal por ordinal	Tau-b de Kendall	,365	,134	2,715	,007
N de casos válidos		45			

Fuente: Elaboración propia

Tabla 4.25 Cuando se requiere, tenemos el asesoramiento para realizar de manera óptima nuestra labor. * Seguridad informática

		En general el nivel de seguridad informática es:					
		Muy bajo	Bajo	Regular	Alto	Muy alto	Total
Cuando se requiere, tenemos el asesoramiento para realizar de manera óptima nuestra labor.	En desacuerdo	6	2	0	2	0	10
	Casi en desacuerdo	0	4	0	0	0	4
	Indeciso	1	2	1	3	0	7
	Casi de acuerdo	2	4	6	2	0	14
	De acuerdo	0	3	2	2	3	10
Total		9	15	9	9	3	45

Fuente: Elaboración propia

Medidas simétricas

		Valor	Error estandarizado asintótico	T aproximada	Significación aproximada
Ordinal por ordinal	Tau-b de Kendall	,391	,120	3,184	,001
N de casos válidos		45			

Fuente: Elaboración propia

Tabla 4.26 Constantemente me actualizo en el rubro de la seguridad de información. * Seguridad informática

		En general el nivel de seguridad informática es:					
		Muy bajo	Bajo	Regular	Alto	Muy alto	Total
Constantemente me actualizo en el rubro de la seguridad de información.	En desacuerdo	7	3	0	1	0	11
	Casi en desacuerdo	1	3	2	1	0	7
	Indeciso	0	2	0	1	0	3
	Casi de acuerdo	1	5	4	2	0	12
	De acuerdo	0	2	3	4	3	12
Total		9	15	9	9	3	45

Fuente: Elaboración propia

Medidas simétricas

		Valor	Error estandarizado asintótico	T aproximada	Significación aproximada
Ordinal por ordinal	Tau-b de Kendall	,533	,099	5,306	,000
N de casos válidos		45			

Fuente: Elaboración propia

Tabla 4.27 Resumen de los indicadores de la variable independiente con la dependiente

Indicadores	**Nivel de Significancia**	**Relación**
Servidor	0.001	Sí
Fibra óptica	0.003	Sí
Terminales	0.000	Sí
Data center	0.009	Sí
Licenciamiento	0.074	No
Software especializado	0.001	Sí
Conocimiento de normas	0.007	Sí
Asesoramiento	0.001	Sí
Conocimiento de seguridad de la información	0.000	Sí

Fuente: Elaboración propia

Ho: "La informática forense no está relacionada con la seguridad informática de la Dirección Nacional de Comunicación y Criminalística de la PNP de Huaraz en el 2015".

Ha: "La informática forense está relacionada con la seguridad informática de la Dirección Nacional de Comunicación y Criminalística de la PNP de Huaraz en el 2015".

Como se observa claramente que las metodologías y herramientas de la informática forense en un 89% tienen una relación directa con la seguridad informática en la Dirección Nacional de Comunicación y Criminalística de la Policía Nacional del Perú – Huaraz – 2015.

Por lo tanto, se rechaza la hipótesis nula, aceptándose la alterna que dice:

"La informática forense está relacionada con la seguridad informática de la Dirección Nacional de Comunicación y Criminalística de la PNP de Huaraz en el 2015".

4.1.5. Prueba de Fiabilidad

Tabla 4.28 Resumen de procesamiento de casos

		N	%
Casos	Válido	45	100,0
	Excluido	0	,0
	Total	45	100,0

Fuente: Elaboración propia

Tabla4.29 Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,923	15

Fuente: Elaboración propia

El Alfa de Cronbach se aplicará para determinar la validez y confiabilidad de las encuestas realizadas a la población en estudio. Cuanto más se aproxime a su valor máximo, 1, mayor es la fiabilidad de la escala. Además, en determinados contextos y por tácito convenio, se considera que valores del alfa superiores a 0,7 o 0,8 (dependiendo de la fuente) son suficientes para garantizar la fiabilidad de la escala.

Se aprecia la cifra de 0.923, el mismo que indica que el instrumento de investigación es fiable. La cifra 15 representa el número de preguntas formuladas para ambas variables.

4.2. Características de la informática forense de la Dirección Nacional de Comunicación y Criminalística de la PNP de Huaraz en el 2015.

Tabla 4.30 Características de la informática forense de la Dirección Nacional de Comunicación y Criminalística

Indicadores	Calificativo
1. Servidor	0.001
2. Fibra óptica	0.003
3. Terminales	0.000
4. Data center	0.009
5. Licenciamiento	0.074
6. Software especializado	0.001
7. Conocimiento de normas	0.007
8. Asesoramiento	0.001
9. Conocimiento de seguridad de la información	0.000

Fuente: Elaboración propia

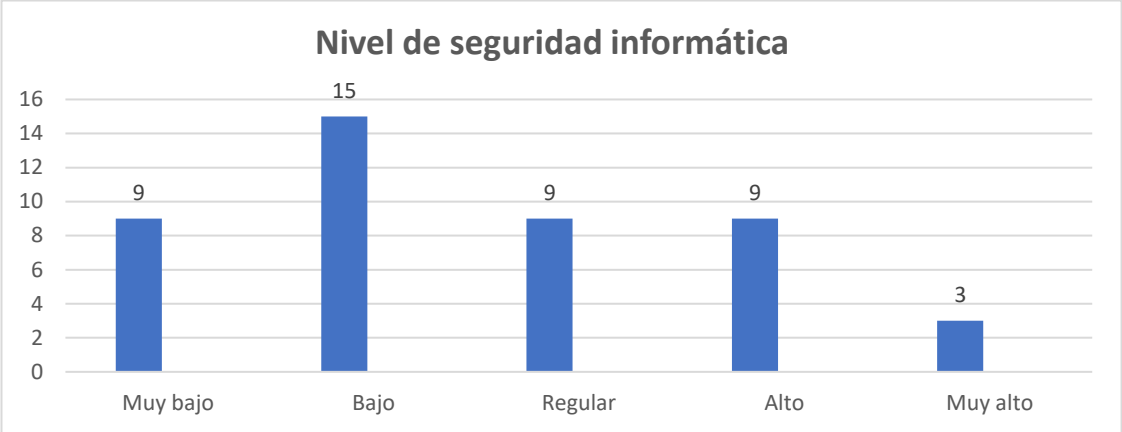
4.3. Nivel de la seguridad informática de la Dirección Nacional de Comunicación y Criminalística de la PNP de Huaraz en el 2015.

Tabla 4.31 Nivel de seguridad informática

		Frecuencia	Porcentaje
Válido	Muy bajo	9	20,0
	Bajo	15	33,3
	Regular	9	20,0
	Alto	9	20,0
	Muy alto	3	6,7
	Total	45	100,0

Fuente: Elaboración propia

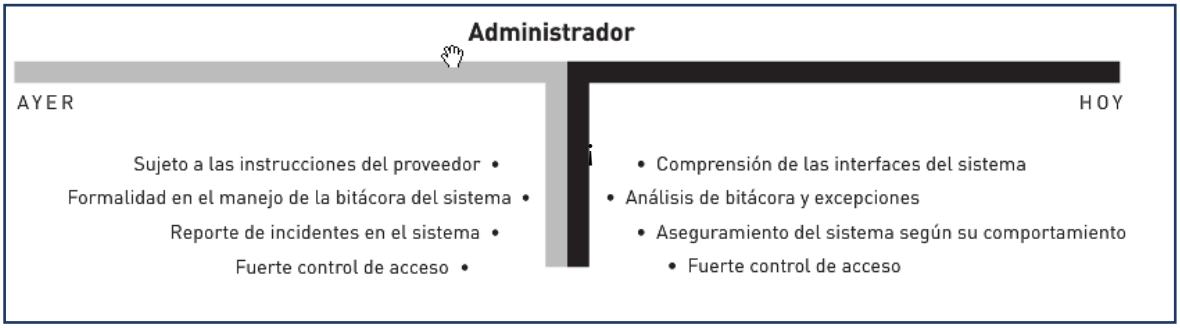
Figura 4.01 Nivel de seguridad informática



Fuente: Elaboración propia

Dentro de la seguridad informática vemos que es muy baja la seguridad que tiene la PNP en la ciudad de Huaraz.

Figura 4.02 Administrador de ayer y hoy



Fuente: (Cano Martinez, 2015)

Los procesos de la PNP – Huaraz evolucionan con las fuerzas del mercado de la tecnología. Para logar la reformulación de la seguridad y el control en un entorno como este, se requiere la seguridad en múltiples variables y especialidades que conjugadas en establezcan un cuerpo conceptual semejante a lo que existe en el pasado, no para restringir y especializar, sino para posibilitar y diversificar el concepto de seguridad. (Cano Martinez, 2015)

V DISCUSION

1. La importancia de la variable x = Aplicación de la metodología y herramientas de la informática forense para reducir el riesgo.

Con la presente investigación se busca aplicar metodologías y Herramientas de la informática forense se busca reducir el riesgo en el crimen cibernético.

2. Realizamos una encuesta a todo el personal de la Dirección nacional de Comunicaciones y Criminalística de la PNP – Huaraz. Las cual fue llenada por orden de su comandante en su formación general.

En esta investigación se han tomado como objeto de estudio la determinación entre la relación de informática forense y seguridad informática, y si es aplicada como indican los estándares en dicha institución estatal.

3. Realizar la determinación entre la relación de informática forense y seguridad informática para la Dirección nacional de Comunicaciones y Criminalística de la PNP - Huaraz.

Dando a Conocer las características de la informática forense y la seguridad informática de la Dirección Nacional de Comunicaciones y Criminalística de la PNP – Huaraz.

Determinaremos el nivel de seguridad informática de la Dirección Nacional de Comunicaciones y Criminalística de la PNP – Huaraz.

4. En este estudio se ha evidenciado que a nivel internacional específicamente en el ecuador las autoras Alvares María y Huamán Verónica desarrollan una tesis en el 2008 en la cual buscan acopar una Herramienta llamada Open Source o (software libre) que evidencia rendimiento y gran diferencia de costo para su proyecto implementación de un departamento de investigación de delitos informáticos con una sección de análisis forense.

5. Sin embargo, se han encontrado aspectos que colapsan con la que debería ser la propia teoría.

Los antecedentes encontrados en relación a los resultados de las encuestas revelan que para los trabajadores de la DININCRI – Huaraz desconocen y es poco importante la aplicación de métodos y herramientas de la informática forense, asi como para los superiores que no implementan el software y el hardware necesario para el desarrollo de dichos métodos y herramientas.

6. Tanto los antecedentes como el personal encuestado coinciden en que la seguridad informática es importante conocerla para desempeñar mejor su función y que ayudaría la aplicación de teoría de la informática forense en la solución de problemas cibernéticos.

En cuanto difieren que a nivel DININCRI - Huaraz no se aplica temas forenses por ende tampoco se desarrollan, a lo que a nivel internacional están en constante investigación y es aplicada y desarrollada en las entidades policiales

7. Gracias a estos hallazgos posiblemente se podrían hacer futuras investigaciones que consignen el tema de (Aplicación de la metodología y herramientas de la informática forense para reducir el riesgo) debido a que es un concepto poco investigado y desarrollado en las entidades policiales en el interior del país, ya que solo se desarrolla en la ciudad capital.

Los investigadores de informática forense podrían aplicar diversos softwares y desarrollar métodos a la necesidad de cada ciudad.

8. Reconoce las limitaciones de la investigación en cualquier parte del proceso.

No existe implementación de software y hardware, redes de comunicaciones ni proyectos de investigación tampoco financiamiento para la investigación.

La disposion de los trabajadores siempre se coordina con un superior Comandante o Coronel en caso de las encuestas se coordinó con un Comandante.

Poco material bibliográfico para realizar la investigación en temas forenses.

La limitación principal es presupuestal para la implementación de laboratorios

9. La seguridad informática está relacionada en un nivel muy bajo con la DIRINCRI – Huaraz ya que los trabajadores desconocen de políticas de seguridad

Así mismo no cuentan con la preparación adecuada la cual todo está centralizado en la capital no teniendo licencia de software.

VI CONCLUSIONES

1. Se evidencia que el nivel de preparación por la informática forense y sus capacidades en actividades en la Policía Nacional del Perú en Huaraz el departamento de **Dirección Nacional de Comunicación y Criminalística**, **es bajo tan solo un 20% del personal no es capacitado para afrontar temas forenses**.

2. La PNP - Huaraz **es débil**. Esta es una conclusión que se evidencia por prácticas de baja responsabilidad, compromiso y definición dentro de los miembros que conforman la división

3. Con la computación forense. Con ello se evidencia que no existe una gran diferencia de habilidades técnicas, las que serían una dificultad para cumplir con un pedido comercial más amplio y con plazos más estrictos. Son pocos los miembros de la PNP que manejan adecuadamente los procesos de la informática forense.

4. El estudio y sus resultados apuntan a afirmar que los fortalecimientos de capacidades en actividades forense tendrían que mejorar en la Policía Nacional Perú – Huaraz a un nivel superior en la que se encuentra.

5. La Policía nacional del Perú. Esta es una conclusión que se evidencia por la baja responsabilidad, compromiso y definición dentro los efectivos policiales que

conforman la **Dirección Nacional de Comunicación y Criminalística**. Con ello se evidencia que no existe una gran diferencia de habilidades técnicas, las que serían una dificultad para cumplir con un pedido de investigación forense más amplio y con plazos más estrictos. Son pocos los artesanos que manejan adecuadamente el acabado de los productos. Tienen limitaciones para elaborar nuevos diseños por falta de creatividad. Tienen poca visión.

VII RECOMENDACIONES

1. Organizar y desarrollar talleres de capacitación para el fortalecimiento las capacidades de la Policía Nacional del Perú - Huaraz en el área que presentan falencias significativas a nivel de capacidades de investigación de la informática forense, de acuerdo a lo encontrado en el estudio realizado.

Esto debe de ser diseñado y ejecutado por los altos mandos de la Policía Nacional del Perú – Huaraz Para ello, generar una demanda de temas a conocer, La demanda de capacitaciones no sólo será un elemento importante para el desarrollo del grupo y se sugiere que estos procesos de capacitación que se organicen sean de corta duración y con temas de interés para la PNP - Huaraz y se deberá contar con la colaboración de las instituciones públicas y privadas y organizaciones. Por otro lado, se tiene como recurso humano.

2. Los convenios con las Universidades del medio sean privadas o públicas para poder especializarse en los diferentes temas que lleva la informática forense.

3. Realizar Convenios con instituciones certificadoras relacionadas a seguridad y a la informática forense.

4. Falta de apoyo para dotar el departamento de tecnología de última generación.

5. No hay ambientes para ejecutar pruebas y desafíos relacionados a la informática forense.

VIII REFERENCIAS BIBLIOGRAFICAS

Bibliografía

Acurio del Pino, S. (2013). *Introducción a la informática forense.* Ecuador.

Álvarez Galarza, M., & Guamán Reibán, V. (2008). *Metodología, Estrategias y Herramientas de la Informática Forense Aplicables para la Dirección Nacional de Comunicaciones y Criminalística de la Policía Nacional.* Tesis , Cuenca.

Arquillo Cruz, J. (2007). *Herramientas de Apoyo para el Análisis Forense de Computado.* Tesis, Andalucia.

Cano Martinez, J. (2015). *Computación forense - Descubriendo los rastros informáticos 2ª edición.* Medellin: Alfaomega.

Cano, J. (2013). *Introducion a la informatica forese.* Medellin: Alfaomega.

Delgado, M. L. (junio de 2007). Análisis Forense Digital.

ERDM DUKE LAW. (2014). *http://www.edrm.net/frameworks-and-standards/edrm-model/*. Obtenido de http://www.edrm.net/frameworks-and-standards/edrm-model/

Esteban Vélez, s. (2014). *https://velezconde.wordpress.com/844-2/*. Obtenido de velezconde's Blog.

Ferro Veiga, J. M. (2015). *Informatica forense, El rastro digital del crimen.* España: amazon.

FYXM.NET. (2014). *FYXM.NET*. Obtenido de http://downloads.fyxm.net/ThumbsDisplay-5662.html

Ministro de Justicia y Derechos Humanos, P. (2014). *http://spij.minjus.gob.pe*. Obtenido de Sistema Peruano de Información Judicial (SPIJ): http://spij.minjus.gob.pe

Muñoz, O. R. (2015). *Estudio de metodologia de análisis forense ante inicidentes de ciberseguridad.* trabajo final de master, Madrid.

Pacheco Campos, H. E., & Moreno Ulloa, J. L. (2012). *Esclarecimiento de hechos delictivos usando informatica forense.* Tesis, Trujillo.

Pineda Villavicencio, G. A. (2015). *Efctos de la auditoria fosense en la investigacion de delitos de activos el el peru 2013-2014.* Tesis, Lima.

Policía Nacional del Perú. (s.f.).

Policía Nacional del Perú. (2001). *pnp*. Obtenido de https://www.pnp.gob.pe/direcciones/dircri/nosotros.html

Ramirez Rivera, G. A. (s.f.). Informatica Forense. *Universidad San Carlos de Guatemala*. Obtenido de https://laconsigna.files.wordpress.com/2008/05/informatica-forense.pdf

Rodríguez Rojas, L. (2011). *SISTEMA EXPERTO PARA EL ANALISIS FORENSE EN DELITOS INFORMATICOS.* Tesis , La paz.

Rodriguez, F., & Domenech, A. (2012). *La informática Forense el rastro digital del crimen.*

Sampieri, H. (2014). *Metodología de la Investigacion* (Quinta ed.). Bogotá: McGraw-Hill.

SS-ISO / IEC 27005: 2013. (2011). *ECNOLOGÍA DE LA INFORMACIÓN.TÉCNICAS DE SEGURIDAD.GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN*. Obtenido de http://webstore.ansi.org/RecordDetail.aspx?sku=SS-ISO%2FIEC+27005%3A2013&gclid=Cj0KEQjwrYbIBRCgnY-OluOk89EBEiQAZER58qQotvMTXi-0F3VzWg6mY4vUHgYRUzRFLON-_IepRuUaAp428P8HAQ

Villacís Ruiz, V. (2006). *Auditoria Forense: Metodología, Herramientas y Técnicas Aplicadas en un siniestro informático de una empresa del sector comercial.* Tesis, Guayaquil.

Wikipedia la enciclopedia libre. (20 de mayo de 2001). *Wikipedia*. Obtenido de http://es.wikipedia.org/wiki/Microsoft_Windows

Zuccardi , G., & Gutiérrez , J. (2006). *Informática Forense.*

Referencias electrónicas

- SPIJ Sistema Peruano de Información Judicial, http://spij.minjus.gob.pe/
- Forenses informáticos, http://delitinfom.blogspot.com/2012/03/concepto-objetivos-y-herramientas-de-la.html (consultada jueves 15 de marzo 2012)
- http://www.youtube.com/watch?v=UhumXfZedM0
- http://www.youtube.com/watch?v=_yYhuCK_Buc
- http://delfirosales.blogspot.com/2011/12/vector-de-ataque-web-con-social.html
- http://velezconde.wordpress.com/844-2/
- https://es.scribd.com/doc/124454177/ISO-27005-espanol
- http://es.wikipedia.org/wiki/Microsoft_Windows
- https://www.pnp.gob.pe/direcciones/dircri/nosotros.html

ANEXO

Anexo 01: Matriz de Consistencia

Problema	Objetivo	Hipótesis	Variable	Indicadores
General	**General**	**General**	**Independiente**	**Independiente**
¿Cuál es la relación que se da entre Informática forense y la seguridad informática de la Dirección Nacional de Comunicación y Criminalística de la PNP?	Determinar la relación entre la informática forense y la seguridad informática de la Dirección Nacional de Comunicación y Criminalística de la PNP de Huaraz.	La informática forense está relacionada con la seguridad informática de la Dirección Nacional de Comunicación y Criminalística de la PNP de Huaraz.	**Informática Forense**	- Servidores - Switch - Widh bada - Data Center - Normas - Frecuencia de cumplir con las políticas de seguridad - Beneficios de usar políticas de seguridad
Específicos	**Específicos**	**Específicos**	**Dependientes**	**Dependientes**
a. ¿Cuáles son las características de la informática forense de la Dirección Nacional de Comunicación y Criminalística de la PNP de Huaraz? b. ¿Cuál es el nivel de la seguridad informática en Dirección Nacional de Comunicación y Criminalística de la PNP de Huaraz?	a. Conocer las características de la informática forense de la Dirección Nacional de Comunicación y Criminalística de la PNP de Huaraz. b. Determinar el nivel de la seguridad informática de la Dirección Nacional de Comunicación y Criminalística de la PNP de Huaraz.	(No se requieren)	**Seguridad Informática**	- Frecuencia de riesgo a los recursos de informática - Incidencia de seguridad por los usuarios - Nivel de gestión de seguridad en los servicios

Fuente: Elaboración propia

Anexo 02: Instrumento de recopilación de datos

Universidad Nacional "Santiago Antúnez de Mayolo"
Escuela de Postgrado

"Aplicación de metodologías y herramientas de la informática forense para reducir el riesgo de la seguridad informática en la dirección nacional de comunicación y criminalística de la PNP, Huaraz, 2015"

Presentación e Instrucciones: *Estamos realizando un estudio respecto a la aplicación de metodologías y herramientas de la informática forense en el riesgo de la seguridad informática a fin de mejorar la labor gracias a la investigación.. Marque con un aspa (X) la alternativa que crea conveniente. No hay respuestas correctas ni incorrectas. Las respuestas serán anónimas. Gracias.*

Cuestionario para especialistas

I. Datos de Identificación

1. **Género:**

   ❑ Femenino ❑ Masculino

2. **Años de labor en la DNCC:**

3. **Grado de Instrucción :**

   ❑ Sin Estudios ❑ Primaria ❑ Secundaria ❑ Técnica ❑ Univ Bachiller ❑ Univ Titulado

II. Datos de Estudio: Informática Forense

1. Se dispone de un **servidor o servidores** exclusivamente para el tema de la informática forense	(1) nunca (2) casi nunca (3) a veces (4) casi siempre (5) siempre
2. Se cuenta con instalaciones de **fibra óptica**	(1) No (2) Quizá no (3) Indeciso (4) Quizás si (5) Si
3. Esta dirección tiene **terminales** para el monitoreo del trabajo de informática forense	(1) nunca (2) casi nunca (3) a veces (4) casi siempre (5) siempre
4. A través de un **Data Center** se logra efectivizar la labor	(1) nunca (2) casi nunca (3) a veces (4) casi siempre (5) siempre

Fuente: Elaboración propia

5. El uso del software se hace gracias al uso de la **licencia** correspondiente.	1 en desacuerdo	2 casi en desacuerdo	3 ni en acuerdo, ni en desac	4 casi de acuerdo	5 de acuerdo
6. Se dispone de **software especializado** en el tema de la informática forense	1 en desacuerdo	2 casi en desacuerdo	3 ni en acuerdo, ni en desac	4 casi de acuerdo	5 de acuerdo
7. Conozco las **normas** correspondientes a las prácticas de la informática forense	1 en desacuerdo	2 casi en desacuerdo	3 ni en acuerdo, ni en desac	4 casi de acuerdo	5 de acuerdo
8. Cuando se requiere, tenemos el **asesoramiento** para realizar de manera óptima nuestra labor.	1 en desacuerdo	2 casi en desacuerdo	3 ni en acuerdo, ni en desac	4 casi de acuerdo	5 de acuerdo
9. Constantemente me **actualizo** en el rubro de la seguridad de información.	1 en desacuerdo	2 casi en desacuerdo	3 ni en acuerdo, ni en desac	4 casi de acuerdo	5 de acuerdo
10. En general la práctica de la informática forense es:	1 pésimo	2 malo	3 regular	4 bueno	5 excelente

Datos de Estudio: Seguridad Informática

1. Soy capaz de detectar **riesgos de información** con mi pericia y los equipos que dispongo.	1 nunca	2 casi nunca	3 a veces	4 casi siempre	5 siempre
2. El sistema que manejo es capaz de **registrar las incidencias** de seguridad.	1 No	2 Quizá no	3 Indeciso	4 Quizás si	5 Si
3. Estoy en condiciones de detectar **delitos informáticos.**	1 en desacuerdo	2 casi en desacuerdo	3 ni en acuerdo, ni en desac	4 casi de acuerdo	5 de acuerdo
4. Mi sistema puede **reportar formalmente** a través de una comunicación algun incidente.	1 en desacuerdo	2 casi en desacuerdo	3 ni en acuerdo, ni en desac	4 casi de acuerdo	5 de acuerdo
5. En general el **nivel** de seguridad informática es:	1 Muy bajo	2 Bajo	3 Regular	4 Alto	5 Muy alto

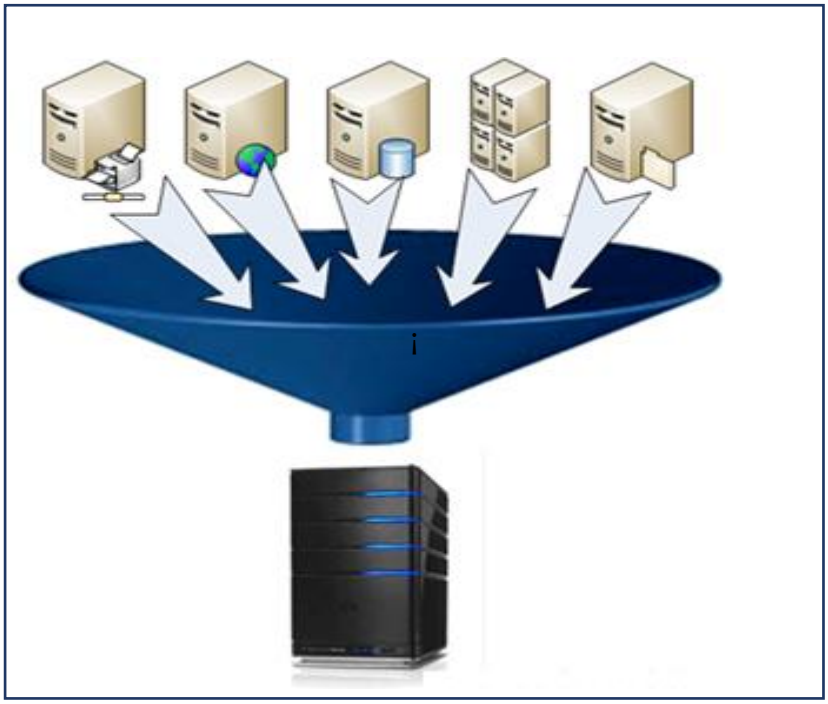
Gracias por su colaboración.

Fuente: Elaboración propia

Anexo 03: Instrumentos usados

Los laboratorios se realizaron con máquinas virtuales simulados con sistemas operativos de Microsoft en sus diferentes versiones se muestra figura 3.01

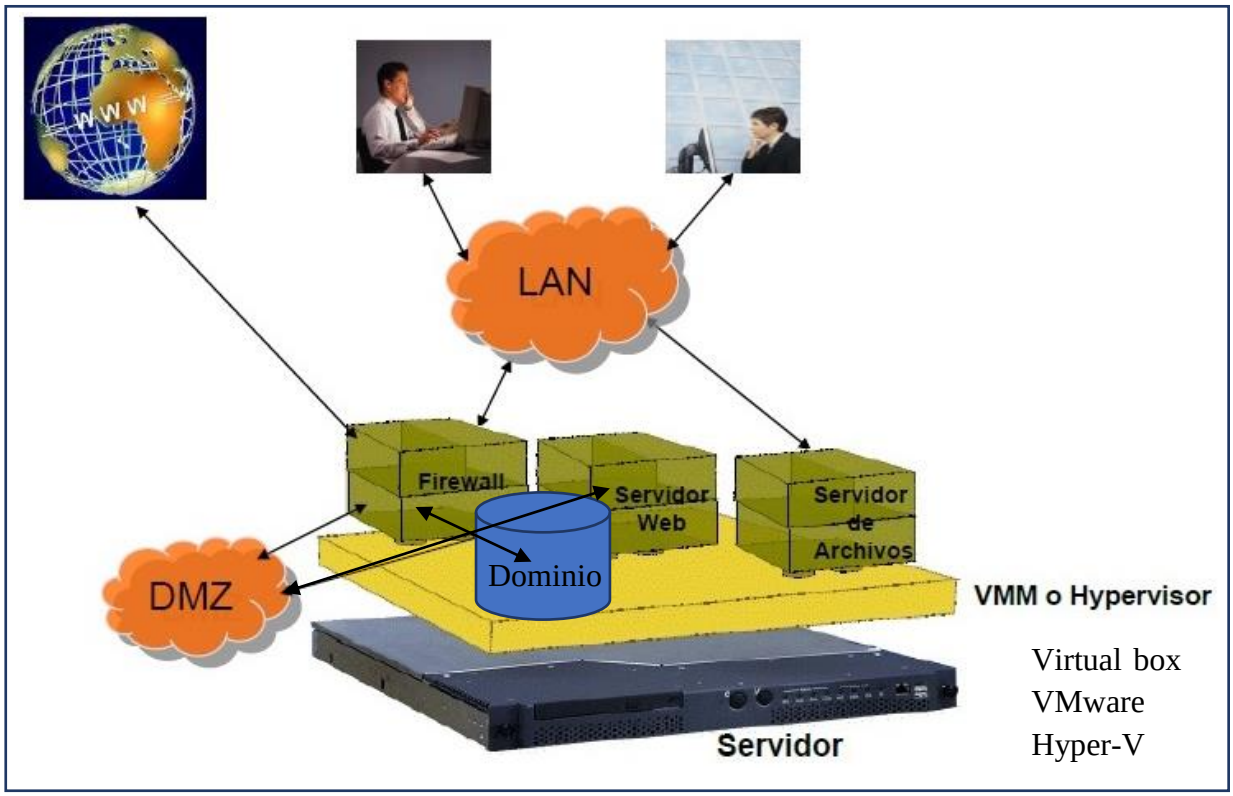
Virtualización de la infraestructura de servicios



Fuente: http://networksandservers.blogspot.pe/2011/10/virtualization-iii.html

Ventajas: Optimización de recursos tecnológicos, reducción de espacio, físico simplicidad de administración, mejor tolerancia a fallos. Se muestra figura 3.02

Plataforma de una red virtualizada



Fuente: Informática Forense, Jornadas de Seguridad Informática nov. 2009

Software sistemas operativos de Microsoft

Microsoft Windows (conocido generalmente como Windows o MS Windows), es el nombre de una familia de distribuciones para PC, smartphone, servidores y sistemas desarrollados y vendidos por Microsoft, y disponibles para múltiples arquitecturas, tales como x86 y x64, ARM.

Las versiones más recientes de Windows son Windows 8.1 y Windows 8 para equipos de escritorio, Windows Server 2012R2 para servidores y Windows Phone 8 y 8.1 para dispositivos móviles.

El 30 de septiembre de 2014, Microsoft presentó Windows 10, la nueva versión del sistema operativo que llegara de forma oficial a finales del 2015, siendo la primera versión que se integrara a todos los dispositivos Windows, eliminando de

esta forma todas las variantes del mismo. Siendo un único sistema operativo para equipos de escritorio, portátiles, smartphones y tablets se espera ofrecer una mejor experiencia eliminando algunos problemas que se presentaron con Windows 8/ 8.1. Se indicó que durante la conferencia build 2015 se darán a conocer más detalles. (Wikipedia la enciclopedia libre, 2001) Se detalla en las tablas 3.01 y tabla 3.02 siguientes.

Windows server 2012R2, Windows server 2012

Windows server 2008R2, Windows server 2008

Windows 10

Windows 8.1

Windows 7

Windows XP SP3

Software sistema operativo de Microsoft

Nombre de Software	Sistema Operativo	Version	Plataforma
Windows server 2012 R2	Windows server 2012 R2	Datacenter	64 Bist
	Windows server 2012 R2	Standard	64 Bist
	Windows server 2012 R2	Essentials	64 Bist
	Windows server 2012 R2	Foundation	64 Bist
Windows server 2012	Windows server 2012	Datacenter	64 Bist
	Windows server 2012	Standard	64 Bist
	Windows server 2012	Essentials	64 Bist
	Windows server 2012	Foundation	64 Bist
Windows server 2008 R2	Windows server 2008 R2	Standard	x86 y 86 - 64 Bist
	Windows server 2008 R2	Enterprise	x86 y 86 - 64 Bist
	Windows server 2008 R2	Datacenter	x86 y 86 - 64 Bist
	Windows server 2008 R2	Web Server	x86 y 86 - 64 Bist
	Windows server 2008 R2	Storage	x86 y 86 - 64 Bist
	Windows server 2008 R2	Small Businnes server	x86 y 86 - 64 Bist
	Windows server 2008 R2	Essential Businnes server	x86 y 86 - 64 Bist
Windows server 2008	Windows server 2008	Standard	x86 y 86 - 64 Bist
	Windows server 2008	Enterprise	x86 y 86 - 64 Bist
	Windows server 2008	Datacenter	x86 y 86 - 64 Bist
	Windows server 2008	Web Server	x86 y 86 - 64 Bist
	Windows server 2008	Storage	x86 y 86 - 64 Bist
	Windows server 2008	Small Businnes server	x86 y 86 - 64 Bist
	Windows server 2008	Essential Businnes server	x86 y 86 - 64 Bist

Fuente: https://es.wikipedia.org/wiki/Anexo:Versiones_de_Microsoft_Windows Versiones_de_Windows

Software sistema operativo de microsoft utilizados

Nombre de Software	Sistema Operativo	Version	Plataforma
Windows server 2012 R2	Windows server 2012 R2	Standard	64 Bist
Windows server 2012	Windows server 2012	Standard	64 Bist
Windows server 2008 R2	Windows server 2008 R2	Enterprise	x86 y 86 - 64 Bist
Windows server 2008 R2	Windows server 2008 R2	Standard	x86 y 86 - 64 Bist
Windows server 2008	Windows server 2008	Enterprise	x86 y 86 - 64 Bist
Windows server 2008	Windows server 2008	Standard	x86 y 86 - 64 Bist

Fuente: https://es.wikipedia.org/wiki/Anexo:Versiones_de_Microsoft_Windows# Versiones_de_Windows

Sistemas operativos de linux (Open source)

Kali Linux 1.0.7

Backtrack 5 r3

Sistemas de virtualización

Mvware

Hyper – v

Virtual Box

Recursos computacionales

Los recursos se detallan en la tabla 3.03:

Laptop Lenovo Core i5

CARACTERISTICAS:

PANTALLA	14 PULG LCD TFT LED	
CPU	INTEL CORE I5 4200M 250 GHZ CACHE L3 3 MB	
MEMORIA	CAPACIDAD	6 GB
	TIPO	DDR3
DISCO DURO	CAPACIDAD	1 TB
	TIPO	SATA
	VELOCIDAD	5400 RPM
OPTICO	DVD SUPERMULTI	
	MARCA	NVIDIA
	CAPACIDAD	1GB
	TIPO	DDR3
CONECTIVIDAD	LAN	VELOCIDAD 10/100 MB/S
	WIRELESS	802.11B 802.11G 802.11N
SONIDO	PUERTOS	COMBO AUDIO/MIC SI
PUERTOS	USB 2.0 USB 3.0	3
	RJ45	1
BATERIA	NRO CELDAS	4
SISTEMA OPERATIVO VERSION WINDOWS 10		

Fuente: Elaboración propia

Laptop HP COMPAQ Core i5

CARACTERISTICAS:

PANTALLA	15.6 PULG LCD TFT LED	
CPU	INTEL CORE I5 4200M 250 GHZ CACHE L3 3 MB	
MEMORIA	CAPACIDAD	8 GB
	TIPO	DDR3
	EXPANSION MAXIMA	16 GB
DISCO DURO	CAPACIDAD	750 GB
	TIPO	SATA
	VELOCIDAD	5400 RPM
OPTICO	DVD SUPERMULTI	
VIDEO	INDEPENDIENTE	SI
	MARCA	NVIDIA
	CAPACIDAD	4GB
	TIPO	DDR3
CONECTIVIDAD	LAN	VELOCIDAD 10/100/1000 MB/S
	WIRELESS	802.11B 802.11G 802.11N
	BLUETOOTH	SI
SONIDO	PUERTOS	COMBO AUDIO/MIC SI
PUERTOS	USB 2.0, USB 3.0	3
	RJ45	1
BATERIA	NRO CELDAS	6
SISTEMA OPERATIVO VERSION WINDOWS 10		

Fuente: Elaboración propia

Anexo 04 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

D.S. N° 052-2008-PCM (Reglamento de la ley de firmas y certificados digitales)

Ley de Firmas y Certificados Digitales LEY Nº 27269

CONCORDANCIAS: D.S. N° 052-2008-PCM (Reglamento de la ley de firmas y certificados digitales) Otras Concordancia

EL PRESIDENTE DE LA REPUBLICA

Por cuanto:

El Congreso de la República

ha dado la Ley siguiente:

LEY DE FIRMAS Y CERTIFICADOS DIGITALES

Artículo 1.- Objeto de la ley

La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita.

CONCORDANCIA: D.S. Nº 004-2007-PCM, Art. 2, R.SBS Nº 1270-2007

Artículo 2.- Ámbito de aplicación

La presente ley se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

CONCORDANCIAS: D.S. Nº 004-2007-PCM, Arts. 1 y 55; D.S. N° 052-2008-PCM, Reglamento, Art. 73

DE LA FIRMA DIGITAL

Artículo 3.- Firma digital

La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

DEL TITULAR DE LA FIRMA DIGITAL

Artículo 4.- Titular de la firma digital

El titular de la firma digital es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.

Artículo 5.- Obligaciones del titular de la firma digital

El titular de la firma digital tiene la obligación de brindar a las entidades de certificación y a los terceros con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas.

DE LOS CERTIFICADOS DIGITALES

Artículo 6.- Certificado digital

El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

Artículo 7.- Contenido del certificado digital

Los certificados digitales emitidos por las entidades de certificación deben contener al menos:

1. Datos que identifiquen indubitablemente al suscriptor.
2. Datos que identifiquen a la Entidad de Certificación.
3. La clave pública.
4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
5. Número de serie del certificado.
6. Vigencia del certificado.
7. Firma digital de la Entidad de Certificación.

Artículo 8.- Confidencialidad de la información

La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los fines señalados en la presente ley.

Así mismo la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital.

Artículo 9.- Cancelación del certificado digital

La cancelación del certificado digital puede darse:

1. A solicitud del titular de la firma digital.
2. Por revocatoria de la entidad certificante.
3. Por expiración del plazo de vigencia.
4. Por cese de operaciones de la Entidad de Certificación.

Artículo 10.- Revocación del certificado digital

La Entidad de Certificación revocará el certificado digital en los siguientes casos:

1. Se determine que la información contenida en el certificado digital es inexacta o ha sido modificada.
2. Por muerte del titular de la firma digital.
3. Por incumplimiento derivado de la relación contractual con la Entidad de Certificación.

CONCORDANCIA: D.S. Nº 004-2007-PCM, Art. 32

Artículo 11.- Reconocimiento de certificados emitidos por entidades extranjeras

Los Certificados de Firmas Digitales emitidos por entidades extranjeras tendrán la misma validez y eficacia jurídica reconocida en la presente ley, siempre y cuando tales certificados sean reconocidos por una entidad de certificación nacional que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, del procedimiento, así como la validez y la vigencia del certificado.

(*) Artículo modificado por el Artículo Único de la Ley Nº 27310, publicada el 17-07-2000, cuyo texto es el siguiente:

"Artículo 11.- Los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en la presente Ley, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente." (Ministro de Justicia y Derechos Humanos, 2014)

LEY DE DELITOS INFORMÁTICOS LEY Nº 30096

CAPÍTULO I

FINALIDAD Y OBJETO DE LA LEY

Artículo 1. Objeto de la Ley

La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

CAPÍTULO II

DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS

Artículo 2. Acceso ilícito

El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.

Artículo 3. Atentado contra la integridad de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Artículo 4. Atentado contra la integridad de sistemas informáticos

El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

CAPÍTULO III

DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES

Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

CAPÍTULO IV

DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

Artículo 6. Tráfico ilegal de datos

El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

Artículo 7. Interceptación de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un

sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

CAPÍTULO V

DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

Artículo 8. Fraude informático

El que, a través de las tecnologías de la información o de la comunicación, 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 VI

DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA

Artículo 9. Suplantación de identidad

El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

CAPÍTULO VII

DISPOSICIONES COMUNES

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Artículo 11. Agravantes

El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

1. El agente comete el delito en calidad de integrante de una organización criminal.

2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.

4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales. (Ministro de Justicia y Derechos Humanos, 2014)

Ley de Propiedad Intelectual

Artículo modificado por el Artículo 1 de la Ley N° 28289, publicada el 20-07-2004, cuyo texto es el siguiente:

"Artículo 217.- Reproducción, difusión, distribución y circulación de la obra sin la autorización del autor.

Será reprimido con pena privativa de libertad no menor de dos ni mayor de seis años y con treinta a noventa días-multa el que, con respecto a una obra, una

interpretación o ejecución artística, un fonograma o una emisión o transmisión de radiodifusión, o una grabación audiovisual o una imagen fotográfica expresada en cualquier forma, realiza alguno de los siguientes actos sin la autorización previa y escrita del autor o titular de los derechos:

A. La modifique total o parcialmente.

B. La distribuya mediante venta, alquiler o préstamo público.

C. La comunique o difunda públicamente por cualquiera de los medios o procedimientos reservados al titular del respectivo derecho.

Inciso modificado por el Artículo 1 de la Ley N° 29263, publicada el 02 octubre 2008, cuyo texto es el siguiente:

"c. La comunique o difunda públicamente, transmita o retransmita por cualquiera de los medios o procedimientos reservados al titular del respectivo derecho."

D. La reproduzca, distribuya o comunique en mayor número que el autorizado por escrito.

La pena será no menor de cuatro años ni mayor de ocho y con sesenta a ciento veinte días multa, cuando el agente la reproduzca total o parcialmente, por cualquier medio o procedimiento y si la distribución se realiza mediante venta, alquiler o préstamo al público u otra forma de transferencia de la posesión del soporte que contiene la obra o producción que supere las dos (2) Unidades

Impositivas Tributarias, en forma fraccionada, en un solo acto o en diferentes actos de inferior importe cada uno. Impositivas Tributarias, en forma fraccionada, en un solo acto o en diferentes actos de inferior importe cada uno." (Ministro de Justicia y Derechos Humanos, 2014)

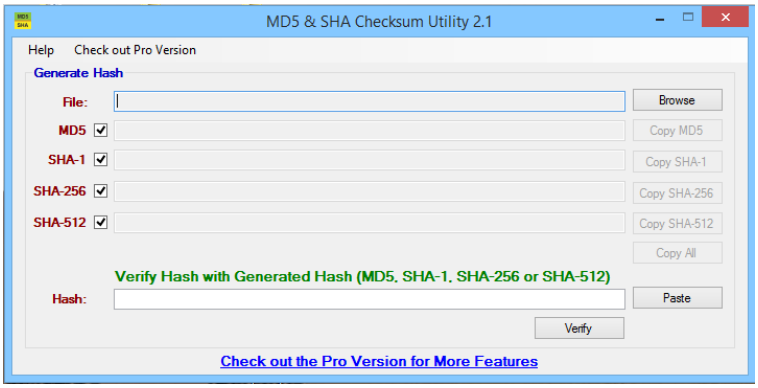
Anexo 05: Descripción de las herramientas

A continuación, se detallan los softwares a utilizar en una análisis forense o recuperación de evidencias.

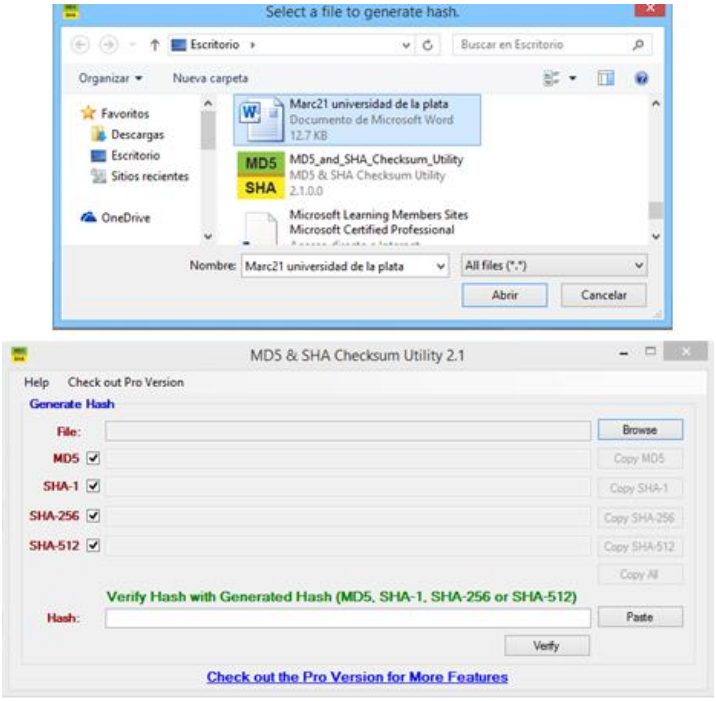
Software MD5 & SHA Checksum Utilily 2.1

MD5, SHA-1, SHA-512 Utilidad de la suma de comprobación es una herramienta que le permite verificar la integridad de un archivo mediante la búsqueda de su MD5, SHA-1 y SHA-512 firmas, como su nombre indica. Sus características pueden ser aplicando metodología.

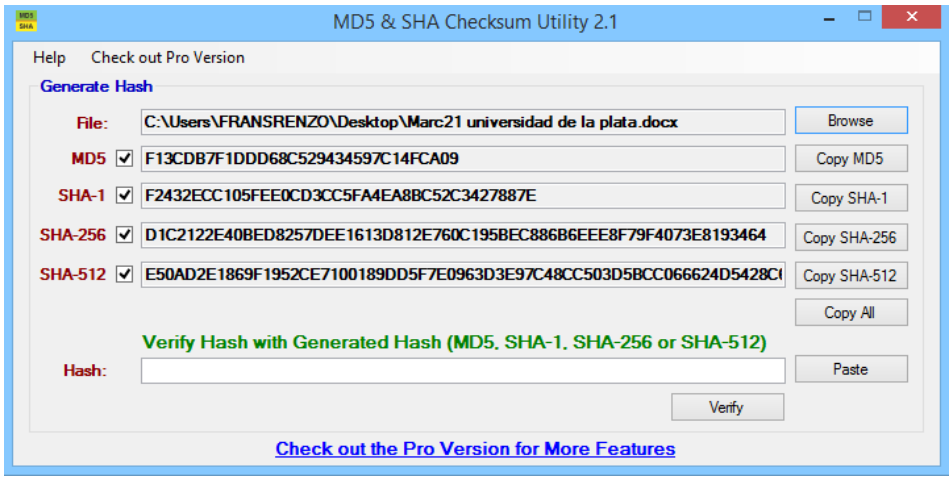
Aplicando MD5, SHA-1 y SHA-512



En la figura se muestra la ubicación del archivo para obtener la codificación MD5 o SHA 1



En la figura se muestra la codificación MD5 o SHA.



Se copia el checksum MD5 y SHA-512

MD5

F13CDB7F1DDD68C529434597C14FCA09

SHA-512

E50AD2E1869F1952CE7100189DD5F7E0963D3E97C48CC503D5BCC0666

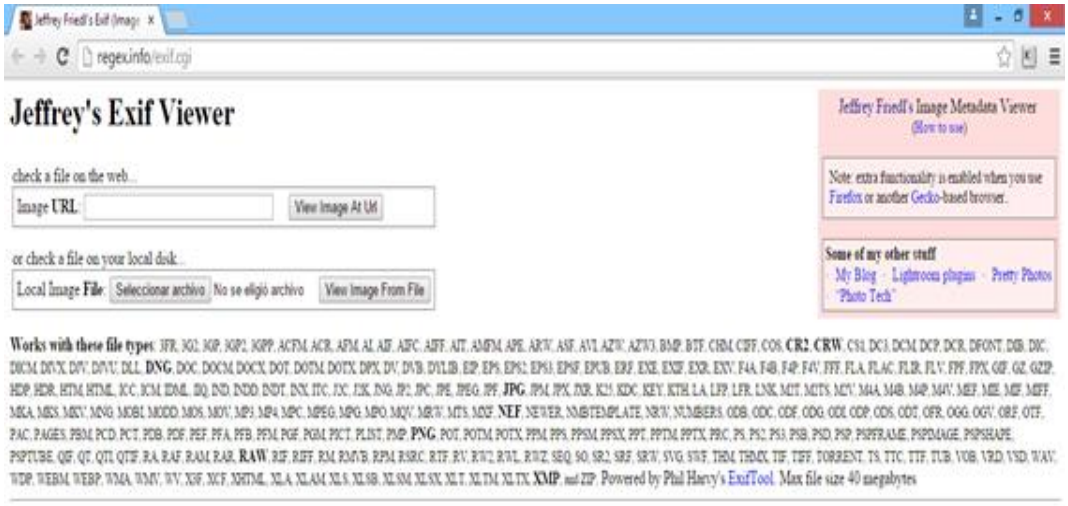
24D5428C6C425079D41306724991B6AFD9330FD4A011EF8ED7C73395D0

EAB92D97A4F86

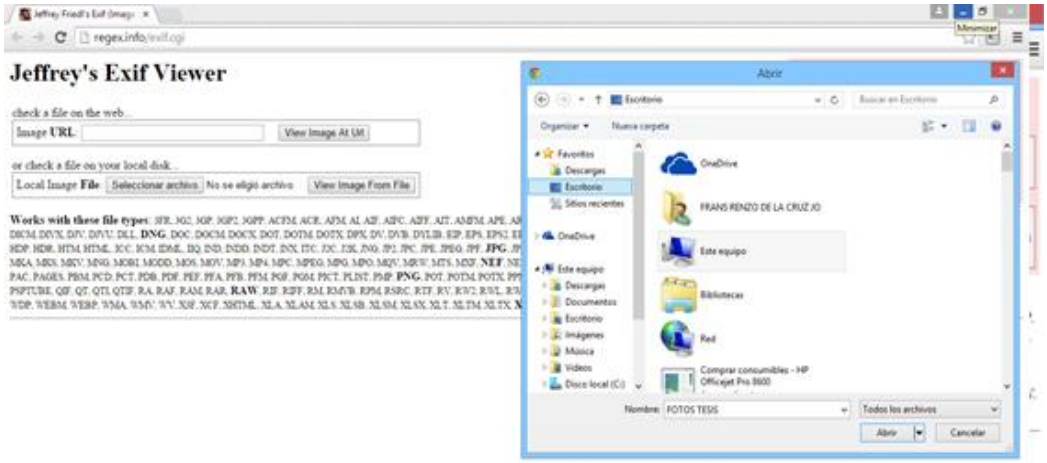
Software Jeffrey's Exif Viewer

En este aplicativo diseñado por web para analizar la información que contiene las fotos para un análisis forense la Url de la página web es http://regex.info/exif.cgi.

En la ventana se adjunta el archivo o foto para poder ser analizada la información de la foto.



En la ventana se muestra a ubicación del archivo o foto



Software Thumbs Display

Descripción ThumbsDisplay 1.0.2

ThumbsDisplay es una herramienta que necesita para mostrar Thumbs.DB y Vista thumbcache de archivos. Usted puede usar este software en una variedad de formas que le permitan procesar todos estos archivos con la mayor eficacia posible. Siendo realistas, la capacidad de imprimir una sola imagen en miniatura en una página entera resultados de formato en una imagen borrosa bastante pobre. Pero hoy en día, si usted necesita para mostrar a alguien el contenido que se ha encontrado sólo en un archivo de imagen en miniatura que se dejan tener que estirarse la imagen usted mismo en alguna herramienta para que pueda ser visto por las personas que están tratando de mostrar. Esta herramienta combina pantalla, la presentación de informes y ampliar en una sola herramienta que es fácil de usar.

Características ThumbsDisplay 1.0.2

Mostrar todos los archivos de miniaturas: thumbs.db, thumbcache_idx.db, thumbcache_32.db, thumbcache_96.db, thumbcache_256.db, thumbcache_1024.db y thumbcache_sr.db. Encuéntralos en todas las localidades rápidamente utilizando la incorporada en el localizador.

a. Muestra todas las imágenes en miniatura con el nombre de archivo original y marca de tiempo.

b. Imprimir imágenes individuales como una página entera o seleccionar entre los tres formatos de informe: Informe, Hoja de contactos y todos los artículos

d. Copie imágenes individuales en el portapapeles para su inclusión en un documento o guardarlos como archivos en formato JPEG o BMP.

e. Mostrar miniaturas en tres tamaños: 96x96 (original) 150x150 o 200x200.

Información de seguridad ThumbsDisplay

No se puede descargar cualquier grieta o número de serie de ThumbsDisplay en esta página. Cada software que puede descargar en nuestro sitio es legal. No hay crack, número de serie, truco o clave de activación para ThumbsDisplay

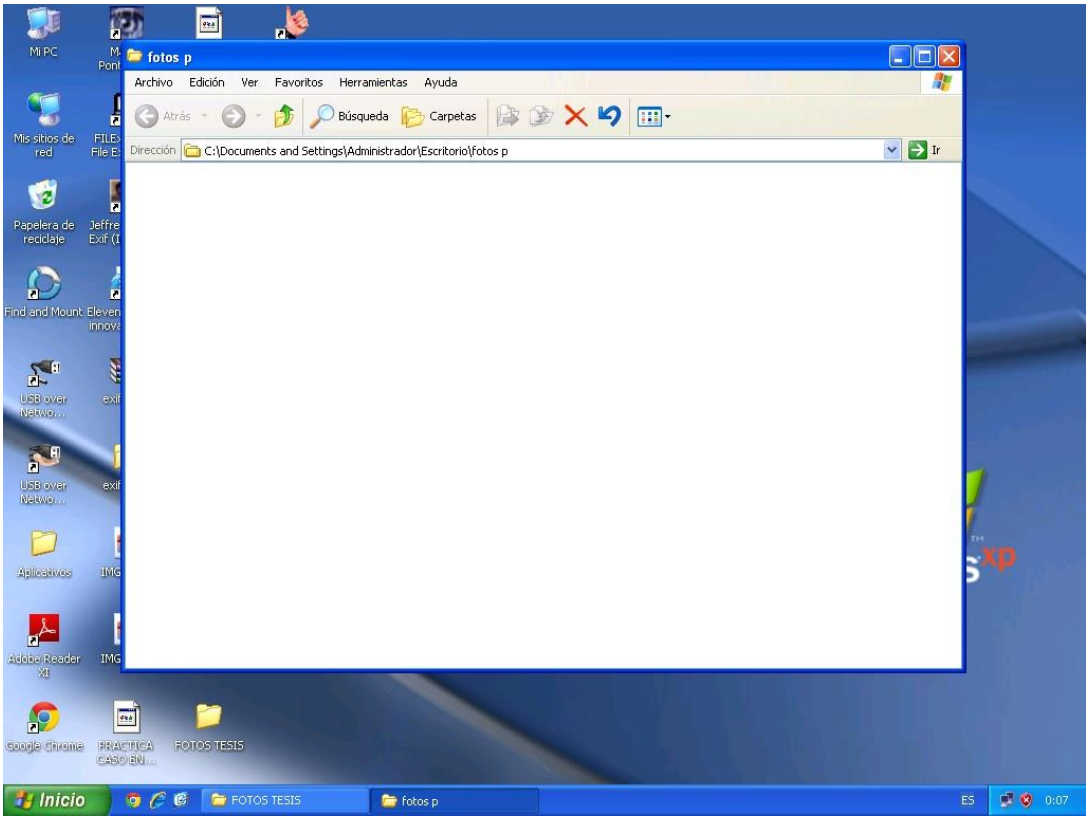
presentes aquí. Nuestra colección también no contiene ningún keygen, porque los programas keygen se están utilizando de manera ilegal que nosotros no apoyamos. Todo el software que se puede encontrar aquí es de descarga gratuita y legal.

Paquete de instalación ThumbsDisplay se prepara para su descarga desde nuestros servidores de descarga rápida. Se comprueba por posibles virus y se ha demostrado ser 100% limpio y seguro. Varios antivirus líderes se han utilizado para probar ThumbsDisplay, si contiene virus. No hay infecciones se han encontrado y descargar ThumbsDisplay es completelly sin problemas debido a esa razón. Nuestros expertos en detección de malware probados ThumbsDisplay con varios programas espía y los programas de detección de malware, incluyendo malware fyxm.net encargo y detección de spyware, y absolutamente impresionante sin malware o spyware se encontró en ThumbsDisplay.

Todo el software que se puede encontrar en nuestros servidores, incluyendo ThumbsDisplay, es freeware, shareware o de código abierto, algunos de los paquetes de software son demo, versiones de prueba o de parche y si es posible (licencia de dominio público), también sede de las versiones oficiales completas de software.

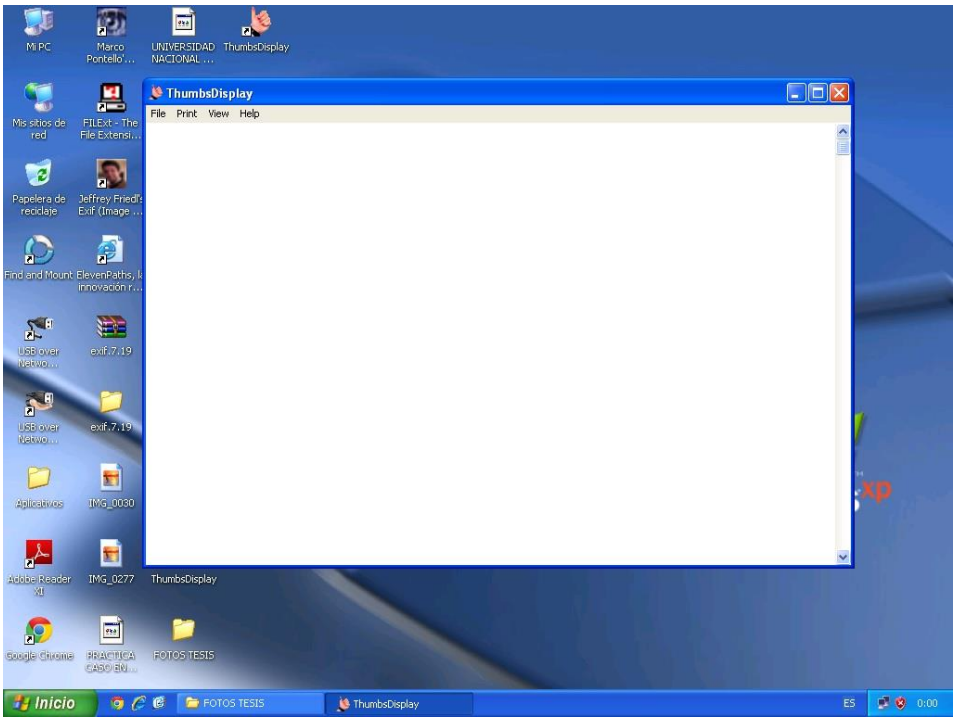
Porque queremos ser uno de los sitios más rápidos de descarga en la web, ofrecemos todo el software que incluye ThumbsDisplay en nuestro servidor. Fyxm.net sí apoya el software libre, sin embargo, no apoyamos warez o las descargas ilegales. (FYXM.NET, 2014)

En esta imagen se muestra que la carpeta fotos está vacía

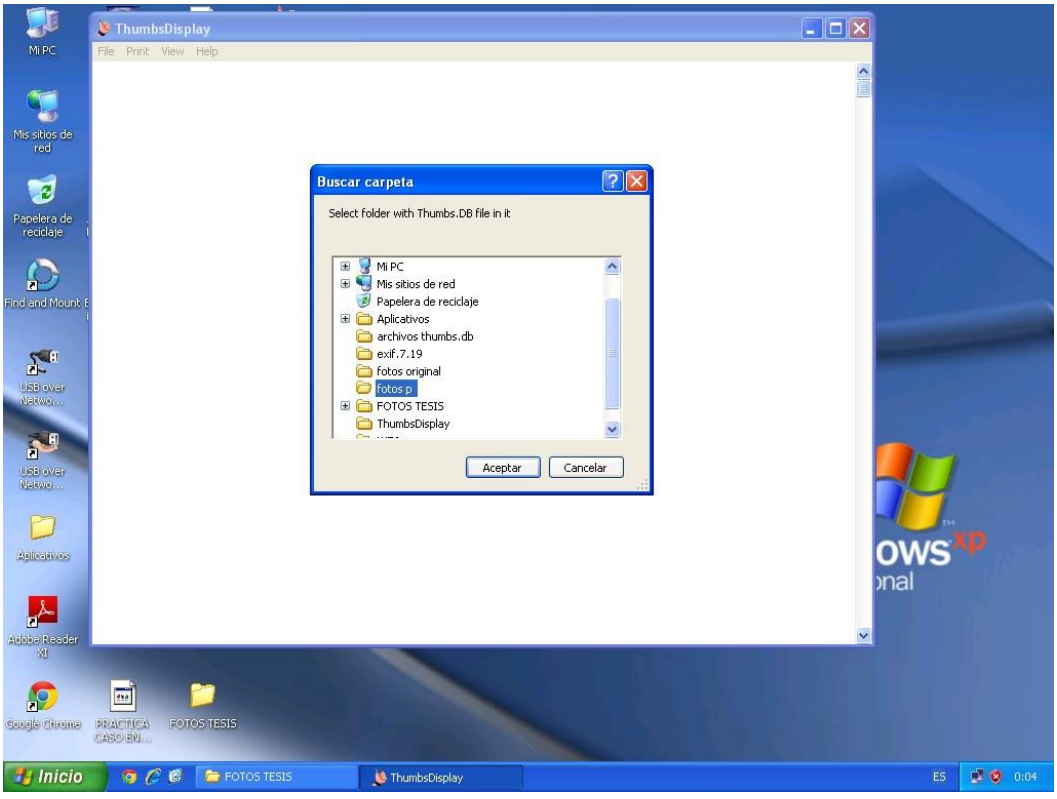


En esta imagen se muestra la ubicación del aplicativo ThumbsDisplay

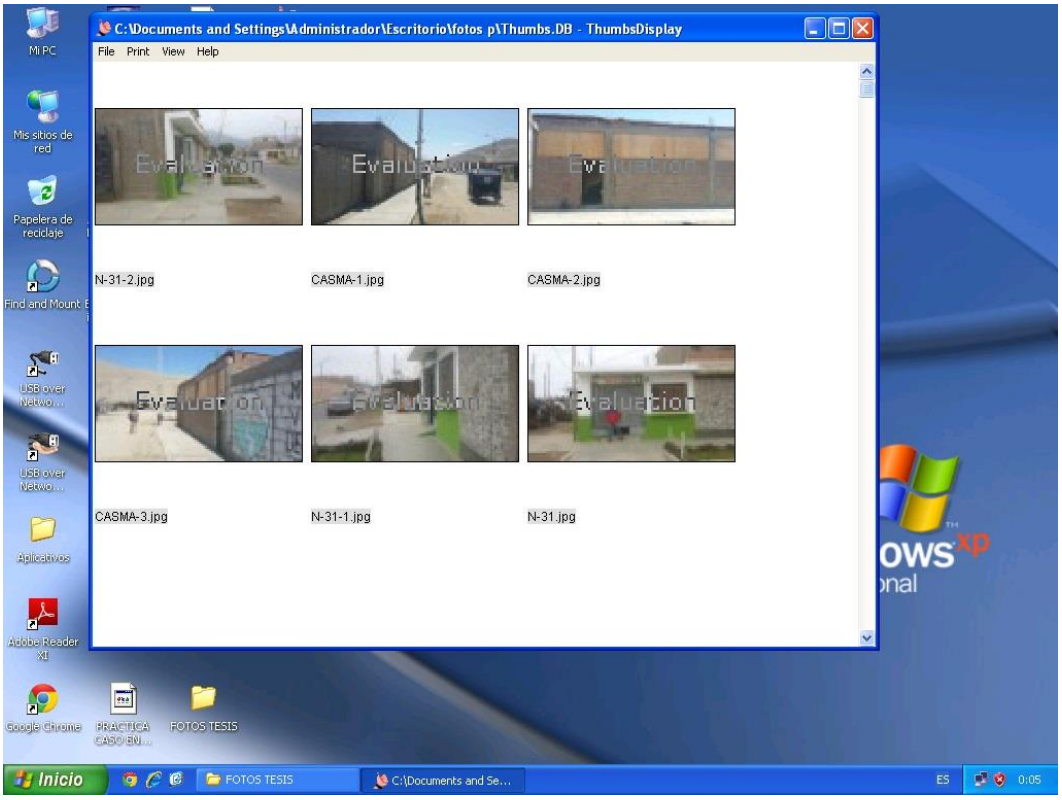
En esta imagen se muestra la ejecución del software ThumbsDisplay



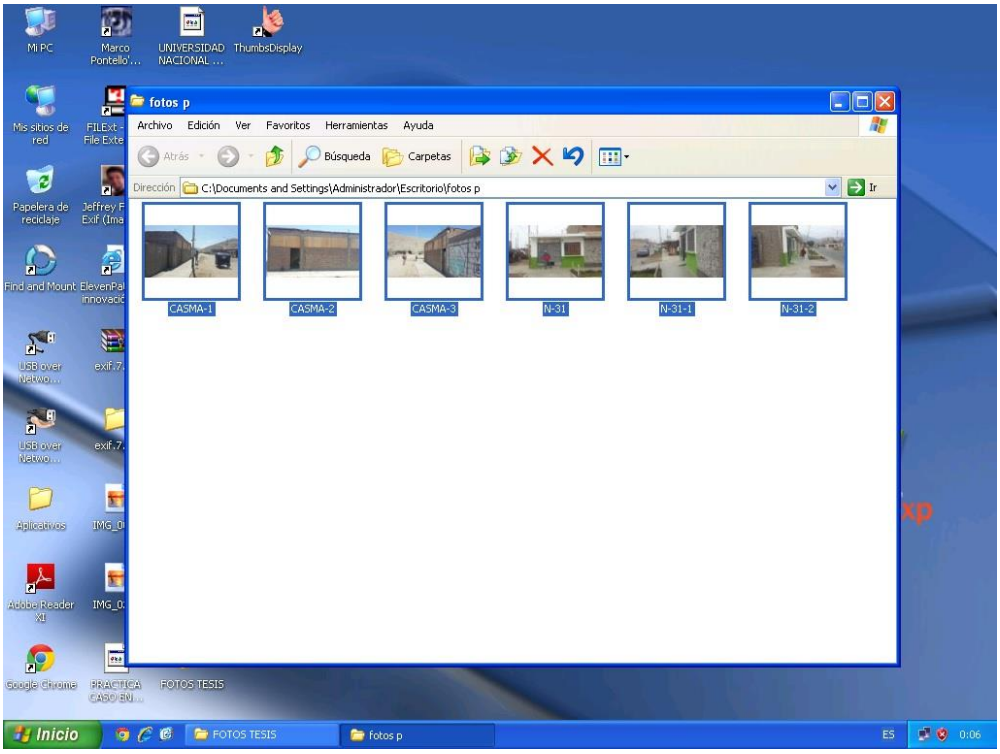
En esta imagen se muestra la selección de la carpeta fotos



En esta imagen se muestra la ubicación de las fotos borradas



En esta imagen se muestra la ubicación las fotos borradas en tamaño más pequeño



Software GetDataBack recuperación de información de disco duro

Se puede restaurar los datos cuando el sistema operativo no reconozca el disco o cuando se haya perdido, no solo el directorio principal, sino toda la información del directorio. Esto funciona con algoritmos avanzados que aseguran que todos los directorios y subdirectorios se recompongan tal y como eran, y que los archivos largos se reconstruyan correctamente, es seguro ya que es de lectura, el programa nunca intentará escribir en la unidad desde la que se están recuperando los datos.

Runtime's DiskExplorer para FAT

El editor de discos para sistemas de archivos de tipo FAT permite explorar el disco duro tan igual que un navegador e ir directamente a la tabla de partición, al registro de arranque, a FAT al directorio principal, a un sector o clúster determinado. Es posible elegir los siguientes modos de vista: hexadecimal, texto, directorio, FAT, tabla de partición y registro de arranque.

DiskExplorer contiene distintas funciones útiles para la recuperación de datos y particiones FAT: buscar en el disco texto, registros de arranque, tablas de partición y subdirectorios. La información de volumen proporciona detalles del registro de arranque de la partición.

Runtime's DiskExplorer para NTFS

El editor de discos para sistemas de archivos del tipo NTFS que permite explorar el disco NTFS y recuperar los datos de forma satisfactoria: en disco NT saltando directamente a la tabla de partición, al registro de arranque, a la MFT (tabla del fichero maestro) o al directorio principal. Es posible elegir

entre los siguientes modos de vista: hexadecimal, texto, MFT, detalles de MFT, asignación de índice y tabla de partición.

Recomendación para el uso del disco duro

Hay dos posibilidades de edición de datos: modo de escritura virtual y modo de escritura directa (no recomendado). Puede crearse un volumen virtual cuando se haya perdido el registro de arranque o esté dañado.

Cómo escoger el producto adecuado.

Producto	Función	Usuario	SO
GetDataBack for FAT	Recuperación de nidades/particiones o archivos individuales borrados debido a que la tabla de partición, el sector de arranque, la FAT o el directorio principal se hayan perdido o estén corruptos, o cuando se hayan formateado o dañado con fdisk, por un virus o por un corte de corriente.	Usuarios normales y avanzados	Windows 98
GetDataBack for NTFS	Recuperación de unidades/particiones o archivos individuales borrados debido a que la tabla de partición, el sector de arranque, la tabla del fichero maestro (MFT) o el directorio principal se hayan perdido o estén corruptos, o cuando se hayan formateado o dañado con fdisk, por un virus o por un corte de corriente.	Usuarios normales y avanzados	Windows NT, 2000, XP, 2003, Vista, Windows 7, Windows 8
DiskExplorer for FAT	Acceso "low-level" al disco duro, edición, recuperación de archivos individuales y clonación de plataformas	Usuarios avanzados	Windows 95, 98, ME
DiskExplorer for NTFS	Acceso "low-level" al disco duro, edición, recuperación de archivos individuales y de directorios completos, y clonación de plataformas	Usuarios avanzados	Windows NT, 2000, XP, 2003, Vista, Windows 7, Windows 8

Fuente: http://runtime.org/spanish/notas.htm

No se recomienda la utilización de GetDataBack y DiskExplorer cuando los datos se hayan perdido a causa de un error físico del disco duro, cuando éste haga ruidos extraños, deje de girar o cuando no sea reconocido por el BIOS.

En este caso de que la unidad tenga un error físico, recomendamos que termine inmediatamente de recuperar datos y que envíe la unidad a un servicio especializado de recuperación de datos para, como mínimo, hacer una imagen de la unidad que sirva de guía para la recuperación.

Para la recuperación de datos GetDataBack recomienda el siguiente procedimiento:

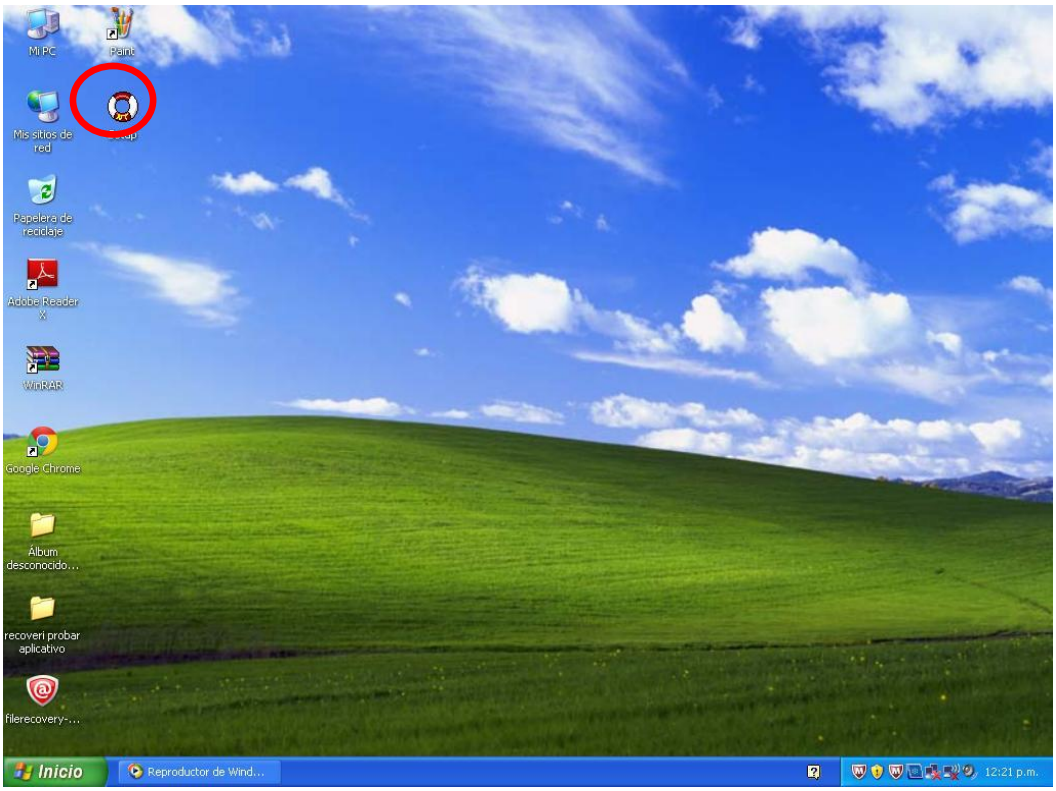
No instale GetDataBack en el disco duro o partición desde la que desea recuperar datos. Instale el programa en otro ordenador que funcione correctamente. Monte la unidad que desea recuperar de tal forma que el segundo ordenador sea el máster. Asegúrese de que la unidad queda conectada correctamente y que sea reconocida por el BIOS.

Comprobar la calidad de los archivos recuperados antes de abonar el programa.

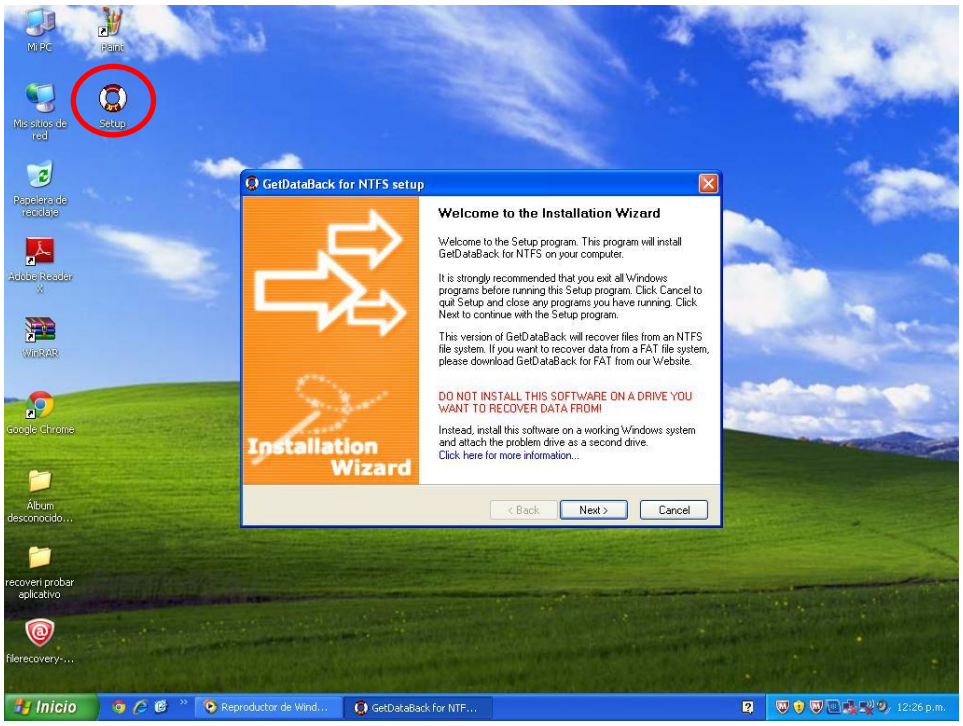
Antes de adquirir una licencia de GetDataBack, se recomienda que compruebe la calidad de los archivos recuperados en el paso **5** de la recuperación de datos. Aunque normalmente los archivos que se ven en el paso 3 han de poder abrirse después de copiarse, es posible que (especialmente cuando los archivos estaban extremadamente fragmentados) GetDataBack muestre los nombres de los mismos, pero que no puedan abrirse.

Para comprobar el contenido de los archivos no estén defectuosos, seleccione algunos archivos en el paso 3 y pulse la tecla F3 para abrir el navegador de archivos incluido con el programa. Con este navegador es posible mostrar el contenido de distintos formatos de archivo (.txt, .docx, .bmp, .jpg, .xlsx), en caso de que éste no sea compatible, el contenido se visualizará en formato hexadecimal. Se puede hacer doble clic sobre el archivo para abrirlo con la aplicación correspondiente.

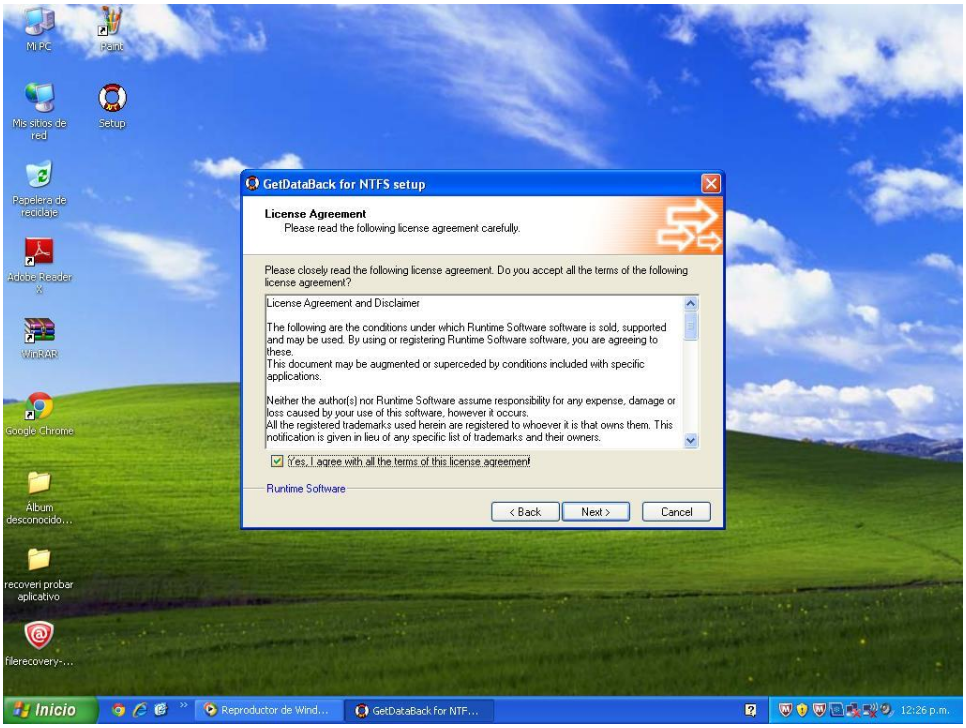
En esta imagen se muestra el software demo GetDataBack



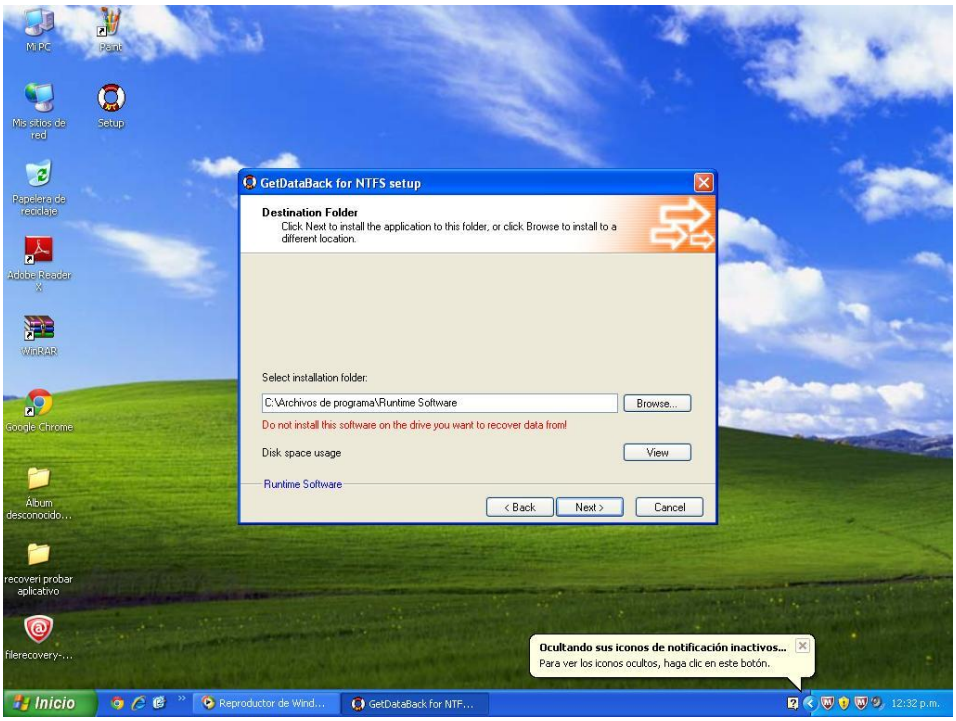
Hacemos Clic en el instalador y sale la imagen. Seguidamente clic en Next



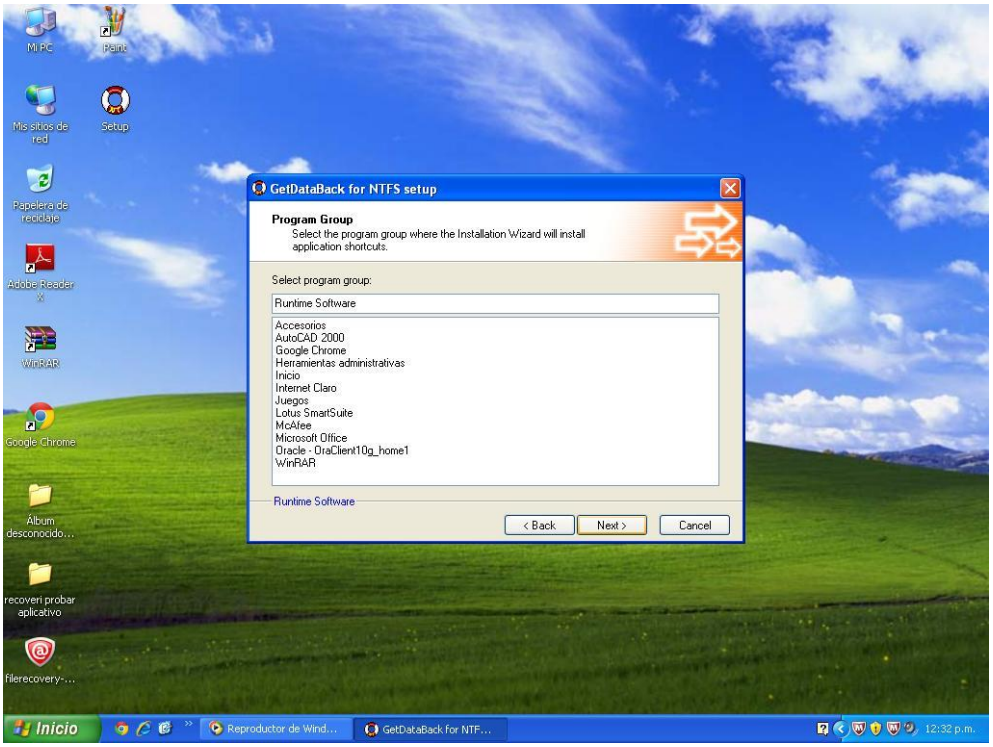
Se hace Clic en el instalador y nos sale esta imagen a continuación presionamos Next.



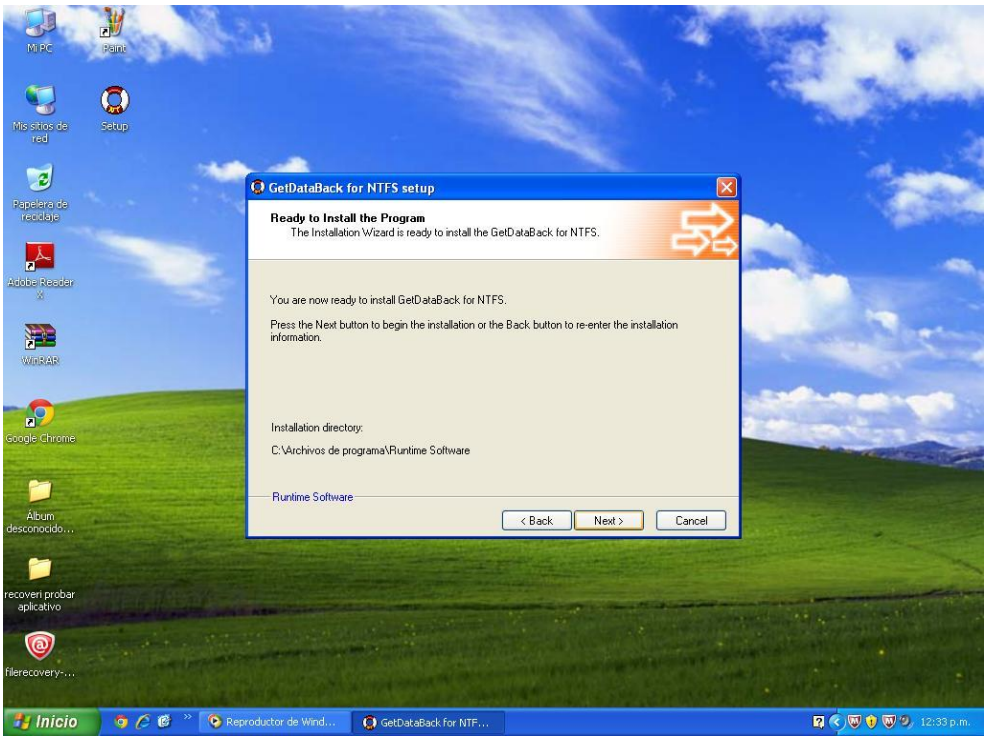
Realizamos la instalación por defecto y hacemos Clic en Next.



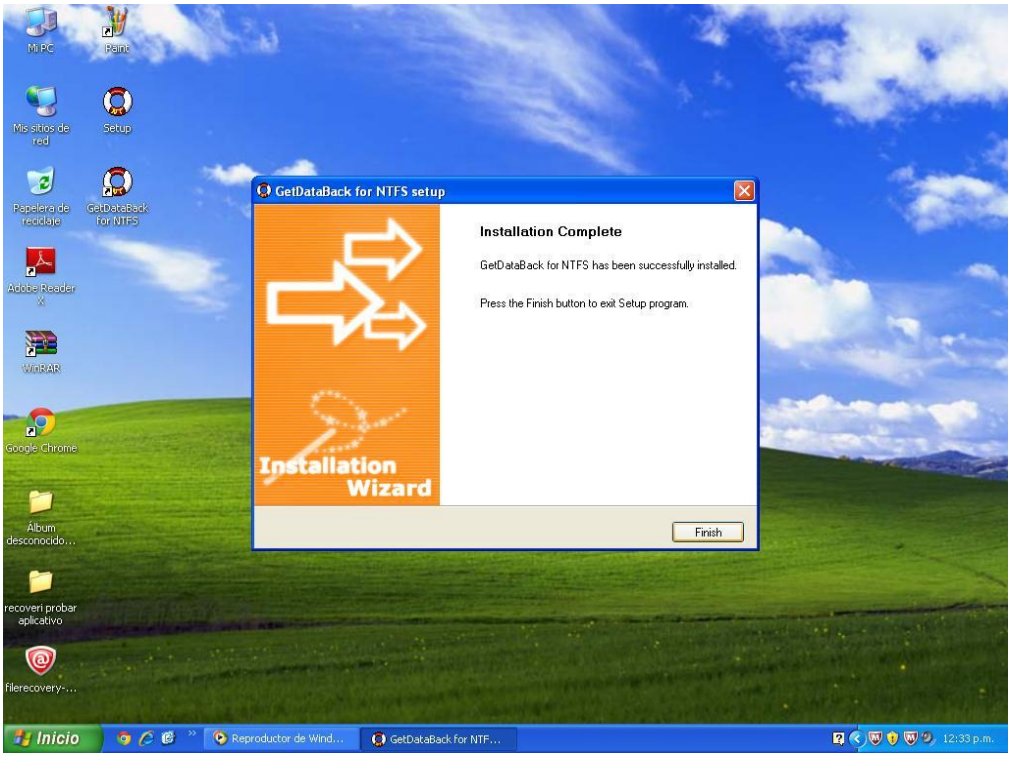
Seguimos con la instalación por defecto y hacemos Clic en Next..



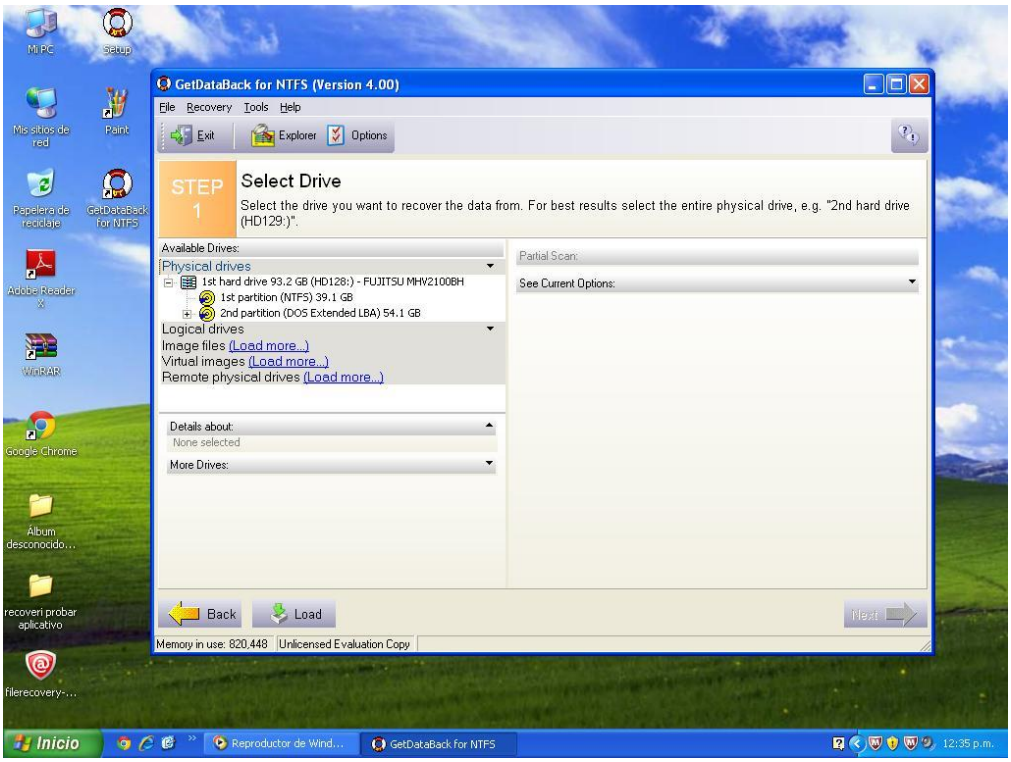
Se sigue la instalación por defecto y hacemos Clic en Next.



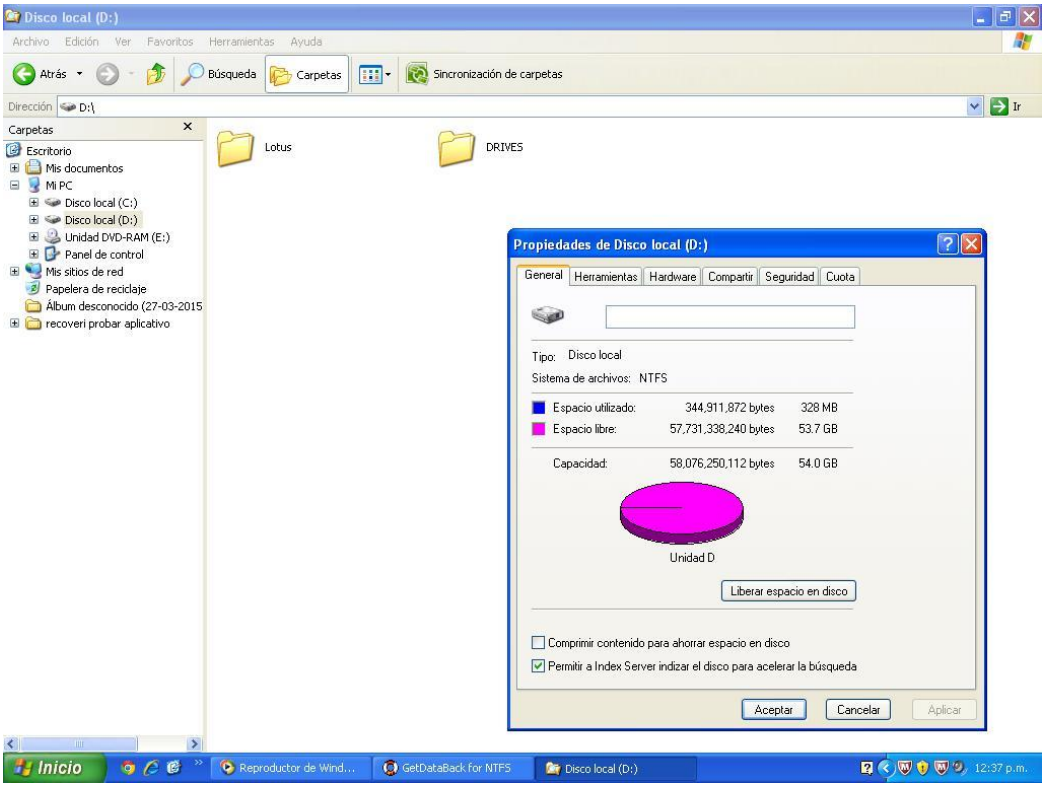
En la imagen se finaliza la instalación hacemos Clic en Finish



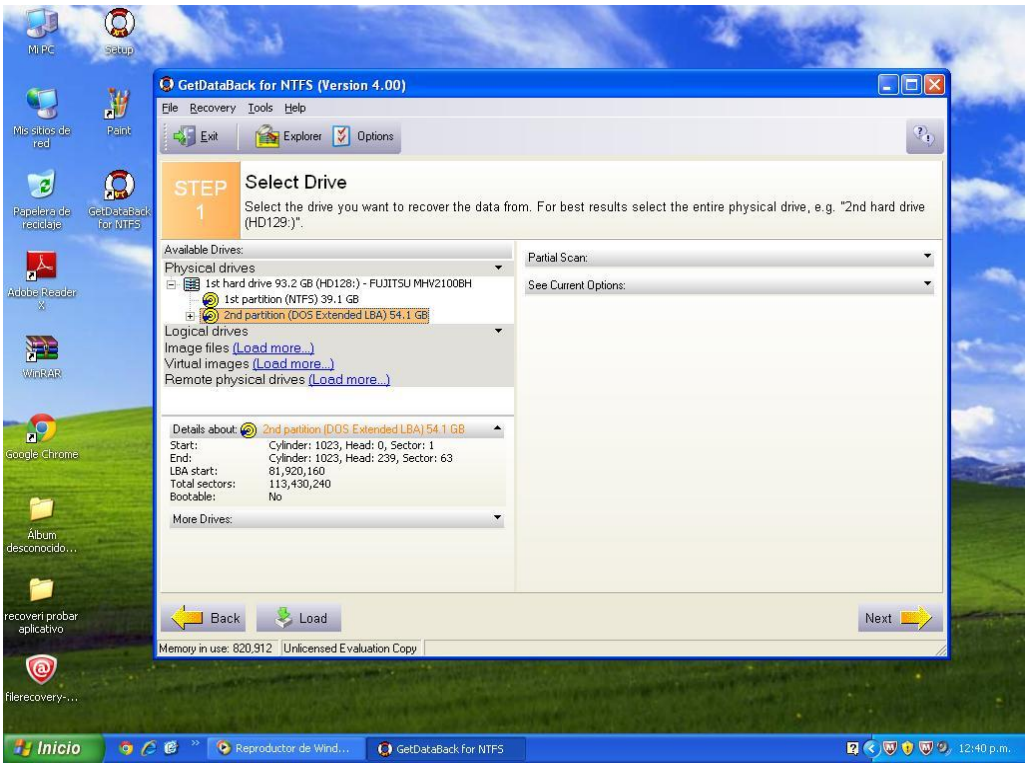
En la imagen se muestra el software GetDataBack ejecutado listo para recuperar la información que se perdió o fue borrada



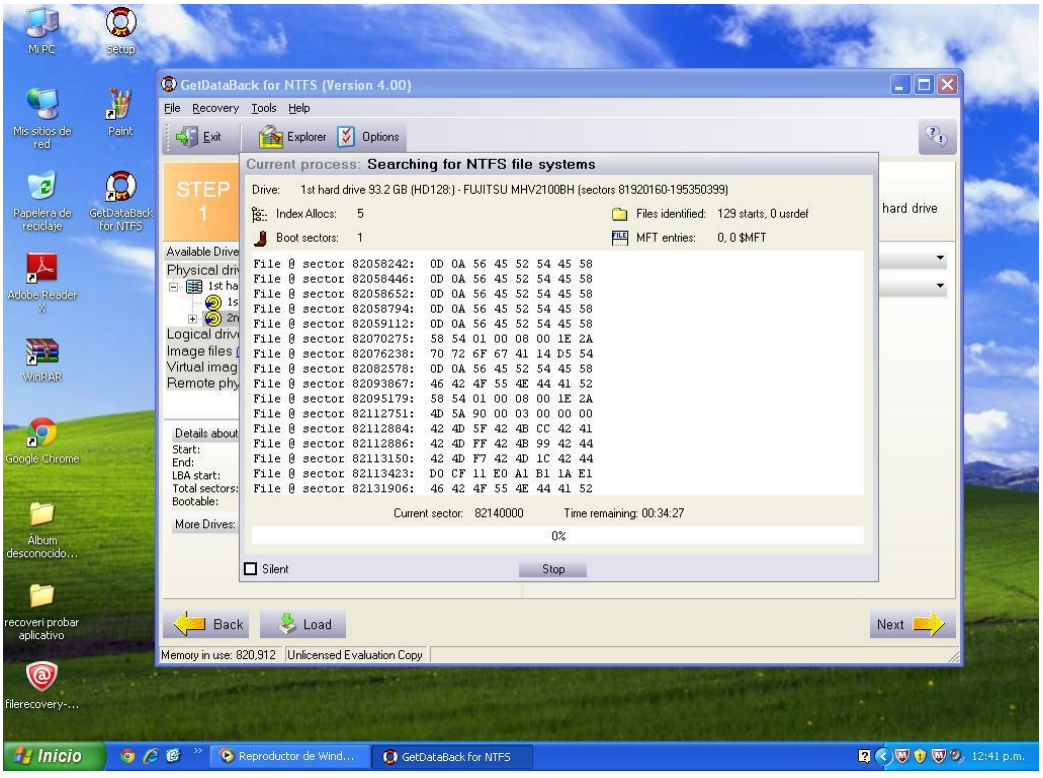
En esta imagen se visualiza el disco duro, la capacidad de almacenamiento, y nos damos cuenta que el disco duro no tiene mucha información.



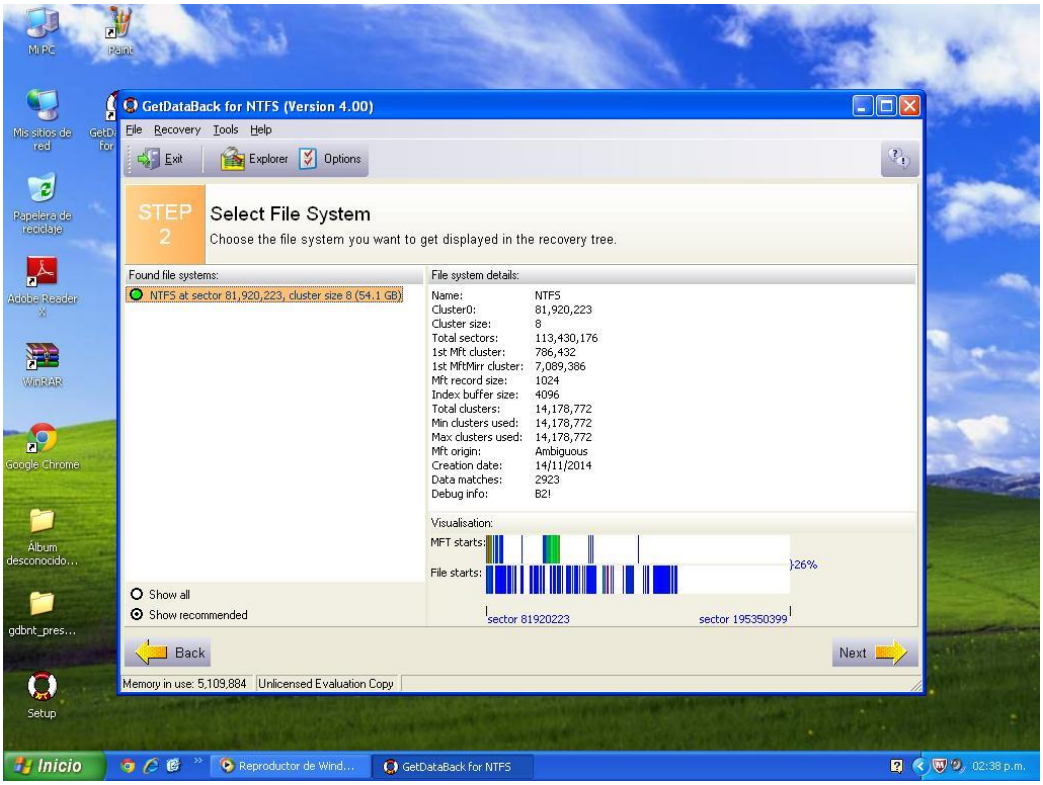
En la imagen se muestra el disco duro, la capacidad de almacenamiento del disco a recuperar.



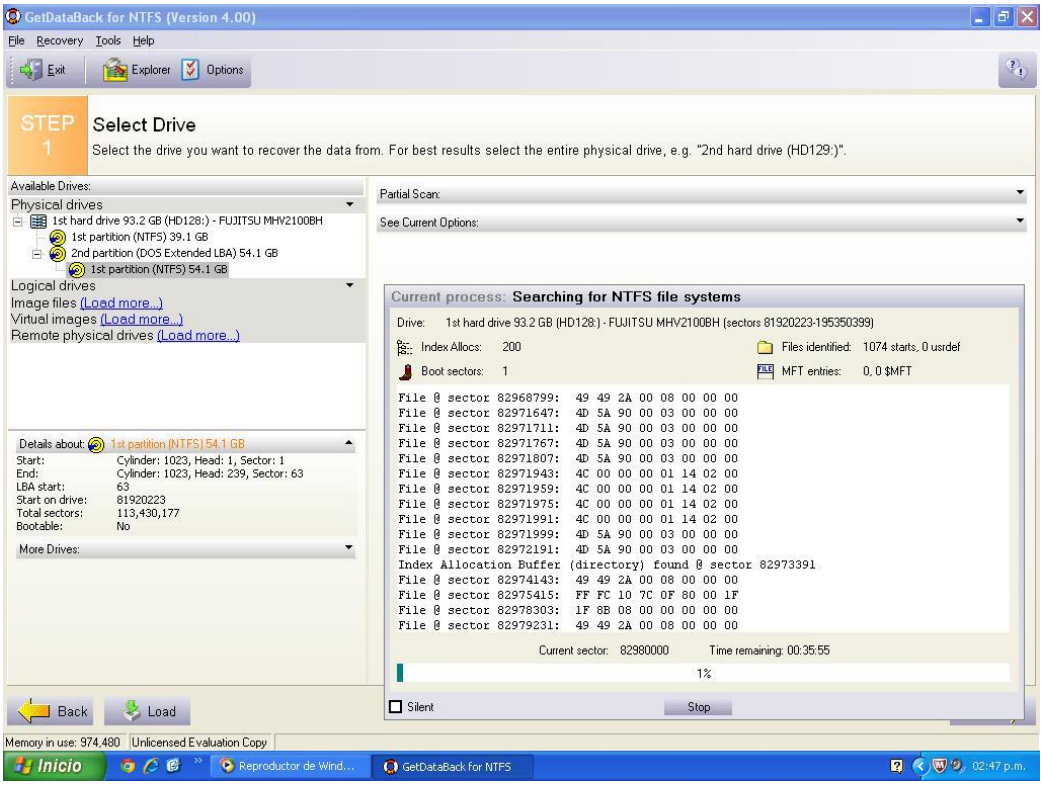
En la imagen se muestra el proceso del disco duro.



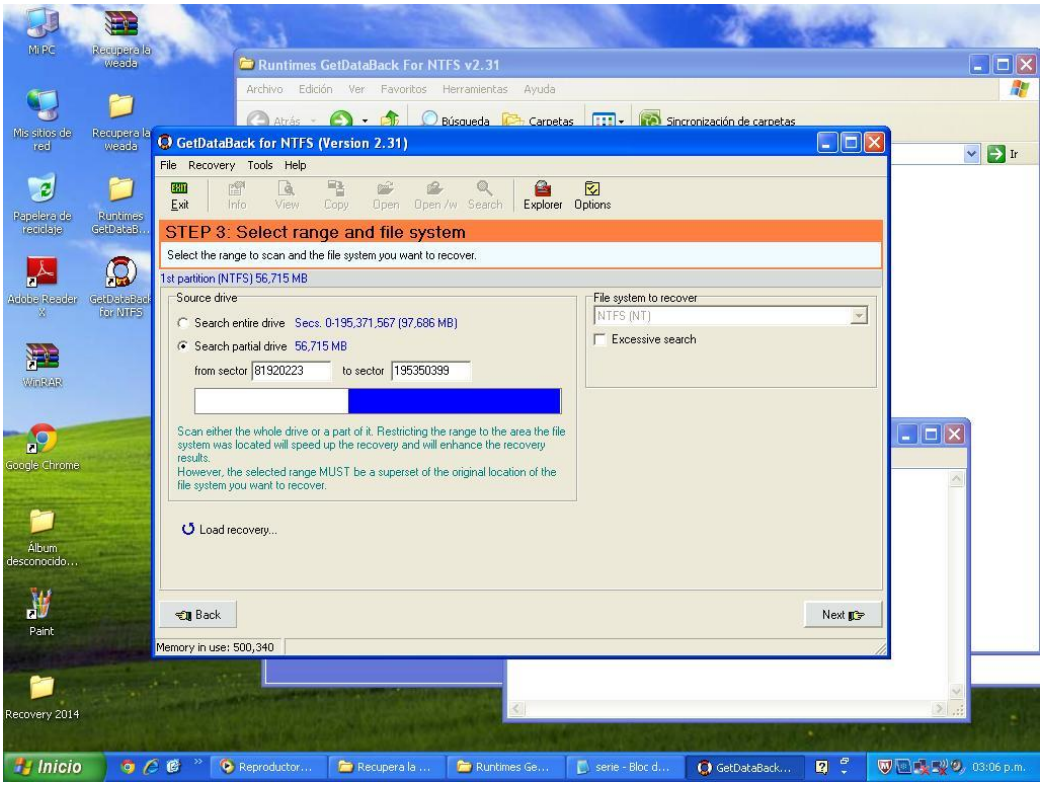
En la imagen se muestra que el disco duro está procesando.



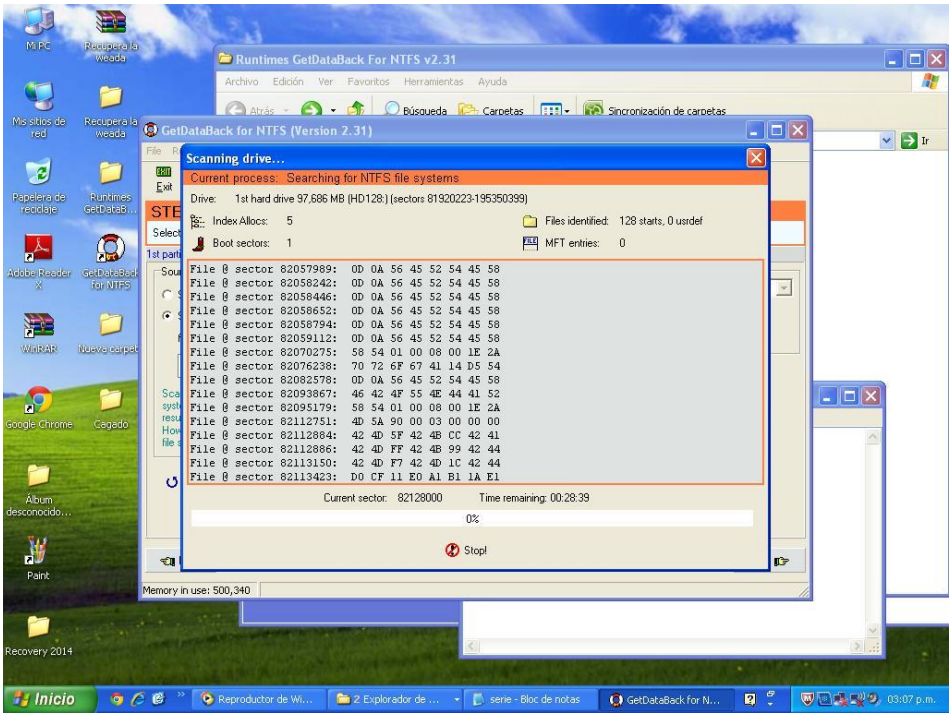
En la imagen se muestra el disco duro, la capacidad, y el proceso del disco duro.



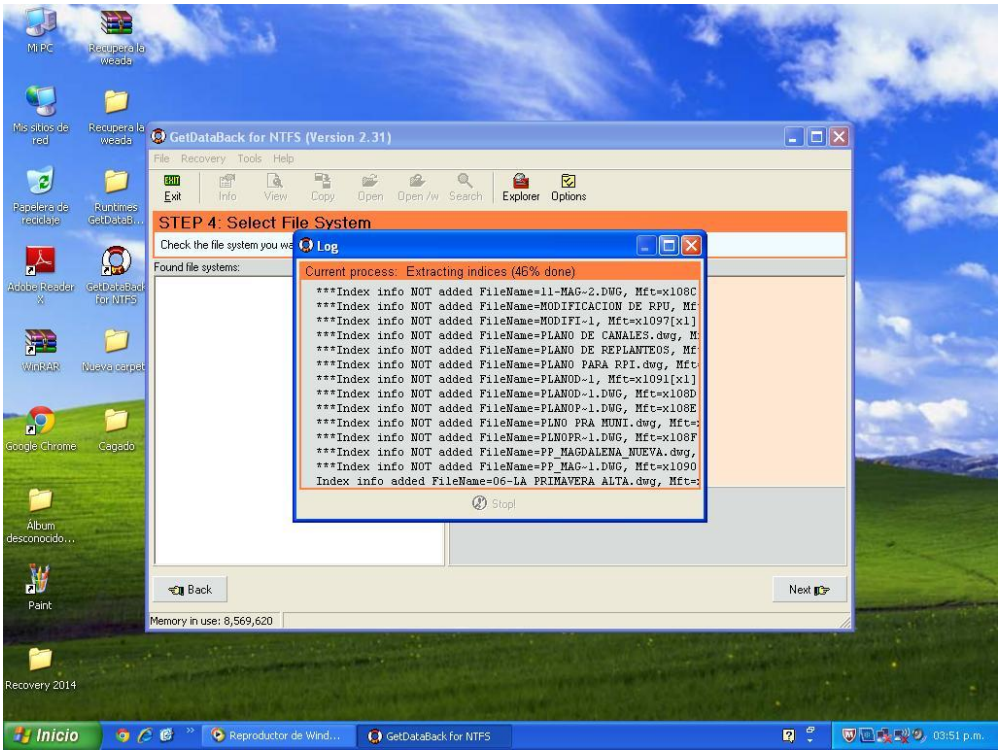
En la imagen se muestra el selector del disco duro a recuperar.



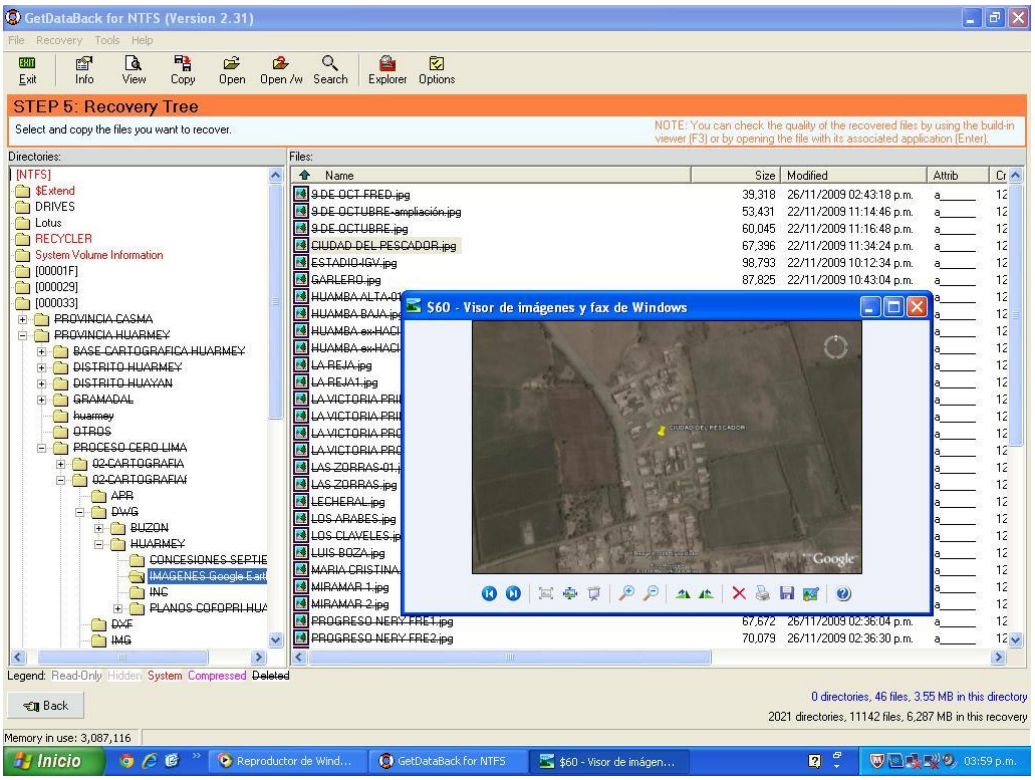
En la imagen se muestra el procesamiento del disco duro y el porcentaje (%)



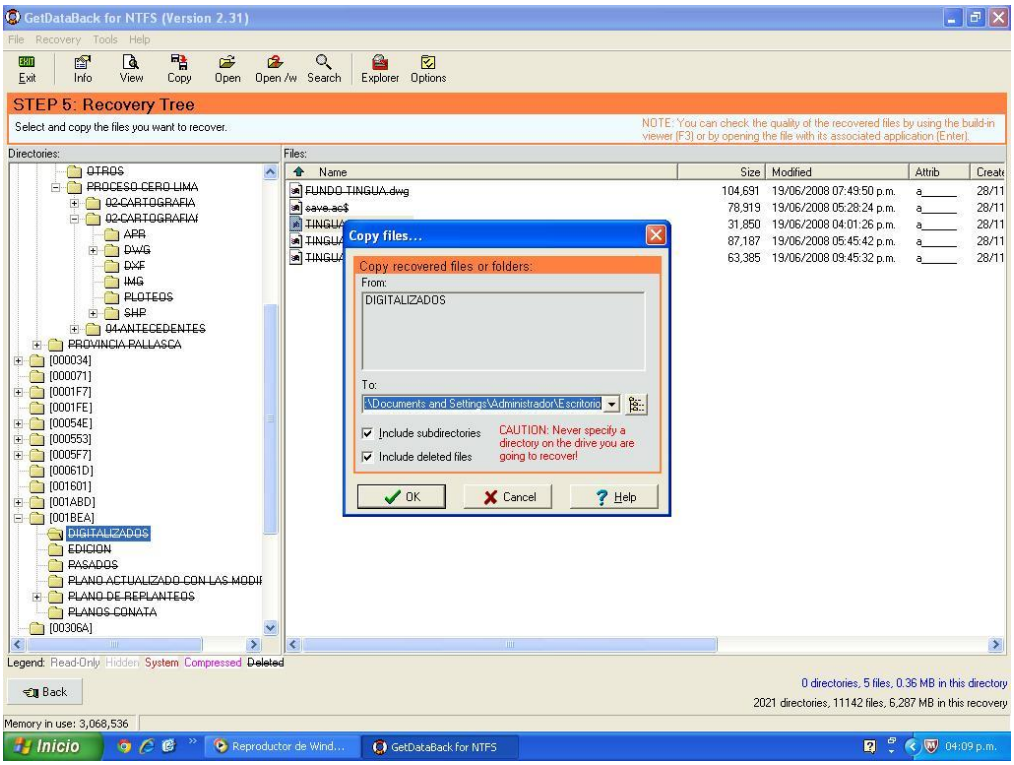
En la imagen se muestra el disco duro, procesando.



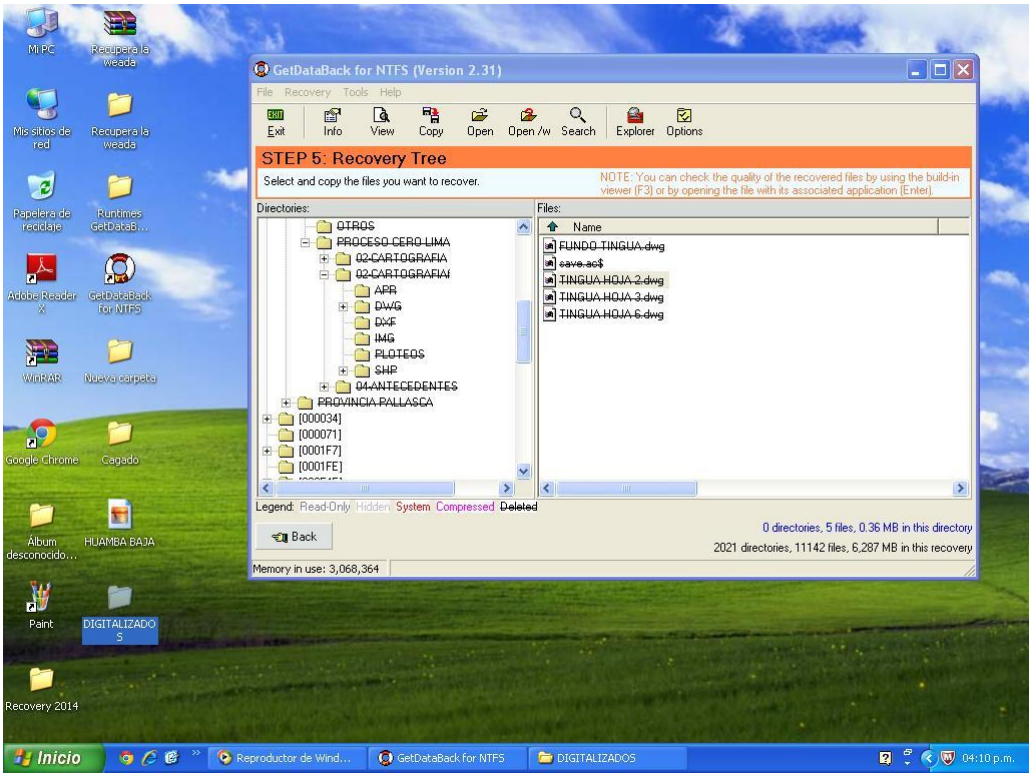
En la imagen se muestra la recuperación de la información del disco duro, se ejecuta una imagen que se muestra en la figura.



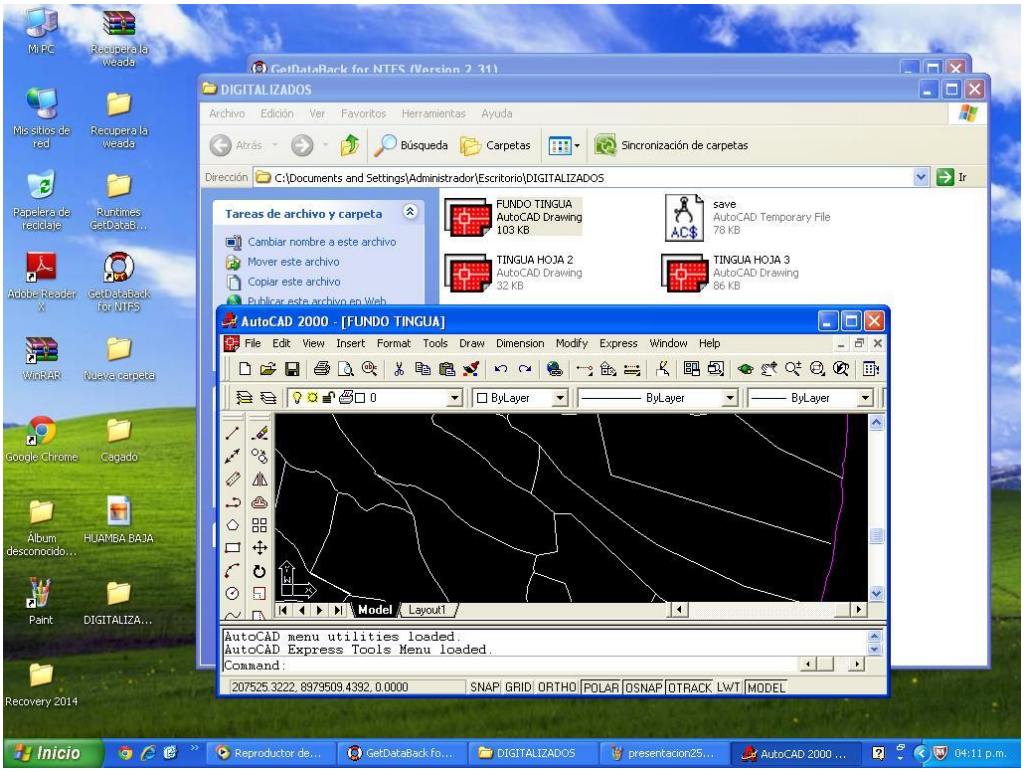
En la imagen se muestra la recuperación de la información y se transfiere la información recuperada.



En la imagen se muestra la recuperación de la información y la ubicación de la carpeta digitalizados.



En la imagen se muestra los archivos recuperado.



Software Activo@FileRecovery Recuperación de información de disco duro

Activo@FileRecovery proporciona para Windows la capacidad de detectar eficazmente la recuperar archivos y discos perdidos debido a la eliminación accidental, formateo de discos, virus y otras razones.

El paquete profesional también incluye integrado Active@Disk Editor (Hex Viewer una utilidad para la inspección de datos de bajo nivel), virtual RAID reconstructor, siendo capaz de recuperar las matrices de discos RAID dañados, file Organizador necesario reorganizar y cambiar el nombre archivos detectados por sus firmas.

La edición Ultimate extiende el paquete profesional con Active@Boot Disk Lite: una imagen ISO que se puede utilizar para crear un CD/DVD o USB de arranque con una versión ligera de Windows 7 (WinPE 3.1) o Linux (SUSE Linux 13) que se ejecuta en la memoria RAM. Es la única manera de recuperar sus datos cuando el sistema no es de arranque y no se puede adjuntar la corrompida unidad de disco duro a otra máquina. Se suministra Linux LiveCD arranca las últimas UEFI sistemas de arranque seguro y BIOS regular.

Características principales

Recuperación de información de dañados Microsoft FAT /exFAT, NTFS/NTFS + EFS, Unix UFS, los sistemas de archivos de Linux Ext2/ Ext3/ Ext4/ Btrfs Soporta discos duros FDD/ HDD/ IDE/ SATA/ eSATA/ SCSI/ SSD arrays de discos de disco RAID, discos flash USB y tarjetas de memoria, unidades USB externas y discos USB3.

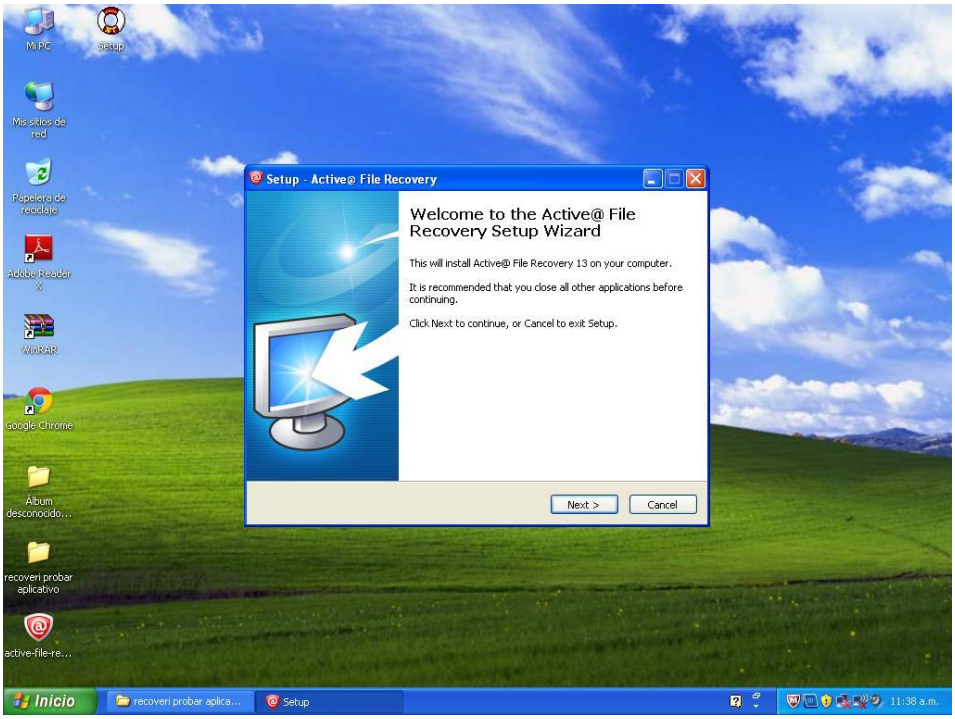
Recupera archivos extra grandes, comprimidos, cifrados y fragmentados en NTFS, archivos simplemente eliminados pueden recuperarse basan en NTFS Diario (Archivo registro). Crea y recupera de Raw (sector por sector de la copia), las imágenes y las imágenes de disco creadas por terceros RAW comprimidos.

Añadido método de recuperación para la detección de archivos por sus firmas cuando no hay otros métodos trabajan Active @ Tecnología de exploración le permite reconocer archivos basados en firmas de archivo para los siguientes 123 tipos de archivo: Documentos, Imágenes, Música, Vídeos. La recuperación

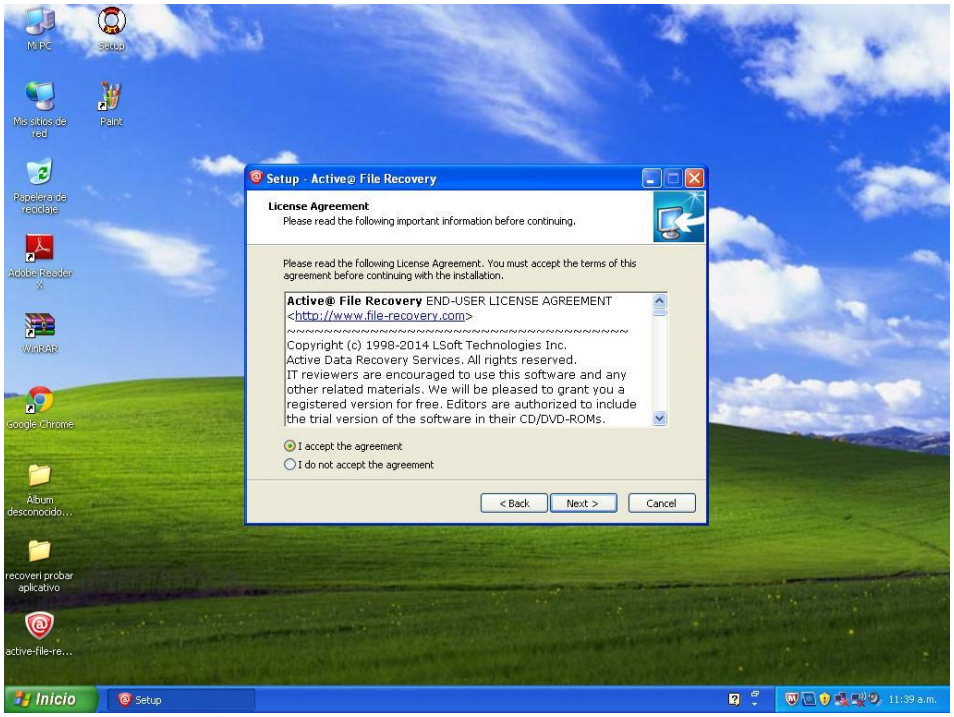
de los datos en que no arranca debido a un desplome de la firma de archivo para los siguientes Recuperación de los datos en que no arranca debido a un desplome de la computadora, ataques de virus, daños por el programa malicioso, o PCs de fallo de alimentación (paquete Ultimate)

En la imagen se muestra el software demo Activo@File Recovery.

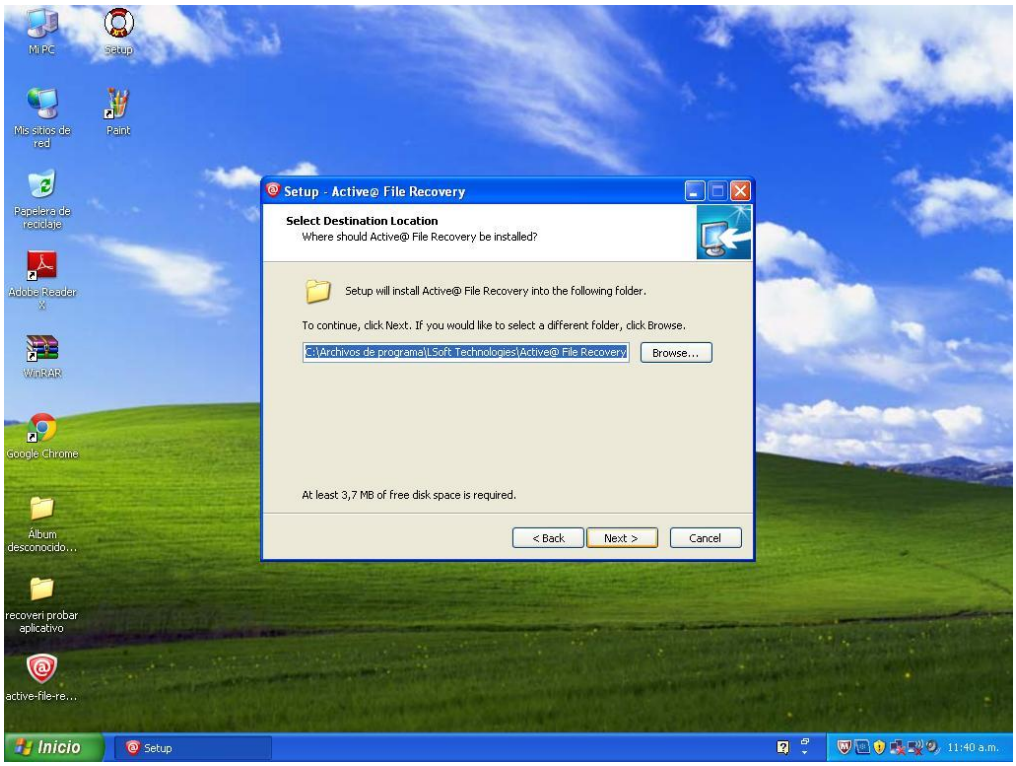
En la imagen se muestra la instalación el software Activo@File Recovery hacemos clic en Next..



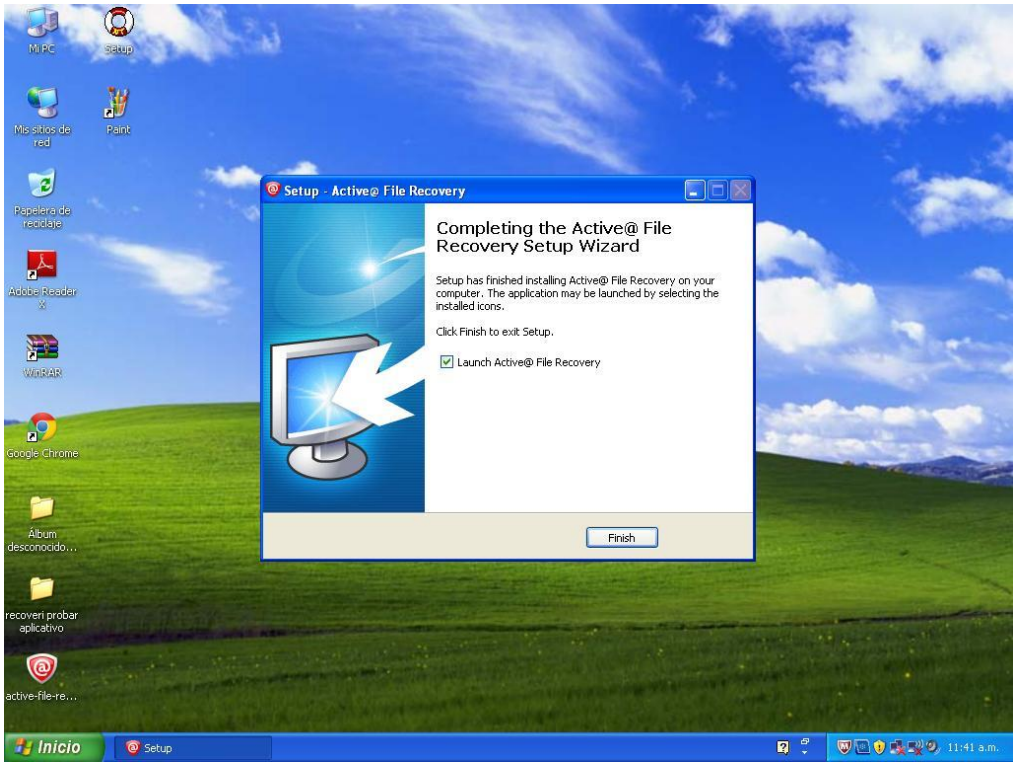
En la imagen se muestra dos opciones hacemos clic en la primera opción hacemos en clic en Next.



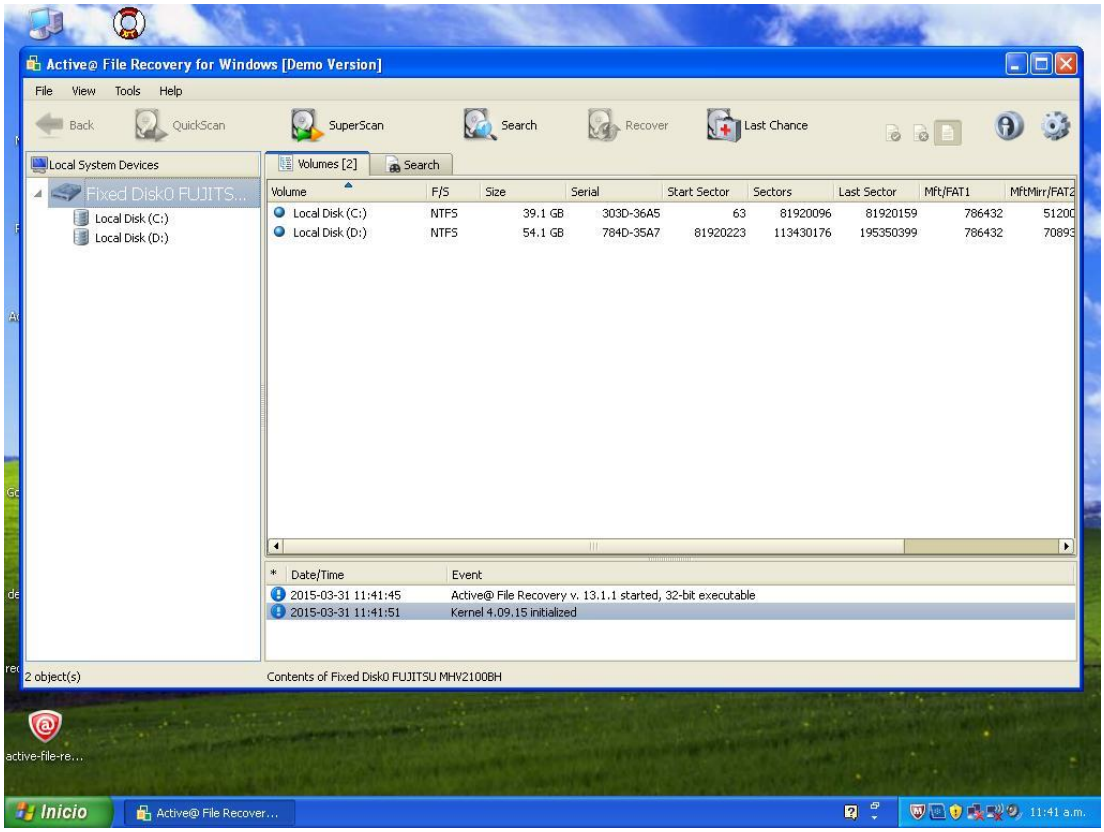
En la imagen se muestra la ubicación de la instalación solo instalamos por defecto y hacemos clic en Next.



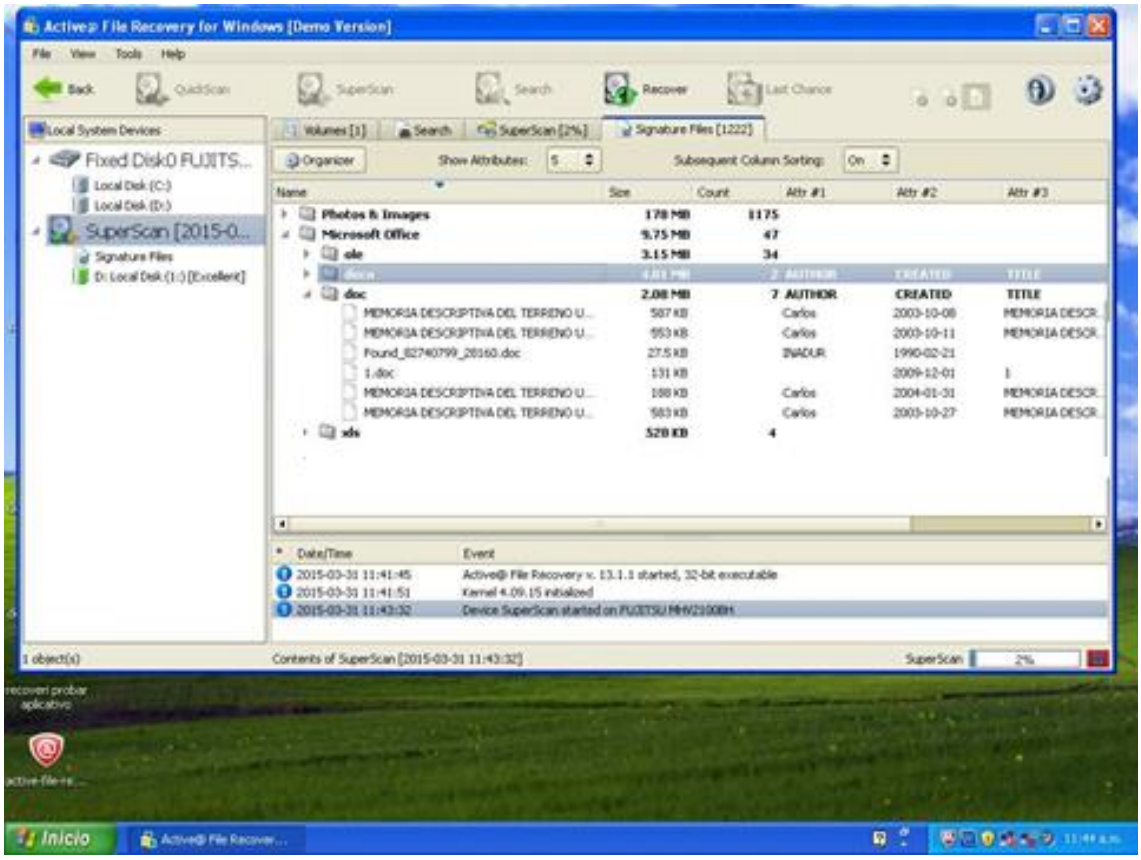
En la imagen que nos sale hacemos clic en finish. Finalizando la instalación



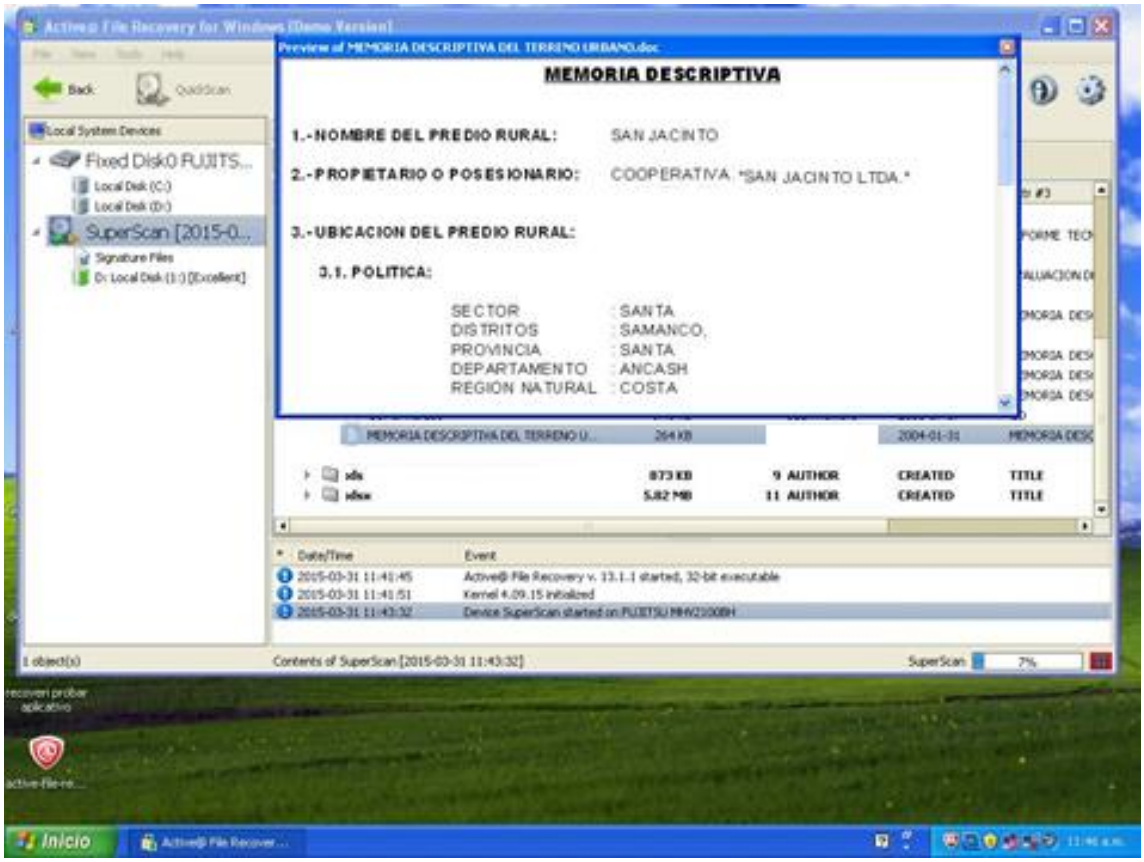
En la imagen se muestra la cantidad de discos duros y su capacidad de almacenamiento.



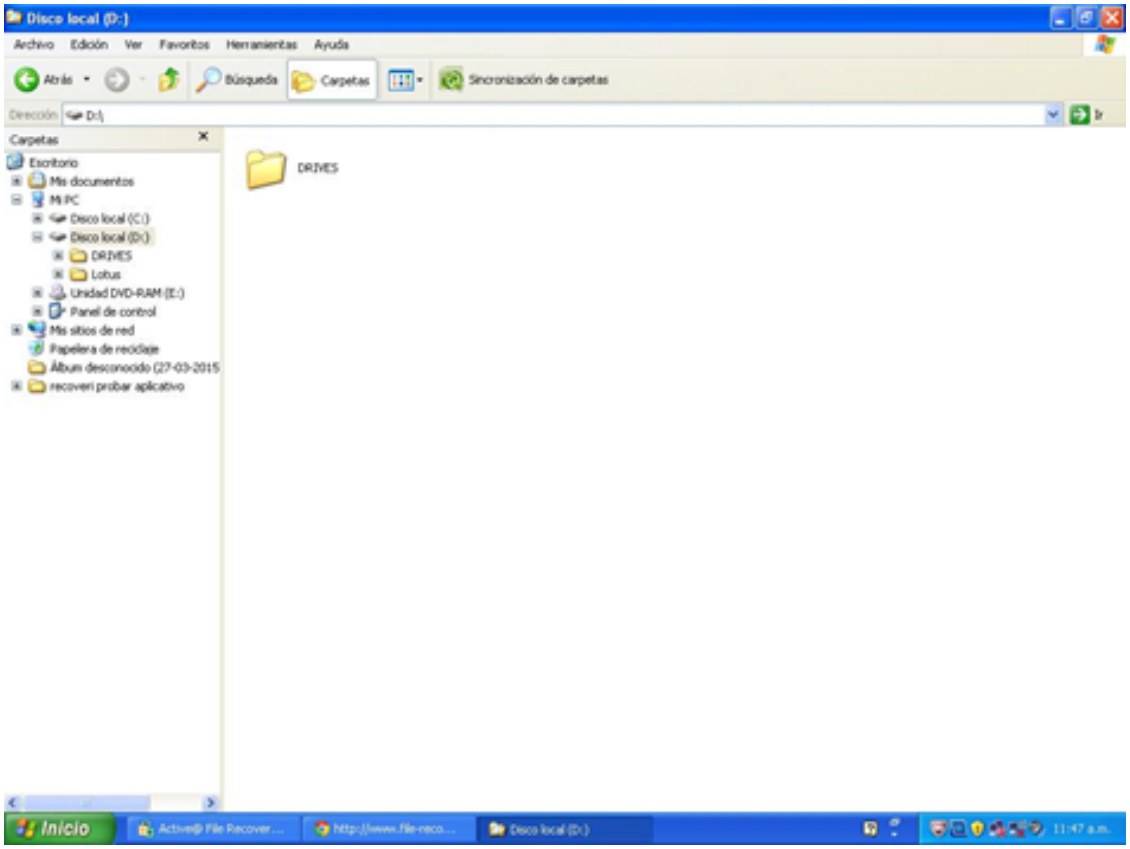
En la imagen se hace clic en Super Scan y nos muestra la posible información de recuperación.



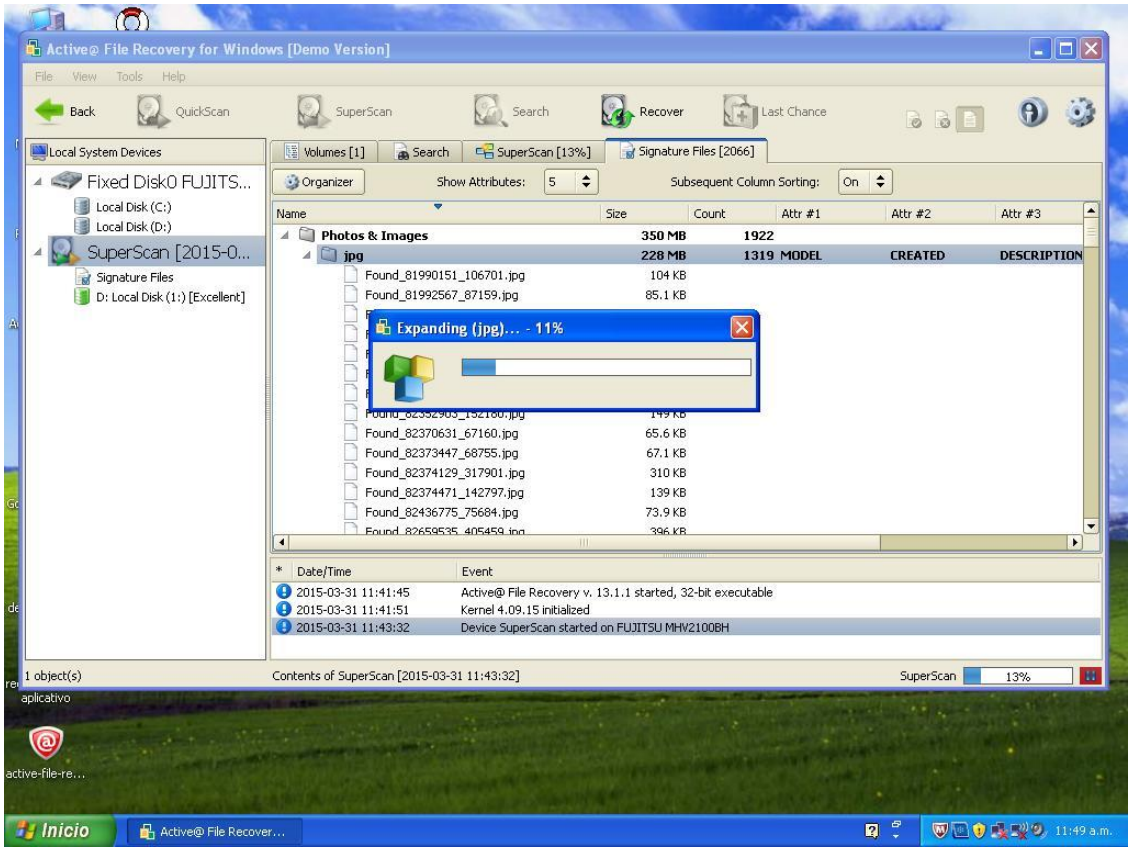
En la imagen se muestra la información seleccionamos el archivo que dice memoria descriptiva del predio y se visualiza.



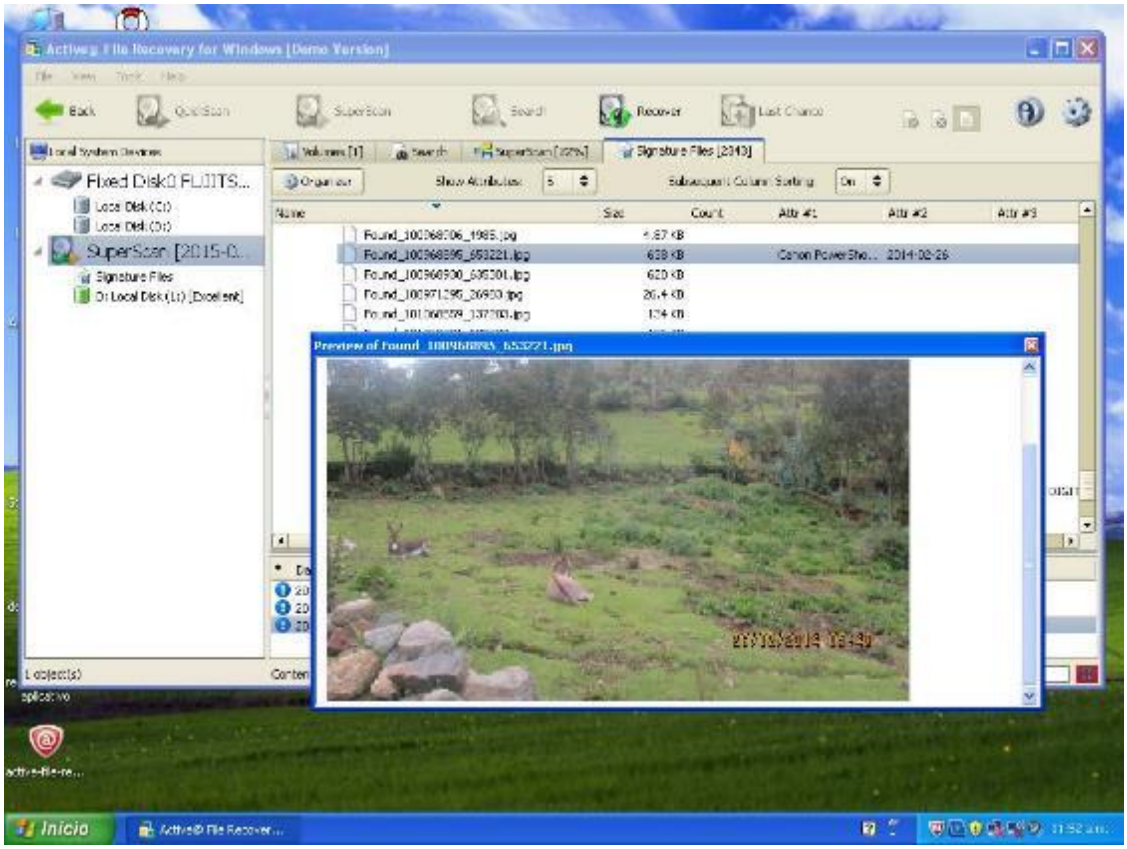
En la imagen se muestra el disco d la cual se borró la información.



En la imagen se muestra el disco d y se procesa la información a recuperar.



En la imagen se muestra el contenido del disco d que fue recuperada, la foto del disco d.



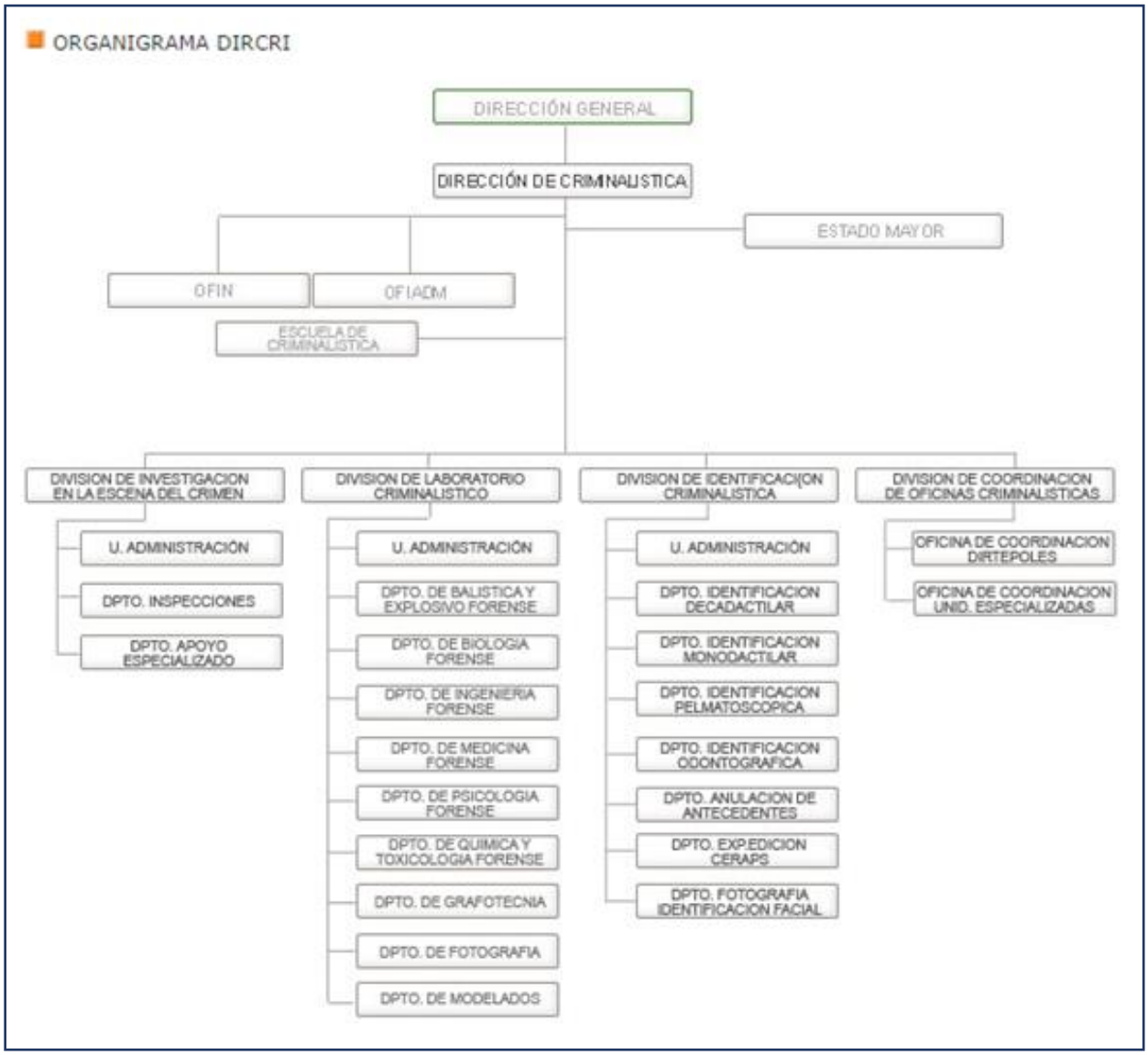
Anexo 06: Resultado del Análisis de la situación actual

En la actualidad no existe un área especializada para resolver los problemas con el crimen cibernético y lo que propongo con este proyecto es desarrollar una metodología de investigación que nos permita llegar a la solución del problema causado por el crimen cibernético.

Análisis de organigrama funcional (Policía Nacional del Perú, 2001)

El siguiente organigrama de la Dirección de criminalística de la sede principal nos revela que en la ciudad de Lima existe el área de Ingeniería Forense para atender casos de crimen cibernético. En la ciudad de Huaraz no existe esta área especializada, por lo que los casos presentados deberán ser enviados a la ciudad capital para su posterior solución.

Organigrama funcional de la PNP



Fuente: Policía Nacional Perú

Evaluación de la capacidad instalada

En la ciudad de Huaraz la Policía Nacional del Perú sede Huaraz no se cuenta con la oficina, "Dirección Nacional de Comunicaciones y Criminalística de la Policía Nacional del Perú – Huaraz"

Análisis de fortalezas, oportunidades, debilidades y amenazas

Análisis Foda

FORTALEZAS	OPORTUNIDADES
Se pueden resolver mayor cantidad de problemas relacionados al crimen cibernético	Tenemos la posibilidad de implementar un área especializada y aportar al mismo
Que estos a su vez ayuden a resolver problemas judiciales	Se generarán puestos de trabajo contando con especialistas
Nuevos sistemas de organización de tareas eficiente	Implantación de aplicativos de calidad
DEBILIDADES	**AMENAZAS**
No hay logística	Que no exista sostenibilidad en el proyecto
no hay presupuesto	No tomen en cuenta los resultados
Falta de personal de investigación.	Posible fracaso en implantación de aplicativos.

Fuente: propia

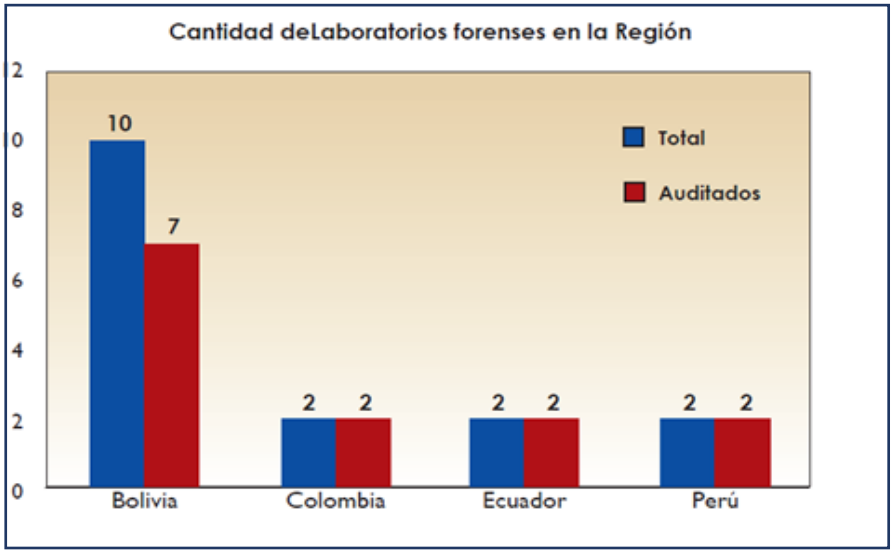
Resultado identificación y descripción de requerimientos.

como se muestra los países miembros de la Comunidad Andina poseen una infraestructura que les permite realizar el análisis de ilícitas por medio de la utilización de laboratorios forenses que dotados de instalaciones, equipos instrumentales y personal para dar soporte a las diferentes autoridades del nivel judicial y operativo para que tengan herramientas que le permitan estructurar programas y tomar decisiones en contra del flagelo.

Para este fin cada País Miembro de la CAN ha diseñado una red nacional de laboratorios que les permiten realizar la identificación pericial en la región y que se encuentran divididos de acuerdo a la siguiente figura.

Figura 4.02 Laboratorios forenses en la Región. Bolivia Colombia Ecuador Perú.

Figura 4.02 Cantidad de laboratorios en la región



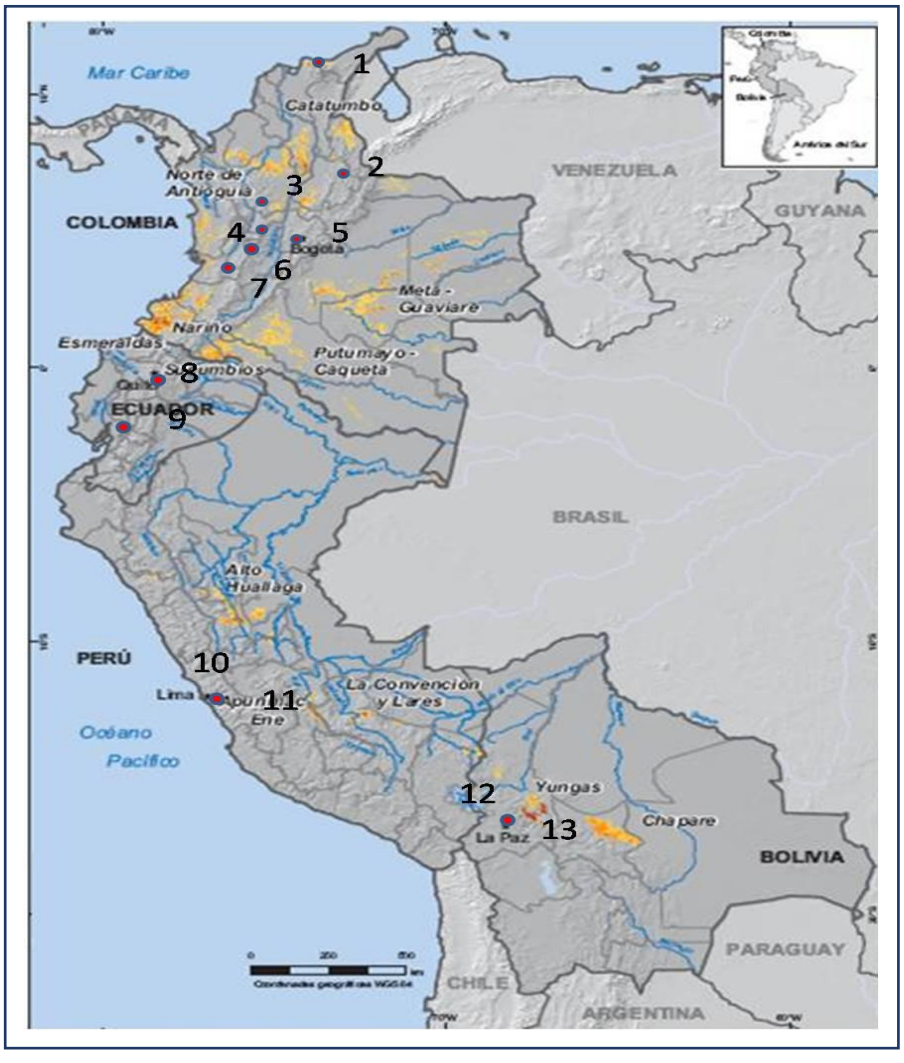
Fuente: CAN

En comparación entre los Países Miembros de la CAN, Colombia tiene la mayor cantidad de laboratorios forenses y/o criminalísticas encargados de realizar la

identificación pericial, ilícitas. La característica principal de estos laboratorios es que son utilizados por las autoridades judiciales con el propósito de realizar el estudio de los elementos materiales probatorios con el propósito de esclarecer la verdad de los hechos investigados.

En el siguiente mapa se muestra la distribución de los laboratorios en los Países Miembros de la Región Andina, que fueron objeto del presente diagnóstico figura 4.03 Distribución de los laboratorios forenses de los países miembros de la Comunidad Andina de Naciones

Figura 4.03 Mapa de la región

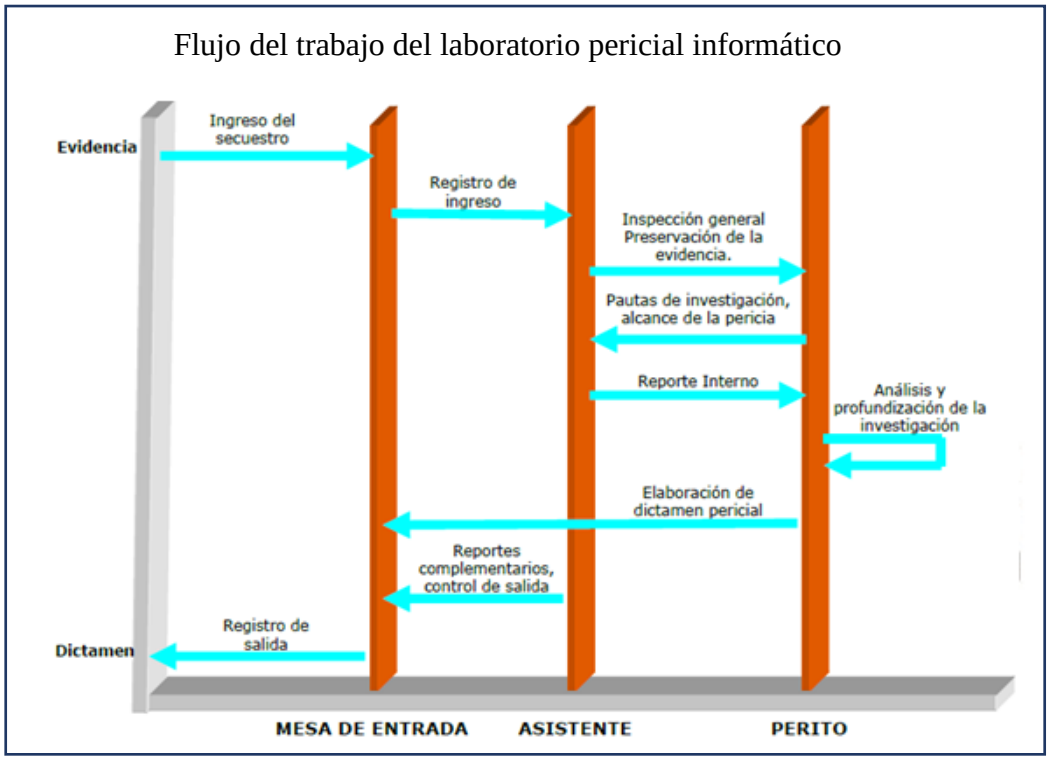


Fuente: CAN

Procesos internos del negocio

Los procesos internos del negocio se muestran en la estructura del laboratorio y el proceso de recopilación de pruebas.

Organización interna del laboratorio



Fuente: C HFI computer hacking forensin investigator

Requerimientos

Las sustentaciones de la metodología deben estar sujeta de acuerdo a la necesidad de la aplicación de la metodología

El modus operandi

- Que asegure el éxito
- Que proteja su identidad

- Efecto escape

Los tipos de información datos almacenados y datos generados

- Datos almacenados
  - Datos comunes
  - Datos ofimática
  - Música
  - Video
  - Fotografía
- Datos generados
  - Cookie, historial
  - Log de sistemas
  - Chats de las redes sociales
  - Envió de correo

La información se debe recuperar con el siguiente cuidado para no perder evidencias

- Preservar la evidencia - integral
- Acopio de evidencias
- Etiquetar y documentar
- Recopilación de la información
- Cadena de custodia
- Codificación hash

Asi mismo el personal requiere ser capacitado en forense informática, ingeniería forense, que se asignen presupuesto por parte del Ministerio del Interior con la finalidad que la ciudad de Huaraz cuente con esta oficina y así se disminuya el crimen cibernético.

Resultados Diseño de la funcionalidad de la solución

Construir un conjunto de herramientas de investigación de equipos.

Nosotros al investigar cada caso debemos tomar en cuenta estrictamente cada paso a seguir, porque sólo así podremos llegar a la verdad de manera acertada. Desde que tomamos en cuenta la evidencia, desarrollamos las técnicas y construimos un conjunto de herramientas de investigación de equipos para poder llegar a la solución. Los especialistas en investigación forense son parte importante del organigrama los cuales deberán actuar con el apoyo de programas informáticos, equipos y demás técnicas.

Informática forense metodología de investigación

Fuente: C HFI computer hacking forensin investigator

Informe de diagnostico

Para la presente tesis el tema de investigación es fundamental porque será de mucha ayuda a la "Dirección Nacional de Comunicaciones y Criminalística de la Policía Nacional del Perú" en la actualidad no se cuenta con esta división de la policía nacional ni con especialistas en crimen cibernético, ni con personal con conocimientos en informática forenses para la cual todos los casos que se presentan son derivados a la ciudad de Lima

Medidas de mejoramiento

- Evaluación del caso.
- Reunir las pruebas que se pueden presentar en el tribunal de justicia o en las empresas.

- Mantener una cadena de custodia para cada pieza del soporte original que indica donde los medios de comunicación ha sido la razón cuya posesión ha estado entrando
- Obtener la debida autorización por escrito de un tomador de decisiones autorizadas para llevar a cabo la investigación ordenador
- La primera persona en el lugar de la incidencia se debe recoger y preservar la mayor cantidad posible de pruebas.

Descripción del procedimiento

El caso de Ciro Castillo se realizó un análisis forense informático a las fotografías.

Video de referencia en el caso Ciro Castillo

https://www.youtube.com/watch?v=STvweJ0M19M

https://www.youtube.com/watch?v=R95MNR2Rii8

Procedimiento en el caso según la evidencia que no se realizó para el caso especifico

- Cadena de custodia hace referencia a la retención de la cámara fotográfica de forma inmediata para que no tenga futuras manipulaciones.
- Codificación hash a la memoria de la cámara
- Codificación hash a cada una de las fotos

Caso Van Der Sloot verificación a que páginas web a ingresado la persona en una computadora.